2020-05-15

Contributions to Information Theoretically Secure Communication

Sharifian, Setareh

UNIVERSITY OF CALGARY

Contributions to Information Theoretically Secure Communication

by

Setareh Sharifian

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

GRADUATE PROGRAM IN COMPUTER SCIENCE

CALGARY, ALBERTA
MAY, 2020

Abstract

Secure communication ensures the integrity and confidentiality of communication between connected devices. An information-theoretic approach to secure communication gives the strongest confidentiality guarantee by assuming that the attacker has unlimited computing power. The earliest formal model and definition of information-theoretic secure communication is by Shannon, who employed a secret key shared between communicating parties to provide confidentiality. An alternative elegant information-theoretic approach to secure communication views the natural characteristics of the environment (i.e., channel's noise) as a resource to build security functionalities. This approach was first proposed by Wyner, and the corresponding secure communication model is called the *wiretap channel model*. These two approaches introduce two primary resources for providing information-theoretic secure communication: the shared secret key and physical properties of the communication medium.

In this thesis, we study how to employ the above two resources for secure message transmission. We study this by using channel's noise in the wiretap channel model. In this model, a sender is connected to the receiver and the adversary through two noisy channels. We propose a new wiretap encoding scheme with strong secrecy that provides perfect secrecy and reliability, asymptotically. The construction treats the noise in the adversary's channel as a source of randomness that is extracted and used to hide the message from the adversary. We realize the wiretap channel model using cooperative jamming to evaluate the performance of wiretap codes in practice. We consider a model called keyed wiretap channel that unifies Wyner's model with Shannon's model of perfect secrecy for information systems, and propose a keyed encoding schemes with strong secrecy and other properties that are attractive in practice.

We also study two-party information-theoretic secret key agreement when the two parties have access to samples of a common source of randomness and use a single message transmission to arrive at a shared random key. We propose a secret key agreement protocol in this setting, prove its security, and show its superior performance compared to other known protocols with the same properties. Finally, we propose an information-theoretic secret key agreement over a virtual wiretap channel created by cooperative jamming.

Acknowledgements

First of all, I would like to thank my supervisor, Dr. Reihaneh Safavi-Naini for her extensive support, patience and guidance during my studies, and for the opportunity to work in her exceptional research group.

My sincere thanks goes to my supervisory committee, Dr. Michael J. Jacobson and Dr. Carey Williamson for providing valuable directions to improve my research outcome. I'm also thankful to Dr. Christoph Simon, Günther Ruhe and Dr. Prakash Narayan who provided me with constructive comments on this thesis. I appreciate that despite their busy schedule, they accepted to be members of my examining committee.

I would especially like to thank Fuchun Lin and Alireza Poustindouz for their significant collaborations.

I would like to thank the fellows of the ISPIA lab and the vibrant academic community of the department of computer science at the University of Calgary whom I had the pleasure of working with during my research tenure.

I am also thankful to my friends Sepideh Avizheh, Niloufar Dadkhah, Mahshid Marbouti, and all those who were my best friends and companions on this journey.

Last but not the least, I am thankful to my wonderful family for their unlimited support during my studies. I owe a great debt to my brother, mother, and father without whom none of this would be possible.

Dedicated to the memory of all the dear stolen lives of flight PS752.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
AWGN	Additive White Gaussian Noise
BiT	Basic iJam Transmission
BISC	Binary Input Symmetric Channel
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BSC	Binary Symmetric Channel
DHKE	Diffie-Hellman Key Exchange
DL	Discrete Logarithm
DMC	Discrete Memoryless Channel
DS	Distinguishing Security
ei-UHF	efficiently invert Universal Hash Function
ECC	Error Correcting Code
FLR	Finite-Length Rate
FFT	Fast Fourier Transform
HtE	Hash-then-Encode
IC	Interference Channel
IFFT	Inverse Fast Fourier Transform
IID	Independent Identically Distributed
IoT	Internet of Things
ItE	Invert-then-Encode
KEM	Key Encapsulation Mechanism
KHtE	Keyed Hash-then-Encode
KXtX	Keyed eXtract-then-Xor

LDPC	Low-Density Parity-Check
LHL	Leftover Hash Lemma
LTE	Long-Term Evolution (wireless standard)
LWE	Learning With Errors
MAC	Multiple Access Channel
MIS	Mutual Information Security
OFDM	Orthogonal Frequency-Division Multiplexing
OM-SKA	One-Message Secret Key Agreement
OTP	One-Time Pad
OW-SK	One Way Secret Key
PD	Public Discussion
QAM	Quadrature Amplitude Modulation
RDS	Random message Distinguishing Security
RFID	Radio Frequency IDentification
RItE	Repeat Invert-then-Encode
RSA	Rivest, Shamir, and Adleman (cryptosystem)
SKA	Secret Key Agreement
SS	Semantic Security
SSH	Secure SHell
SSL	Secure Socket Layer
TLS	Transport Layer Security
TWC	Two Way Channel
UHF	Universal Hash Function
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
XtX	eXtract-then-Xor

"What Tarquin the proud communicated in his garden with the beheaded poppies was understood by the son but not by the messenger."

- Johann Georg Hamann

Chapter 1

Introduction

In a basic secure communication model, a sender transmits information in the form of a message to a receiver over a communication channel. The transmission is subject to undesired effects of the communication medium known as *noise*, and a third entity eavesdrops the communication. The ultimate goal is to send the message "reliably" and "securely" in the presence of noise and an eavesdropper. "Reliability" means the receiver is able to recover the original message with high probability, and "security" implies that the eavesdropper only obtains negligible information about the message. Encoding schemes and encryption protocols are designed and implemented to satisfy these two goals. The secure communication model is useful for studying the security of many real-world communication systems, such as the wireless communication systems where the broadcast nature of communication becomes the Achilles' heel of security by allowing unauthorized users (eavesdroppers with a radio receiver) to capture the communication that may carry confidential information.

The conventional approach is to meet the above goals separately. Error correcting codes are applied to the physical layer of communication to provide reliability. Communication at higher layers of the network protocol stack is assumed to be noise-free due to the application of error correcting codes. Cryptographic protocols are then used at the higher layers of the protocol stack to provide security requirements. For example, the Transport Layer Security (TLS) protocol [109] forming a significant proportion of secure communication on the Internet is implemented at the transport layer and uses public-key cryptography to authenticate the communicating parties and to establish a shared secret key, which is then used for message encryption in symmetric cryptography.

Most of the public-key cryptosystems assume the eavesdropper's computational power is bounded, and the system's security relies on the computational difficulty of solving certain problems. Two examples of these problems are discrete logarithm (DL) and integer factorization problems that form the basis of the security of Diffie-Hellman Key Exchange (DHKE) protocol, and RSA cryptosystem, respectively. Providing security

by relying on the difficulty of solving hard problems is not sufficient because computation hardware is getting cheaper every day, and some of the computational security schemes that are currently considered secure may no longer be in the future. Moreover, the security of these protocols is threatened since Peter Shor [124] gave efficient (polynomial-time) quantum algorithms to factor large numbers and compute discrete logarithms, which breaks all of today's Internet secure protocols with the deployment of the quantum-computer. Recent developments in quantum computers have led to the announcement by security agencies [128] to move to quantum-safe algorithms, and this has been followed by standardization efforts [26] in this domain.

Concerns about the breakdown of computational cryptosystems can be addressed by the information-theoretic security approach that removes computational assumptions. However, the security of such a system may rely on the availability of a secret key [115] or some correlated randomness [92] to communication parties, or requires assumptions about the probabilistic behavior of nature, for instance of a noisy channel [143] or a quantum measurement [14]. Shannon [115] initiated the study of secure communication problem from an information-theoretic perspective. He considered a noiseless communication scenario, in which the sender and the receiver share a secret key that is unknown to an eavesdropper. Used as a one-time-pad (OTP), this secret key enables secure transmission of the confidential messages.

This thesis is concerned with information-theoretically secure encoding and key agreement for secure communication. In this work, the inherent noise over the communication channel and the secret shared key are the main resources for secure message encoding and any kind of shared correlated randomness is the main resource for secret key agreement (SKA). To use noise in the communication channel, one needs to consider the physical layer of the channel and so the thesis studies the physical layer security.

1.1 Objectives

In this thesis, which is a collection of papers (manuscript-based thesis), three research problems are targeted in the context of information-theoretic security.

Problem 1: How to securely transmit a message using noisy channels?

Problem 2: How to securely transmit a message using noisy channels and a secret key?

Problem 3: How to establish an information-theoretic secret key?

Each problem is deliberated in a particular and well-studied information-theoretic communication model that allows formalization of the study and portraying the detailed objectives. The models are introduced briefly in the following.

- *Wiretap Channel Model*: In the communication model that is known as the "wiretap channel model", instead of limiting the computational power of the eavesdropper, the assumption is that the channel

from the transmitter to the legitimate receiver (main channel) has a physical advantage over the channel from the transmitter to the eavesdropper, who is also referred to as the "wiretapper" in this context. The physical advantage is associated with the noise level over the main and wiretapper's channels and is exploited to enable secure communication by deploying wise coding and pre-coding schemes. The wiretap channel model was first proposed by Wyner [143] for degraded channels (where the wiretapper receives a noisy version of the receiver's view) and then extended by Csiszár and Körner [34] to model any broadcast communication concerned with confidentiality. This model turns out to be a powerful model for capturing wireless secure communication requirements. When the physical advantage of the receiver's channel over the eavesdropper's cannot be guaranteed, the application of the wiretap channel model in wireless communication is possible by the introduction of artificial noise using a technique called "cooperative jamming" [81, 86, 132], in which a helper party introduces an artificial noise in the channel to provide secrecy.

- *Keyed Wiretap Channel Model*: A keyed wiretap channel model is a variation of the wiretap channel model in which a secret key is pre-shared between the legitimate communication parties. The goal is to take advantage of the noise over the adversary's channel as well as the secret key that is shared by the participants. These two are primary resources available to the sender and the receiver for securing communication, without making any computational assumption. Yamamoto [145] initiated the study of the (noisy) wiretap channel with a shared secret key.

- *Source Model for Key Agreement*: In the *source model* of key agreement, two legitimate parties Alice and Bob have samples of two correlated random values, and an eavesdropper Eve has side-information in the form of a third random value correlated with Alice's and Bob's. Alice and Bob communicate over a noise-free public channel that is visible to Eve, to extract a common shared key that is perfectly secret from Eve. The setting was independently considered by Maurer [92] and Ahlswede and Csiszár [2], and has been widely studied since. The source model can be realized by a satellite broadcasting a random string that is received by nodes over noisy channels.

1.1.1 Problem 1: How to securely transmit a message using noisy channels?

One of the central problems of security is studied: Alice wants to send a message reliably and securely over a channel in presence of an adversary Eve. The wiretap channel model is used for the study of this problem. The resulting encoding scheme is referred to as a *wiretap channel encoding* scheme. In this model (See Figure 1.1), the sender (Alice) is connected to the receiver (Bob) and the wiretapper through two communication channels, namely the main channel T and the wiretapper's channel W. The outputs of the two channels are

publicly known probabilistic functions of the input. The sender uses a randomized encoding algorithm Enc to encode a message m to a codeword (ciphertext) X that is the input to the two channels. The receiver and the wiretapper will receive $Y = \mathsf{T}(X)$ and $Z = \mathsf{W}(X)$ through their respective channels. The receiver will use a decoding function $\mathsf{Dec}(Y)$ to recover a message $\hat{m}$. The decoding will be in error if $m \neq \hat{m}$. The wiretapper's view of the communication is denoted by Z.

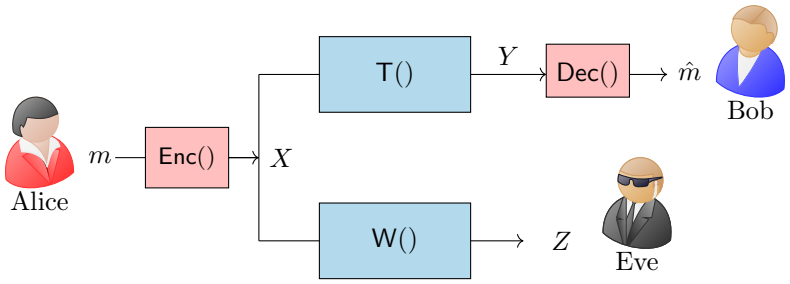

Figure 1.1: Wiretap channel encoding

The goal of the coding scheme is to provide secrecy against the wiretapper, and reliability for Bob. Secrecy is evaluated by finding a bound on the average information leakage, and reliability is quantified by the probability of error for a uniformly distributed message space [34, 143]. The definition of secrecy was later strengthened to bound the *total* information leakage in [90] and then to bound the total information leakage for *any* message distribution in [11]. The latter notion is the strongest existing secrecy notion for the wiretap channel and is shown to be equivalent with *semantic security* and *distinguishing security* notions of [58], adjusted for communication over the wiretap channel.

The *efficiency* of a wiretap coding system is measured by the *rate* $R(n)$, which is the ratio of the message length to n, the number of times that the wiretap channel is used for transmitting the encoded block with secrecy and reliability. The number n is referred to as the "number of channel uses" in this thesis. The rate R is achievable over a wiretap channel if there exists a family of wiretap codes indexed by n, such that as n grows, their rate approaches R and the error probability and information leakage vanish. The *secrecy capacity* of a wiretap channel is the highest achievable rate of all the coding schemes. Wyner [143] and respectively, Csiszár and Körner [34], calculated the secrecy capacity of the corresponding wiretap channel in their works using a non-constructive argument.

Explicit construction of capacity-achieving wiretap coding systems was a continuing open problem. Capacity-achieving schemes have been proposed recently for a limited class of communication channels. Existing constructions can be categorized into two different kinds: those that are based on a specific error correcting code [87, 136], and *modular constructions* that separate coding for secrecy from coding for reliability (for the main channel) and so are not restricted to a specific error correcting code (ECC)[11, 66, 138].

An important step forward in the construction of wiretap encryption system is due to Bellare, Tessaro and Vardy [11] who proposed the notion of semantic security for wiretap codes and introduced an elegant explicit modular construction of capacity-achieving wiretap codes that provide semantic security for the encoded message.

Modular constructions are attractive from theoretical and practical viewpoints, and provide flexibility in the choice of error correcting codes, which is particularly important in practice. The proposed wiretap construction in [11] is an example of wiretap modular construction. At the heart of the construction is a *seeded encoding* system that assumes a public random string called the *seed* can be shared by the sender and the receiver for encoding. The instantiation of this seeded encoding uses *invertible extractors* (See Section 1.3.4) that was first introduced in [28] for a different type of wiretap channel model [100]. Bellare et al. [11] introduced a generic approach called seed recycling to show that the seed can be amortized over many message blocks and so in the final construction, the public discussion channel is not needed. The proof of security uses a two step approach: first, security is proved for a random message and then, it is proved that for certain types of seeded encryption systems and wiretap channels, security against a random message implies security for any message. The authors left the direct security proof of their construction as an open problem.

Wireless communication is a setting in which the wiretap model naturally arises. However, in many settings, the eavesdropper channel is not sufficiently noisy, and so the setting does not provide secrecy capacity. One can also create the effect of a wiretap channel for an eavesdropper by using techniques such as *cooperative jamming*, where the communicating parties cooperate to *jam* the eavesdropper's view. The existence of a helper jammer ensures that the legitimate parties have enough physical layer advantage over the eavesdropper that enables them to communicate securely [81, 86, 132]. It is required to carefully analyse the interaction between the helper jammer and other communication parties, estimate parameters of the realized wiretap channel and choose an appropriate coding scheme for secure communication. The next step is to evaluate the performance of the system in practice to disclose deficiencies of the existing coding techniques once the performance of the system is evaluated.

Objectives

My objectives toward the problem of secure message encoding using noisy channels are listed below:

- To propose a new modular construction of a wiretap coding system with proof of semantic security and achieving capacity for a broad class of wiretap channels. It is also desired to have a construction with the potential of being combined with keyed encoding schemes to take advantage of a shared key

when available.

- To improve the computational efficiency of the construction, and to estimate the parameters of the encoding system for finite-length messages for comparing the construction with other existing constructions in practical scenarios.
- To explore the implementation of wiretap codes in practice, in particular, model and analyze a secure communication protocol that uses cooperative jamming as an instance of creating a virtual wiretap channel.

1.1.2 Problem 2: How to securely transmit a message using noisy channels and a secret key?

Shannon initiated the study of secure message encoding with a shared key from an information-theoretic viewpoint [115, 116]. His solution was to first meet reliability through the application of error correcting codes, and then provide security over the reliable communication by the OTP encryption scheme. In OTP, the pad is the random secret key that is XORed with the message to completely hide it from the eyes of the eavesdropper. Shannon showed perfect security against an eavesdropping adversary is obtained if the shared secret key is at least as long as the message.

Combining Shannon's secret key based secure communication [116], and Wyner's wiretap channel [143] approaches results in reducing the length of the required key of OTP. This model is called the *keyed wiretap channel model* that is first considered in [145] and followed by [78, 94, 141]. In this framework, the randomness of the wiretapper's channel is treated as an extra resource for partially hiding the message, and can reduce the required key length of the OTP system for completely hiding the message. In the general keyed wiretap channel model of [78], Alice wants to send a message privately to Bob through the main channel T, while Eve intercepts the communication through the channel W, and a secret key with given rate is shared between Alice and Bob. The rate of a shared key is defined as the key length divided by n, the number of channel uses. Similarly, the rate of an encoding scheme is defined as the length of the codeword divided by n. The achievable rate of an encoding family is the asymptotic rate of the encoding system that is achieved as n grows, and the secrecy capacity is the highest achievable rate. From the wiretap channel point of view, the secrecy capacity of a keyed wiretap channel is increased by the rate of the shared key as long as it does not exceed the reliability capacity of the main channel. This is shown in [78], where the general secrecy capacity of a keyed wiretap channel is derived by showing the existence of a random encoding scheme.

The *secrecy* of a keyed encoding scheme for a keyed wiretap channel is defined for a uniformly distributed message space, and stronger secrecy notions for *any* message distribution have never been considered. Explicit

construction of a keyed encoding scheme for this setting has been recently proposed in [141], which is based on the application of specific error correcting codes called *polar codes* [6] in the construction.

Objectives

My objectives for the problem of secure message transmission using noisy channels and a shared secret key are listed below:

- To make the secrecy notion of encoding over the keyed wiretap channel stronger.
- To use all the available resources (in particular, the secret key and the channel noise) in a communication setting to achieve information-theoretic security. An ideal construction for this purpose enables secure communication when at least one of the resources is available.

1.1.3 Problem 3: How to establish an information-theoretic secret key?

Establishing a shared secret key between two parties is one of the fundamental problems in cryptography. Once such a secret key is established, through the OTP, a secure message transmission protocol is immediately constructed.

Source model secret key agreement that is also referred to as secret key agreement by public discussion from correlated randomness, was initiated by Maurer [92] and Ahlswede and Csiszár [2] independently. In this model, Alice and Bob have two dependent samples of a correlated randomness source, namely X and Y, respectively, and an eavesdropper Eve has side-information in the form of a third dependent sample Z. Alice and Bob communicate over a reliable public channel that is visible to (but not physically vulnerable by) Eve, to extract a common shared key that is perfectly secret from Eve. The correlated randomness can be generated from different processes, for example when the samples of a beacon that broadcasts randomness are received by all parties over their individual channels (e.g., a satellite broadcasting samples of a random source (See Figure 1.2), or Alice simply generating a random string X and sending it over the wiretap channel, resulting in Y and Z, at Bob and the wiretapper, respectively. Maurer [92] showed that when a public discussion channel, in addition to the correlated randomness, is available to Alice and Bob, they are able to establish a shared secret key even if the channel secrecy capacity is zero. He also showed that this setting is a "minimum" setting, meaning that without any initial correlated randomness, secret key agreement is impossible.

One-message secret key agreement (OM-SKA) is a class of secret key agreement protocols under the source model with two distinctive properties, namely (i) only one-way communication from Alice to Bob is allowed, and (ii) Alice is only allowed to send *one message* to Bob for the purpose of key agreement. This

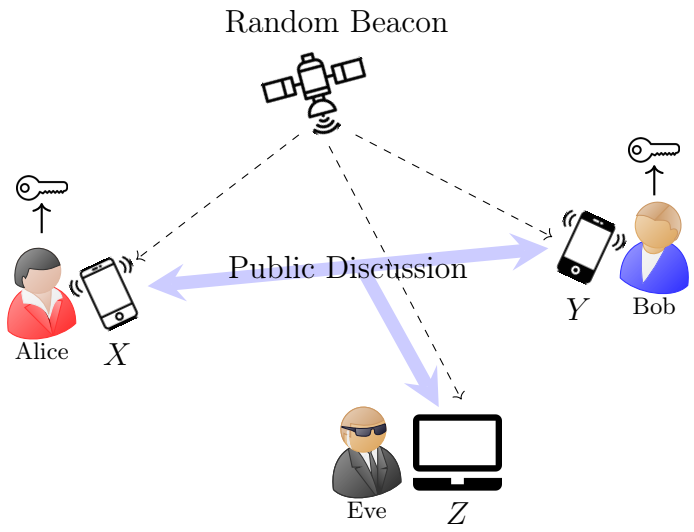

Figure 1.2: Source model key agreement

problem was first explored by Holenstein and Renner in [74], where the first explicit OM-SKA protocols were proposed. The study was followed in [105] and [29] and other explicit OM-SKA protocols based on polar codes were proposed. One-message key agreement protocols are sometimes preferred over interactive alternatives, especially by small devices with power constraints, since the cost of interaction for secret key agreement can become excessive for conventional key sizes. Moreover, the environment may change (e.g., in ad hoc networks) during the interaction or transmission of more than one message, and the initial physical assumptions may not hold and therefore, the security is not guaranteed anymore.

The *efficiency* of a secret key agreement protocol when Alice, Bob and Eve have n samples of the correlated random source is measured in terms of the secret key rate (achievable key length divided by n). The highest asymptotic ($n \to \infty$) key rate that can be achieved in a setting is the *secret key capacity* of the setting. Bounds on the secret key capacity in source model are given in [2] and [92]. The non-asymptotic efficiency of a SKA protocol is important in the real-life deployment of the protocol. This has been recently noted in [68], where bounds on secret key length of an interactive SKA are established in finite blocklength regime using higher order approximations. However, such analysis for OM-SKA does not exist in literature.

Wiretap channel codes for secure message transmission can also be used for SKA: Alice generates a random key and sends it (as a message) securely to Bob. The secret key in this setting can only be established when the main channel has physical advantage over the wiretapper's channel. The physical advantage can be "virtually" generated by cooperative jamming.

Objectives

My objectives on the secret key agreement problem are listed below:

- To formally analyze the generated key in a practical protocol proposed in [59] that uses self-jamming technique, and to use an abstract wiretap channel model to propose a complementary SKA protocol(s) for establishing an information-theoretic secure key in this framework.
- To propose a practical OM-SKA protocol with an analysis for finite blocklength.

1.2 Contributions

The contributions of this thesis are in the form of four published papers, one poster paper and three unpublished papers that cover the above objectives. These contributions are given in three parts, where each part is directed by one of the introduced research problems. The list of papers included in this thesis is given in Table 1.1.

In the following, three main parts of this thesis are introduced. Contained papers in each part are listed, and corresponding contributions of each paper are elaborated.

1.2.1 Modular semantically secure wiretap encoding

Highlights of the contributions: Semantic security is the strongest notion of secrecy for wiretap encoding. The proposed construction in P.1 guarantees semantic security for encoding and improves the efficiency of previously known constructions. The application of wiretap codes in practice requires a framework to evaluate their efficiency for the encoding of finite-length messages. Such a framework is proposed in P.2. Another important step toward the application of wiretap codes in practice is the study of techniques or communication settings that realizes wiretap channels. In P.3, realization of a wiretap channel through the cooperative jamming is studied.

P.1 *Hash-then-Encode: A Modular Semantically SecureWiretap Code [120].*

Contributions: A new modular construction of a wiretap encoding system with efficient encoding and decoding is proposed. The construction is called *Hash-then-Encode (***HtE***)* as the encoding consists of a hash function calculation, followed by an error correcting code application and decoding consists of encoding an error correcting code, followed by a hash function calculation. This makes the proposed wiretap encoding/decoding operations the most computationally efficient among existing modular constructions because it skips the hash inversion step used in other constructions [11, 66, 138].

ID	Publication	Publication Type	Chapter	Problem
P1	S. Sharifian, F. Lin, and R. Safavi-Naini, "Hash-then-Encode: A Modular Semantically Secure Wiretap Code," in *Proceedings of the 2nd Workshop on Communication Security (WCS 2017)*. Springer, 2018, pp. 49–63	Conference paper	Chapter 2	Problem 1
P2	S. Sharifian, R. Safavi-Naini, and F. Lin, "Post-Quantum Security using Channel Noise," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: ACM, Oct 2018, pp. 2288–2290	Poster paper	Chapter 3	Problem 1
P3	S. Sharifian, R. Safavi-Naini, and F. Lin, "A Virtual Wiretap Channel for Secure Message Transmission," in *International Conference on Cryptology in Malaysia*. Springer, 2017, pp. 171–192	Conference paper	Chapter 4	Problem 1
P4	S. Sharifian and R. Safavi-Naini, "A Modular Semantically Secure Wiretap Code with Shared Key for Weakly Symmetric Channels," in *2019 IEEE Information Theory Workshop (ITW)*. IEEE, Aug 2019, pp. 1–5	Conference paper	Chapter 5	Problem 2
P5	S. Sharifian, R. Safavi-Naini, and F. Lin, "Semantically Secure Keyed Wiretap Encoding Schemes," *Journal of Cryptology*, 2020, manuscript submitted for review.	Journal paper (under review)	Chapter 6	Problem 2
P6	S. Sharifian, A. Poostindouz, and R. Safavi-Naini, "A One-Round Key Agreement Protocol with Information-Theoretic Security," *ISIT*, 2020, manuscript submitted for review. [Online]. Available: `http://arxiv.org/abs/1905.04280`	Conference paper (under review)	Chapter 7	Problem 3
P7	S. Sharifian, F. Lin, and R. Safavi-Naini, "Secret Key Agreement using a Virtual Wiretap Channel," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. IEEE, May 2017, pp. 1–9	Conference paper	Chapter 8	Problem 3
P8	R. Safavi-Naini and S. Sharifian, "Generalized KEM and its Combiners," *ITC*, 2020, manuscript submitted for review.	Conference paper (under review)	Appendix C	Bonus Problem

Table 1.1: Table of contributions

- The semantic security of the construction is proved using the framework in [11] and the capacity-achieving of the construction is shown for a large class of wiretap channels.
- A general construction of invertible Universal Hash Family (UHF) from XOR-UHFs is given.
- The proposed construction can easily be modified to also take advantage of a possibly existing shared secret key between the sender and the receiver (this is noted in Chapter 6 where the keyed wiretap channel encoding is studied).

P.2 *Post-quantum Security using Channel Noise [121].*

Contributions: Long-term security in general and post-quantum security in particular is a strong requirement for Internet of Things (IoT) systems that consist of low-complexity devices with energy constraints. Modular wiretap schemes are computationally efficient secure encoding methods that guarantee long-term security. The application of wiretap codes in practice requires a concrete estimate of performance parameters for finite-length messages.

- A framework for comparing the efficiency of modular constructions is proposed by defining the finite-length rate (FLR).
- The finite-length rate of two modular semantically secure wiretap encoding schemes (**HtE** in [120] and **ItE** in [12]) are compared for conventional IoT message blocks.

P.3 *A Virtual Wiretap Channel for Secure Message Transmission[119].*

Contributions: The iJam protocol, proposed by Gollakota and Katabi [59], uses friendly jamming by the receiver to establish an information-theoretically secure shared key between the sender and the receiver. The protocol relies on the Basic iJam Transmission protocol (BiT protocol) that uses properties of OFDM (Orthogonal Frequency-Division Multiplexing) to create uncertainty for Eve in receiving the sent information, and uses this uncertainty to construct a secure key agreement protocol.

- An abstract model for BiT protocol as a wiretap channel is proposed, which is referred to as a *virtual wiretap channel*.
- Parameters of the virtual wiretap channel are theoretically estimated.
- The secrecy capacity of the virtual wiretap channel is derived, and a secure message transmission protocol with provable semantic security for the channel is designed.

1.2.2 Modular semantically secure keyed wiretap encoding

Highlights of the contributions: In P.4, the notion of secrecy for keyed wiretap encoding is strengthened by defining semantic security for keyed wiretap channels and a new construction that guarantees semantic security and achieves the capacity for a limited class of wiretap channels is proposed. In P.5, the construction has been improved to provide secrecy for keyed encoding over a large class of wiretap channels. The proof techniques of P.5 can be used for finite-length analysis of the encoding scheme.

P.4 *A Modular Semantically Secure Wiretap Code with Shared Key for Weakly Symmetric Channels [117].*

Contribution: Information-theoretic security for a keyed wiretap channel setting emerges from two resources, namely, the shared secret key, and the physical advantage of the receiver's channel due to noisier view of the wiretapper. The proposed keyed wiretap encoding scheme is called **KHtE** (Keyed Hash-then-Enocde), which can be viewed as an extension of the wiretap coding construction, **HtE** [120] that allows us to take advantage of the available shared key besides the wiretapper's channel noise for providing confidentiality.

- Semantic security and seeded encription are defined for keyed wiretap encoding.
- A modular semantically secure construction of keyed wiretap codes that achieves secrecy capacity of weakly symmetric wiretap channels is proposed.
- Concrete parameters of the construction to achieve a desired level of secrecy and reliability are derived for finite-length messages.

P.5 *Semantically Secure Keyed Wiretap Encoding Schemes [123].*

Contribution: The **HtE** construction in [120] fails to achieve security when the secrecy capacity of the wiretap channel is zero, and the **KHtE** construction in [117] is not secure when a shared key doesn't exist. In this chapter, a modular keyed wiretap encoding scheme called $\mathbf{KHtE}^*$ is proposed that can be constructed from *any* error correcting code and is secure even in the absence of a shared key or when the secrecy capacity of the wiretap channel is zero.

- Semantic security of the constructions are shown for *any* wiretap channel.
- The schemes are shown to be capacity-achieving for weakly symmetric wiretap channels.
- In the absence of a shared key, the proposed constructions are compared with other modular wiretap encoding schemes in terms of secrecy, capacity-achieving and types of required error correcting codes in the construction.

- A framework for converting any seeded encoding scheme to seedless encoding scheme with small secrecy sacrification is proposed.

1.2.3 Information-theoretic secret key agreement

Highlights of the contributions: An information-theoretic secret key agreement protocol is proposed in P.6 that only requires the transmission of one message. The efficiency of this protocol is evaluated and compared to other one-message secret key agreement protocols. The analysis of the protocol gives a precise approximation of the maximum possible secret key length that can be established by the protocol for a given secrecy and reliability levels. In P.7, secret key agreement over a wiretap channel that is realized by a specific cooperative jamming technique is studied, and efficient secret key agreement protocols are proposed.

P.6 *A One-Round Key Agreement Protocol with Information-Theoretic Security [122].*

Contributions: An explicit construction of a source model OM-SKA protocol is proposed that achieves the one-way secret key (OW-SK) capacity of the model. Following the SKA framework of [24], the two main steps in the protocol are *information reconciliation* and *privacy amplification*. In order to find sharp bounds on finite achievable key length, a reconciliation method inspired by information spectrum analysis of [68] and tight bounds in [108] are used.

- An OM-SKA protocol is proposed and its security is analyzed.
- Finite-length lower-bound for the key length and upper-bound for communication cost is derived and compared with the OM-SKA protocol in [73].
- It is shown that the proposed construction achieves the OW-SK capacity in source model.

P.7 *Secret Key Agreement using a Virtual Wiretap Channel [118].*

Contributions: In this chapter, key agreement using the physical layer properties of communication channels is studied. It is shown in [119] that iJam creates a *virtual* wiretap channel for the adversary through a subprotocol between the sender and the receiver that uses self-jamming by the receiver. This wiretap model is used to design secret key agreement protocols with provable security.

- Three protocols are proposed. Two of them use the wiretap channel once from Alice to Bob, and the third protocol uses two wiretap channels, one from Alice to Bob, and one in the opposite direction for secret key agreement.
- Security proof and efficiency analysis for the protocols are given.

1.3 Background

The results of the chapters contained in this thesis are built on a common background from probability theory and information theory. In this section, basic definitions, essential inequalities, and fundamental relations that are repeatedly used in the thesis are summarized for the ease of reference. However, each chapter of this thesis (as an independent manuscript) is self-contained and introduces more specialized preliminaries that are tailored for that chapter.

Notations[1]: A random variable X is defined by a set $\mathcal{X}$ and a probability distribution $\Pr(X)$ over $\mathcal{X}$. The variable takes a value $x \in \mathcal{X}$ with probability $\Pr(X = x)$. For two random variables X and Y, P_{XY} denotes their joint distribution, $P_{X|Y}$ denotes the conditional distribution of X when Y is given, and P_X denotes the marginal distribution of X. The expected value of a random variable X is denoted by $\mathbb{E}(X)$ and is given by $\mathbb{E}(X) = \sum_{x \in \mathcal{X}} x \cdot \Pr(X = x)$.

The uppercase U is reserved for uniform distribution and $U_{\mathcal{X}}$ denotes uniform distribution over $\mathcal{X}$ and U_ℓ denotes uniform distribution over $\{0,1\}^\ell$. Bold lowercase letters are used to denote vectors and bold uppercase letters to denote matrices. Sans-serif capital letters denote functions or associated functions with channels. To denote concatenation we use "$\|$". All the logarithms are in base 2.

1.3.1 Inequalities

Markov's inequality [110, Proposition 2.1]. Let X be a non-negative random variable and suppose that $\mathbb{E}(X)$ exists. For any $a > 0$,

$$\Pr(X > a) \leq \frac{\mathbb{E}(X)}{a}. \tag{1.1}$$

Jensen's inequality [30, Theorem 2.6.2]. Let f be a convex function and X be a random variable, then

$$\mathbb{E}(\mathsf{f}(X) \geq \mathsf{f}(\mathbb{E}(X)). \tag{1.2}$$

1.3.2 Information measures

For a random variable $X \in \mathcal{X}$ with distribution $P_X(x)$, the **Shannon entropy** is denoted by $H(X)$ and is defined as:

$$H(X) \triangleq -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x). \tag{1.3}$$

[1] In different chapters of this thesis, slightly different notations for showing the same concepts may have been used (e.g., m and $\mathbf{m}$ for denoting the message). However, all notations are introduced at the beginning of each chapter. Here, we have referred to the most recent notations used in Part II of this thesis.

For random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ with joint distribution P_{XY}, conditional distribution $P_{X|Y}$, and marginal distributions P_X and P_Y, **joint entropy** $H(X,Y)$, **conditional entropy** $H(X|Y)$, and **mutual information** $I(X;Y)$, are respectively given by

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{XY}(x,y)\log P_{XY}(x,y), \tag{1.4}$$

$$H(X|Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{XY}(x,y)\log P_{X|Y}(x|y), \tag{1.5}$$

$$I(X;Y) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{XY}(x,y)\log \frac{P_{XY}(x,y)}{P_X(x)P_Y(y)}. \tag{1.6}$$

Lemma 1.1. *[30] The following relationship holds between mutual information and Shannon entropy.*

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y). \tag{1.7}$$

The **min-entropy** of a random variable $X \in \mathcal{X}$ with distribution $P_X(x)$ is denoted by $H_\infty(X)$ and is defined as:

$$H_\infty(X) \triangleq -\log\Big(\max_x\big(P_X(x)\big)\Big). \tag{1.8}$$

The **statistical distance** between two random variables X and Y over a set $\mathcal{U}$ is defined as:

$$\mathrm{SD}(X,Y) \triangleq \frac{1}{2}\sum_{u\in\mathcal{U}} |\Pr(X=u) - \Pr(Y=u)|. \tag{1.9}$$

The **collision probability** of a random variable X with distribution P_X is defined as:

$$CP(X) \triangleq \sum_{x\in\mathcal{X}} P_X(x)^2. \tag{1.10}$$

1.3.3 Communication channels

In a communication system, a *channel* is a physical transmission medium such as a wire or environment through which an information signal is transmitted from one or more senders to one or more receivers. The communication channel is modeled with a randomized function that maps an input random variable X to an output random variable Y. The input random variable X represents symbols from the input alphabet $\mathcal{X}$ that are generated with some probability distribution P_X, and are input to the channel. The random variable Y represents symbols from the output alphabet $\mathcal{Y}$ with probability distribution P_Y that are received

from the channel. A realization of the random variable X is the information signal that the sender wants to transmit. The received information signal is the corresponding realization of the output random variable Y.

A channel is called discrete when its input and output alphabet sets are discrete sets. Such a channel is memoryless (DMC) if its output at any time interval only depends on its input in the corresponding time interval.

A channel as a randomized mapping is described by the conditional probability of each output symbol given an input symbol. Suppose members of the input alphabet $\mathcal{X}$ are indexed from 1 to $|\mathcal{X}|$ and members of the output alphabet are labeled from 1 to $|\mathcal{Y}|$. The transition probability matrix of the channel is denoted by $\mathbf{CH}$. Then $p_{i,j}$, the element of i-th row and j-th column in matrix $\mathbf{CH}$, is $p_{i,j} = \Pr(Y = y_j | X = x_i)$.

A DMC with input alphabet $\mathcal{X}$, output alphabet $\mathcal{Y}$ and transition probability matrix $\mathbf{CH}$ is denoted with $\mathsf{CH}\langle \mathcal{X}, \mathcal{Y}, \mathbf{CH} \rangle$. The other way of describing the channel is as a probabilistic function, where $\mathsf{CH}(X) = Y$ denotes a channel with input X and output Y. The probability distribution of Y is dependent on the probability distribution of X and the channel. $\mathsf{CH}^n(\cdot)$ denotes the function that is obtained from n independent applications of the channel.

A message $m \in \mathcal{M}$ can be transmitted over the channel provided that an appropriate *encoding function* Enc maps $\{0,1\}^b$ to $\mathcal{X}^n$ and a corresponding *decoding function* Dec maps $\mathcal{Y}^n$ to $\{0,1\}^b$, where n is the number of channel uses. For ideal encoding/decoding functions we have $\mathsf{Dec}(\mathsf{CH}^n(\mathsf{Enc}(m))) = m$. Due to channel randomization, there is a probability that the above equation doesn't hold. The error probability of a pair of encoding/decoding functions is defined as:

$$P_e = \max_{m \in \mathcal{M}} \Pr[\mathsf{Dec}(\mathsf{CH}^n(\mathsf{Enc}(m))) \neq m], \tag{1.11}$$

where probability is taken over the randomness of the channel. The encoding function adds redundancy to the message to limit the error probability.

The rate of the transmission (bits per channel use) is defined by $R = {}^{b}\!/_{n}$. Rate ρ is achievable for a family of encoding/decoding functions, if $\lim_{n\to\infty} P_e = 0$, and $\rho = \lim_{n\to\infty} R$. Usually rate R is a function of n, the number of channel uses. In these cases, the rate is denoted by $R(n)$ to show the dependency of the rate on n. The **capacity** of CH, denoted by (C_{CH}), is the maximum of all achievable rates. Shannon in [115] showed the channel capacity is given by:

$$\mathrm{C}_{\mathsf{CH}} = \max_{P_X} I(X; \mathsf{CH}(X)). \tag{1.12}$$

A channel is called **symmetric** when the rows of the channel's transition probability matrix are permu-

tations of one another and the columns are also permutations of each other.

An example of a symmetric channel is the **Binary Symmetric Channel** (BSC). Such a channel flips the input with probability p. The BSC function is captured in Figure 1.3.

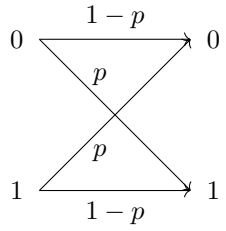

Figure 1.3: A binary symmetric channel

An important class of symmetric channels are described by **additive noise channels**. For an additive noise channel, the input and output alphabet set of the channel are the same Galois field with q elements denoted by $\mathbb{F}_q$. For random variable $Z \in \mathbb{F}_q$, the additive noise channel is modeled as:

$$\mathcal{CH}(X) = X \oplus Z, \tag{1.13}$$

where addition is over $\mathbb{F}_q$ and Z is independent from X.

CH_2 is **degraded** with respect to CH_1 when CH_2 is the cascade of CH_1 and CH_3. In this case, we have $\mathbf{CH}_2 = \mathbf{CH}_1 \times \mathbf{CH}_3$, where "$\times$" denotes matrix multiplication. The case is captured in Figure 1.4.

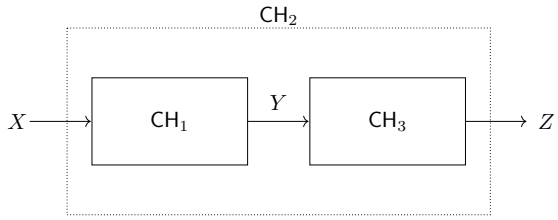

Figure 1.4: A degraded channel

1.3.4 Randomness extraction

Randomness extractors aim to extract randomness from imperfect sources. The existence of such functions is proven in [99].

A random variable $X \in \{0,1\}^m$ where $H_\infty(X) \geq d$ (i.e., if for all $x \in \{0,1\}^m$, $Pr[X = x] \leq 2^{-d}$) is called an (m, d)-source. We can extract at most d bits of randomness from this variable.

A (d,ϵ)-**strong extractor** is a function $\mathsf{EXT}:\{0,1\}^m\times\mathcal{S}\rightarrow\{0,1\}^\ell$ such that for any (m,d)-source X and a uniformly random S over $\mathcal{S}$ we have $\mathbf{SD}\Big(\mathsf{EXT}\big((X,S),S\big);\big(U_\ell,S\big)\Big)\leq\epsilon$.

An **inverter** for the extractor $\mathsf{EXT}(\cdot,\cdot)$ is the function $\mathsf{INV}:\{0,1\}^r\times\mathcal{S}\times\{0,1\}^b\rightarrow\{0,1\}^n$, if for a uniform $R\in\{0,1\}^r$ and for all $S\in\mathcal{S}$ and $Y\in\{0,1\}^b$, the random variable $\mathsf{INV}:(S,R,Y)$ is uniformly distributed over all preimages of Y under $\mathsf{EXT}(S,\cdot)$.

One of the known constructions for randomness extractors is obtained by using **hash functions**. A family $\{\mathsf{h}_s|s\in\mathcal{S}\}$ of functions $\mathsf{h}_s:\mathcal{X}\rightarrow\mathcal{Y}$ is a 2-Universal Hash Family if for any $x\neq x^{'}$, $\Pr\{\mathsf{h}_S(x)=\mathsf{h}_S(x^{'})\}\leq\frac{1}{|\mathcal{Y}|}$, where the probability is on the uniform choices over $\mathcal{S}$.

(Leftover Hash Lemma (LHL))[76, 77]: Let $\mathsf{h}(\cdot)$ be a randomly chosen function from $\mathcal{H}:\{0,1\}^m\rightarrow\{0,1\}^\ell$ and let $\ell=d-2\log{}^1\!/\!_\epsilon$, then for any (m,d)-source X,

$$\mathbf{SD}\Big(\big(\mathsf{h}_S(X),S\big);\big(U_\ell,S\big)\Big)\leq\epsilon. \tag{1.14}$$

1.4 Organization

This thesis is based on eight manuscripts, seven included in the main body and one in the appendix. The thesis is organized in three main parts and three appendices. The content of each part is a collection of papers, each given as a separate chapter. Part I is on modular semantically secure wiretap encoding and consists of chapters 2 to 4. In Chapter 2, a modular semantically secure wiretap code is proposed. In Chapter 3, the efficiency of the construction is evaluated, and in Chapter 4, a realization of a wiretap channel is discussed. The second part of this thesis is on modular semantically secure keyed wiretap codes and consists of Chapters 5 and 6. In Chapter 5, the construction of a new keyed wiretap code is proposed for a limited class of channels. This construction is refined in Chapter 6 to provide semantic security for a wider class of communication channels. The third part of this thesis is on information-theoretic secret key agreement and consists of two chapters. In Chapter 7, a one-message secret key agreement protocol is proposed and its efficiency is discussed. In Chapter 8, information-theoretic secret key agreement protocols over a realization of a wiretap channel are proposed. The thesis is concluded in Chapter 9.

Part I

Modular Semantically Secure Wiretap Encoding

Chapter 2

Hash-then-Encode: A Modular Semantically Secure Wiretap Code[1]

Abstract. We propose a modular construction of a semantically secure wiretap code that achieves the secrecy capacity of a large class of wiretap channels. The security of the construction is proved by interpreting the construction as an instance of an invertible extractor, and use the framework in [11] to complete the proof. The construction has computation for encoding and decoding equivalent to hashing, and the smallest effective transmission rate among known modular capacity-achieving constructions. We also give a modular construction of invertible Universal Hash Families (UHF) from XOR-UHFs that is of independent interest.

2.1 Introduction

Consider a scenario where Alice wants to send a message to Bob over a (noisy) channel that is eavesdropped by Eve. Alice and Bob do not share a key and Eve is computationally unbounded. Wyner [143] made the ingenious observation that noise in Eve's channel can be used as the cryptographer's resource to provide security, while providing reliability for the communication. In *Wyner wiretap model,* and its extension by Cziszár and Körner [34], the sender is connected to the receiver and the eavesdropper (wiretapper) through two noisy channels, referred to as the *receiver's channel,* T, (also called the *main channel*) and the *wiretapper's channel*, W, respectively. It has been proved [34, 143] that communication with secrecy and reliability is possible if the wiretapper's channel is "noisier" than the receiver's channel. Wiretap model captures wireless communication scenarios where a sender's transmitted message can be intercepted by a nearby eavesdropper, and so the sent message is received by the intended receiver and the wiretapper through the two channels T

[1]The content of this chapter is published as a paper [120] in proceedings of WCS 2017.

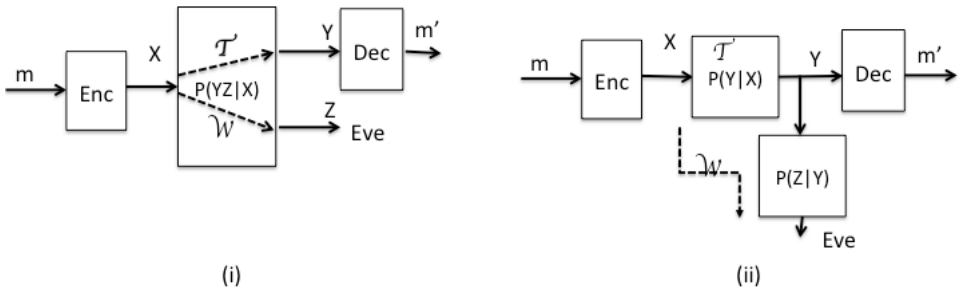

Figure 2.1: (i) Wiretap channel with the main channel T and the wiretapper's channel W; (ii) Degraded wiretap channel with main channel T and the wiretapper's channel W that is the concatenation of two channels.

and W, respectively. The model has intrigued the research community and has generated a huge amount of research because of the promise of information-theoretic security without the need for a shared secret key.

Wiretap model. In the wiretap model (See Figure 2.1) the sender uses a randomized encoding (also called encryption) algorithm $\mathsf{Enc} : \{0,1\}^b \to \{0,1\}^n$ that encodes (encrypts) a message $\mathbf{m}$ and generates a codeword (ciphertext) X, that is the input to the receiver's channel T and the wiretapper's channel W. The receiver will use a decoding (decryption) function $\mathsf{Dec} : \{0,1\}^n \to \{0,1\}^b$ on Y, to recover a message $\mathbf{m}'$. The decryption will be in error if $\mathbf{m}' \neq \mathbf{m}$. The wiretapper's view of the communication is denoted by Z. The goal of the encryption system is to provide secrecy and reliability for the receiver.

Wyner defined *security and reliability* as asymptotic values of $I(M;Z)/b$, and $\Pr[\mathsf{Dec}(Y) \neq M]$ when $b \to \infty$, respectively, assuming messages are uniformly distributed. Here $I(A;B)$ is the mutual information between the two random variables A and B, and M denotes the random variable corresponding to message space. The security definition of wiretap model has been strengthened by replacing the rate of leakage of information, $I(M;Z)/b$, with the total information leakage $I(M;Z)$ in [90], and more recently with $\max_{P_M} I(M;Z)$ in [11], which is shown to be equivalent to the *semantic security* [58].

The *transmission efficiency* of wiretap encryption systems is measured by the *rate*, $R = \frac{b}{n}$, of sending messages with secrecy and reliability. The secrecy capacity of a wiretap channel is denoted by C_s, and is the highest achievable rate of communication, satisfying the security and reliability requirements.

It has been shown that when T and W are symmetric and W is degraded with respect to T, secrecy capacity is given by $C_s = C_{\mathsf{T}} - C_{\mathsf{W}}$, where C_{T} and C_{W} are Shannon (reliability) capacity of the receiver's and the wiretapper's channels, respectively.

An explicit construction of capacity-achieving wiretap encryption systems with efficient encoding and decoding has been a longstanding open problem. The first explicit capacity-achieving construction for a large class of wiretap channels was by using polar codes and their properties [87]. More recently, capacity-achieving modular constructions with efficient encoding and decoding have been proposed [11, 66, 138].

These constructions can use any capacity-achieving error correcting code and because of the flexibility in the choice of the error correcting code, are attractive in practice.

In the existing modular constructions, wiretap encoding has two steps: the first step is a randomized coding using an *invertible seeded extractor*, and the second step is an Error Correcting Code (ECC) that encodes the output of the first step. The extractor is implemented using a *Universal Hash Family (invertible UHF)*. The seed for the UHF may be pre-shared by the sender and the receiver [66], or sent reliably (without secrecy) across the main channel [11, 138]. In this latter case, the seed can be used for encryption of a long message with many blocks, and its required transmission is thus amortized over many blocks of the message. All known wiretap encoder constructions require inverting a hash function. The commonly used construction for invertible UHF uses multiplication over finite fields for forward hashing, and finding the inverse of a field element followed by a finite field multiplication for inverting the hash.

Wiretap codes are evaluated in asymptotic regime. That is, when the message length approaches infinity. In practice, however, wiretap codes will be primarily used for sending single finite-length messages. This will be a common setting in networks of small devices that commonly occurs in the future Internet of Things (IoT). In such settings, the seed must be sent with each message and its length will not be amortized over many blocks. Hence the effective rate of communication must take the seed length into account.

2.1.1 Our work

We start by giving a modular construction of an invertible UHF from any XOR-UHF. A hash function $h : \mathcal{X} \to \mathcal{Y}$ maps the elements of a domain $\mathcal{X}$ to the elements of $\mathcal{Y}$. In our applications $|\mathcal{Y}| < |\mathcal{X}|$ and so $\mathbf{y} \in \mathcal{Y}$ corresponds to a set $h^{\text{Inv}}(\mathbf{y})$ of pre-images. An inverter function for h is a randomized function that for any $\mathbf{y} \in \mathcal{Y}$ outputs, randomly (and uniformly), an element of the pre-image set $h^{\text{Inv}}(\mathbf{y})$.

A UHF (Definition 2.3) is a family of hash functions with the same domain and range indexed by the *seed*, and has the property that for any pair of different elements $\mathbf{x}, \mathbf{x}' \in \mathcal{X}$ we have $\Pr[h_S(\mathbf{x}) = h_S(\mathbf{x}')] \leq \varepsilon$, where probability is over the random choice of the seed. The family is invertible if there is an inverter function for each member of the family.

A modular construction of invertible UHF. In Section 2.3, we show a modular construction of an invertible UHF. The construction uses an XOR-UHF (Definition 2.4) that maps $\mathcal{X} \to \mathcal{Y}$, and the XOR property requires that for any pair of different elements $\mathbf{x}, \mathbf{x}' \in \mathcal{X}$ we have $\Pr[h_S(\mathbf{x}) \oplus h_S(\mathbf{x}') = \mathbf{a}] \leq \varepsilon$ for any $\mathbf{a} \in \mathcal{Y}$, where probability is over the random choice of the seed. The resulting invertible UHF maps $\mathcal{X} \times \mathcal{Y} \to \mathcal{Y}$ and has the same ε.

Leftover Hash Lemma (LHL) (Lemma 2.2) shows that a UHF family can be used as a seeded extractor.

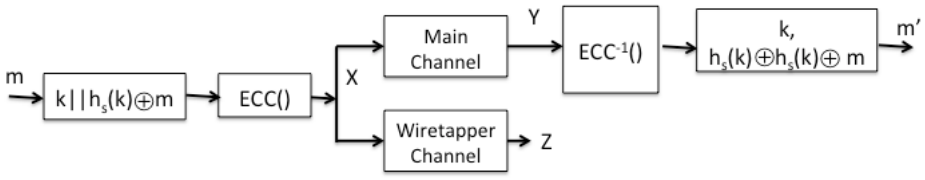

Figure 2.2: Hash-then-Encode (**HtE**) construction

Our result thus, gives an *invertible* seeded extractor from any XOR-UHF with the property that the inversion operation of a hash function is simply computing a hash function (a member of UHF). Invertible extractors (and invertible UHF) are of interest because of their applications to the construction of wiretap codes (both Wyner wiretap and wiretap II), and secret sharing schemes from codes [33].

A new modular construction of capacity-achieving wiretap encryption system. Our main contribution is a new modular construction of a semantically secure wiretap encryption system with efficient encoding and decoding that for a large family of channels achieves the channel secrecy capacity. We call the construction *Hash-then-Encode (**HtE**)* as wiretap encoding amounts to calculating a hash function (from the XOR-UHF), followed by using an ECC. This makes our wiretap encoding operation the most efficient among existing modular constructions of wiretap codes. We prove the semantic security and capacity-achieving properties of our construction by showing that it fits within the framework of [11] and so their approach can be used to prove the required properties. We consider the application of wiretap codes in practice, and define the *effective rate* of the codes as the total transmission, including the seed, divided by the message length. The first (and the only) other construction of capacity-achieving wiretap code with semantic security, called Invert-then-Encode (ItE), is in [11, 138]. We show that for the same level of semantic security and reliability, our construction needs a shorter seed and so has a higher effective rate, compared to the construction in [11, 138]. Our construction is shown in Figure 2.2.

2.1.2 Related works

Wiretap channel is a widely studied area. Wyner's original model [143] considers a *degraded channel* (See (i) of Figure 2.1) where W is the concatenation of T and a second noisy channel W'. Csiszár and Körner [34] extended this model to the broadcast setting (See (ii) of Figure 2.1). The known modular constructions of wiretap codes result in capacity-achieving constructions for Wyner's original model. Hayashi and Matsumoto [66] used invertible UHFs to construct capacity-achieving modular wiretap encryption systems where security is proved for uniformly distributed messages. Bellare et al. [11] introduced the notion of semantic security for wiretap codes and gave the first modular construction that provides semantic security. They also gave a construction [12], referred to as **XtX** whose encoding resembles our construction, but the capacity-achieving

property of the construction was left as an open question. Our work answers this question using a new interpretation of the construction in terms of invertible UHF. Section 2.4.2 provides more details.

2.2 Preliminaries

Probability Distributions. We use uppercase letters X to denote random variables and bold lowercase letters $\mathbf{x}$ to denote their corresponding realization. U_Ω denotes the uniform random variable over Ω. In particular U_ℓ denotes the uniform variable over $\{0,1\}^\ell$. The calligraphic letters $\mathcal{X}$ are used for sets of elements. $|\mathcal{X}|$ denotes the number of elements in a set. By $X \in \mathcal{X}$, we mean random variable's distribution is over $\mathcal{X}$. In particular, $\mathbf{x} \xleftarrow{\$} \mathcal{X}$ means element $\mathbf{x}$ is chosen with probability $\frac{1}{|\mathcal{X}|}$ and $X \xleftarrow{\$} \mathcal{X}$ means X is a variable with uniform distribution over $\mathcal{X}$. $\Pr[X = \mathbf{x}]$ (or $P_X(\mathbf{x})$) denotes the probability of the random variable $X = \mathbf{x}$.

For two random variables X and Y, $P_{X|Y}$ denotes their conditional distribution. For a random variable $X \in \mathcal{X}$ with distribution $P_X(\mathbf{x})$, the Shannon entropy is $H(X) = -\sum_{\mathbf{x}\in\mathcal{X}} P_X(\mathbf{x}) \log P_X(\mathbf{x})$. The *min-entropy* $H_\infty(X)$ is given by $H_\infty(X) = -\log(\max_{\mathbf{x}}(P_X(\mathbf{x})))$. The *average conditional min-entropy* [44] is defined as, $\tilde{H}_\infty(X|Y) = -\log \mathbb{E}_{\mathbf{y}\in\mathcal{Y}} \max_{\mathbf{x}\in\mathcal{X}} P_{X|Y}(\mathbf{x}|\mathbf{y})$. The *statistical distance* of two random variables $X, Y \in \Omega$ is given by, $\mathrm{SD}(X;Y) = \frac{1}{2}\sum_{\omega\in\Omega} |\Pr(X=\omega) - \Pr(Y=\omega)|$. We say X and Y are ε-close if $\mathrm{SD}(X;Y) \le \varepsilon$.

Lemma 2.1. *[108] The ε-smooth min-entropy $H^\varepsilon_\infty(P)$ of a distribution P is defined as:*

$$H^\varepsilon_\infty(P) = \max_{Q:\mathbf{SD}(P;Q)\le\varepsilon} H_\infty(Q).$$

Let $X_1, \ldots, X_n$ be independent samples from a distribution X on a finite set $\mathcal{X}$ and let $\delta > 0$. Then for $\varepsilon = 2^{-\frac{n\delta^2}{2\log^2(|\mathcal{X}|+3)}}$ one has $H^\varepsilon_\infty(X_1, \ldots, X_n) \ge nH(X) - n\delta$.

A *random source* is a random variable with lower-bound on its min-entropy. We say a random variable $X \in \{0,1\}^n$ is an (n,d)-*source* if $H_\infty(X) \ge d$.

Randomness extractors. Randomness extractors extract close to uniform randomness from a random source with some guaranteed entropy. Randomness extractors have found wide applications in cryptography. For more details on randomness extractors see [99].

Definition 2.1. A function $\mathrm{Ext} : \{0,1\}^n \times \mathcal{S} \to \{0,1\}^\ell$ is a strong (seeded) (d,ε) extractor if for any (n,d)-source X we have

$$\mathrm{SD}((S, \mathrm{Ext}(X,S)); (S, U_\ell)) \le \varepsilon,$$

where S is chosen uniformly from $\mathcal{S}$.

Definition 2.2. Let V be a random variable possibly dependent on X, Ext is called a (d, ε) average case strong extractor, if for all (V, X) with $\tilde{H}_\infty(X|V) \geq d$,

$$\mathrm{SD}((S, V, \mathrm{Ext}(X, S)); (S, V, U_\ell)) \leq \varepsilon,$$

where S denotes a random seed chosen uniformly from $\mathcal{S}$.

Randomness extractors can be constructed from *(2-)Universal Hash Families* (UHFs) using the so called *Leftover Hash Lemma* [77].

Definition 2.3. A family $\{h_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ of functions $h_{\mathbf{s}} : \mathcal{X} \to \mathcal{Y}$ is a UHF if for any $\mathbf{x} \neq \mathbf{x}'$,

$$\Pr[h_S(\mathbf{x}) = h_S(\mathbf{x}')] \leq \frac{1}{|\mathcal{Y}|},$$

where S denotes a random seed chosen uniformly from $\mathcal{S}$.

Definition 2.4. A family $\{h_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ of functions $h_{\mathbf{s}} : \mathcal{X} \to \mathcal{Y} = \{0,1\}^\ell$ is an XOR-UHF if for any $\mathbf{x} \neq \mathbf{x}'$,

$$\Pr[h_S(\mathbf{x}) \oplus h_S(\mathbf{x}') = \mathbf{a}] \leq \frac{1}{|\mathcal{Y}|}, \text{ for all } \mathbf{a} \in \{0,1\}^\ell,$$

where S denotes a random seed chosen uniformly from $\mathcal{S}$.

Remark 2.1. *XOR-UHF implies UHF. The UHF family $\mathcal{H}_{mult}$ is defined using finite field multiplication. Let $\mathcal{X} = \{0,1\}^n$, $\mathcal{Y} = \{0,1\}^\ell$ and $\mathcal{S} = \{0,1\}^n$. Then $\mathcal{H}_{mult} = \{h_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ with $h_{\mathbf{s}} : \mathcal{X} \to \mathcal{Y}$ defined as follows is an XOR-UHF.*

$$h_{\mathbf{s}}(\mathbf{x}) = (\mathbf{s} \odot \mathbf{x})|_\ell, \tag{2.1}$$

where $\odot$ is the finite field multiplication and $|_\ell$ is the ℓ lower order (index) components of the vector representation of a finite field element.

The following average-case version of LHL is due to [44].

Lemma 2.2. *Let $\{h_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ be a UHF with $h_{\mathbf{s}} : \{0,1\}^n \to \{0,1\}^\ell$. Let X and Z be random variables over $\{0,1\}^n$ and $\{0,1\}^*$, respectively satisfying $\tilde{H}(X|Z) \geq \ell + 2\log\frac{1}{\varepsilon} - 2$. Let S be uniform over $\mathcal{S}$. Then*

$$SD((S, Z, h_S(\mathbf{x})); (S, Z, U_\ell)) \leq \varepsilon.$$

This, according to Definition 2.2, says that UHF is an average-case $(\ell + 2\log\frac{1}{\varepsilon} - 2, \varepsilon)$ strong extractor.

Modular constructions of wiretap encryption systems use *invertible extractors*, first used in the construction of wiretap II codes [28].

Definition 2.5. [28] Let Σ be a finite alphabet and consider the mapping $f : \Sigma^n \to \Sigma^\ell$. A function $f^{\text{Inv}} : \Sigma^\ell \times \{0,1\}^r \to \Sigma^n$ is called *an inverter for* f if the following conditions hold:

1. (Inversion) Given $\mathbf{y} \in \Sigma^\ell$ such that the pre-image set $f^{Inv}(\mathbf{y})$ is nonempty, for every $\mathbf{r} \in \{0,1\}^r$ we have $f(f^{\text{Inv}}(\mathbf{y}, \mathbf{r})) = \mathbf{y}$.
2. (Uniformity) $f^{\text{Inv}}(U_{\Sigma^\ell}, U_r) = U_{\Sigma^n}$.

An inverter is called *efficient* if there is a randomized algorithm that runs in worst case polynomial time and, given $\mathbf{y} \in \Sigma^\ell$ and the randomness $\mathbf{r}$, computes $f^{\text{Inv}}(\mathbf{y}, \mathbf{r})$. A mapping is *invertible* if it has an efficient inverter.

A family of functions is invertible if all its members is invertible.

In [11], invertibility is defined for *regular* extractors. A seeded extractor is regular if for every seed $\mathbf{s}$, every point in the range of $\text{Ext}(\cdot, \mathbf{s})$ has the same number of pre-images. An inverter of a regular extractor takes a seed $\mathbf{s}$ and a point $\mathbf{y}$ in the range of $\text{Ext}(\cdot, \mathbf{s})$ as input, and returns a uniformly selected element of the pre-image set of $\mathbf{y}$ under that seed. The two definitions of invertibility become the same when each map f in Definition 2.5 is surjective. This is the case for our construction.

Definition 2.6 (Seeded Randomized Encryption $E^{[S]}$)**.** Let $\{E^{[\mathbf{s}]} | \mathbf{s} \in \mathcal{S}\}$ be a family of randomized encoders with $E^{[\mathbf{s}]} : \mathcal{M} \times \{0,1\}^r \to \mathcal{X}$. A seeded randomized encryption $E^{[S]}$ is a probabilistic encryption algorithm that uniformly samples a seed $\mathbf{s} \xleftarrow{\$} \mathcal{S}$ and encrypts using the function $E^{[\mathbf{s}]}$. For each $E^{[\mathbf{s}]}$ there exists a decoder $D^{[\mathbf{s}]}$ such that $D^{[\mathbf{s}]}(E^{[\mathbf{s}]}(\mathbf{m})) = \mathbf{m}$, for any $\mathbf{m} \in \mathcal{M}$.

Modular constructions of wiretap encryption consist of a seeded randomized encryption step and an ECC step.

2.3 A modular construction of efficiently invertible UHFs (ei-UHF)

Let $\mathcal{H} = \{h_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ be a family of (possibly non-invertible) XOR-universal hash functions. We propose a modular construction for an invertible UHF, $\mathcal{G}$, called ei-UHF, that expands the domain of $\mathcal{H}$ while keeping the range the same. The important property of the construction is that inversion of ei-UHF has almost the same computational cost as (forward) hashing in $\mathcal{H}$.

Lemma 2.3 (ei-UHF)**.** *Let $\mathcal{H} = \{h_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ be a family of XOR-universal hash functions $h_{\mathbf{s}} : \mathcal{X} \to \mathcal{Y}$. Define $g_{\mathbf{s}} : \mathcal{X} \times \mathcal{Y} \to \mathcal{Y}$ as follows.*

$$g_{\mathbf{s}}(\mathbf{x}, \mathbf{y}) = h_{\mathbf{s}}(\mathbf{x}) \oplus \mathbf{y}. \tag{2.2}$$

The set $\mathcal{G} = \{g_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ is a family of universal hash functions.

Moreover, for $\mathbf{y} \in \mathcal{Y}$, and any $\mathbf{r} \in \mathcal{X}$ define,

$$g_{\mathbf{s}}^{Inv}(\mathbf{y}, \mathbf{r}) = (\mathbf{r}, h_{\mathbf{s}}(\mathbf{r}) \oplus \mathbf{y}). \tag{2.2'}$$

Then $\{g_{\mathbf{s}}^{Inv} | \mathbf{s} \in \mathcal{S}\}$ is the set of inverter functions for $\mathcal{G}$. The computation cost of inversion of ei-UHF is equal to the forward hashing of XOR-UHF together with an XOR.

Proof. For any $(\mathbf{r}, \mathbf{y}) \neq (\mathbf{r}', \mathbf{y}')$, we first show that,

$$\Pr[g_S(\mathbf{r}, \mathbf{y}) = g_S(\mathbf{r}', \mathbf{y}')] \leq \frac{1}{|\mathcal{Y}|}.$$

According to (2.2),

$$g_S(\mathbf{r}, \mathbf{y}) = g_S(\mathbf{r}', \mathbf{y}') \Leftrightarrow h_S(\mathbf{r}) \oplus h_S(\mathbf{r}') = \mathbf{y} \oplus \mathbf{y}'.$$

If $\mathbf{r} \neq \mathbf{r}'$, from the XOR-Universality of $\mathcal{H} = \{h_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ we have

$$\Pr[h_S(\mathbf{r}) \oplus h_S(\mathbf{r}') = \mathbf{y} \oplus \mathbf{y}'] \leq \frac{1}{|\mathcal{Y}|}.$$

If $\mathbf{r} = \mathbf{r}'$, by the assumption $(\mathbf{r}, \mathbf{y}) \neq (\mathbf{r}', \mathbf{y}')$, we have $\mathbf{y} \neq \mathbf{y}'$. This implies

$$\Pr[h_S(\mathbf{r}) \oplus h_S(\mathbf{r}') = \mathbf{y} \oplus \mathbf{y}'] = 0,$$

which concludes the first part of the proof.

To verify that $g_{\mathbf{s}}^{\mathrm{Inv}}$ is an inverter of $g_{\mathbf{s}}$, we first verify inversion:

$$g_{\mathbf{s}}(\mathbf{r}, h_{\mathbf{s}}(\mathbf{r}) \oplus \mathbf{y}) = h_{\mathbf{s}}(\mathbf{r}) \oplus (h_{\mathbf{s}}(\mathbf{r}) \oplus \mathbf{y}) = \mathbf{y}, \text{ for any } \mathbf{r} \in \mathcal{X}.$$

To show uniformity, by (2.2'), for every $\mathbf{r}$ there is a pre-image. If $\mathbf{r}$ is sampled uniformly from $\mathcal{X}$, then $g_{\mathbf{s}}^{\mathrm{Inv}}(U_{\mathcal{Y}} \times U_{\mathcal{X}}) = U_{\mathcal{X} \times \mathcal{Y}}$.

For efficiency, we note that computing $g_{\mathbf{s}}^{\mathrm{Inv}}$ consists of computing $h_{\mathbf{s}}$ and XOR, which are both efficient operations. □

ei-UHF is *regular* because for each $\mathbf{y}$ the size of the pre-image set is $|\mathcal{X}|$. We use an instance of ei-UHF where the XOR hashing is based on $\mathcal{H}_{mult}$. The original $\mathcal{H}_{mult}$ uses the same set for domain and seed. The lemma below shows a modification of $\mathcal{H}_{mult}$ that removes this restriction.

Lemma 2.4. *Let $\mathcal{X} = \{0,1\}^r$ and $\mathcal{Y} = \{0,1\}^b$. Let $\mathcal{S} = \{0,1\}^r$ if $r \geq b$ and $\mathcal{S} = \{0,1\}^b$, otherwise. Let $h_{\mathbf{s}} : \mathcal{X} \to \mathcal{Y}$ be defined as follows.*

$$h_{\mathbf{s}}(\mathbf{x}) = \begin{cases} (\mathbf{s} \odot \mathbf{x})|_b, & \text{if } r \geq b \\ \mathbf{s} \odot (\mathbf{x}||0^{b-r}), & \text{otherwise,} \end{cases} \tag{2.3}$$

where $\odot$ is the finite field multiplication and $|_b$ denotes the first b bits of the vector representation of a finite field element. Then $\mathcal{G} = \{g_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ with $g_{\mathbf{s}} : \mathcal{X} \times \mathcal{Y} \to \mathcal{Y}$ defined in (2.2) is a family of ei-UHF.

The proof is given in Appendix B.1.

2.4 The HtE (Hash-then-Encode) construction

The ei-UHF construction together with an ECC give a modular construction of wiretap codes (single block *seeded encryption* [11]) from an XOR-UHF and an ECC.

2.4.1 Hash-then-Encode (HtE)

Let $\mathcal{H} = \{h_{\mathbf{s}} | \mathbf{s} \in \mathcal{S}\}$ where $h_{\mathbf{s}} : \{0,1\}^k \to \{0,1\}^b$, be an XOR-UHF satisfying $h_{\mathbf{s}}(0^k) = 0^b$, and ECC be an error correcting code.

HtE construction,*assuming the seed is available at the receiver,* works as follows. To encode a message $\mathbf{m} \in \{0,1\}^b$,

1. Seed selection: $\mathbf{s} \xleftarrow{\$} \mathcal{S}$; seed is available to the decoder.
2. Encoding: $\mathbf{HtE}(\mathbf{k}, \mathbf{s}, \mathbf{m}) = ECC(\mathbf{k} \| h_{\mathbf{s}}(\mathbf{k}) \oplus \mathbf{m})$, where $\mathbf{k} \xleftarrow{\$} \{0,1\}^k$.
3. Decoding: The received block is decoded using the decoder of ECC, and parsed to obtain $(\mathbf{x}, \mathbf{y})$. The message $\mathbf{m} = h_{\mathbf{s}}(\mathbf{x}) \oplus \mathbf{y}$.

In practice, the seed is sent to the receiver reliably using an error correcting code. This reduces the transmission efficiency of the system as the total required transmission for a single message grows. To prove the security of the **HtE** construction and also address the inefficiency of sending the seed, we follow the approach in [11]. In the following, we provide an outline of this approach, and then use it to complete security and efficiency proofs of **HtE** construction.

Invert-then-Encode (ItE) and Repeated ItE (RItE).

In [11], a modular construction of wiretap codes that provides semantic security, the strongest notion of cryptographic security for encryption systems, is proposed. The construction is a seeded encryption system and its security and efficiency are proven using two components. The first component is a single block seeded encryption system that assumes the random "seed" is known to the decryption function, and with this assumption proves semantic security of the construction. To remove the assumption of knowing the seed, it can be reliably (using error correction) sent over the channel. The authors show that for long messages, the same seed can be used for the encryption of many message blocks, and so the transmission cost of sending the seed will become negligible for long messages.

The modular construction, called **ItE** (Invert-then-Encode), uses two building blocks: an invertible extractor and an ECC. For long messages **RItE** (Repeat Invert-then-Encode) construction is used that repeatedly uses **ItE** on consecutive blocks of a message, using the same seed. Semantic security of **RItE** is then reduced to semantic security of **ItE** [11, Lemma 12]. *This proof is general and applicable to any seeded encryption with semantic security.*

Semantic security of **ItE** construction is proved in two steps: in the first step ([11, Lemma 13]), a weaker notion of security known as *random message distinguishing security (RDS)* is proved for the construction. *This result is general and is applicable when the extractor is regular and the adversary's channel is symmetric.* The next step ([11, Lemma 14]) proves that RDS implies semantic security when the seeded encryption satisfies two properties: being *separable* and *message linear*.

Security and efficiency of HtE.

Using an approach similar to [11], we will use Repeat-Hash-then-Encode, to amortize the seed length over many message blocks. The security reduction of **RHtE** to **HtE** follows from Lemma 2 in [11].

To prove semantic security of **HtE** when the seed is shared, the main observation is that the **HtE** construction can be seen as using the inverter function of ei-UHF construction, to obtain a pre-image for the message $\mathbf{m}$, and then using an ECC. Thus the construction fits the **ItE** framework, and to prove semantic security we must show that $\mathbf{HtE}(\mathbf{k}, \mathbf{s}, \mathbf{m})$ is *separable and message linear*. (We noted that the construction of ei-UHF results in a *regular* invertible extractor.)

Lemma 2.5. $\mathbf{HtE}(\mathbf{k}, \mathbf{s}, \mathbf{m})$ *satisfies the following two properties.*

1. (separable): $\mathbf{HtE}(\mathbf{k}, \mathbf{s}, \mathbf{m}) = \mathbf{HtE}(\mathbf{k}, \mathbf{s}, 0^b) \oplus \mathbf{HtE}(0^k, \mathbf{s}, \mathbf{m})$, for any $\mathbf{k} \in \{0,1\}^k$, $\mathbf{s} \in \mathcal{S}$ and $\mathbf{m} \in \{0,1\}^b$;
2. (message linear): $\mathbf{HtE}(0^k, \mathbf{s}, \mathbf{m}_1 \oplus \mathbf{m}_2) = \mathbf{HtE}(0^k, \mathbf{s}, \mathbf{m}_1) \oplus \mathbf{HtE}(0^k, \mathbf{s}, \mathbf{m}_2)$, for any $\mathbf{s} \in \mathcal{S}$ and $\mathbf{m}_1, \mathbf{m}_2 \in \{0,1\}^b$.

Proof. We show $\mathbf{HtE}(\mathbf{k}, \mathbf{s}, \mathbf{m}) = ECC(\mathbf{k}||h_{\mathbf{s}}(\mathbf{k}) \oplus \mathbf{m})$ satisfies these two properties. Note that ECC is linear and ei-UHF is constructed from an XOR-UHF that satisfies $h_{\mathbf{s}}(0^k) = 0^b$.

1. Separable:

$$\begin{aligned} ECC\left(\mathbf{k}||h_{\mathbf{s}}(\mathbf{k}) \oplus \mathbf{m}\right) &= ECC\left((\mathbf{k}||h_{\mathbf{s}}(\mathbf{k}) \oplus 0^b) \oplus (0^k||0^b \oplus \mathbf{m})\right) \\ &= ECC\left(\mathbf{k}||h_{\mathbf{s}}(\mathbf{k}) \oplus 0^b\right) \oplus ECC\left(0^k||0^b \oplus \mathbf{m}\right) \\ &= ECC\left(\mathbf{k}||h_{\mathbf{s}}(\mathbf{k}) \oplus 0^b\right) \oplus ECC\left(0^k||h_{\mathbf{s}}(0^k) \oplus \mathbf{m}\right), \end{aligned}$$

   where the second equality follows from the linearity of ECC and the last equality from $h_{\mathbf{s}}(0^k) = 0^b$;

2. Message linear:

$$\begin{aligned} ECC\left(0^k||h_{\mathbf{s}}(0^k) \oplus (\mathbf{m}_1 \oplus \mathbf{m}_2)\right) &= ECC\left(0^k||\mathbf{m}_1 \oplus \mathbf{m}_2\right) \\ &= ECC\left(0^k||\mathbf{m}_1\right) \oplus ECC\left(0^k||\mathbf{m}_2\right) \\ &= ECC\left(0^k||h_{\mathbf{s}}(0^k) \oplus \mathbf{m}_1\right) \\ &\quad \oplus ECC\left(0^k||h_{\mathbf{s}}(0^k) \oplus \mathbf{m}_2\right), \end{aligned}$$

   where the first and the last equalities follow from $h_{\mathbf{s}}(0^k) = 0^b$, and the second equality from the linearity of ECC .

□

2.4.2 Achieving the capacity

The RDS advantage $\mathbf{Adv}^{rds}$ of $\mathbf{HtE}$ with respect to a wiretapper's channel $\mathsf{W} : \mathcal{X} \to \mathcal{Z}$ is defined as,

$$\mathbf{Adv}^{rds}(\mathbf{HtE}, \mathsf{W}) = \mathbb{E}[\mathbf{SD}((\mathsf{W}(\mathbf{HtE}(K, S, M)), M)); (\mathsf{W}(\mathbf{HtE}(K, S, M')), M))]$$

where $\mathbb{E}()$ denotes the expectation over all choices of $S \in \mathcal{S}$, and M and M' are two messages that are chosen from the message space, independently and with uniform distribution. Let $ECC(\cdot)$ be an error correcting code from $n = k + b$ to N bits; using [9, Lemma 5.5], $\mathbf{Adv}^{rds}(\mathbf{HtE}; \mathsf{W})$ is bounded as,

$$\mathbf{Adv}^{rds}(\mathbf{HtE}, \mathsf{W}) \leq 2 \cdot 2^{\frac{-n\delta^2}{2\log^2(|\mathcal{Z}|+3)}} + 2^{-\frac{n-N(\log|\mathcal{Z}|-H(\mathsf{W})+\delta)-b+2}{2}}.$$

The right hand side is $2\varepsilon_1 + \varepsilon_2$ where $\varepsilon_1 = 2^{\frac{-n\delta^2}{2\log^2(|\mathcal{Z}|+3)}}$ is from *entropy smoothing Lemma* (Lemma 2.1), and $\varepsilon_2 = 2^{-\frac{n-N(\log|\mathcal{Z}|-H(\mathsf{W})+\delta)-b+2}{2}}$ is from the extractor (Lemma 2.2). The parameter $0 < \delta < 1$ bounds the difference between the smooth min-entropy of multiple independent samples and n times Shannon entropy

of an individual sample (See Lemma 2.1). In the second expression, $H(\mathsf{W}) = H(Z|X = x)$ for any $x \in \mathcal{X}$. Note that since W is a symmetric channel, $H(\mathsf{W})$ is independent of choice of x. Moreover, the symmetry of the channel implies $H(Z|X) = H(Z|X = x) = H(\mathsf{W})$.

As long as $b \leq n - N(\log|\mathcal{Z}| - H(\mathsf{W}) + \delta) + 2$, for any δ chosen as above, one can choose sufficiently large n and N, to achieve arbitrarily small $\mathbf{Adv}^{rds}$. Therefore, the maximum achievable rate is

$$lim_{N\to\infty}\frac{n - N(\log|\mathcal{Z}| - H(\mathsf{W}) + \delta) + 2}{N} = lim_{N\to\infty}[\frac{n}{N} - (\log|\mathcal{Z}| - H(\mathsf{W}))].$$

When both the receiver and the wiretapper's channels are symmetric, and W is degraded with respect to T, the secrecy capacity is given by the difference between Shannon's capacities of the two channels: $C_{\mathsf{T}} - C_{\mathsf{W}}$. The construction achieves the secrecy capacity when i)$\lim_{N\to\infty}\frac{n}{N} = C_{\mathsf{T}}$ and ii) $\log|\mathcal{Z}| - H(\mathsf{W}) = C_{\mathsf{W}}$. The first condition is satisfied by using an error correcting code that achieves the secrecy capacity of T, and the second condition is satisfied if a uniform input to the wiretapper's channel produces a uniform output.

An extension of the **ItE** construction that achieves the secrecy capacity for an arbitrary symmetric wiretapper's channel, including continuous output alphabet channels is proposed in [131]. The extension uses a letter splitting function on the wiretapper's channel output [2] that effectively copies the wiretapper's channel output symbols so that the more probable symbols are repeated more. This creates an almost uniform distribution over the splitting function output symbols. The combination of the splitting function and the wiretapper's channel is equivalent to the original wiretapper's channel. Hence, the letter splitting function indeed creates an equivalent channel with almost uniform output, and application of **ItE** over this channel asymptotically achieves the secrecy capacity. This extension can also be used for the **HtE** construction with similar results, that is the construction achieves the capacity for any symmetric channel.

To obtain concrete parameters and derive the exact expressions for the secrecy capacity, we consider the case that the main channel is noiseless, and W is a BSC_p. In this case, we have $\mathcal{X} = \mathcal{Z} = \{0, 1\}$ and $H(\mathsf{W}) = h_2(p)$, where $h_2(\cdot)$ is the binary entropy function. Now as n grows, ε_1 goes to 0. Moreoever, $\varepsilon_2 = 2^{-\frac{n-n(1-h_2(p)+\delta)-b+2}{2}}$ will also go to 0 as long as we have $h_2(p) - \delta - R > 0$, where $R = \frac{b}{n}$ is the information rate of **HtE** in this special case. As noted earlier, δ can be chosen arbitrarily small, and so we have R approaching $h_2(p)$, which is the secrecy capacity of the wiretap channel.

Comparison of XtX and HtE

Figure 2.3 shows the two constructions eXtract-then-Xor (XtX) [12] and **HtE**. However, a subtle difference between the two constructions results in the latter to be capacity-achieving, while the former is not. The

[2] The paper [131] constructs an optimal letter splitting function using a greedy algorithm.

main reason is that **XtX** does not use all the noise in the adversary's channel and so effectively overprotects the message. To better explain this difference, we first review **XtX**.

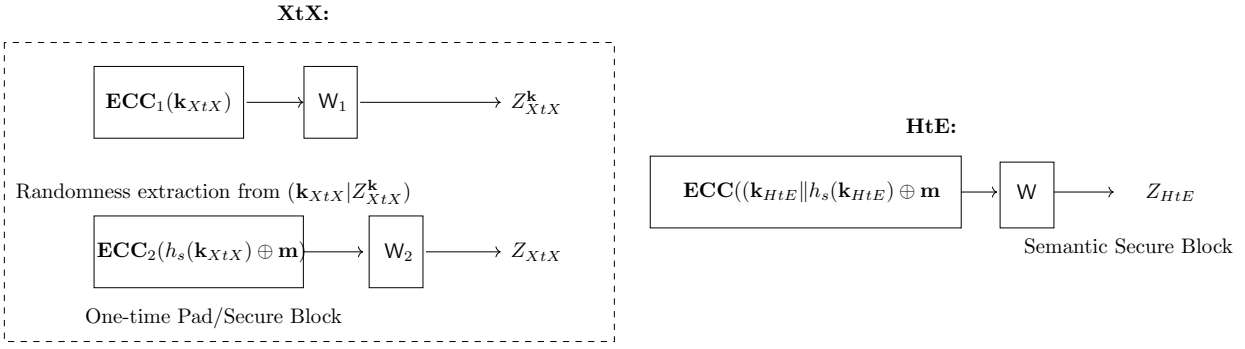

Figure 2.3: The encoded blocks in **XtX** and **HtE**

XtX construction uses a family of hash functions $\mathcal{H} = \{h_{\mathbf{s}}|\mathbf{s} \in \mathcal{S}\}$, together with two capacity-achieving error correcting codes En_1 and En_2 (for the main channel). For a hash function $h_{\mathbf{s}} : \{0,1\}^{k_{XtX}} \to \{0,1\}^b$ in $\mathcal{H}$ the encoder output consists of two blocks, $En_1 : \{0,1\}^{k_{XtX}} \to \{0,1\}^{n_1}$ and $En_2 : \{0,1\}^{b+|\mathcal{S}|} \to \{0,1\}^{n_2}$. The two encoding blocks of **XtX** are defined as ([12], Section 5.2):

$$En_1 = ECC_1(\mathbf{k}_{XtX}),$$

$$En_2 = ECC_2(h_{\mathbf{s}}(\mathbf{k}_{XtX} \oplus \mathbf{m}).$$

Assuming that the receiver's and the wiretapper's channels are *splittable,* the channel is independently applied to the output of En_1 and En_2. Let $\mathsf{W}_1 : \{0,1\}^{n_1} \to \{0,1\}^{d_1}$ and $\mathsf{W}_2 : \{0,1\}^{n_2} \to \{0,1\}^{d_2}$ denote applications of the wiretapper's channel on En_1 and En_2, respectively. The generalized leftover hash lemma [12, Lemma 5.1] is used to extract randomness from $\mathbf{k}_{XtX}$, given the wiretapper's view $Z^{\mathbf{k}}_{XtX}$. Thus $h_{\mathbf{s}}(\mathbf{k}_{XtX})$ results in an (almost) random pad that (almost) perfectly hides the message $\mathbf{m}$. Note that although $\mathbf{k}_{XtX}$ is sent over the channel, because of the noise in adversary's channel W_1, its value will be seen with uncertainty by the adversary, and this uncertainty is extracted in the form of the pad. This shows that the available noise in W_2 does not contribute to security, and the scheme uses only part of the channel noise.

*In **HtE** construction,* the adversary's channel is applied on the whole encoded block. This enables us to use extractable noise (of the channel) on the whole block, for providing security and (asymptotically) achieves the secrecy capacity.

Scheme (encryption step)	Capacity-achieving	Semantic security	Enc/Dec computation	Effective rate
[66]: $\mathrm{Inv}(h_S)(\mathbf{m})$	✓	×	$\mathbb{F}_{2^{b+r}}$ mult.,$F_{2^{b+r}}$ inv.	pre-shared seed
XtX: $R \parallel (h_S(R) \oplus \mathbf{m})$	×	✓	$\mathbb{F}_{2^{b+r}}$ mult.,XOR	$\frac{b}{2(b+r)+b}$
ItE: $\mathrm{Inv}(h_S)(\mathbf{m})$	✓	✓	$\mathbb{F}_{2^{b+r}}$ mult.,$F_{2^{b+r}}$ inv.	$\frac{b}{2(b+r)}$
HtE: $K \parallel (h_S(K) \oplus \mathbf{m})$	✓	✓	$F_{2^{\max\{b,r\}}}$ mult., XOR	$\frac{b}{(b+r)+\max\{b,r\}}$

Table 2.1: Comparing the encryption step of seeded wiretap codes (assume main channel is noise free and the hashing is multiplication in finite field). [66] assume a pre-shared seed and only consider strong secrecy. The length of R in **XtX** [12] is chosen such that $\lim_{n\to\infty} \frac{|\mathbf{m}|}{|R|} = C_s$ and only achieves asymptotic rate $\frac{C_s}{1+C_s} < C_s$. **ItE** and **HtE** are both semantically secure and capacity-achieving with efficient encoding/decoding.

2.4.3 Effective rate for short messages

In application scenarios such as communication between an RFID (Radio Frequency Identification) tag and a reader, a single message must be protected against wiretappers. There are four seeded constructions of wiretap codes, three are capacity-achieving. We define the *effective communication rate* of a seeded encryption with σ bits security by R^σ =(mess. len.)/(enc. block len. + seed len.). Here, σ bit security means that the adversary's advantage is bounded by $2^{-\sigma}$.

Table 2.1 compares these constructions, and clearly shows that **HtE** has the most efficient encoding and decoding computation, and achieves the highest effective rate in finite-length regime.

2.5 Concluding remarks

We proposed a new modular construction of wiretap codes with semantic security that enjoys efficient encoding and decoding, and achieves the capacity for a large class of channels. To prove security, we used the framework of [9] that uses a number of steps. Providing a compact security proof for the construction is an interesting open problem.

Our construction has the interesting property that the computational costs of encoding and decoding are almost the same and is equivalent to the cost of finding a hash value. Thus, with an appropriate choice of the hash function, one could construct a linear-time wiretap code. We will explore this in our future work.

Ackowledgement. This work in part is supported by Natural Sciences and Engineering Research Council of Canada.

Chapter 3

Post-Quantum Security using Channel Noise[1]

Abstract. Post-quantum secure communication has attracted much interest in recent years. Known computationally secure post-quantum key agreement protocols are resource intensive for small devices. These devices may need to securely send frequent short messages, for example to report the measurements of a sensor. Secure communication using physical assumptions provides information-theoretic security (and so is quantum-safe) with small computational overhead. Security and efficiency analysis of these systems however is asymptotic. In this poster, we consider two secure message communication systems, and derive and compare their security and efficiency for finite-length messages. Our results show that these systems indeed provide an attractive alternative for post-quantum security.

3.1 Introduction

Internet of Things (IoT) promises universal connectivity of billions of sensors that will sense our environment and automate many aspects of our lives [140]. In many scenarios, data that is collected by sensors and exchanged among devices are highly sensitive and must be protected over a long period of time. Most of today's cryptographic algorithms and protocols assume a computationally bounded adversary, and for their security rely on the computational difficulty of solving problems such as discrete logarithm (DL) and integer factorization problems. These problems are the basis of the security of Diffie-Hellman Key Exchange (DHKE) protocol, and RSA cryptosystem. Peter Shor [124] proposed efficient (polynomial-time) quantum algorithms for both DL and integer factorization problems that effectively breakdown the cryptographic infrastructure of the Internet, if a quantum-computer is developed. Recent developments in quantum technologies has led to the announcement by security agencies [128] to move to quantum-safe algorithms and this has been

[1]The content of this chapter is published as a poster [121] in proceedings of CCS 2018.

followed by standardization efforts [26] in this domain.

To provide post-quantum security one can use computational assumptions and use problems like Learning With Error (LWE) [103], for which no quantum algorithm is known, and use secure key agreement protocols that are based on these assumptions. Many such protocols including the ones in [4] and [20] are not suitable for resource constrained devices that are common in IoT systems. For example, according to [20], establishing a key with 144 bits of classical security and 130 bits of quantum security roughly requires 22.5 Kbytes of communication using Frodo (an LWE-based key exchange) protocol, while a practical RSA key agreement protocol with 128 bits of claimed classical security and no quantum security requires almost 0.7 Kbytes of communication.

An alternative approach to providing post-quantum private communication is by using physical layer assumptions. Physical layer security adds a layer of security to communication that is afforded by small devices and can be complemented by extra layers of security using traditional cryptographic systems [97]. Using physical layer assumptions for securing communication dates back to Wyner's pioneering work [143] on providing communication secrecy using the channel noise. Wyner's innovation was to treat the noise in the environment as a resource for cryptography. *Wyner wiretap model* is extended by Csiszár and Körner [34] to a broadcast channel model. In this model, the sender is connected to the receiver and the eavesdropper (wiretapper) through two noisy channels, referred to as the receiver's channel, T, (also called the main channel) and the wiretapper's channel, W, respectively. The works in [34, 143] proved that in this model, secure communication with asymptotic perfect secrecy and reliability is possible without using any secret key, as long as the wiretapper's channel is "noisier" than the main channel. Wiretap model can be realized by wireless communication systems in which an eavesdropper at a relatively far distance from the broadcast station receives a weaker form of the broadcast message compared to the legitimate closer receivers. The model is attractive to the research community as well as system developers who are interested in lightweight but strong cryptographic solutions because it promises information-theoretic security with long-term security guarantee without the need for a shared secret key.

The design of a wiretap protocol requires correct estimation of the noise over communication channels that may be challenging. In an IoT setting, however, since many sensors sense the environment, building a model of the environment and noise in the communication channel can be robustly done. Wiretap codes are traditionally analyzed in the asymptotic regime. While this analysis is essential to gain confidence about security, for real-world applications, one needs to estimate concrete performance parameters of the codes in the finite-length regime. To compare the efficiency of wiretap codes in practice, the rate of secure communication for finite-length messages must be found. Finite-length comparison of wiretap codes, in addition to estimating the decoding error of the receiver (reliability error), must also consider the secrecy

level that is offered by the code for the finite-length messages. This is a challenging problem that has found significant attention in recent years [102]. In this poster, we outline an approach for evaluating the security of modular wiretap codes and use it to compare two constructions.

3.2 Approach

A capacity-achieving wiretap code is an encoding scheme for a wiretap channel that achieves the highest theoretically possible rate of secure message transmission (number of securely transmitted message bits per channel use). Explicit constructions of wiretap codes can be divided into those that are based on a specific error correcting code [87, 136], and constructions that separate *coding for security* (or *secure coding*), from *coding for reliability* (for the main channel), and so are not restricted to a specific error correcting code (ECC). The latter constructions are called *modular* that are attractive from a practical viewpoint due to their flexibility in the choice of error correcting codes. These constructions are *seeded encryption systems* and require a random seed to be shared by a transmitter and a receiver. The seed can be sent by the sender to the receiver over the main channel using an error correcting code to provide reliability. The seed length does not affect the asymptotic efficiency of the system because it can be reused for encrypting multiple blocks. The only two constructions that provide semantic security are in [120] and [11]. We will focus on these constructions.

In this work, we first propose a framework for comparing the efficiency of modular constructions by defining the finite-length rate (FLR), and then compare the FLR for the two modular constructions called *Hash-then-Encode (**HtE**)* [120]- and *Invert-then-Encode (**ItE**)* [11].

Finite-length Efficiency. In [120], the *effective communication rate* of a seeded wiretap code is introduced that takes into account the length of the seed. This rate will be used to define and subsequently compare the finite-length rate (FLR) of the security coding components of the two known seeded wiretap constructions i.e., **HtE** and **ItE**.

Definition 3.1. The *effective communication rate* of a seeded encryption system, taking into account the transmission cost of the seed, is $R = \dfrac{\text{message length}}{\text{encryption block length + seed length}}$.

For finite-length messages, security and reliability losses will be non-zero values and must be estimated for a given message length and wiretapper's channel. This analysis in general is complex and will require finite-length analysis of the specific ECC that is used for correcting errors in the receiver's channel, or obtaining general bounds on the decoding error for a finite-length ECC [102]. The following definition of FLR considers the security and reliability of the finite-length wiretap codes.

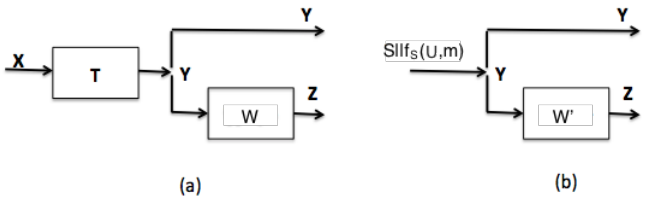

Figure 3.1: (a) Degraded wiretap channel; (b) Using $IdECC()$ to remove noise from the receiver's channel.

Definition 3.2. For a wiretap channel $\mathsf{W}(\cdot)$ and a single message block $\mathbf{m}$ of length b, a wiretap code with encoder $\mathsf{WtEnc}(\cdot)$ has the finite-length rate (ϵ, δ)-$FLR^{[b]}(\epsilon, \delta)$, if

1. For any $\mathbf{m}_0$ and $\mathbf{m}_1$,
$$\mathrm{SD}[\mathsf{W}(\mathsf{WtEnc}(\mathbf{m}_0)); \mathsf{W}(\mathsf{WtEnc}(\mathbf{m}_1))] \leq \varepsilon.$$

2. For any message $\mathbf{m}_A$ sent by Alice, the corresponding message $\mathbf{m}_B$ received by Bob will satisfy
$$\max_{\mathbf{m}_A \in \{0,1\}^b} \Pr[\mathbf{m}_A \neq \mathbf{m}_B] \leq \delta.$$

3. For any message $\mathbf{m}$, the encoding rate satisfies
$$\frac{b}{|\mathsf{WtEnc}(\mathbf{m})|} \geq FLR^{[b]}(\epsilon, \delta).$$

In seeded encryption systems, the ciphertext of a message $\mathbf{m}$ is $ECC_{\mathsf{T}}(S||f_S(U, \mathbf{m}))$, where ECC_{T} is a capacity-achieving (for channel T) error correcting code, and $f_S(U, \mathbf{m})$ is the secrecy coded block, where U is the randomness of encoding. For these codes, the *effective* (ϵ, δ)-FLR (item 3 in definition above) will be replaced by,
$$\frac{b}{|S| + |ECC_{\mathsf{T}}(S||f_S(U, \mathbf{m}))|} \geq FLR^{[b]}(\epsilon, \delta). \tag{3.1}$$

In modular constructions, an error correcting code is used to provide reliability for the receiver's channel. This code slightly affects parameters of the secrecy coding part of the construction, which makes the finite-length analysis of the wiretap encryption dependent on the choice of the error correcting code. To avoid this dependency, and focus on the secrecy coding part, we introduce an *ideal error correcting code for a degraded wiretap channel*.

An ideal error correcting code, denoted by $IdECC(\mathsf{W})$, for a degraded wiretap channel $(\mathsf{W} = \mathsf{W}' \circ \mathsf{T})$, is an error correcting code with an pair of encoder and decoder, $(IdEnc, IdDec)$, satisfying the following properties: for a message $\mathbf{x}$ of any length,

(i) $IdDec(\mathsf{T}(IdEnc(\mathbf{x}))) = \mathbf{x}$, and (ii) $IdDec(\mathsf{W}(IdEnc(\mathbf{x}))) = \mathsf{W}'(\mathbf{x})$, and (iii) the rate of the code is fixed for all message lengths.

In other words, the ideal encoder (i) allows perfectly reliable transmission over the receiver's channel T for any message, and (ii) it partially removes noise from the wiretapper's channel resulting in the wiretapper's channel $\mathsf{W}'(\mathbf{x})$ for Eve, and allowing Eve's view Z to have (possibly stronger) correlation with the message, and (iii) the required redundancy of the error correction is proportional to the message length. Figure 3.1 illustrates the effect of an ideal ECC on a degraded wiretap channel. Figure 3.1(a) is a degraded wiretap channel with $\mathbf{x} = IdECC(s||f_s(\mathbf{m}))$, and Figure 3.1(b) shows the effect of the $IdECC()$ on the secrecy coded block.

Because of the constant rate of the code for all message lengths, for comparing the performance of wiretap codes over the wiretap channel $(\mathsf{T} = BSC_{p_1}, \mathsf{W} = BSC_{p_2})$, one only needs to compare its performance over the wiretap channel $(\mathsf{T} = BSC_0, \mathsf{W}' = BSC_p)$.

3.3 Results

To obtain the effective rate $FLR^{[b]}(\epsilon)$ of a construction, we need to derive the encryption block length for a given message length b, at the secrecy level $\epsilon = 2^{-\sigma}$, in the noiseless main channel setting. For **ItE**, we will use an expression in [131] (Expression (7)) that relates these parameters. For the **HtE** construction, the expression (3.1) in Theorem 3.1 gives the required relation.

Theorem 3.1. *The **HtE** construction provides semantic security for a wiretap channel (with symmetric main and wiretapper's channels), and when the wiretapper's channel is BSC_p, for semantic security level σ, the length of the randomness k satisfies the following inequality,*

$$2\sigma \leq (k+b)h_2(p) \cdot \log 5(\sqrt{2k(\sigma+3)} + \sqrt{2b(\sigma+3)}) - b - 7, \tag{3.2}$$

where $h_2(p)$ is the binary entropy function, that is $h_2(p) = -p\log p - (1-p)\log(1-p)$.

The proof is given in Appendix B.2.

To obtain the seed length that is required for the encoder, the extractor should be specified. For **ItE**, the hash function family $\mathcal{H}_{mult} : \{0,1\}^{r+b} \times \{0,1\}^{r+b} \to \{0,1\}^b$ is used which, on seed $S \in \{0,1\}^{r+b} \backslash 0^{b+r}$ and input $X \in \{0,1\}^{b+r}$, outputs the first b bits of $X \odot S$. Here, $\odot$ is multiplication over $GF(2^{b+r})$. For **HtE**, a variation of this extractor is used in [120, Lemma 4] that for inputs $X_1 \in \{0,1\}^b$ and $X_2 \in \{0,1\}^k$ the seed length is $\max(b,k)$. We use these two instantiations to calculate and compare the effective rates of the **HtE** and **ItE** constructions.

Figures 3.2 and 3.3 graph the FLR of the constructions, as a function of message length, for secrecy levels $\sigma = 32$ and $\sigma = 64$ bits, respectively. We consider a single block encryption. Comparing the constructions for a fixed wiretapper's channel (fixed p in BSC_p) shows that for small p and very small message block lengths, **ItE** slightly outperforms **HtE**. However, for larger message lengths and/or noisier wiretapper's channel, when $p \geq 0.15$ and $b \geq 5000$, $FLR^{[b]}(\epsilon)$ for **HtE** is always higher than for **ItE**.

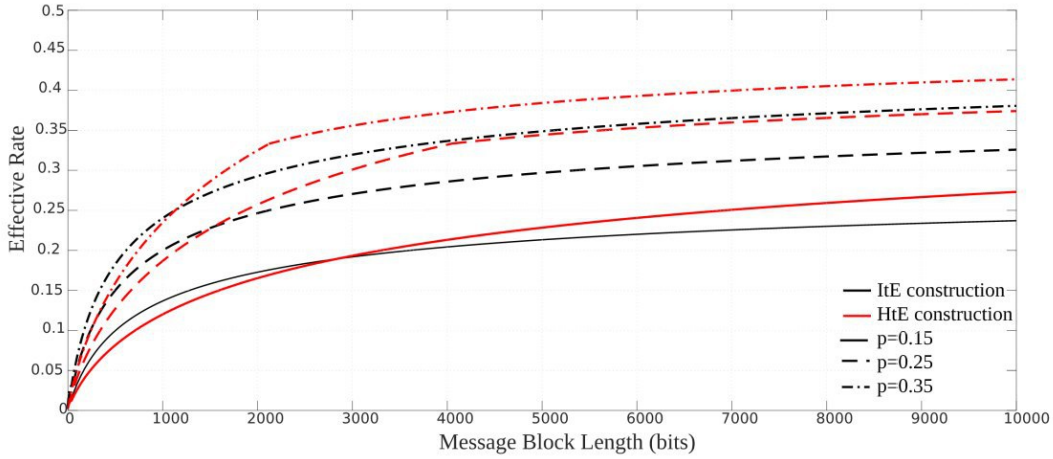

Figure 3.2: The effective rate of **ItE** and **HtE** over a BSC_p with $\sigma = 32$ bits. Flipping probabilities are $p = 0.15, 0.25, 0.35$.

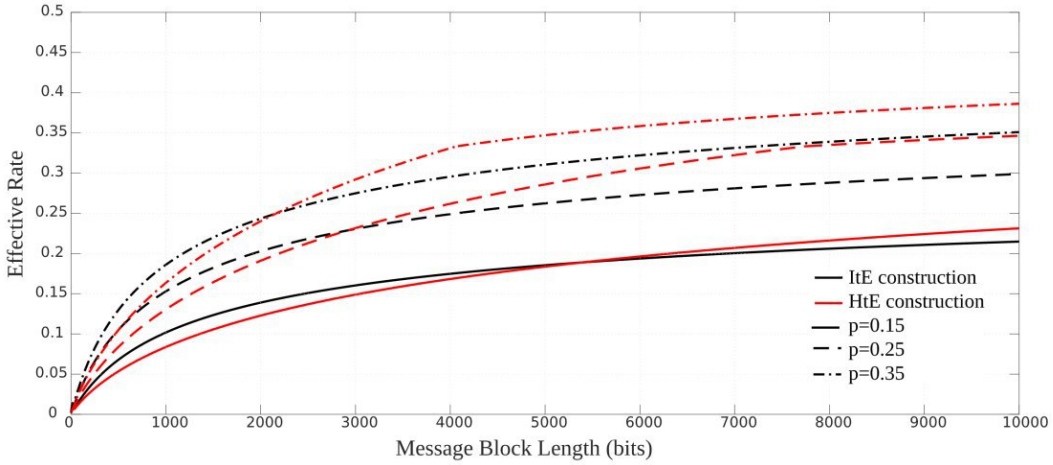

Figure 3.3: The effective rate of **ItE** and **HtE** over a BSC_p with $\sigma = 64$ bits. Flipping probabilities are $p = 0.15, 0.25, 0.35$.

The break in the graphs associated with **HtE** is because the seed length is given by $\max\{b, k\}$, and for each noise level, as the message length increases, there is a value of b for which $s = \max\{b, k\} = b$. When $k = b$, we have $FLR^{[b]}(\epsilon) = \frac{1}{3}$. Both figures show that for message lengths bigger than this value of b, $FLR^{[b]}(\epsilon)$ of **HtE** is higher than the corresponding value of **ItE**.

σ(bits) \ b (bits)	$0.5Kbit$	$1Kbit$	$4Kbit$
32	$78Kbit$	$91Kbit$	$155Kbit$
64	$136Kbit$	$151Kbit$	$223Kbit$

Table 3.1: Length of the secure message block with **HtE**

A typical message length in an IoT setting to provide an acceptable level of reliability is $0.5K$ to $4K$ bits. The noise level can be estimated with the BER (Bit Error Rate) of the system, which is typically less than 10^{-2} [95]. Table 3.1 shows the required communication for transmitting a single message of lengths $0.5K, 1K$ and $4K$ bits, security levels $\sigma = 32$ bits and 64 bits, and $p = 10^{-2}$, using **HtE**.

3.4 Conclusion

Modular wiretap coding provides long-term security with efficient computation and communication, and therefore is an attractive solution for post-quantum communication security in an IoT setting. This approach can be viewed as complementing and enhancing end-to-end communication security of the system.

We compared the finite-length rate of two modular coding schemes (**HtE** and **ItE**) that provide semantic security. Both these schemes have computationally efficient encoding and decoding algorithms. Our results show that in most cases **HtE** has a higher finite-length rate than **ItE**. We derived the length of the encrypted secure block for typical IoT message blocks.

Chapter 4

A Virtual Wiretap Channel for Secure Message Transmission[1]

Abstract. In Wyner wiretap channel, a sender is connected to a receiver and an eavesdropper through two noisy channels. It has been shown that if the noise in the eavesdropper's channel is higher than the receiver's channel, information-theoretically secure communication from Alice to Bob, without requiring a shared key, is possible. The approach is particularly attractive noting the rise of quantum computers and possibility of the complete collapse of today's cryptographic infrastructure. If the eavesdropper's channel is noise-free, however, no secrecy can be obtained.

The iJam protocol, proposed by Gollakota and Katabi [59], is an interactive protocol over noise-free channels that uses friendly jamming by the receiver to establish a secure shared key between the sender and the receiver. The protocol uses properties of OFDM (Orthogonal Frequency-Division Multiplexing) to create uncertainty for Eve (hence noisy view) in receiving the sent information, and uses this uncertainty to construct a secure key agreement protocol. The protocol has been implemented and evaluated using extensive experiments that examines the best eavesdropper's reception strategy.

In this chapter, we develop an abstract model for BiT (Basic iJam Transmission) protocol as a *wiretap channel* and refer to it as a *virtual wiretap channel*. We estimate parameters of this virtual wiretap channel, derive the secrecy capacity of this channel, and design a secure message transmission protocol with provable semantic security using the channel. Our analysis and protocol gives a physical layer security protocol, with provable security that is implementable in practice (BiT protocol has already been implemented).

[1]The content of this chapter is published as a paper [119] in proceedings of MyCrypt 2016.

4.1 Introduction

Wireless communication provides flexible communication for mobile users, and with the increasing number of sensors and growth of IoT (Internet of Things) systems, will soon become the dominant form of communication. Wireless communication is vulnerable to passive eavesdropping. Wired Equivalent Privacy (WEP) is a security algorithm that was introduced to provide security for wireless access points, and was later replaced by Wi-Fi Protected Access (WPA) protocol [112]. Other communication security protocols such as Secure Socket Layer (SSL) [52] and Secure Shell (SSH) [146] are used for providing secure services over networks. All these protocols rely on public-key infrastructure to establish a secure shared key between the sender and the receiver. Shor [124] proposed a quantum algorithm that efficiently solves the discrete logarithm and integer factorization problems, rendering today's public-key infrastructure completely insecure if a quantum computer is invented. With advances in quantum technologies and projection of 10 years [39] to the development of such computers, the interest in the development of quantum-resistant cryptographic systems is rapidly growing.

In this chapter, we consider information-theoretically secure communication systems that are secure against an adversary with unlimited computational power. Information-theoretic security against a passive eavesdropper can be achieved using one-time-pad. This assumes sender and receiver share a secret key that is uniformly random and is of the same length as the message. The key must be chosen afresh for every message. These requirements severely limit the application of one-time-pad in practice. Wyner [143] proposed an ingenious model for information-theoretically secure communication that is particularly suited for securing wireless communication. In Wyner wiretap model, a sender Alice is connected to a receiver Bob over a *main channel*. The eavesdropper, called Eve, receives the communication from the sender through a second channel referred to as the *wiretapper's channel*. Wyner proved that as long as the wiretapper's channel is a degraded version of the main channel (or more generally noisier than the main channel), there exists an encoding method that provides information-theoretic security for the receiver against Eve. A *wiretap code* is a randomized code that is used by the sender to encode the message. Wiretap channel allows achieving quantum-resistant security using physical layer properties of the communication channels and complements the security that is provided at the higher layers of the protocol stack by using traditional cryptographic protocols. The security definition of wiretap channels has been strengthened over time with the latest security notion being semantic security: the strongest security notion for message confidentiality. Wiretap channels, however, rely on noise in the channel and need a correct estimate of the noise level in the wiretapper's channel.

In [59], an innovative interactive physical layer protocol for key establishment over a *noiseless channel*

with security against a passive eavesdropper was introduced. The protocol was implemented and shown to provide security in practice, by measuring the received signal at Eve, and using the best decoding strategies to recover the sent information at Eve. The protocol uses cooperative jamming where the receiver sends a jamming signal that is combined with the sender's signal at Eve and creates an uncertain view of the communication for Eve, and uses that for providing security. One can view the approach as the sender and the receiver cooperatively creating a *virtual wiretap channel* and use that to establish a shared key.

In this chapter, we follow this intuition and model the main building block of iJam, referred to as *Basic iJam Transmission (BiT) protocol*, as a virtual wiretap channel, and use it to provide efficient quantum-resistant secure message transmission with provable security.

4.1.1 Our work

The BiT protocol uses a coordinated jamming signal of the receiver to construct a noisy view of transmission for Eve. This is achieved by the sender repeating its transmitted information block in two consecutive time subintervals, and the receiver randomly jamming one of the time samples of the two subintervals. Coordinated jamming ensures that the receiver is able to perfectly receive the time samples that allow them to reconstruct a complete copy of the sent information block, while Eve will have a combination of jammed and unjammed samples, which results in an uncertain view. This is shown to be achievable using appropriate choices of modulation and transmission technique (OFDM and 2^q-QAM modulation - See Section 4.2.1 for description).

We analyze BiT and show how it can be modelled as a virtual wiretap channel. Since the receiver is able to perfectly recover the transmitted information block, the corresponding virtual wiretap channel has a noiseless main channel. We estimate the parameters of this channel and use them to compute the secrecy capacity of the virtual wiretap channel that gives the best asymptotic efficiency for message transmission over this channel.

The modelling also allows us to adapt existing constructions of wiretap codes for providing message secrecy. We show how to use the wiretap encoding (seeded encryption) scheme of [11] to encode messages and then transmit the codeword using information block coding of the BiT protocol. The BiT protocol creation of a virtual wiretap channel ensures the seeded encryption will result in message transmission with information-theoretic semantic security. The protocol achieves optimal efficiency asymptotically. The system thus provides provable quantum-resistant security, and is implementable in practice (thanks to starting from an already implemented protocol).

In Section 4.6, we show how this interpretation of BiT (a mechanism to add uncertainty to Eve's view)

can be used to extend the application of physical layer security protocols that use the wiretap model. In particular, we consider a setting where transmission in the physical channel from the sender to the receiver is corrupted by Additive White Gaussian Noise (AWGN), but Eve has a noise-free channel. Using the known results for wiretap channels, secure communication using wiretap codes in this setting is impossible. Using BiT protocol in this setting however, introduces uncertainty in Eve's view and so can enable secure communication. Figure 4.3 shows how to effectively use the BiT protocol to create a virtual wiretap channel when both the main channel and the wiretapper's channel are noisy. The noise in the main channel is the physical noise, while the noise in the wiretapper's channel is the result of the BiT protocol. Alice can send secret messages to Bob as long as the virtual wiretap channel is a stochastically degraded broadcast channel.

4.1.2 Related works

Wiretap channel model was proposed by Wyner [143]. The model has attracted the attention of theoreticians and practitioners, resulting in a large body of work on the topic. A number of generalizations of the model has been proposed [34, 84, 85], and the notion of security has been strengthened [11, 98] over years, bringing it on par with the strongest notion of security in cryptography. It has been proved that secure communication is possible if the eavesdropper's channel (signal reception ability) is worse than the receiver's [34]. There are efficient constructions of wiretap codes [11, 87, 136], with the more recent ones using a modular approach that can be used with any error correcting code.

Some of physical layer security protocols are constructed by injecting a jamming signal in the eavesdropper's view [81, 86, 132]. It has been shown that cooperative jamming can increase the secrecy capacity [133–135]. In a general cooperative jamming setting, a trusted *helper* jams the transmitted signal. The legitimate receiver has some information about the jamming signal, which is their advantage over the eavesdropper who is entirely oblivious to the jamming signal. This results in an inferior channel for the eavesdropper and so allows secure communication in presence of the eavesdropper. This type of jamming has also been referred to as "helping" [144], or "friendly" [62] jamming. BiT protocol uses a variation of friendly jamming in which the receiver plays the role of the trusted helper.

The BiT protocol [59] was used to construct a secret key agreement protocol (called iJam). The iJam key agreement uses multiple invocations of the BiT protocol to establish a secret key that is generated as the XOR of multiple random strings, each transmitted in one invocation of BiT. The security of iJam has been experimentally evaluated.

Organization. Section 4.2 gives the background and an outline of the BiT protocol. Section 4.3 is an example that motivates our approach, for modeling BiT as a virtual wiretap channel. In Section 4.4, we

give our model of BiT as a virtual wiretap channel when the transmission from the sender to the receiver is noise-free. Section 4.5 introduces a physical layer protocol for message transmission using a known seeded encryption algorithm and the BiT protocol. In Section 4.6, we study the case that the transmission from the sender to the receiver is corrupted by AWGN. Conclusion and future works are given in Section 4.7. In Appendix B.3.1, we provide approximation data and graphs of the information rate for the message transmission protocol in Section 4.5. In Appendix B.3.2, we provide an example of the noisy virtual main channel and virtual wiretapper's channel of Section 4.6.

4.2 Preliminaries and notations

We use uppercase letters X to denote random variables and bold lowercase letters to denote their corresponding realization. By $\Pr[X = \mathbf{x}]$, we mean the probability that X takes the value $\mathbf{x}$. This is also shown as $P_X(\mathbf{x})$. Calligraphic letters $\mathcal{X}$ denote sets, and $|\mathcal{X}|$ denotes the cardinality (number of elements) of a set. For two random variables X and Y, P_{XY} denotes their joint distribution, $P_{X|Y}$ denotes their conditional distribution, and P_X denotes X's marginal distribution. All *log*s are in base 2 and $\|$ is used to denote concatenation of two binary strings. For a random variable $X \in \mathcal{X}$, Shannon entropy is given by $H(X) = -\sum_{\mathbf{x}\in\mathcal{X}} P_X(\mathbf{x}) \log P_X(\mathbf{x})$. For two random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ with joint probability distribution $P_{XY}(\mathbf{x}, \mathbf{y})$ and conditional probability distribution $P_{X|Y}(\mathbf{x}|\mathbf{y})$, the *conditional entropy* $H(X|Y)$ is defined as:

$$H(X|Y) \quad = -\sum_{\mathbf{x}\in\mathcal{X}} \sum_{\mathbf{y}\in\mathcal{Y}} P_{XY}(\mathbf{x}, \mathbf{y}) \log P_{X|Y}(\mathbf{x}|\mathbf{y}),$$

and the *mutual information* between the two is given by $I(X;Y) = H(X) - H(X|Y)$. The min-entropy of a random variable $X \in \mathcal{X}$, denoted by $H_\infty(X)$, is given by $H_\infty(X) = -\log(\max_{\mathbf{x}}(P_X(\mathbf{x})))$. The *statistical distance* between two random variables $X, Y \in \mathcal{X}$ is defined by

$$\mathrm{SD}(X, Y) \triangleq \frac{1}{2} \sum_{\mathbf{x}\in\mathcal{X}} |Pr(X = \mathbf{x}) - Pr(Y = \mathbf{x})|.$$

A communication channel is modelled as a probabilistic function that maps an input alphabet $\mathcal{X}$ to an output alphabet $\mathcal{Y}$. The channel $\mathsf{W}(X) = Y$ takes input $X \in \mathcal{X}$, and outputs $Y \in \mathcal{Y}$. The probability distribution of Y depends on the distributions of X and the probabilistic function $W(\cdot)$. In many communication systems, input and/or output of the channel take values from real numbers. These are called *continuous channels*. An AWGN channel is a continuous channel in which the random variables X and Y corresponding to the input and output of the channel respectively, are related as $Y = X + N$, where N is the noise and is a random variable that is drawn from a zero-mean Gaussian distribution with variance $\frac{N_0}{2}$;

that is, $\mathcal{N}(0, \frac{N_0}{2})$. If the noise variance is zero or the input is unconstrained, there exist an infinite subset of inputs that are distinguishable at the output with arbitrarily small error probability. However, in practice the variance is always non-zero and the input is always power-limited. The input signal energy for each bit of the transmitted information block is denoted by E_b. This constrains the input signal energy and power. In a discrete channel W, the input and output alphabets are discrete sets. The channel is specified by a *transition probability matrix* $\mathbf{P}_{\mathsf{W}}$, where rows and columns are labelled by the input and output alphabets, respectively, and entries are conditional probabilities, $\mathbf{P}_{\mathsf{W}}[\mathbf{x}, \mathbf{y}] = p_{\mathbf{xy}} = P_r(Y = \mathbf{y}|X = \mathbf{x})$. A channel is called *strongly symmetric* if the rows of the transition matrix are permutations of one another, and so is the case for the columns. The channel $\mathsf{W}(\cdot)$ is *symmetric* if there exists a partition of the output set $\mathcal{Y} = \mathcal{Y}_1 \cup \cdots \cup \mathcal{Y}_n$, such that for all i, the sub-matrix $\mathbf{P}_{\mathsf{W}_i} = \mathbf{P}_{\mathsf{W}}[\mathcal{X}, \mathcal{Y}_i]$ is strongly symmetric.

Wiretap channel model. In the general wiretap model, also called the *broadcast model* [34], a sender is connected to the receiver through the *main* channel $\mathsf{W}_1 : \mathcal{X} \to \mathcal{Y}$, and to the eavesdropper through a second channel $\mathsf{W}_2 : \mathcal{X} \to \mathcal{Z}$, called the *wiretapper's channel*. Thus, $\mathsf{WT} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$. In Wyner's original model, the wiretapper's channel is a *degraded* version of the main channel, and the Markov chain $X - Y - Z$ holds. We consider the original Wyner wiretap model. The goal of wiretap channel coding is to provide communication secrecy and reliability. Efficiency of wiretap codes is measured by the information rate, which is the number of information bits that can be transmitted reliably and secretly, per usage of the wiretap channel. One can also use a normalized form $R/\log|\Sigma|$ of the communication rate (cf. [61]), where Σ is the code alphabet. For example, the information rate of linear codes is usually defined as the ratio of the code dimension to the block length. The information rate of wiretap codes is upper-bounded by the *secrecy capacity* C_s of the wiretap channel.

Theorem 4.1. *[84] The secrecy capacity of Wyner wiretap channel when* W_1 *and* W_2 *are symmetric is given by*

$$C_s = C_{\mathsf{W}_1} - C_{\mathsf{W}_2},$$

where C_{W_1} *and* C_{W_2} *are the (reliability) channel capacities of* W_1 *and* W_2.

Since the capacity of a broadcast channel depends on the conditional marginal distributions only [17], the above capacity result also holds for a stochastically degraded broadcast channel that is defined below.

Definition 4.1. A broadcast channel $\mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ with conditional marginals $\mathsf{W}_1 : \mathcal{X} \to \mathcal{Y}$ and $\mathsf{W}_2 : \mathcal{X} \to \mathcal{Z}$ is said to be *stochastically degraded* if there exists a third channel $\mathsf{W}_3 : \mathcal{Y} \to \mathcal{Z}$ such that,

$$\mathbf{P}_{\mathsf{W}_2}[\mathbf{x}, \mathbf{z}] = \sum_{\mathbf{y} \in \mathcal{Y}} \mathbf{P}_{\mathsf{W}_3}[\mathbf{y}, \mathbf{z}] \mathbf{P}_{\mathsf{W}_1}[\mathbf{x}, \mathbf{y}], \tag{4.1}$$

or equivalently

$$\mathbf{P}_{\mathsf{W}_2} = \mathbf{P}_{\mathsf{W}_3} \times \mathbf{P}_{\mathsf{W}_1}.$$

4.2.1 QAM and OFDM

OFDM is a multicarrier modulation scheme that is widely used in modern wireless technologies and standards such as 4G mobile communications, WiMax, LTE and 802.11 a/g/n [114]. In OFDM, the information is transmitted using many narrowband signals at different frequencies, each carrying a small amount of information (number of bits). The narrowband signals may use modulations such as Quadrature Amplitude Modulation (QAM), which can be expressed as:

$$s(t) = A_I cos 2\pi f_c t - A_J sin 2\pi f_c t, \quad 0 < t < T,$$

where A_I and A_J are the amplitude for in-phase and quadrature phase components, f_c is the carrier frequency, and T is the symbol time duration. The *OFDM signal* is constructed at the transmitter by (i) taking N (for example N = 64 in 802.11) QAM modulated signals, and (ii) applying Inverse Fast Fourier Transform (IFFT) to obtain OFDM time samples that will be sent over the channel. For N carrier frequencies, let $\mathbf{a}_k$ denote the OFDM time sample in the k-th time interval and obtained using IFFT:

$$\mathbf{a}_k = \sum_{n=0}^{N-1} \mathbf{A}_n e^{i2\pi kn/N} \qquad k = 0, 1, ..., N-1, \tag{4.2}$$

where $\mathbf{A}_n$ is a complex number. Each *OFDM symbol* consists of N *time samples* $(\mathbf{a}_0, \mathbf{a}_1, ..., \mathbf{a}_{N-1})$. The transmitted signal is a sequence of OFDM time samples, each with Gaussian distribution. This is because each OFDM sample is a linear combination of N modulated *signals,* which because of central limit theorem results in a Gaussian distribution.

4.2.2 iJam and Basic iJam Transmission (BiT) protocol

iJam [59] is a protocol for key agreement between two parties, and uses BiT protocol as a subprotocol. Our focus is on BiT protocol. BiT protocol is a protocol between a sender and a receiver who also takes the role of a jammer, resulting in outputs for the receiver and the eavesdropper. The sender sends each OFDM symbol twice (the symbol and its identical copy) in two consecutive subintervals. Thus, the time interval for sending an OFDM symbol is twice a subinterval (effectively doubling the sending time). An OFDM symbol is received as a sequence of time samples. The receiver randomly jams a time sample in the original symbol in the first subinterval, or its copy in the second subinterval. Jamming is by sending a Gaussian distributed

jamming signal with the same distribution as the transmitted time samples, over the channel. The receiver will receive unjammed (clean) time samples of the two subintervals, and reconstruct the OFDM symbol with perfect reliability.

4.2.3 Eavesdropper's strategies

In BiT, the sent time sample and the jamming signal will be combined at Eve's receiver. Thus for each OFDM symbol, Eve will receive two copies, each consisting of some jammed and some clean time samples. The eavesdropper can use different decoding strategies. They may treat the jamming signal as the noise and try to decode in presence of jamming; or they can implement interference cancellation or joint decoding in an attempt to simultaneously decode the jamming signal and the original transmission. In [59], the authors discuss strategies that can be used for the receiver's jamming signal to reduce the detectability of the jammed samples. For example the jammer can transmit at an excessively high rate in an attempt to remove the possibility of joint decoding. This is because according to multiuser information theory, decoding multiple signals is impossible if the total information rate is outside the capacity region [137].

4.3 BiT as a virtual wiretap channel – An example

BiT is an interactive physical layer protocol between Alice and Bob that takes an input from Alice and Bob, and generates outputs for Bob and Eve. Alice's input is an information signal consisting of two copies of an input block of information bits; Bob's input is a coordinated jamming signal. The output of Bob is a block of information bits sent by Alice, and Eve's output is an element of Alice's space of block of information bits. We use a small example to provide intuition for our approach. In Example 4.1, we consider a scenario where Alice wants to send a 2-bit information block $\mathbf{x}$ to Bob. Let $\mathbf{x}_s$ denote a 4-QAM modulated signal that carries the information block $\mathbf{x}$. For this small example, the OFDM symbol consists of only one signal ($N = 1$) and there is only a single time sample. Alice's input to the BiT protocol is two copies of the OFDM symbol (in this case $\mathbf{x}_s$), i.e. $(\mathbf{x}_s, \mathbf{x}_s)$ that are sent in two consecutive time subintervals. Bob's coordinated jamming signal is sent coordinated with Alice's transmission: Bob randomly chooses one of the two subintervals, corresponding to the two copies, and sends the jamming signal in that time slot. For example, when Bob jams the second time slot, the jamming signal is $(\text{-}, \text{J}'_s)$.

Bob will receive the signal corresponding to the unjammed time slot and will obtain the information block $\mathbf{x}$. Continuing with the above example, if Bob's input to the BiT protocol is $(\text{-}, \text{J}'_s)$, he receives $(\mathbf{x}_s, \text{-})$.

Eve will receive a combination of the signals sent by Alice and Bob, $V_s = (\mathbf{x}_s, \mathbf{x}_s + J_s)$ where J_s is the jamming signal that is received by Eve's antenna. If Eve cannot sufficiently distinguish the jammed signal

from the unjammed one, the result will likely to cause an error in decoding. We denote Eve's decoder output by $\mathbf{z}$.

The above protocol can be seen as creating a wiretap (broadcast) channel from Alice to Bob and Eve that can be described by the probability distribution $\Pr(\mathbf{y}, \mathbf{z}|\mathbf{x})$, where $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ are the input of Alice, and outputs of Bob and Eve, respectively, as information blocks. Since $\mathbf{y} = \mathbf{x}$, the channel is characterized by $\Pr(\mathbf{z}|\mathbf{x})$, which represents the cumulative effects of the jamming detection, and the decoding error caused by the jamming signal J_s.

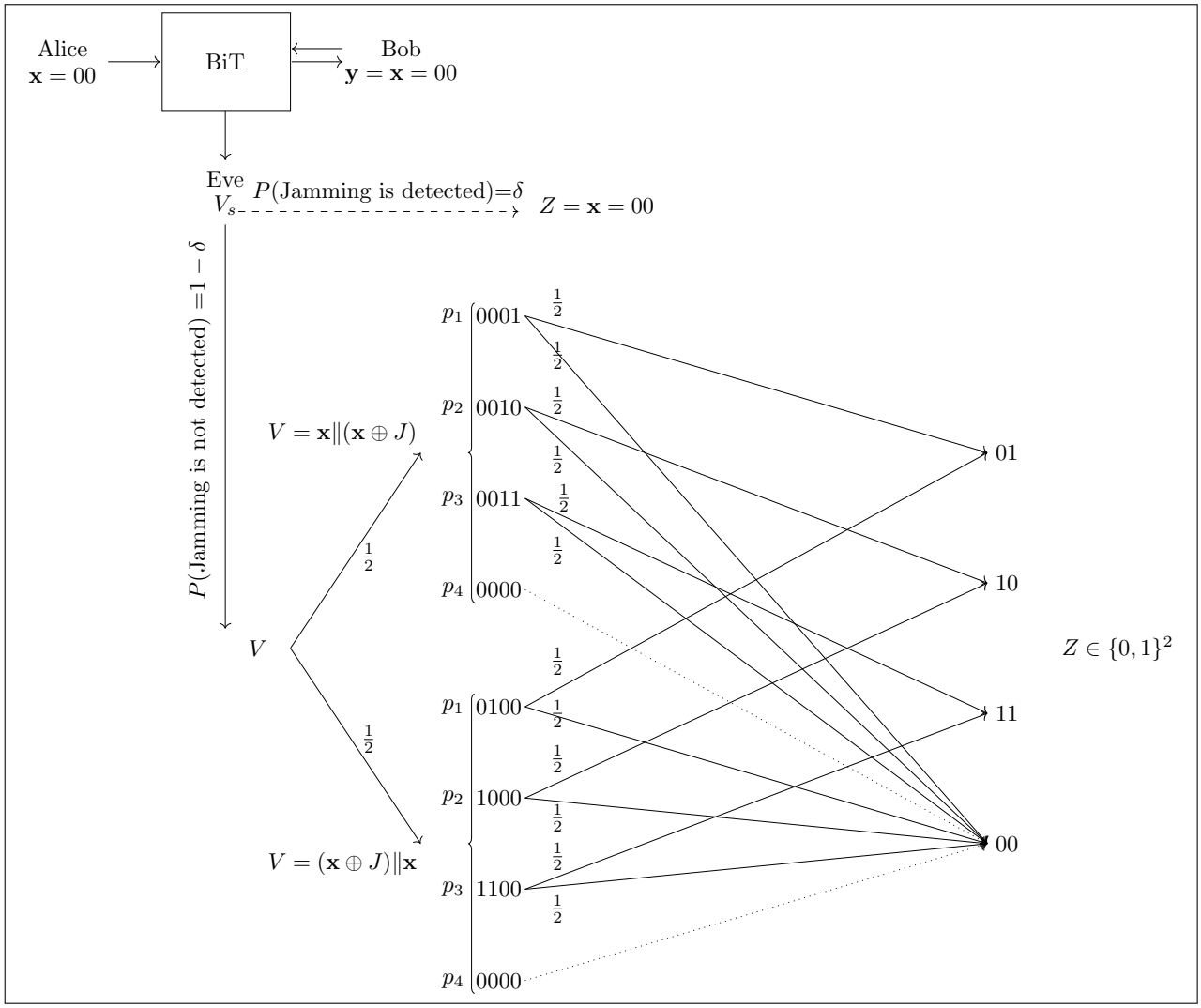

Figure 4.1: BiT when a single 4-QAM (OFDM with $N = 1$) is used.

Example 4.1. *Let* $\mathbf{x}$ *be a 2-bit information block that is sent using the BiT protocol and the 4-QAM modulation with frequency* f_1*. Figure 4.1 shows the transmission of an information block* $\mathbf{x} = 00$ *using the BiT protocol. The process of Eve constructing their view of the channel is represented using a graph. In the*

graph, the physical output of the BiT protocol at Eve's side is a pair of signals denoted by V_s. One of the two signals is jammed and Eve tries to figure out which one. If Eve fails to distinguish the jammed signal from the clean one, V_s is decoded across one of the two edges labelled by $V = (\mathbf{x} \oplus J)\|\mathbf{x}$ and $V = \mathbf{x}\|(\mathbf{x} \oplus J)$, respectively. The list of 4-tuples following these edges, represent Eve's decoder's outputs after receiving the signal pairs and assuming the jammed subinterval is not detected. The next set of edges represent Eve's decision of information block based on the decoder's output. Note that when the decoder output is (0000)*, Eve decides correctly. In all other cases, Eve might make an error. For simplicity, we assume the decoder's output of the two subintervals are different, Eve randomly chooses one of the two (they know one of the two are correct). The receiver, who is also the jammer, can always perfectly locate the unjammed subinterval and hence have a perfect reception* $\mathbf{y} = \mathbf{x} = 00$ *. In the following, we provide more details on how the probability of Eve's outputting a particular information block can be obtained.*

Eve receives two copies of the OFDM (here a 4-QAM) symbol denoted by V_s. Eve may use various decoding approaches to distinguish the jammed signal from the unjammed one. If Eve can detect the jammed subinterval (e.g., high reception power), they can distinguish the jammed subinterval and can correctly receive the sent information block: they will simply discard the jammed subinterval and decode the unjammed one. Suppose Eve detects the correct jammed signal with probability $0 < \delta < 1$ *(the dashed arrow in Figure 4.1). This will create the output* $Z = \mathbf{x} = 00$ *for Eve. If Eve's decoder cannot detect the jammed signal, the best thing they can do is to decode each OFDM symbol and then use the information about the BiT protocol (repeated symbol) to find the sent information block. Eve's OFDM symbol decoder takes V_s and outputs either $V = \mathbf{x}\|(\mathbf{x} \oplus J)$ or $V = (\mathbf{x} \oplus J)\|\mathbf{x}$, depending on the receiver's choice of the jammed subinterval. Here J is a 2-bit random variable capturing the effect of the jamming on Eve's OFDM symbol decoding. The random variable J depends on the jamming signal power, the location of the adversary, and Eve's decoding capabilities, and does not depend on the sent OFDM symbol. Let $P[J = \alpha]$ denote the probability that jamming creates an offset α to the original information block. In our example, we set $P[J = 01] = p_1,\ P[J = 10] = p_2,\ P[J = 11] = p_3$ and $P[J = 00] = p_4$. To find the original transmitted information block, the adversary maps $V \in \{0,1\}^4$ to $Z \in \{0,1\}^2$. When $J = 00$, V consists of two identical information blocks and so is correctly mapped to the transmitted information block $\mathbf{x}$ (dotted arrows in Figure 4.1). When $J \neq 00$, Eve randomly chooses the decoded OFDM symbol of one of the two subintervals for $Z = \mathbf{z}$. One can use other distributions to choose the output OFDM symbol that better models the adversary's receiver. To summarize, the probability that Eve correctly outputs the correct sent information block $\mathbf{x} = 00$ consists of (i) the probability of Eve correctly detecting the jammed subinterval with probability δ,(ii) the probability that Eve cannot successfully detect the jammed interval, but $J = 00$ with probability $(1 - \delta)p_4$ and, (iii) the probability of jamming is not detected,*

$J \neq 00$ but Eve's guess of the sent information block is correct with probability $(1-\delta)\frac{1-p_4}{2}$). Therefore:

$$P[Z = 00|X = 00] = \delta + (1-\delta)p_4 + (1-\delta)\frac{1-p_4}{2} = \delta + (1-\delta)\frac{1+p_4}{2}.$$

Next, we study the probability of Eve having an incorrect output. To simplify the discussion, let $p_1 = p_2 = p_3 = \frac{(1-p_4)}{3}$. Then for any $\mathbf{x}' \in \{0,1\}^2$ such that $\mathbf{x}' \neq \mathbf{x}$, we have $P[Z = \mathbf{x}'|X = 00] = (1-\delta)\frac{1-p_4}{6}$.

For any $\mathbf{x} \in \{0,1\}^2$, the probability that the adversary obtains the correct information block is calculated similar to $\mathbf{x} = 00$. Let $\eta = \delta + (1-\delta)\frac{1+p_4}{2}$. The result of the above process specifies the probabilities of the wiretapper's channel as follows:

$$P[Z = \mathbf{x}|X = \mathbf{x}] = \eta,$$
$$P[Z = \mathbf{x}|X \neq \mathbf{x}] = \frac{1-\eta}{3}.$$

Thus, the transition matrix of the virtual wiretapper's channel W is as follows.

$$\mathbf{P}_{\mathsf{W}} = \begin{bmatrix} \eta & \frac{1-\eta}{3} & \frac{1-\eta}{3} & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \eta & \frac{1-\eta}{3} & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \frac{1-\eta}{3} & \eta & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \frac{1-\eta}{3} & \frac{1-\eta}{3} & \eta \end{bmatrix},$$

In summary, using BiT results in Eve receiving the information block $\mathbf{x}$ through a probabilistic channel with output $Z \in \{0,1\}^2$, resulting in a wiretapper's channel that is noisier than the main channel (which is noiseless), hence enabling secure communication.

Remark 4.1. *According to [59], when the three conditions described in Sections 4.2.1, 4.2.2 and 4.2.3 are met, we can have $\eta < 1$ (the above example does not satisfy Section 4.2.1, so $\eta = 1$). We use the above example for the purpose of illustrating ideas.*

4.4 Virtual wiretap channel model

In the following, we extend the above ideas to the general case where a complex OFDM signal is used.

Eavesdropper's view. Consider an OFDM signal with N frequencies where each signal uses 2^q-QAM modulation. Let $X \in \{0,1\}^{Nq}$ denote the information block that is transmitted using an OFDM symbol $(\mathbf{a}_0, \mathbf{a}_1, \cdots, \mathbf{a}_{N-1})$. By invoking the BiT protocol, for each information block, $2N$ time samples are generated and sent over $2N$ consecutuve time intervals. Eve receives $2N$ time samples. For the two corresponding

samples, one is a clean sample and the other is the jammed one. Let $V_s \in \mathbb{C}^{2N}$ be the random variable representing the $2N$ time samples. The received signal is mapped into an Nq-bit information block using the following eavesdropper decision unit (that includes their jamming detection, OFDM decoder and information block decision).

$$\mathsf{E} : \mathbb{C}^{2N} \to \{0,1\}^{Nq}.$$

There are two cases:

1. *The recovery of the information block is successful.* The adversary can correctly detect all N jammed samples, for example by examining the received signal power [130]. Using all the correct time samples, the adversary correctly recovers the OFDM symbol and the information block, respectively. There are two other cases in which information block recovery is successful; one is when the jamming signal does not change any of the time samples, and the other case is when the adversary's random guess for the clean sample is correct for all the clean samples. We denote the probability that the adversary recovers the information block correctly by η, for $0 < \eta < 1$.

2. *The recovery of the information block fails.* If the adversary cannot correctly detect even one of the jammed time samples, because of the use of Fast Fourier Transform (FFT) on the time samples, all the recovered frequency samples will be affected and the recovered information block will be incorrect. For the simplicity of calculations, we assume Eve outputs any of the incorrect information blocks from the set $\{0,1\}^{Nq} \backslash \{X\}$, with the same probability, that is each possible incorrect $2^{Nq} - 1$ string occurs with probability $\frac{1-\eta}{2^{Nq}-1}$. As noted earlier, this can be replaced by other distributions that better estimate Eve's reception.

Let the random variable $Z \in \{0,1\}^{Nq}$ denote the information block that is output by Eve's decision unit E; that is, $Z = \mathsf{E}(V)$. We refer to Z as *Eve's view.* The conditional distribution of Eve's view of the sent information block X is denoted by $Z|X$ and is given as follows:

$$P[Z = \mathbf{x}|X = \mathbf{x}] \simeq \eta,$$
$$P[Z = \mathbf{x}|X \neq \mathbf{x}] \simeq \frac{1-\eta}{2^{Nq}-1}.$$

Thus, we have a virtual noisy channel $W : \{0,1\}^{Nq} \to \{0,1\}^{Nq}$ with the following transition matrix:

$$\mathbf{P}_{\mathsf{W}} = \begin{bmatrix} \eta & \frac{1-\eta}{2^{Nq}-1} & \cdots & \frac{1-\eta}{2^{Nq}-1} \\ \frac{1-\eta}{2^{Nq}-1} & \eta & \cdots & \frac{1-\eta}{2^{Nq}-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1-\eta}{2^{Nq}-1} & \frac{1-\eta}{2^{Nq}-1} & \cdots & \eta \end{bmatrix}. \tag{4.3}$$

We call this channel a *virtual wiretapper's channel* from the sender to Eve, represented by $Z = \mathsf{W}(X)$.

Receiver's view. The receiver always knows the unjammed time sample and so is effectively connected to the sender via a noiseless main channel.

Definition 4.2. Let η denote the probability that Eve correctly recovers an information block that is sent using a BiT that uses OFDM with N-frequencies, each using 2^q-QAM. We define a virtual wiretap channel and denote it by $\mathrm{BiT}^N_{\eta,q}$. This wiretap channel has noiseless main channel and the transition probability matrix of the wiretapper's channel is given by $\mathbf{P}_{\mathsf{W}}$ in (4.3).

Theorem 4.2. *The secrecy capacity of $BiT^N_{\eta,q}$ wiretap channel is given by*

$$C_s(BiT^N_{\eta,q}) = -\{\eta \log \eta + (1-\eta) \log \frac{1-\eta}{(2^{Nq}-1)}\}.$$

Proof. Channel $\mathsf{W}(\cdot)$ is symmetric and degraded (according to Definition 4.1) with respect to the noiseless main channel.

The secrecy capacity of the wiretap channel is given by Theorem 4.1.

$$C_s = H(X|Z) - H(X|Y) = H(X|Z),$$

where X is uniform, and Y and Z are the output of the main channel and the wiretapper's channel, respectively. Note that in the above equation $H(X|Y) = 0$ because the main channel is noiseless. Using the transition probability matrix, we have

$$\begin{aligned} H(X|Z) &= \sum_{z \in \{0,1\}^{Nq}} P[Z = z] H(X|Z = z) \\ &= -\{\eta \log \eta + (1-\eta) \log \frac{1-\eta}{(2^{Nq}-1)}\}. \end{aligned} \tag{4.4}$$

□

4.5 Secure message transmission using BiT

BiT had been introduced in [59] to construct a key agreement protocol. Using the above model, we construct a secure message transmission protocol with *provable security*. We will use capacity-achieving wiretap coding construction in [11] that provides semantic security, and has efficient encryption and decryption functions. The wiretap construction in [11] is for binary input symmetric channels. The q-ary channel alphabet is from [9, Section 5.5] and its extension [12].

4.5.1 A semantically secure wiretap code

The construction is a seeded encryption and uses an invertible extractor.

Definition 4.3. [44] A function $\mathsf{EXT} : Sds \times \{0,1\}^n \to \{0,1\}^\ell$ is a (d,ϵ)-strong, average-case extractor if, $\mathrm{SD}((\mathsf{EXT}(S,X),Z,S);(U,Z,S)) \leq \epsilon$ for all pairs of correlated random variables (X,Z) over $\{0,1\}^n \times \{0,1\}^*$, assuming $\tilde{H}_\infty(X|Z) \geq d$.

Seeded encryption. For a public uniformly distributed random variable $S \in Sds$ and an arbitrarily distributed message $M \in \{0,1\}^b$, the seeded encryption function $\mathsf{SE} : Sds \times \{0,1\}^b \to \{0,1\}^{nNq}$, outputs a ciphertext $\mathsf{SE}(S,M)$. The corresponding seeded decryption function is $\mathsf{SDE} : Sds \times \{0,1\}^{nNq} \to \{0,1\}^b$ such that for all $S \in Sds$ and $M \in \{0,1\}^b$ we have $\mathsf{SDE}(S,\mathsf{SE}(S,M)) = M$.

Inverting extractors. The function $\mathsf{INV} : \{0,1\}^r \times Sds \times \{0,1\}^b \to \{0,1\}^{nNq}$ is an inverter for the extractor $\mathsf{EXT}(\cdot,\cdot)$ in Definition 4.3, if for a uniform $R \in \{0,1\}^r$ and for all $S \in Sds$ and $Y \in \{0,1\}^b$, the random variable $\mathsf{INV} : (S,R,Y)$ is uniformly distributed over all preimages of Y under $\mathsf{EXT}(S,\cdot)$.

Let $Sds = \{0,1\}^{nNq} \backslash 0^{nNq}$. For inputs $S \in Sds$ and $X \in \{0,1\}^{nNq}$ and $nNq > b$, the function $\mathsf{EXT} : Sds \times \{0,1\}^{nNq} \to \{0,1\}^b$ is defined as follows:

$$\mathsf{EXT}(S,X) = (S \odot X)|_b,$$

where $\odot$ denotes the multiplication over $\mathbb{F}_2^{nNq} = \{0,1\}^{nNq}$, and $X|_b$ denotes the first b bits of X. An efficient inverter for $\mathsf{EXT}(S,X)$ is given by $\mathsf{INV}(S,R,M) = S^{-1} \odot (M \| R)$, where S^{-1} denotes the multiplicative inverse of S in $\mathbb{F}_2^{nNq}$ and R is a uniformly distributed variable over $\{0,1\}^{n-b}$. For the message block $M \in \{0,1\}^b$, $S \in Sds$, and $R \xleftarrow{\$} \{0,1\}^r$, the seeded encryption function $\mathsf{SE}(S,M)$ is defined as follows:

$$X = \mathsf{SE}(S,M) = \mathsf{INV}(S,R,M) = S^{-1} \odot (M \| R).$$

4.5.2 Using the wiretap construction with $\text{BiT}^N_{\eta,q}$

Let ENC denote the construction that uses wiretap coding for $\text{BiT}^N_{\eta,q}$.

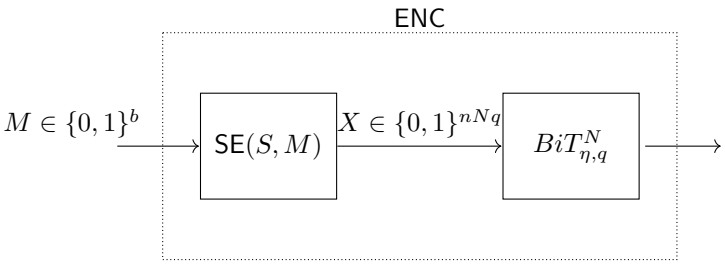

Figure 4.2: Secure message transmission based on BiT protocol

As illustrated in Figure 4.2, the encryption block ENC consists of two sub-blocks:

1. A seeded wiretap encryption code $\mathsf{SE} : Sds \times \{0,1\}^b \to \{0,1\}^{nNq}$ that encrypts each information block of size b bits into a codeword of size nNq bits.

2. The $\text{BiT}^N_{\eta,q}$ block that breaks the codeword into Nq-bit units, and sends it using the BiT protocol.

To capture the efficiency of the proposed message transmission protocol, we define the communication rate $\mathcal{R}$ of the system as the number of transmitted bits that are sent with security and reliability, in each application of $\text{BiT}^N_{\eta,q}$. This is similar to the definition of rate in the wiretap channel literature (cf. [34]).

Definition 4.4. The rate of the message transmission protocol over $\text{BiT}^N_{\eta,q}$ in Figure 4.2 is $\mathcal{R} = \frac{b}{n}$.

The rate of the ENC block in Figure 4.2 asymptotically approaches the secrecy capacity of the virtual wiretap channel $\text{BiT}^N_{\eta,q}$. The construction provides semantic security and reliability. The codeword length from $\mathsf{SE}(S, M)$ is $nNq = b + r$, where b is the total length of the message and r is the length of the concatenated random string. For σ bit semantic security, the length of r is given in [131] as recalled below:

$$r \geq \lceil 2(\sigma + 1) + \sqrt{n} \log(2^{Nq} + 3)\sqrt{2(\sigma + 3)} + (n)\psi(\mathsf{W})\rceil,$$

where $\psi(\mathsf{W}) = |\log \mathcal{Z}| - H(\mathsf{W}) = Nq - H(X|Z)$ in the above equation. The secrecy capacity of $\text{BiT}^N_{\eta,q}$ for $N = 64$ and various values of η and q are given in the Appendix B.3.1.

4.6 BiT over noisy receiver's channel

In Wyner wiretap model, the secrecy capacity is zero when the main channel is noisy while the eavesdropper's channel is noise-free. That is, one cannot expect any secure communication from Alice to Bob. BiT creates

a virtual wiretap channel for Eve when the physical channel between Alice and Bob is noise-free. In the following, we will show that when the receiver's physical channel is corrupted by Additive White Gaussian Noise (AWGN) (while the eavesdropper's physical channel remains noise-free), BiT can be used to introduce noise in Eve's channel and make secure communication possible. Figure 4.3 shows the application of BiT when the main channel is corrupted by AWGN.

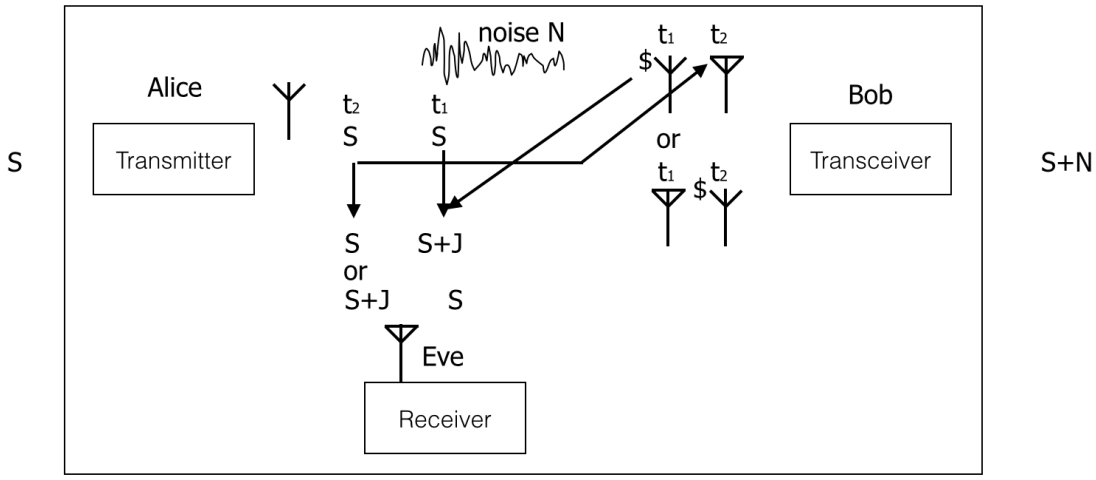

Figure 4.3: BiT protocol when Bob's physical channel is noisy

Eavesdropper's view. The eavesdropper's channel is the same as in Section 4.4, created by the BiT protocol. This is because the noise only affects the transmission in the main channel. Eve receives $V_s = (\mathbf{x_s} \oplus J_s) \| \mathbf{x_s}$ or $V_s = \mathbf{x_s} \| (\mathbf{x_s} \oplus J_s)$, and the eavesdropper's channel transition probability is given by $\mathbf{P_W}$ in (4.3).

Receiver's view. The receiver's channel, however, is corrupted by AWGN. We first consider the effect of AWGN on a *single* 2^q*-QAM signal* (i.e., OFDM with a single frequency) and then generalize it to an OFDM with N frequencies.

Let $\mathsf{AWGN}(\cdot)$ denote the AWGN channel where the noise is added to the input. Bob knows which subinterval is jammed. Therefore, his reception is one OFDM symbol corrupted by the AWGN noise. That is

$$\mathsf{AWGN}(\mathbf{x}_s) = \mathbf{x}_s + N_s,$$

where N_s denotes the random signal corresponding to the white Gaussian noise. Let $\mathsf{B}(\cdot)$ be the function that maps Bob's received signal to an Nq-bit string. The virtual main channel from Alice to Bob is defined

as:

$$Y = \mathsf{M}(X) = \mathsf{B}(\mathsf{AWGN}(\mathbf{x}_s)).$$

Let the transition probability matrix of a 2^q-QAM signal that is corrupted by AWGN be denoted by $\mathbf{P}_{\mathsf{M},q}$. Using the error probability calculation of Binary Phase Shift Keying (BPSK) in [57] Chapter 6.1.2, the 4-QAM transition probability matrix will be given as:

$$\mathbf{P}_{\mathsf{M},2} = \begin{bmatrix} (1-P_b)(1-P_b) & P_b(1-P_b) & P_b(1-P_b) & P_b^2 \\ P_b(1-P_b) & (1-P_b)(1-P_b) & P_b^2 & P_b(1-P_b) \\ P_b(1-P_b) & P_b^2 & (1-P_b)(1-P_b) & P_b(1-P_b) \\ P_b^2 & P_b(1-P_b) & P_b(1-P_b) & (1-P_b)(1-P_b) \end{bmatrix},$$

where the probability P_b is computed as follows:

$$P_b = Q(\sqrt{\frac{E_b}{N_0}}),$$

and E_b is the energy-per-bit of the input signal, $\frac{N_0}{2}$ is the variance of the AWGN, and $Q(z)$ is the probability that a Gaussian random variable x with mean 0 and variance 1 takes a value larger than z, namely,

$$Q(z) = \mathrm{P}[x > z] = \int_z^\infty \frac{1}{2\pi} e^{-x^2/2} dx.$$

The function $Q(\cdot)$ can be efficiently computed using approximations such as the one in [80].

For an *OFDM signal with N frequencies*, assuming noise independently corrupts each frequency, the transition probability matrix $\mathbf{P}_{\mathsf{M}}$ will be given as,

$$\mathbf{P}_{\mathsf{M}} = \mathbf{P}_{\mathsf{M},q}^{\otimes N}. \tag{4.5}$$

We thus have a virtual wiretap channel for the BiT protocol in the setting where the receiver's physical channel is an AWGN (and the eavesdropper has a noise-free physical channel).

Definition 4.5. Let η denote the probability that Eve correctly recovers an information block that is sent using a BiT that uses OFDM with N-frequencies, each using 2^q-QAM. We define a virtual wiretap channel for the setting where the receiver's physical channel is an AWGN and denote it by AWGN-BiT$^N_{\eta,q}$. This wiretap channel has a noisy main channel with transition probability matrix given by $\mathbf{P}_{\mathsf{M}}$ in (4.5) and a

wiretapper's channel with the transition probability matrix given by $\mathbf{P}_{\mathsf{W}}$ in (4.3).

Theorem 4.3. *The secrecy capacity of AWGN-BiT$^N_{\eta,q}$ is given by,*

$$C_s = C_{\mathsf{M}} - C_{\mathsf{W}},$$

if the matrix $\mathbf{R} = \mathbf{P}_{\mathsf{W}} \times \mathbf{P}_{\mathsf{M}}^{-1}$ *is the transition probability matrix of a channel, namely,* $\mathbf{R}$ *satisfies the following two conditions,*

1. $\mathbf{R}$ *does not have any negative component,*
2. *The sum of the components in each row of* $\mathbf{R}$ *is equal to* 1.

Remark 4.2. *Condition 1 in Theorem 4.3 can be satisfied by imposing a relation between* η *(the parameter characterizing the virtual wiretapper's channel* W*) and* P_b *(the parameter characterizing the virtual main channel* M*). Condition 2 can be verified directly by computation. We provide more details by giving an example for N=1 in Appendix B.3.2.*

Proof. From $\mathbf{R} = \mathbf{P}_{\mathsf{W}} \times \mathbf{P}_{\mathsf{M}}^{-1}$, we have

$$\mathbf{R} \times \mathbf{P}_{\mathsf{M}} = \mathbf{P}_{\mathsf{W}}.$$

Conditions 1 and 2 are sufficient to ensure that $\mathbf{R}$ is a transition probability matrix for a channel and so using Definition 4.1, $\mathbf{P}_{\mathsf{W}}$ is a stochastically degraded channel with respect to $\mathbf{P}_{\mathsf{M}}$. The rest of the proof follows from Theorem 4.1. □

4.7 Conclusion and future works

BiT uses an innovative way of coordinated jamming to construct a virtual wiretap channel and enables information-theoretically secure communication without a shared key. We showed how to model BiT as a virtual wiretap channel, estimate its parameters, and use the model to design a provably secure message transmission protocol.

BiT is a subprotocol of the iJam protocol that had been implemented and experimentally analyzed. By formal modelling of the BiT protocol and developing a provably secure message transmission scheme based on that, we have effectively constructed a keyless information-theoretically secure message transmission system that can be used in practice.

Our scheme asymptotically achieves the secrecy capacity of the virtual wiretap channel. The primary assumption underlying our modelling is that the decoding error probability of Eve can be estimated. This

probability depends on factors such as the sender and receiver (jamming) signal power, and the location and receiving equipments of the eavesdropper. An interesting direction for future work would be to design protocols that are more robust with respect to the imprecise estimation of the error probability. Extending our analysis and approach to other physical layer security protocols is also an interesting direction for future work.

Part II

Modular Semantically Secure Keyed Wiretap Encoding

Chapter 5

A Modular Semantically Secure Wiretap Code with Shared Key for Weakly Symmetric Channels[1]

Abstract. We study the problem of secure communication over a wiretap channel when the sender and the receiver have access to a shared secret key. We propose a modular secure construction of wiretap codes for a shared key setting that achieves secrecy capacity for weakly symmetric wiretap channels, and has computationally efficient encoding and decoding. The construction's security and reliability guarantees are in terms of semantic security, which is the strongest notion of security for these channels, and worst case error, respectively. We give concrete parameters of the construction for finite-length messages to obtain a desired level of security and reliability.

5.1 Introduction

Alice and Bob are connected by a noisy channel that is eavesdropped by an adversary Eve with unlimited computational power. Alice wants to send a message to Bob such that (i) with a high probability, Bob correctly receives the message, and (ii) the eavesdropper does not learn anything about the message.

Shannon [115],[116] gave a two-step solution to this problem: first, provide reliable communication to the receiver (by using channel codes), and then provide security against the eavesdropper by using an OTP (One-Time-Pad) encryption system, using a shared secret key. The main drawback of this solution is that each message needs a fresh shared secret key whose entropy is lower bounded by the message entropy.

Wyner [143] pioneered a new approach to the problem by introducing the wiretap model where Alice's transmission to Bob is also received by Eve, through a second channel that is a degraded version of Bob's channel, and showed that the extra noise in Eve's reception can be used to provide confidentiality. Csiszar

[1]The content of this chapter is published as a paper [117] in proceedings of ITW 2019.

and Korner [34] extended this model to the case that Alice is connected to Bob and Eve through two independent channels: the *main channel* and the *wiretapper*'s channel, respectively, and proved that secure and reliable communication is possible as long as the main channel is more "capable" (See expression (12) in [34]) than the wiretapper's one. A very attractive aspect of this approach is that Alice and Bob do not need a shared secret key, and it is sufficient to use randomized coding to achieve (asymptotic) perfect secrecy for the communication. One of the challenges of this approach is that depending on the difference between the quality of the main and the wiretapper's channel, one may have to send the message at a very low rate (the number of securely transmitted information bits divided by the total number of channel use).

A natural question is if the two models can be combined: that is, use a secret key to achieve higher rate, while taking advantage of the noise in Eve's channel to shorten the key. This problem is first considered by Yamamoto [145] and later by Merhav [94], Kang et al.[78] and Schaefer et al. [113], under different assumptions and reception quality criteria. Kang et al. [78] derived the secrecy capacity of wiretap channels with shared key under weak secrecy condition, and used random codes for a uniformly distributed message space to prove the achievability result. The capacity result (See Theorem 5.1) reduces to wiretap channel capacity when the secret key rate is zero. Wang et al. [141] proposed a construction of capacity-achieving codes for wiretap channels with shared key under strong secrecy condition (the total leakage rather than the leakage rate), using polar codes.

Constructions of message transmission with perfect secrecy. The only secure message transmission construction with perfect information-theoretic secrecy in a shared key setting is OTP. Early constructions of wiretap codes rely on special classes of error correcting codes, for example LDPC codes in [98, 136], and polar codes in [87]. Modular constructions of wiretap codes [66] separate randomization of the encoder for achieving secrecy, from error correction for reliability, and can work with any capacity-achieving error correcting code that satisfies the requirement of the construction. Bellare et al. [11] introduced semantic security of wiretap codes, and proposed a modular capacity-achieving construction for binary input degraded symmetric wiretap channels. The construction is later shown to achieve the same properties for degraded symmetric wiretap channels in [131]. Other modular constructions of capacity-achieving wiretap codes with semantic security are by Tyagi et al.[138] for Gaussian wiretap channels, and Sharifian et al. [120] for discrete symmetric wiretap channels.

5.1.1 Our work

We propose a modular capacity-achieving construction of wiretap codes with key (*keyed wiretap* for short) that provides semantic security. The construction can be instantiated to have efficient encoding and decoding.

Similar to all modular constructions of wiretap codes, the construction uses a *seed*, which is a random string shared by Alice and Bob (e.g., can be sent over a reliable channel). Compared to existing constructions of keyed wiretap codes in [78], [113] and [141], our construction has the unique properties of being modular and providing semantic security. The construction can be used for weakly symmetric channels, which includes the class of channels for which modular semantically secure wiretap code (without key) is known [11, 120]. Extending these latter constructions to keyed wiretap setting is an interesting open question.

5.2 Preliminaries

5.2.1 Notations and background

Random variables are denoted by capital letters and their corresponding realizations are denoted by lowercase letters. Sets are denoted by calligraphic letters e.g., $\mathcal{X}$ and the size of $\mathcal{X}$ is denoted by $|\mathcal{X}|$. A function $\mathsf{f}(\cdot)$ (either deterministic or randomized) is denoted by Sans-serif letters. $U_{\mathcal{X}}$ denotes uniform distribution over $\mathcal{X}$, and U_ℓ denotes uniform distribution over $\{0,1\}^\ell$. We use "$\|$" to denote concatenation. All logarithms are in base 2. A Markov chain among random variables X, Y, and Z, is denoted by $X - Y - Z$, and the corresponding probabilities satisfy $P(yz|x) = P(y|x) \cdot P(z|y)$. A sequence of random variables is denoted by $X^n = (X_1, X_2, ..., X_n)$.

The statistical distance between X and Y over $\mathcal{R}$ is defined as $\mathbf{SD}(X,Y) = \frac{1}{2}\sum_{r\in\mathcal{R}} |P[X=r] - P[Y=r]|$. The min-entropy of a random variable is a measure of the number of its extractable random bits, and is given by $H_\infty(X) = -\log(\max_x P_X(x))$. The maximum number of extractable random bits from a random variable is given by its *smooth min-entropy* [107] defined as $H^\epsilon_\infty(X) = \max_{Y:SD(X,Y)\leq\epsilon} H_\infty(Y)$.

A (γ,ε) *strong seeded extractor* is a family of functions $\mathsf{Ext} : \mathcal{X}\times\mathcal{S} \to \mathcal{Y}$, that for any X with $H_\infty(X) \geq \gamma$, we have $\mathbf{SD}((S, \mathsf{Ext}(X,S)), (U_\ell, S)) \leq \varepsilon$, where S is uniformly sampled from $\mathcal{S}$. A special class of extractors is *pairwise Universal Hash Family (UHF)* [76]. A family $\{\mathsf{h}_s | s \in \mathcal{S}\}$ of functions $\mathsf{h}_s : \mathcal{X} \to \mathcal{Y}$ is a pairwise UHF if for any $x \neq x'$, and all $\alpha, \beta \in \mathcal{Y}$, $\Pr[\mathsf{h}_S(x) = \alpha \wedge \mathsf{h}_S(x') = \beta] \leq \frac{1}{|\mathcal{Y}|^2}$, where S denotes a random seed chosen uniformly from $\mathcal{S}$. In our construction, we use a UHF called $\mathcal{H}_{mult}$: let t and b be two integers and $t < b$. Then the hash family $\mathcal{H}_{mult} = \{h_s : s \in \{0,1\}^b \backslash \{0^b\}\}$ is defined as $h_s(x) = (x\|\mathbf{0}^{t-b}) \odot s$. Here, $\odot$ is multiplication over $GF(2^b)$.

5.2.2 Channels

A discrete memoryless channel (DMC) is a probabilistic function $\mathsf{W} : \mathcal{X} \to \mathcal{Y}$ that maps an element of $\mathcal{X}$ to a probability distribution over $\mathcal{Y}$, and is specified by the transition probabilities $P_{Y|X}$. The transition

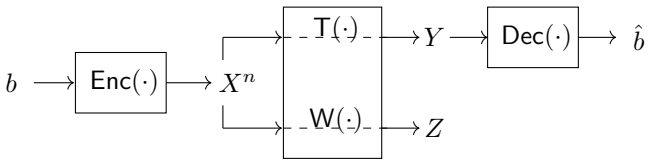

Figure 5.1: Wiretap Channel Model

probability matrix of the channel represents the transition probability of the channel from input x to output y. For a codeword of length n channel symbol $\mathsf{W}^n : \mathcal{X}^n \to \mathcal{Y}^n$ and the transition probability is $P^n_{Y|X}(y^n|x^n) := \Pi^n_{i=1} P_{Y|X}(y_i|x_i)$. A DMC $\mathsf{W} : \mathcal{X} \to \mathcal{Y}$ is said to be *weakly symmetric* if every row of the transition matrix is a permutation of every other row, and the sum of elements in each column is the same for all columns [30].

The *capacity of a transmission channel* W is denoted by $\mathbf{C}_{\mathsf{W}}$, and is the highest rate in bits per channel use at which information can be sent over the channel with error probability approaching zero as information size grows. When $\mathsf{W} : \mathcal{X} \to \mathcal{Y}$ is a weakly symmetric channel, its capacity is given in [30, Theorem 8.2.1] by $\mathbf{C}_{\mathsf{W}} = \log|\mathcal{Y}| - H(\text{row of transition matrix})$.

Wiretap channel model. In a general wiretap (also called broadcast [34]) channel $\mathsf{WT} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ (See Figure 5.1), a sender is connected to the receiver through the *main* channel $\mathsf{T} : \mathcal{X} \to \mathcal{Y}$, and to the eavesdropper through a second channel $\mathsf{W} : \mathcal{X} \to \mathcal{Z}$, called the *wiretapper's channel*; the transition probability of the channel pair is described by $P_{YZ|X}$, where $X \in \mathcal{X}, Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$. In Wyner's original model [143], the wiretapper's channel is a *degraded* version of the main channel, and the Markov chain $X - Y - Z$ holds.

A wiretap encoder is a *randomized encoding* algorithm $\mathsf{Enc} : \mathcal{M} \to \mathcal{X}^n$ that encodes a message $b \in \mathcal{M}$, to a codeword X^n. The receiver receives $Y^n = \mathsf{T}(\mathsf{Enc}(b))$ and uses a deterministic decoding function $\mathsf{Dec}(\cdot)$ to recover a message $\hat{b}$. The decryption will be in error if $\hat{b} \neq b$. A randomized encoding system must provide (i) reliability for the receiver, and (ii) secrecy against the eavesdropper.

Reliability: For $0 < \sigma < 1$, we define reliability as follows:

$$\max_{b \in \mathcal{M}} \Pr[(b \neq \hat{b})] < \sigma \tag{5.1}$$

Distinguishing security. We use the following distinguishing-based definition for secrecy.

$$\begin{aligned} Adv^{ds}(\mathsf{Enc}; \mathsf{W}) &= \max_{b_0, b_1} \mathbf{SD}(\mathsf{W}(\mathsf{Enc}(b_0)); \mathsf{W}(\mathsf{Enc}(b_1))) \\ &\leq 2 \max_{b} \mathbf{SD}(\mathsf{W}(\mathsf{Enc}(b)); U_{\mathcal{Z}}) < \epsilon \end{aligned} \tag{5.2}$$

for any $0 < \epsilon < 1$. This is the strongest security notion for confidentiality in cryptography, and is equivalent to semantic security [58].

Secrecy rate: The rate of an encoding scheme for a given wiretap channel is defined as $\mathbf{R}(n) = \frac{\log |\mathcal{M}|}{n}$, where n is the number of channel use. A rate $\mathbf{R}$ for a wiretap channel W is *achievable* if there exists a family of wiretap codes indexed by the codeword length, n, such that as $n \to \infty$, $\sigma(n)$ and $\epsilon(n)$ in the *reliability* and *distinguishing security* definition approach zero, and $\mathbf{R}(n)$ approaches $\mathbf{R}$. From now on, for simplicity of the representation, we abuse the notation and denote $\mathbf{R}(n)$, $\sigma(n)$ and $\epsilon(n)$ by $\mathbf{R}_n$, σ_n and ϵ_n respectively[2].

The *secrecy capacity* of a wiretap channel is the highest achievable rate as defined above, and has been proved [34] to be $\mathbf{C}_s = \max_{V-X-YZ}(I(V;Y) - I(V;Z))$, where the maximum is taken over all random variables V satisfying $V - X - YZ$.

For a degraded wiretap channel ($X - Y - Z$ holds), when the main channel T and the Eve's channel W are weakly symmetric, the capacity is achieved for uniform distribution over X, and the capacity is given by $\mathbf{C}_s = \mathbf{C}_{\mathsf{T}} - \mathbf{C}_{\mathsf{W}}$ [84][3].

5.3 Wiretap channel with shared key

We consider a discrete memoryless wiretap channel $\mathsf{WT} : \mathcal{X}^n \to \mathcal{Y}^n \times \mathcal{Z}^n$ where $\mathsf{T}(\cdot)$ is the main channel, and $\mathsf{W}(\cdot)$ is the wiretapper's channel. The sender wants to send a private message $b \in \mathcal{M}$ to the receiver. A uniformly distributed secret key $K \in \mathcal{K}$ with rate $\mathbf{R}_K = \frac{log|\mathcal{K}|}{n}$ is shared between the sender and the receiver.

Definition 5.1. For a wiretap channel with shared secret key rate $\mathbf{R}_K > 0$, a secrecy rate $\mathbf{R} > 0$ is achievable if there exists a family of wiretap codes with rate $\mathbf{R}_n$, and reliability and security parameters σ_n and ϵ_n, respectively (expressions (5.1) and (5.2)), such that as $n \to \infty$, we have $\sigma_n, \epsilon_n \to 0$, and $\mathbf{R}_n \to \mathbf{R}$. The secrecy capacity $\mathbf{C}_s$ is the supremum of all achievable secrecy rates.

Keyed seeded encryption: Modular constructions of wiretap codes use seeded extractors, and are referred to as *seeded encryption* [11]. Seeded encryption schemes are randomized coding schemes without a shared key. The seed is a random string that is shared over the main channel reliably, and is assumed to be known by the eavesdropper. The following extends the definition of seeded encryption to include the shared key of the sender and the receiver.

Definition 5.2. For a wiretap channel with a shared key as described above, an $(n, \sigma_n, \epsilon_n)$ *keyed seeded encryption scheme* ($0 < \sigma_n, \epsilon_n < 1$) consists of a seeded encryption algorithm $\mathsf{SKEnc} : \mathcal{S} \times \mathcal{K} \times \mathcal{M} \to \mathcal{X}^n$,

[2]We will also use b_n and $\hat{b}_n$ instead of $b(n)$ and $\hat{b}(n)$ later.

[3]In [84] the result is stated for symmetric DMCs. Using [84, Theorem 4] implies that the same result holds when both channels are weakly symmetric.

and a seeded decryption algorithm $\mathsf{SKDec} : \mathcal{S} \times \mathcal{K} \times \mathcal{Y}^n \to \mathcal{M}$, that satisfy the following reliability and distinguishing security properties:

Reliability.

$$\mathop{\mathbb{E}}_{K,S}\left[\max_{b\in\mathcal{M}} \Pr[\mathsf{SKDec}_S(\mathsf{T}(\mathsf{SKEnc}_S(b,k)) \neq b]\right] < \sigma_n$$

Distinguishing security.

$$\begin{aligned}
&Adv^{ds}(\mathsf{SKEnc};\mathsf{W}) = \mathop{\mathbb{E}}_{K}[\max_{b_0,b_1} \\
&\mathbf{SD}((S,\mathsf{W}(\mathsf{SKEnc}_S(b_0,k)));(S,\mathsf{W}(\mathsf{SKEnc}_S(b_1,k))))] \\
&\leq 2\mathop{\mathbb{E}}_{K}\left[\max_{b} \mathbf{SD}((S,\mathsf{W}(\mathsf{SKEnc}(b,k)));(S,U_{\mathcal{Z}^n}))\right] < \epsilon_n
\end{aligned}$$

Remark. *Our definition of reliability uses the worst-case error probability, and the distinguishing-based security definition does not assume a specific probability distribution for messages. It is easy to see that the upper-bounds in [78] and [113] for achievable rate and secrecy capacity will also hold for our definitions that are more demanding (i.e., our notions of reliability and security imply those of these latter works).*

We recall the following theorem that gives the capacity of a wiretap channel with shared key, when message space is uniformly distributed.

Theorem 5.1 ([78])**.** *The secrecy capacity of the general wiretap channel with a shared key of rate* $\mathbf{R}_K$ *under reliability and security conditions given by [78, Eq.(1), Eq.(2)] respectively, is*

$$\max_{U-V-X-YZ} \min\big([I(V;Y|U) - I(V;Z|U)]^+ + \mathbf{R}_K, I(V;Y)\big),$$

where $[a]^+$ *is the maximum between 0 and a. The secrecy capacity of a degraded wiretap channel with shared secret key is therefore* $\max_{X-Y-Z} \min\big(I(X;Y) - I(X;Z) + \mathbf{R}_K, I(X;Y)\big)$.

In the next section, we describe our seeded encryption construction for keyed wiretap channel, and show that its rate achieves the above capacity for weakly symmetric channels.

5.4 The capacity-achieving construction

Overview: In a keyed wiretap channel setting, the sender and receiver have two resources to achieve confidentiality: a shared secret key, and the fact that the wiretapper's channel is noisier than the main channel. Each of these resources can be optimally and independently used for providing confidentiality, and so one would expect that the capacity of a keyed wiretap channel to be the sum of these two capacities. In

[78], it is shown that the secrecy capacity of this setting is indeed the sum of the capacities of the two cases. Note that the shared key is available at the sender and the receiver before transmission starts, while the noise advantage is provided once the message is transmitted over the channel. The desired scheme should use the shared key at the sender for partially masking the message such that in combination with the channel noise, the transmitted message is perfectly hidden from the wiretapper. We propose a scheme that extends a wiretap coding construction, known as **HtE** (Hash-then-Encode) [120] that allows us to take advantage of the available key rate. We call the new construction **KHtE** (Keyed Hash-then-Enocde). We first introduce the construction and show how to choose its parameters for the desired security and reliability guarantees, and then prove for a weakly symmetric wiretap channel, the secrecy rate of the construction approaches the secrecy capacity of the system as the code length increases.

5.4.1 The KHtE construction

For a message space $\mathcal{M} = \{0,1\}^b$, a wiretap channel $\mathsf{WT} : \{0,1\}^\ell \to \{0,1\}^e \times \{0,1\}^d$, and the shared key of t bits, let $\mathsf{h}_s : \{0,1\}^t \to \{0,1\}^b$ be a family of pairwise universal hash functions, and $\mathsf{ECC} : \{0,1\}^{\hat{b}} \to \{0,1\}^{n.\ell}$ be a family of error-correcting codes for the main channel. Let a random secret key $K \in \{0,1\}^t$ and a random seed S be shared by the sender and the receiver. The seed S can be generated by the sender and sent to the receiver over a reliable (public) channel. Note that publicly shared randomness is also used in random code constructions and is not considered in computing the secrecy rate of the construction. The seed length of our proposed construction is significantly shorter than the public randomness in this latter case (public randomness in random coding is exponential in n, while in our proposed construction the seed length is $n.\log|\mathcal{M}|$). Our proposed keyed seeded encryption function denoted by $\mathbf{KHtE}[\mathsf{h}_s, \mathsf{ECC}]$, uses a UHF and a capacity-achieving error correcting code (ECC) with encoding and decoding function pairs $\mathsf{ECC.enc}$ and $\mathsf{ECC.dec}$, respectively. For a message $b \in \mathcal{M}$, the encryption (randomized encoding with secret key) and decryption (decoding with secret key) functions are defined as follows.

1. *Encryption*:

$$\mathbf{KHtE.enc}(S, K, b) = \mathsf{ECC.enc}((\mathsf{h}_S(K) \oplus b) \| U_{\hat{b}-b}).$$

2. *Decryption*: For a received vector Y we have

$$\mathbf{KHtE.dec}(S, K, Y) = \mathsf{ECC.dec}(Y) \oplus \mathsf{h}_S(K).$$

Theorem 5.2. *Consider a degraded weakly symmetric wiretap channel (both channels are weakly symmetric) with the main channel* $\mathsf{T} : \{0,1\}^\ell \to \{0,1\}^e$ *and the wiretapper's channel* $\mathsf{W} : \{0,1\}^\ell \to \{0,1\}^d$*, a message*

space $\mathcal{M} = \{0,1\}^{b_n}$ *and a shared secret key with a non-zero rate* $\mathbf{R}_K$. *Let* $\mathsf{ECC}:\{0,1\}^{\hat{b}_n} \to \{0,1\}^{n.\ell}$, $(\hat{b}_n \geq b_n)$ *be a family of capacity-achieving error-correcting codes for channel* T *such that the maximum error probability for length* n *(channel use) code is bounded by* σ_n, *and let* $\mathsf{h}_s : \{0,1\}^{n.\mathbf{R}_K} \to \{0,1\}^{b_n}$ *be a pairwise universal hash function such that* $n.\mathbf{R}_K < b_n$. *Then the* **KHtE** *construction gives a* $(n, \sigma_n, 4\epsilon_n)$ *keyed seeded encryption scheme (Definition 5.2) that achieves secrecy capacity of the channel, if*

$$b_n \leq n.\mathbf{R}_K + \hat{b}_n - n.\mathbf{C}_{\mathsf{W}} - \sqrt{n}\log(2^\ell + 3).\sqrt{2log\frac{1}{\epsilon_n}} + 2log\epsilon_n. \tag{5.3}$$

Here, $\mathbf{C}_{\mathsf{W}}$ *is the capacity of the wiretapper's channel.*

Proof overview: To prove Theorem 5.2, we first prove Lemma 5.1. The lemma shows that a uniformly distributed shorter key can be expanded to a longer key that is close to uniform, using the channel noise. To complete the proof, we show that when parameters of **KHtE** are chosen with respect to Lemma 5.1, the rate of **KHtE** achieves the capacity expression of Theorem 5.1 as n grows.

KHtE in practice: For a wiretap setting with shared key rate $\mathbf{R}_K$, Theorem 5.2 gives an asymptotically tight upper-bound on the length of the message with concrete reliability and security guarantees. To use the construction in practice, one determines the minimum n for the error correcting code family ECC of the main channel T, such that the decoding error of the code with length n (channel symbol) is $\sigma_n \leq \sigma$. The corresponding input size for this error correcting family is $\hat{b}_n$. Then for a chosen ϵ_n, expression (5.3) gives the maximum length of message b_n that can be encrypted.

Lemma 5.1. *Let* $\{\mathsf{h}_s | s \in \mathcal{S}\}$ *be a family of pairwise UHFs* $\mathsf{h}_s : \{0,1\}^t \to \{0,1\}^b$, *where* $b \geq t$ *and* $\mathsf{f} : \{0,1\}^{\hat{b}} \to \{0,1\}^\ell$ *be an injective function* ($\ell \geq \hat{b}$), $\mathsf{W} : \{0,1\}^\ell \to \{0,1\}^d$ *be a weakly symmetric channel, where* $\max_{x\in\{0,1\}^\ell, z\in\{0,1\}^d} Pr(\mathsf{W}(x) = z) \leq 2^{-\nu}$, *and* $K \in \{0,1\}^t$ *be a uniformly random variable such that* $b \leq t + \nu + \hat{b} - d + 2\log\epsilon$. *Then*

$$\mathbf{SD}\left((S, \mathsf{W}(\mathsf{f}(h_S(K) \| U_{\hat{b}-b}))); (S, U_\ell)\right) \leq \epsilon. \tag{5.4}$$

Proof. Let P_V be the distribution of the channel's output for a reference input $\mathbf{r} \in \{0,1\}^\ell$. Then for the random variable $V \in \{0,1\}^d$ with distribution P_V we have $H_\infty(V) \leq \nu$. Since W is weakly symmetric, the distribution of the channel output for other inputs (not equal to $\mathbf{r}$) in $\{0,1\}^\ell$ can be obtained by applying a permutation on the channel output set with distribution P_V (i.e., a permutation on V). Therefore, $\mathsf{W}(\mathsf{f}(\mathsf{h}_S(K) \| U_{\hat{b}-b})) = \tau_{\mathsf{f}((\mathsf{h}_S(K) \| U_{\hat{b}-b})}(V)$, where $\tau_x(V)$ is the permutation on the channel output set with distribution P_V that results in the output distribution that is generated by x input to the channel.

According to [76, claim 2], any distribution over a finite set Δ with collision probability $\frac{1+2\epsilon^2}{|\Delta|}$ is ϵ-close

to the uniform distribution. We now bound the collision probability of $(S, \tau_{\mathsf{f}((\mathsf{h}_S(K)\|U_{\hat{b}-b})}(V))$ as follows:

$$\begin{aligned}
&\Pr[\Big(S, \tau_{\mathsf{f}((\mathsf{h}_S(K)\|U_{\hat{b}-b})}(V)\Big) = \Big(S^{'}, \tau_{\mathsf{f}((\mathsf{h}_{S'}(K')\|U'_{\hat{b}-b})}(V')\Big)] \\
&= \Pr[S = S^{'}] \cdot \Pr[U_{\hat{b}-b} = U^{'}_{\hat{b}-b}] \cdot \\
&\qquad \Pr[\tau_{\mathsf{f}((\mathsf{h}_S(K)\|u)}(V) = \tau_{\mathsf{f}((\mathsf{h}_S(K')\|u)}(V')],
\end{aligned}$$

where u is uniformly sampled from $\{0,1\}^{\hat{b}-b}$. Note that since f is injective, $\mathsf{h}_S(K)\|u = \mathsf{h}_S(K)\|u'$, if and only if $u = u'$. Thus

$$\begin{aligned}
&\Pr[\Big(S, \tau_{\mathsf{f}((\mathsf{h}_S(K)\|U_{\hat{b}-b})}(V)\Big) = \Big(S^{'}, \tau_{\mathsf{f}((\mathsf{h}_{S'}(K')\|U'_{\hat{b}-b})}(V')\Big)] \\
&\leq \tfrac{2^{b-\hat{b}-k}}{|\mathcal{S}|} \cdot \Big(2^{-\nu} \\
&\qquad + \Pr[\tau_{\mathsf{f}((\mathsf{h}_S(K)\|u)}(V) = \tau_{\mathsf{f}((\mathsf{h}_S(K')\|u)}(V') | K \neq K']\Big).
\end{aligned}$$

Now $\Pr[\tau_{\mathsf{f}((\mathsf{h}_S(K)\|u)}(V) = \tau_{\mathsf{f}((\mathsf{h}'_S(K')\|u)}(V') | K \neq K'] =$

$$\begin{aligned}
&\textstyle\sum_{v\in\{0,1\}^d} \sum_{v'\in\{0,1\}^d} \Big(\Pr[V = v] \cdot \Pr[V' = v'] \cdot \\
&\qquad \Pr[\tau_{\mathsf{f}((\mathsf{h}_S(K)\|u)}(v) = \tau_{\mathsf{f}((\mathsf{h}_S(K')\|u)}(v') | K \neq K']\Big).
\end{aligned}$$

$\Pr[\tau_{\mathsf{f}((\mathsf{h}_S(K)\|u)}(v) = \tau_{\mathsf{f}((\mathsf{h}_{S'}(K')\|u)}(v')]$ is either zero, or is non-zero for $\mathsf{f}(\mathsf{h}_S(K)) = x_1$ and $\mathsf{f}(\mathsf{h}_S(K')) = x_2$. Since f is injective, this is equivalent to $\mathsf{h}_S(K) = \mathsf{f}^{-1}(x_1)$ and $\mathsf{h}_S(K') = \mathsf{f}^{-1}(x_2)$, and since $\mathsf{h}_S(\cdot)$ is pairwise independent, we have

$$\begin{aligned}
&\Pr[\tau_{h_S(K)\|u}(v) = \tau_{h_S(K')\|u}(v')] \leq \\
&\Pr[\mathsf{h}_S(K) = \mathsf{f}^{-1}(x_1) \wedge \mathsf{h}_S(K') = \mathsf{f}^{-1}(x_2) | K \neq K'] \leq 2^{-2b}.
\end{aligned}$$

Finally,

$$\begin{aligned}
&\Pr[\tau_{\mathsf{h}_S(K)}(V) = \tau_{\mathsf{h}_S(K')}(V')] \\
&\quad \leq 2^{-2b} \cdot \textstyle\sum_v \sum_{v'} \Pr[V = v] \cdot \Pr[V' = v'] \leq 2^{-2\nu-2b}.
\end{aligned}$$

Therefore, the collision probability can be bounded as:

$$\begin{aligned}
&\Pr[\big(S, \tau_{\mathsf{f}(\mathsf{h}_S(K))}(V)\big) = \Big(S^{'}, \tau_{\mathsf{f}(\mathsf{h}_{S'}(K'))}(V^{'})\Big)] \\
&\quad \leq \tfrac{1}{|\mathcal{S}|2^d} \cdot \left(2^{-(t+\nu+\hat{b}-b-d)} + 2^{-(2\nu+b+\hat{b}-d)}\right).
\end{aligned} \tag{5.5}$$

Since $b \leq t + \nu + \hat{b} - d + 2\log\epsilon$, the first term $2^{-(t+\nu+\hat{b}-b-d)} \leq \epsilon^2$ and since $2t \leq 2b$, the second term is also bounded by ϵ^2. Therefore, the collision probability is bounded by $\frac{2\epsilon^2}{|\mathcal{S}|2^d} \leq \frac{1+2\epsilon^2}{|\mathcal{S}|2^d}$ and the statistical distance is bounded by ϵ. □

Proof of Theorem 2. We need to prove (i) reliability, (ii) security and (iii) capacity-achieving property of the scheme for the given channel.

Reliability: Since the ECC in the construction is capacity-achieving, we have $\lim_{n\to\infty} \sigma_n = 0$. Thus, the decryption error of **KHtE** is σ_n, which approaches 0 as n grows. Moreover, $\lim_{n\to\infty} \mathbf{R}_{\mathsf{ECC}} = \lim_{n\to\infty} \frac{\hat{b_n}}{n} = C_{\mathsf{T}}$.

Security: To prove security of the construction, let the distribution $\mathsf{W}^n(\mathbf{r}^n)$ for a reference $\mathbf{r}^n \in \{0,1\}^{n.\ell}$ be V^n. Since W is weakly symmetric and W^n is discrete memoryless, then W^n is weakly symmetric, and the output of the channel for an input $x^n \neq \mathbf{r}^n$ is a permutation of V^n denoted by $\tau_{x^n}(V^n)$. Since the channel is memoryless, V^n is n independent identically distributed (IID) samples of W output, and $H(V^n) = n \cdot H(V)$. Let V_{ϵ_n} be the random variable over $\{0,1\}^{n.\ell}$ that satisfies the smooth min-entropy of V^n, that is $\mathbf{SD}(V_{\epsilon_n}; V^n) \leq \epsilon_n$ and $H_\infty^{\epsilon_n}(V^n) = \max_{\hat{V}_{\epsilon_n}:\mathbf{SD}(V^n;\hat{V}_{\epsilon_n})\leq\epsilon_n} H_\infty(\hat{V}_{\epsilon_n}) = H_\infty(V_{\epsilon_n})$. From [107, Lemma 4.2], we have

$$H_\infty(V_{\epsilon_n}) = H_\infty^{\epsilon_n}(V^n) \geq n.H(V) - n\delta_n, \tag{5.6}$$

where $\delta_n = \log(2^\ell + 3).\sqrt{2log\frac{1}{\epsilon_n}/n}$.

Since W is a weakly symmetric channel, $\mathbf{C}_{\mathsf{W}} = d - H(V)$. Then, from (5.3), (5.6),

$$b_n \leq n.\mathbf{R}_K + H_\infty(V_{\epsilon_n}) + \hat{b}_n - n.d + 2log\epsilon_n. \tag{5.7}$$

Now consider an abstract channel $\mathsf{W}_{\epsilon_n} : \{0,1\}^{n.\ell} \to \{0,1\}^{n.d}$, where the output distribution of $\mathbf{r}^n \in \{0,1\}^{n.\ell}$ is V_{ϵ_n} and for any other $x^n \neq \mathbf{r}^n$, the distribution is given by $\tau_{x^n}(V_{\epsilon_n})$, where τ_{x^n} is a permutation on the output set. This abstract channel W_{ϵ_n} by definition is weakly symmetric.

Suppose $\mathsf{ECC}(\mathsf{h}_S(K) \oplus b \| U_{\hat{b}-b})$ is used as the input to the channel W_{ϵ_n}. From Lemma 5.1, we have

$$\mathbf{SD}\left((S, \tau_{(\mathsf{ECC}(\mathsf{h}_S(K))}(V_{\epsilon_n}) \oplus b \| U_{\hat{b}-b}))); (S, U_{n.\ell})\right) \leq \epsilon_n.$$

On the other hand, since $\mathbf{SD}(V^n, V_{\epsilon_n}) \leq \epsilon_n$, from the triangular inequality it follows that,

$$\mathbf{SD}\left((S, \tau_{(\mathsf{ECC}(\mathsf{h}_S(K))}(V^n) \oplus b \| U_{\hat{b}-b}))); (S, U_{n.\ell})\right) \leq 2\epsilon_n$$

$$\Rightarrow \mathbf{SD}\left((S, \mathsf{W}^n(\mathsf{ECC}(\mathsf{h}_S(K) \oplus b \| U_{\hat{b}-b}))); (S, U_{n.\ell})\right) \leq 2\epsilon_n.$$

Thus, $Adv^{ds}(\mathbf{KHtE}) \leq 4\epsilon_n$ (from the distinguishing advantage in Definition 5.2), and for $\epsilon_n = O(1/n^2)$, the *ds* advantage goes to zero as n grows.

Capacity-achieving: The achievable rate of the construction is b_n/n. We have

$$\begin{aligned} b_n &\leq \hat{b}_n + n.R_K - n.C_W - \sqrt{n}\log(2^\ell + 3).\sqrt{2log\frac{1}{\epsilon_n}} + 2log\epsilon_n \\ &\Rightarrow \frac{b_n}{n} \leq \frac{\hat{b}_n}{n} - C_{\mathsf{W}} - \frac{\sqrt{n}}{n}(\log(2^\ell + 3)) - \frac{2log(\frac{1}{\epsilon_n})}{n} + n.\mathbf{R}_K \\ &\Rightarrow \mathbf{R} \leq \lim_{n\to\infty} \frac{b_n}{n} = (C_{\mathsf{T}} - C_{\mathsf{W}}) + \mathbf{R}_K. \end{aligned}$$

From Shannon's coding theorem, we have $\mathbf{R} \leq I(X;Y)$. Finally, the combination of the latter two inequalities completes the proof:

$$\begin{aligned} \mathbf{R} &\leq \min\big((C_{\mathsf{T}} - C_{\mathsf{W}}) + \mathbf{R}_K, I(X;Y)\big) \\ &= \max_{X-Y-Z} \min\big([I(X;Y) - I(X;Z) + \mathbf{R}_K, I(X;Y)\big), \end{aligned}$$

where the upper bound is achieved when b_n in (5.3) is set to its maximum. □

Concluding remarks. We gave a modular and semantically secure construction of a capacity-achieving wiretap code with shared secret key that has efficient encoding and decoding. This is the only known construction that takes advantage of the shared key and the wiretap channel, and achieves semantic security. The construction works for weakly symmetric channels. Extending this result to more general discrete memoryless channels, and extending other known modular construction of wiretap codes (with semantic security) to support shared secret key, are interesting research questions.

Acknowledgments. This research is in part supported by Natural Sciences and Engineering Research Council of Canada (NSERC), Discovery Grant program.

Chapter 6

Semantically Secure Keyed Wiretap Encoding Schemes[1]

Abstract. In the wiretap model, the sender is connected to the receiver and the eavesdropper through two noisy channels, called the main channel and the wiretapper's channel, respectively. When the main channel is noisier than the wiretapper's channel, a wiretap code can be used to achieve (asymptotically) perfect secrecy and perfect reliability for message transmission. The efficiency of a wiretap code is in terms of its achievable *rate* that is defined as the number of bits that is transmitted reliably and securely, in each use of the channel when the channel is used sufficiently many times. Capacity-achieving constructions provide the highest achievable rate for encoding over a wiretap channel.

In a keyed wiretap channel, the sender and the receiver can also take advantage of a secret key that is shared between them to increase the secrecy rate. We propose a modular construction of a capacity-achieving keyed wiretap code for weakly symmetric channels. The modular construction allows to separate coding for secrecy and coding for reliability, and so can be used with any capacity-achieving error correcting code. The construction optimally uses the available secrecy capacity of the underlying wiretap channel, and its secrecy rate reduces to the key rate if the secrecy rate of this channel is zero. This is the first explicit construction that provides semantic security for any discrete memoryless wiretap channel with binary alphabet input. Our security proof gives an achievability bound on the rate of the construction that can be used to evaluate the efficiency of the construction in the finite-length regime.

[1] The content of this chapter is submitted to the Journal of Cryptology [123].

6.1 Introduction

We study the problem of secure communication from an information-theoretic perspective: Alice and Bob are connected by a noisy channel that is eavesdropped by a computationally unbounded adversary Eve; Alice wants to send a message reliably and securely over the channel. Reliability means the receiver should be able to recover the message with high probability, and the security condition implies Eve not to obtain more than negligible information about the message by eavesdropping the channel.

Shannon considered the above problem and proposed the first formal model and definition of the information-theoretic secure communication [115],[116]. His approach toward the secure communication problem is to meet the reliability and security requirements, consecutively. That is, first remove the noise from the channel by using error correcting codes, and then provide security against the eavesdropper by using an OTP (One-Time Pad) encryption system that uses a shared key. Despite the theoretical importance of this solution as the first and the only encryption scheme with perfect secrecy, the practicality of this solution is questioned since each message needs to be encrypted with a fresh shared key whose entropy is at least as much as the message entropy.

The information-theoretic approach to physical layer security is pioneered by Wyner [143]. He introduced the wiretap channel to model a setting in which Alice's transmission to Bob is also received by Eve through a second channel, which is a degraded (i.e., noisier) version of Bob's channel (See Figure 6.1(ii)). Wyner's brilliant idea was to use the extra noise at Eve's reception to provide confidentiality. Csiszár and Körner [34] extended this model to the case that Alice is connected to Bob and Eve through two independent channels: *receiver's channel* (also called the *main channel*), and the *wiretapper's channel*, respectively (Figure 6.1(i)), and proved that secure and reliable communication is possible as long as the main channel is more "capable" (See expression (12) in [34]) than the wiretapper's one.

The rate of secure message transmission in a wiretap setting is defined as the number of bits securely transmitted in each application of the channel. The secrecy capacity is the highest achievable rate of transmitting the message from Alice to Bob satisfying reliability and security conditions. The explicit capacity-achieving schemes for Wyner's setup are known only for degraded channels. The early constructions of capacity-achieving wiretap codes use special classes of codes e.g., LDPC codes in [98, 136], and polar codes in [87]. A modular construction of a wiretap code [66] separates randomization for achieving secrecy from error correction for reliability, and can be used with any capacity-achieving error correcting code. Bellare et al. [11] strengthened the security of wiretap codes by introducing semantic security, and proposed a modular construction that is capacity-achieving and provides semantic security. Other modular constructions of capacity-achieving wiretap codes with semantic security are by Tyagi et al.[138] for Gaussian wiretap

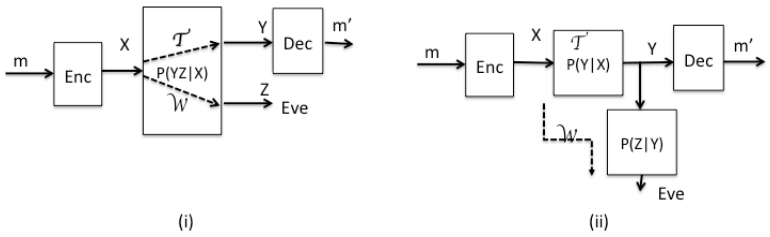

Figure 6.1: (i) Wiretap channel with the main channel T and the wiretapper's channel W; (ii) Degraded wiretap channel with the main channel T and the wiretapper's channel W that is the concatenation of two channels.

channels, and Sharifian et al. [120] for discrete symmetric wiretap channels.

A very attractive aspect of these constructions is that Alice and Bob do not need a shared secret key. When the wiretapper's channel is noisier than the main channel, wiretap codes increase the randomization of the noise difference in the wiretapper's view by using sufficient randomization in the encoder and provide asymptotic perfect secrecy for the communication. Modular constructions are even more appealing from the practical viewpoint due to their flexibility in the choice of error correcting codes. The drawback of wiretap encoding schemes, however, is that secure communication is not possible when the main channel is noisier than the wiretapper's channel, and the achievable rate of secure communication is small when the difference between the quality of the main and the wiretapper's channel is small.

A natural question is if Wyner's approach can be combined with Shannon's OTP encryption system: that is, use the secret key to achieve higher rate, while taking advantage of the noise in Eve's channel. Alternatively, the noise in Eve's channel is used to reduce the key length of the OTP encryption scheme. As a result, Shannon's model of perfect secrecy [116] and Wyner's model [143] can be understood under a unified framework that combines the conventional information-theoretic security approaches. Yamamoto [145] initiated the study of the wiretap channel with a shared secret key. This model is studied in a few works including [78, 94, 113]. The secrecy capacity of a general wiretap channel with a shared secret key is given in [78] and the first explicit construction of a wiretap code with a shared secret key is given in [117]. This construction is modular and is shown to provide semantic security, and achieve the secrecy capacity when the main channel and Eve's channel are weakly symmetric. The construction, however, requires the key rate to be positive.

In this work, we improve the construction of [117] to provide secure encoding over the keyed wiretap channels that reduces to a conventional wiretap code when the key rate is zero. We show the proposed construction is semantically secure for discrete memoryless channels with binary alphabet input. No other known explicit wiretap code or keyed wiretap code is shown to provide semantic security for this wide class of channels. The randomization of the proposed construction is made explicit by transmitting a random seed

publicly to the receiver. We show the secrecy capacity of weakly symmetric wiretap channels with a shared key (and also the conventional wiretap channels) is asymptotically achieved by our proposed construction when the same seed is used for the encryption of multiple messages (message blocks) as the number of blocks goes to infinity. Using the same seed for the encryption of multiple blocks is called *seed recycling*, which is first introduced in [11] to show their proposed construction achieves the secrecy capacity of binary input symmetric channels asymptotically. We show the seed recycling technique can also be used for the encryption of the finite number of message blocks by providing a security guarantee on the encryption of individual blocks encrypted using the same seed.

Organization: The backgrounds are reviewed in Section 6.2. The definitions of wiretap channel and keyed wiretap channel, and the corresponding existing constructions, are given in Section 6.3. In Section 6.4, we propose our keyed wiretap encryption scheme and prove its reliability, security and capacity-achieving properties. In Section 6.5, we study the proposed construction in two special cases, namely, when the shared key doesn't exist, and when the wiretap channel secrecy capacity is zero. We then compare our construction in these special cases with the best known results. In Section 6.6, we elaborate on the application of the construction in practical settings with finite-length messages. Related works are addressed in Section 6.7, and we conclude this work in Section 6.8.

6.2 Preliminaries

6.2.1 Notations

A function $\mathsf{F}(\cdot)$ (either deterministic or randomized) is denoted by Sans-serif letters, and bold capital letters denote matrices. Random variables are denoted by capital letters and their corresponding realizations are denoted by lowercase letters. Sets are denoted by calligraphic letters e.g., $\mathcal{X}$ and the size of $\mathcal{X}$ is denoted by $|\mathcal{X}|$. By $x \xleftarrow{\$} \mathcal{X}$ we mean element x is chosen with probability $\frac{1}{|\mathcal{X}|}$. A sequence of random variables is $X^n = (X_1, X_2, \ldots, X_n)$, and a sequence of realizations of random variables is $x^n = (x_1, x_2, \ldots, x_n)$. When the items of a sequence are dependent on their index, we use "(n)" as a superscript, e.g., $\lambda^{(n)}$.

$\Pr[X = x]$ denotes the probability that the random variable X is equal to x. A probability distribution over X is denoted by P_X, and $P_X(x)$ is an alternative notation for $\Pr[X = x]$. The uppercase U is reserved for uniform distribution, and $U_{\mathcal{X}}$ denotes uniform distribution over $\mathcal{X}$, and U_ℓ denotes uniform distribution over $\{0,1\}^\ell$. To denote concatenation, we use "$\|$". All logarithms are in base 2.

A Markov chain among random variables X, Y, and Z, is denoted by $X - Y - Z$, and probabilities satisfy $P(yz|x) = P(y|x) \cdot P(z|y)$.

For two random variables X and Y, P_{XY} denotes their joint distribution, and $P_{X|Y}$ denotes the conditional distribution of X when Y is given.

For a random variable $X \in \mathcal{X}$ with distribution $P_X(x)$, Shannon entropy is $H(X) = -\sum_{x\in\mathcal{X}} P_X(x) \log P_X(x)$. The *min-entropy* $H_\infty(X)$ is given by $H_\infty(X) = -\log(\max_x(P_X(x)))$. The *average conditional min-entropy* [44] is commonly defined as,

$$\tilde{H}_\infty(X|Y) = -\log \mathbb{E}_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} P_{X|Y}(x|y).$$

The maximum number of extractable random bits from a random variable is given by its *smooth min-entropy*, which is introduced in [107] as:

$$H^\epsilon_\infty(X) = \max_{Y:SD(X,Y)\leq\epsilon} H_\infty(Y).$$

Lemma 6.1. *[107] Let $X^n = X_1, X_2, \ldots, X_n$ be n independent random variables over $\mathcal{X}$, then:*

$$H^\epsilon_\infty(X^n) \geq H(X^n) - n.\delta,$$

where $\delta > 0$ and $\epsilon = \epsilon(\delta, n, |\mathcal{X}|) = 2^{\frac{-n\delta^2}{2\log^2(|\mathcal{X}|+3)}}$.

The *statistical distance* of two random variables is defined as follows. For $X, Y \leftarrow \Omega$,

$$\mathbf{SD}(X;Y) = \frac{1}{2}\sum_{\omega\in\Omega} |\Pr(X=\omega) - \Pr(Y=\omega)|.$$

We say X and Y are ϵ-close if $\mathbf{SD}(X,Y) \leq \epsilon$.

Lemma 6.2. *For any two random variables X and Y over Ω, and every possibly randomized function $\mathsf{F}(\cdot)$, $\mathbf{SD}(\mathsf{F}(X);\mathsf{F}(Y)) \leq \mathbf{SD}(X;Y)$. The equality holds when $\mathsf{F}(\cdot)$ is injective.*

6.2.2 Communication channels

A discrete memoryless channel (DMC) CH is a probabilistic function that is specified by a tuple $\langle \mathbf{CH}, \mathcal{X}, \mathcal{Y}\rangle$, where $\mathcal{X}$ and $\mathcal{Y}$ are the domain and co-domain of the function, respectively, and $\mathbf{CH}$ is a *transition probability matrix* with rows and columns labelled with elements of $\mathcal{X}$ and $\mathcal{Y}$, respectively, and for $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $\mathbf{CH}(x,y) = P_{Y|X}(y|x)$. An input with probability distribution P_X generates an output with probability distribution P_Y, where $P_Y(y) = \sum_{x\in\mathcal{X}} P_X(x)P_{Y|X}(y|x)$. The channel can be written without explicit mention of the channel's transition matrix as a probabilistic function $\mathsf{CH} : \mathcal{X} \to \mathcal{Y}$, where $\Pr(\mathsf{CH}(x) = y) = \mathbf{CH}(x,y)$. The probabilistic nature of the channel has been used by Wyner [143] as a source of randomness

to obstruct the view of the adversary and provide secrecy for communication. In Section 6.4, we treat the channel as a source of randomness and use extractors to extract this randomness.

To transmit a codeword of length n, the channel is used n times. This is shown by $\mathsf{CH}^n\langle\mathbf{CH}^{\otimes n}, \mathcal{X}^n, \mathcal{Y}^n\rangle$. The transition probability of the n times application of a discrete memoryless channel is $P^n_{Y|X}(y^n|x^n) := \Pi^n_{i=1}P_{Y|X}(y_i|x_i)$, for $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$ and $\Pr(\mathsf{CH}^n(x^n) = y^n) = \mathbf{CH}^{\otimes n}(x^n, y^n)$.

A DMC is called *symmetric* if the set of outputs can be partitioned into subsets in such a way that for each subset the transition matrix of probabilities (using inputs as rows and output of subsets as columns) has the property that each row is the permutation of other rows and the columns are also permutations of each other. When $\mathcal{X} = \{0, 1\}$, the channel is known as *Binary Input Symmetric Channel* (BISC). When $\mathcal{X} = \{0, 1\}$ and $\mathcal{Y} = \{0, 1\}$, the channel is a Binary Symmetric Channel (BSC). In this channel, input and output sets are $\{0, 1\}$ and an input bit flips with probability $p \leq 1/2$ (crossover probability).

A channel is said to be *weakly symmetric* if every row of the transition matrix is a permutation of every other row, and all the column sums are equal [30].

For a communication channel $\mathsf{CH} : \mathcal{X} \to \mathcal{Y}$ with input $X \in \mathcal{X}$ and output $Y \in \mathcal{Y}$, channel capacity denoted by C_{CH} is defined as:

$$\mathrm{C}_{\mathsf{CH}} = \max_{P_X} I(X; Y).$$

When $\mathsf{CH} : \mathcal{X} \to \mathcal{Y}$ is weakly symmetric, the channel capacity is [30, Theorem 8.2.1]:

$$\mathrm{C}_{\mathsf{CH}} = \log|\mathcal{Y}| - H(\text{row of transition matrix}).$$

Channel coding

A $(\mathcal{M}, n, \sigma)$-code for channel $\mathsf{CH} : \mathcal{X} \to \mathcal{Y}$ consists of an input set $\mathcal{M}$ as well as an encoding function $\mathsf{Enc} : \mathcal{M} \to \mathcal{X}^n$ and a decoding function $\mathsf{Dec} : \mathcal{Y}^n \to \mathcal{M}$, where

$$\mathrm{P}_e = \max_{m \in \mathcal{M}} \Pr[\mathsf{Dec}\big(\mathsf{Enc}(m)\big) \neq m] \leq \sigma.$$

P_e is called the *maximal error probability*. The *average error probability* is defined similarly as $\tilde{\mathrm{P}}_e = 1/|\mathcal{M}| \Pr[\mathsf{Dec}\big(\mathsf{Enc}(m)\big) \neq m]$. The above codes are also called *error correcting codes* (ECC). We say a code is a "good" error correcting code when its decoding is possible with small maximal error probability.

The *rate* of a code is defined as $\frac{\log|\mathcal{M}|}{n}$ and is in terms of information bits per "channel use". A family of codes indexed by n are a family of $(\mathcal{M}^{(n)}, n, \sigma(n))$-codes, and a rate ρ is said to be *achievable* if there exists a family of codes indexed by n with rate $R(n)$, such that $\sigma(n)$, the maximal error probability, tends

to 0 and $R(n)$ tends to ρ as $n \to \infty$. Although $\tilde{\mathrm{P}}_e \leq \mathrm{P}_e$, in channel coding a small average probability of error implies a small maximal probability of error at essentially the same rate [30, Theorem 8.7.1].

Shannon's channel coding theorem [116] shows the channel capacity is the supremum of all achievable rates. Furthermore, it shows there always exists a family of codes indexed by n that achieves an arbitrary rate ρ below the channel capacity.

6.2.3 Randomness extractors

Randomness extractors extract close to uniform randomness from input sequences that are not uniform but have some guaranteed entropy (See [99] and references there, for more information about randomness extractors). Randomness extractors have found wide applications in cryptography. A *randomness source* is a random variable with lower bound on its min-entropy. We say a random variable $X \in \{0,1\}^n$ is an (n,d)-*source* if $H_\infty(X) \geq d$.

Definition 6.1. A function $\mathsf{Ext} : \{0,1\}^n \times \mathcal{S} \to \{0,1\}^\ell$ is a strong (seeded) (d,ϵ)- extractor if for any (n,d)-source X, $\mathbf{SD}((S,\mathsf{Ext}(X,S));(S,U_\ell)) \leq \epsilon$, where S is chosen uniformly from $\mathcal{S}$.

For some applications, we need an *average-case* strong extractor, which is defined with the help of conditional min-entropy. Let V be a random variable possibly dependent on X. Ext is called a (d,ϵ)-average-case strong extractor if for all (V,X) with $\tilde{H}_\infty(X|V) \geq d$, $\mathbf{SD}((S,V,\mathsf{Ext}(X,S));(S,V,U_\ell)) \leq \epsilon$, where S denotes a random seed chosen uniformly from $\mathcal{S}$.

One of the well-known constructions for randomness extractors is obtained by using *(2-)Universal Hash Families* (UHF) via the so called *Leftover Hash Lemma* (LHL), studied since [77].

Definition 6.2. A family $\{\mathsf{h}_s | s \in \mathcal{S}\}$ of functions $\mathsf{h}_S : \mathcal{X} \to \mathcal{Y} = \{0,1\}^\ell$ is a pair-wise UHF if for any $x, x' \in \mathcal{X}$ that $x \neq x'$, $\Pr[\mathsf{h}_S(x) = a \wedge \mathsf{h}_S(x') = b] \leq \frac{1}{|\mathcal{Y}|^2}$, for all $a \in \{0,1\}^\ell$, where S denotes a random seed chosen uniformly from $\mathcal{S}$.

Definition 6.3. A family $\{\mathsf{h}_s | s \in \mathcal{S}\}$ of functions $\mathsf{h}_s : \mathcal{X} \to \mathcal{Y} = \{0,1\}^\ell$ is an XOR-UHF if for any $x, x' \in \mathcal{X}$ that $x \neq x'$, $\Pr[\mathsf{h}_S(x) \oplus \mathsf{h}_S(x') = a] \leq \frac{1}{|\mathcal{Y}|}$, for all $a \in \{0,1\}^\ell$, where S denotes a random seed chosen uniformly from $\mathcal{S}$.

Remark 6.1. *We note that XOR-UHF implies pair-wise UHF. The following family $\mathcal{H}_{mult}$ of finite field multiplication based universal hash functions are well known for their simplicity and versatility [15, Lemma 1]. Let $\mathcal{X} = \{0,1\}^n$, $\mathcal{Y} = \{0,1\}^\ell$ and $\mathcal{S} = \{0,1\}^n$. Then $\mathcal{H}_{mult} = \{\mathsf{h}_s | s \in \mathcal{S}\}$ with $\mathsf{h}_s : \mathcal{X} \to \mathcal{Y}$ defined as follows is an XOR-UHF:*

$$\mathsf{h}_s(x) = (s \odot x)|_\ell, \tag{6.1}$$

where $\odot$ is the finite field multiplication and $|_\ell$ denotes the first most significant ℓ bits of the vector representation of a finite field element.

Lemma 6.3. *[43, Lemma 3.6] Let $\{\mathsf{h}_s | s \in \mathcal{S}\}$ be a family of XOR-universal hash functions $\mathsf{h}_s : \{0,1\}^n \to \{0,1\}^\ell$. If random variables A over $\{0,1\}^n$ and B over $\{0,1\}^\ell$ are independent, then:*

$$\mathbf{SD}((S, \mathsf{h}_S(A) \oplus B); (S, U_\ell)) \leq \sqrt{2^{-(H_\infty(A)+H_\infty(B)-\ell-1)}}.$$

In other words, $\mathbf{SD}((S, \mathsf{h}_S(A) \oplus B); (S, U_\ell)) \leq \epsilon$, as long as $H_\infty(A) + H_\infty(B) \geq \ell + 2\log(\frac{1}{\epsilon}) + 1$. This says, in particular, that $\mathsf{Ext}(S, A, B) = \mathsf{h}_S(A) \oplus B$ is a two-source (seeded) extractor.

6.3 Wiretap channels and keyed wiretap channels

In a general wiretap (also called broadcast [34]) channel $\mathsf{WT} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ (Figure 6.1(i)), a sender is connected to the receiver through the *main* channel $\mathsf{T} : \mathcal{X} \to \mathcal{Y}$, and to the eavesdropper through a second channel $\mathsf{W} : \mathcal{X} \to \mathcal{Z}$, called the *wiretapper's channel*. The transition probability of the channel pair is described by $P_{YZ|X}$ where $X \in \mathcal{X}, Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$. In Wyner's original model [143], the wiretapper's channel is a *degraded* version of the main channel, and the Markov chain $X - Y - Z$ holds (Figure 6.1(ii)).

6.3.1 Wiretap coding

An $(\mathcal{M}, n, \sigma, \epsilon)$-wiretap code for the above described wiretap channel consists of an input set $\mathcal{M}$ as well as an encoder $\mathsf{Enc} : \mathcal{M} \to \mathcal{X}^n$ and a decoder $\mathsf{Dec} : \mathcal{Y}^n \to \mathcal{M}$ with error probability bounded by σ and security advantage bounded by ϵ. We will discuss the definition of error probability and security advantage later in this section. The encoder provides an input $X \in \mathcal{X}$ to the wiretap channel by using a *randomised encoding* (alternatively called *randomised encryption*) algorithm that encodes a message $m \in \mathcal{M}$ to a codeword X^n. This encoded message is transmitted by n applications of the channel. The receiver receives $Y^n = \mathsf{T}(\mathsf{Enc}(m))$ and uses a deterministic decoding function $\mathsf{Dec}(\cdot)$ to recover a message $\hat{m}$. The decryption will be in error if $\hat{m} \neq m$. The wiretapper's view of the communication is denoted by Z. The randomized encoding system is to provide (i) reliability for the receiver, and (ii) (asymptotic) perfect secrecy against the eavesdropper.

Reliability of a wiretap code

Reliability is satisfied at the receiver's side if the receiver recovers the transmitted message correctly with high probability. For source outputs with blocks of length b, Wyner defined the reliability by bounding the

(normalized) average error probability of recovering a uniformly distributed message, that is:

$$\tilde{\mathrm{P}}_e(n) = \frac{1}{b}\Pr[\mathsf{Dec}(Y^n) \neq M] = \frac{1}{b.|\mathcal{M}|}\sum_{m\in\mathcal{M}}\Pr[\mathsf{Dec}(Y^n) \neq m] < \sigma.$$

On the other hand, Csiszár and Körner [34] defined reliability by bounding the (normalized) maximal error probability:

$$\mathrm{P}_e(n) = \frac{1}{b}\max_{m\in\mathcal{M}}\Pr[(\mathsf{Dec}(Y^n) \neq m)] < \sigma.$$

Although $\tilde{\mathrm{P}}_e(n) \leq \mathrm{P}_e(n)$, the proof of the converse part of Theorem 1 in [34] shows that both definitions lead to the same result for secrecy capacity of the wiretap channel. Note that this does not hold for other types of channels because Dueck in [48] showed that maximum-error probability capacity regions of multiple access channel (MAC), two way channel (TWC), and interference channel (IC) can be strictly smaller than their average error probability capacity regions.

Security of a wiretap code

Security is provided when only negligible information about the transmitted message leaks to the adversary who is eavesdropping the main channel. Wyner and later Csiszár and Körner [34] defined the security of a wiretap channel by bounding the leaked information from the message space $\mathcal{M}$ to the eavesdropper in terms of the normalized mutual information as:

$$\text{Weak Security: } \frac{I(M;Z^n)}{b} < \epsilon, \tag{6.2}$$

where $M \in \mathcal{M}$ denotes the random variable corresponding to the distribution over the message space.

The security definition for wiretap channel was strengthened in [90] and [89], by replacing the above measure with the total information leakage as:

$$\text{Strong Security: } I(M;Z^n) < \epsilon, \tag{6.3}$$

for any $0 < \epsilon < 1$. The weakness of above security definitions was considered by Bellare et al. in [11]. In both above security definitions, it is required to have uniform distribution over the message space. Bellare et al. suggested the so-called *mutual information security* (MIS) definition, instead of *random mutual information security* (MIS-R) definition:

$$\text{Mutual information security: } \max_{P_M} I(M;Z^n) < \epsilon, \tag{6.4}$$

where P_M is the distribution over the message space. This is the strongest security notion for confidentiality in cryptography. Two different strong security definitions, inspired by the cryptographic approach to secrecy, were proposed in [11]. Cryptographers [58] define secure encryption as hiding all partial information about the message. In other words, given the encrypted message (ciphertext), the adversary should have little chance in computing a function of the plain message. This notion of security is referred to as *Semantic Security* (SS) [58]. Bellare et al. extended the semantic security definition to the wiretap setting by bounding the $Adv^{ss}(\mathsf{Enc};\mathsf{W}^n)$ of the encryption function Enc and the wiretapper's channel W^n. The $Adv^{ss}(\mathsf{Enc};\mathsf{W}^n)$ is defined as follows:

$$Adv^{ss}(\mathsf{Enc};\mathsf{W}^n) = \max_{\mathsf{F},P_M}\Big(\max_{\mathsf{A}}\big(\Pr[\mathsf{A}(\mathsf{W}^n(\mathsf{Enc}(M)) = \mathsf{F}(M)\big) - \max_{\mathsf{Sim}}\big(\Pr[\mathsf{Sim}(b) = \mathsf{F}(M)]\big)\Big).$$

This advantage captures the maximum in the difference of two probabilities: first the probability of an adversary A, who receives the encrypted message $\mathsf{Enc}(M)$ through the wiretapper's channel W^n, computes the result of function $\mathsf{F}(\cdot)$ on the message, and second the probability that an algorithm called simulator Sim, with access to only b, the length of the message, can do the same.

The other equivalent security definition in [11] is the extension of indistinguishability in [58] and is called *Distinguishing Security* (DS). This security notion bounds the advantage of the adversary in the following game: initially the adversary outputs two messages m_0,$m_1 \in \mathcal{M}$ and is subsequently given $\mathsf{W}^n(\mathsf{Enc}(m_\beta))$ for a random bit β. The adversary wins the game if it outputs β correctly. The advantage of the adversary in this game is subsequently:

$$\begin{aligned} Adv^{ds}(\mathsf{Enc};\mathsf{W}^n) &= \max_{\mathsf{A},m_0,m_1} 2\Pr[\mathsf{A}(m_0,m_1,\mathsf{W}^n(\mathsf{Enc}(m_\beta))) = \beta] - 1 \\ &= \max_{m_0,m_1} \mathbf{SD}(\mathsf{W}^n(\mathsf{Enc}(m_0);\mathsf{W}^n(\mathsf{Enc}(m_1)). \end{aligned}$$

The challenge bit β is uniformly random over $\{0,1\}$ and the maximum is over all b-bit messages m_0, m_1 and all adversaries A. An encryption system is considered ϵ-indistinguishable when the adversary's advantage in the described game is less than ϵ.

Instead of comparing the distribution of channel's output for two distinct messages, one can compare the distribution of channel's output for a given message with the uniform distribution. This indeed is distinguishability from uniform distribution that we denote by Adv^{dsu}:

$$Adv^{dsu}(\mathsf{Enc};\mathsf{W}) = \max_{m\in\mathcal{M}} \mathbf{SD}(\mathsf{W}^n(\mathsf{Enc}(m));U_{\mathcal{Z}^n})), \tag{6.5}$$

where $U_{\mathcal{Z}^n}$ is the uniform distribution over $\mathcal{Z}^n$. The relation between Adv^{ds} and Adv^{dsu} is straightforward from triangle inequality:

$$\begin{aligned} Adv^{ds}(\mathsf{Enc};\mathsf{W}^n) &= \max_{m_0,m_1\in\mathcal{M}} \mathbf{SD}(\mathsf{W}^n(\mathsf{Enc}(m_0));\mathsf{W}^n(\mathsf{Enc}(m_1))) \\ &\leq \max_{m_0\in\mathcal{M}} \mathbf{SD}(\mathsf{W}^n(\mathsf{Enc}(m_0));U_{\mathcal{Z}^n}) + \max_{m_1\in\mathcal{M}} \mathbf{SD}(\mathsf{W}^n(\mathsf{Enc}(m_1));U_{\mathcal{Z}^n}) \\ &= 2Adv^{dsu}. \end{aligned}$$

Therefore, in order to bound the distinguishing advantage, it is sufficient to bound Adv^{dsu}.

The distinguishing security, semantic security and the mutual information security are shown to be equivalent in [12].

Secrecy rate

The *Secrecy rate* of a wiretap code is $R = \frac{\log|\mathcal{M}|}{n}$. A family of $(\mathcal{M}, n, \sigma(n), \epsilon(n))$-wiretap codes indexed by n achieve the rate ρ if as $n \to \infty$, we have $\sigma(n) \to 0$, $\epsilon(n) \to 0$ and $R(n) \to \rho$.

Secrecy capacity

The *Secrecy capacity* of a wiretap channel $X - YZ$ is the highest achievable rate, and was derived in [34] as follows:

$$\mathrm{C}_s = \max_{V-X-YZ} (I(V;Y) - I(V;Z)), \tag{6.6}$$

where the maximum is taken over all random variables V satisfying $V - X - YZ$.

For a degraded wiretap channel ($X - Y - Z$ holds), when the main channel $\mathsf{T}$and Eve's channel W are weakly symmetric, the above expression is maximized for the uniform distribution and the capacity is given by $\mathrm{C}_s = \mathrm{C}_{\mathsf{T}} - \mathrm{C}_{\mathsf{W}}$ [84][2].

6.3.2 Constructions of wiretap codes

Existing constructions of wiretap codes can be divided into those that are based on a specific error correcting code (e.g., LDPC codes in [98, 136] and polar codes in [87]), and *modular constructions* that separate *coding for security* (or *secure coding*) from coding for reliability (for the main channel), and so are not restricted to a specific error correcting code (ECC). Known modular constructions are [11, 66, 120, 138].

Modular constructions are attractive from theoretical and practical viewpoints since they provide flexibility in the choice of error correcting codes, which is important in practice.

[2]In [84] the result is stated for symmetric DMCs. Using [84, Theorem4] implies that the same result holds when both channels are weakly symmetric.

All known constructions are *seeded encoding*[3] *systems* and require a random seed to be shared by the transmitter and the receiver. The seed can be sent by the sender to the receiver over the main channel using an error correcting code to provide reliability. The seed can be reused, and so the seed length does not affect asymptotic efficiency of the system.

Definition 6.4 (Seeded coding)**.** Given a wiretap channel WT with the main channel $\mathsf{T} : \mathcal{X}^n \to \mathcal{Y}^n$, a seeded coding scheme consists of an encoding/decoding pair, where the seeded *encoding* is a randomized mapping $\mathsf{SEnc} : \mathcal{S} \times \mathcal{M} \to \mathcal{X}^n$ that takes a seed $s \in \mathcal{S}$ and a message $m \in \mathcal{M}$ and returns a code-word $\mathsf{SEnc}_s(m)$. Each seed s defines a deterministic function $\mathsf{SEnc}_s : \mathcal{M} \to \mathcal{X}^n$. A seeded *decoding* function is a deterministic mapping $\mathsf{SDec} : \mathcal{S} \times \mathcal{Y}^n \to \mathcal{M}$ such that $\mathsf{SDec}_S(\mathsf{T}(\mathsf{SEnc}_S(m)) = m$.

The decryption error of SEnc, SDec and T is defined as:

$$\mathbb{E}\left[\max_{m\in\mathcal{M}} \Pr\left[\mathsf{SDec}_S(\mathsf{T}^n(\mathsf{SEnc}_S(m)) \neq m)\right]\right],$$

where the expectation is taken over the choice of $S \xleftarrow{\$} \mathcal{S}$ and $\Pr[\cdot]$ is from channel randomization.

The distinguishing advantage of SEnc is defined as:

$$\begin{aligned} Adv^{ds}(\mathsf{SEnc};\mathsf{W}^n) &= \max_{m_0,m_1\in\mathcal{M}} \mathbf{SD}((S,\mathsf{W}^n(\mathsf{SEnc}_S(m_0)));(S,\mathsf{W}^n(\mathsf{SEnc}_S(m_1)))) \\ &\leq 2\max_{m\in\mathcal{M}} \mathbf{SD}((S,\mathsf{W}^n(\mathsf{SEnc}_S(m)));(S,U_{\mathcal{Z}^n})), \end{aligned} \tag{6.7}$$

Sharing a seed incurs communication cost. To remove the effect of this extra communication on asymptotic rate of wiretap codes, Bellare et al. [9] proposed seed recycling to allow amortizing the cost of seed transmission in encoding a message that consists of many blocks. They showed that the same seed can be used for encoding multiple blocks without losing the security of the whole system, as long as the seed is chosen at random from the adversary's view.

*Hash-then-Encode (***HtE***)* [120] is a seeded encoding that uses an XOR-UHF and an ECC. Suppose $\mathsf{h}_S(\cdot)$ belongs to an XOR-universal family of hash functions, D is a uniformly chosen random variable, and S is a random seed that is shared with the receiver. ECC is a capacity-achieving error correcting code for the receiver's channel. The **HtE** construction works as follows.

- Encoding:

$$\mathbf{HtE}.\mathbf{enc}(m) = \mathsf{ECC}((m \oplus \mathsf{h}_S(D)\|D),$$

[3]In [11], a wiretap encoding scheme with a random seed is called a *seeded encryption* scheme. In this work, however, we use "encryption" only when a secret key is involved in encoding and use *seeded encoding* to refer to a keyless wiretap encoding scheme.

where $D \xleftarrow{\$} \{0,1\}^d$.

- Decoding: **HtE.dec** uses the decoder of ECC to obtain $D \| \big(m \oplus \mathsf{h}_S(D)\big)$ that is concatenation of two parts, and then finds $\mathsf{h}_S(D)$ by applying $\mathsf{h}_S(\cdot)$ on the first part of the block. By XORing $\mathsf{h}_S(D)$ with the second part of the received block, the decoder finds m and recovers the message.

To prove security, **HtE** uses the security proof framework of [11]. In this framework, the security proof is by first showing that the wiretap coding scheme is secure for uniformly distributed messages, and then showing that for a particular class of encoding functions (including their proposed construction), when the wiretapper's channel is symmetric, uniform message distribution security is equivalent to any message distribution security. This proof method is referred as an *indirect* security proof in this chapter. The security proof of **HtE** is effectively by showing that the **HtE** construction fits in the framework of [11]. When the XOR-UHF is $\mathcal{H}_{mult}$ (See Remark 6.1), a single multiplication over a finite field and an XOR is required before the application of ECC.

6.3.3 Wiretap channel with a shared key.

In Shannon's model of secrecy [115], transmitter and receiver share a secret key and the communication channel is assumed noiseless that can be established using a good error correcting code. OTP is proposed by Shannon to provide information-theoretic security for such a reliable communication, which needs a key as long as the message. Wyner, on the other hand, uses noise in the channel to obtain secrecy. One can consider a model that both a shared key and noise in the channel are treated as resources for providing secrecy by combining Shannon's model with the wiretap channel model resulting in a wiretap channel with shared key model. We refer to this model by the *keyed wiretap channel* model.

In the general keyed wiretap channel setting in [78], a discrete memoryless wiretap channel $\mathsf{WT}^n : \mathcal{X}^n \to \mathcal{Y}^n \times \mathcal{Z}^n$ is considered, where $\mathsf{T}(\cdot)$ is the main channel, and $\mathsf{W}(\cdot)$ is the wiretapper's channel. The sender wants to send a message $m \in \mathcal{M}$ privately, to the receiver. A uniformly distributed secret key $K \in \mathcal{K}$, with given rate $R_K > 0$, where $R_K = \frac{log|\mathcal{K}|}{n}$, is shared between the sender and the receiver. A keyed $(\mathcal{M}, n, \sigma(n), \epsilon(n))$-code is used for keyed wiretap *encryption* and is defined in the following.

Definition 6.5. [78] For a uniformly distributed M and K over their corresponding alphabets and any $\sigma(n), \epsilon(n) > 0$, a keyed $(\mathcal{M}, n, \sigma(n), \epsilon(n))$-code consists of a randomized encoder, $\mathsf{KEnc}_Q : \mathcal{K} \times \mathcal{M} \to \mathcal{X}^n$, defined by a conditional probability $Q(x^n|m,k)$ and the decoder $\mathsf{KDec} : \mathcal{K} \times \mathcal{Y}^n \to \mathcal{M}$, where the average error probability of decoding is less than $\epsilon(n)$ and the information leakage to the adversary (Z^n) is smaller than σ_n i.e.,

$$\frac{1}{|\mathcal{K}||\mathcal{M}|}\sum_{m\in\mathcal{M}}\sum_{k\in\mathcal{K}}\sum_{x^n\in\mathcal{X}^n} Q(x^n|m,k)$$
$$\sum_{z^n\in\mathcal{Z}^n}\sum_{y^n:\mathsf{KDec}(K,m)\neq m} \Pr[\mathsf{WT}^n(x^n)=(y^n,z^n)]] \leq \epsilon(n), \tag{6.8}$$

and

$$\frac{1}{n}I(M;Z^n) \leq \sigma(n) \tag{6.9}$$

The equation (6.9) is used in [78] for the secrecy definition and could be modified to the strong secrecy definition ($I(M;Z^n) \leq \sigma(n)$), aiming to have the total amount of information leaked to the eavesdropper small. This secrecy definition for keyed wiretap channel is used in [113]. Any encoding scheme satisfying strong secrecy automatically satisfies weak secrecy due to [19].

For a keyed wiretap channel setting with a given key rate $R_K > 0$, a rate $\rho > 0$ is an achievable secrecy rate if for every $R(n) < \rho$, there exists a family of keyed $(\mathcal{M}, n, \epsilon(n), \sigma(n))$ codes, with rate $R(n)$ such that $\epsilon(n)$ and $\sigma(n)$ approach zero as n grows. The secrecy capacity C_s is given by the supremum of all achievable secrecy rates R.

Secrecy in this setting is provided by two contributors, namely, the shared key and the noise over the wiretapper's channel. The expected result can be captured from two different viewpoints:

- **OTP viewpoint**: The length of the shared key for encrypting (masking) a message is decreased because the noise over the wiretapper's channel can potentially mask part of the message due to wiretap channel model results. The decrease is expected to be at most equal to the wiretap channel's capacity in each channel use.
- **Wiretap channel viewpoint**: The capacity of the wiretap channel is expected to increase at most by the key rate because the random key adds an extra confusion (besides the wiretapper's channel noise) for the adversary.

The secrecy capacity of a wiretap channel with a shared key and uniformly distributed message space is given in [78] and restated in the following.

Theorem 6.1 ([78])**.** *The secrecy capacity of the general wiretap channel with a shared key of rate R_K under reliability and security conditions given by Eq.(6.8) and Eq.(6.9) respectively, is:*

$$\max_{U-V-X-YZ} \min\left([I(V;Y|U) - I(V;Z|U)]^+ + R_K, I(V;Y)\right)$$

where $[a]^+$ *is the maximum between 0 and* a*.*

Theorem 6.1 matches our expectation when combining Shannon's model and the wiretap channel model. The secrecy capacity of the wiretap channel is increased by the key rate. However, the secrecy capacity cannot exceed the reliability capacity of the channel due to Shannon's coding theorem. For weakly symmetric main and Eve's channels T and W, when W is degraded with respect to T, the above expression is maximized for the uniform distribution and the capacity is given by:

$$\mathrm{C}_s = \min\left([\mathrm{C}_{\mathsf{T}} - \mathrm{C}_{\mathsf{W}}]^+ + R_K, \mathrm{C}_{\mathsf{T}}\right). \tag{6.10}$$

6.3.4 Codes for keyed wiretap channel encryption

A variation of Wyner's original scheme based on random coding is proposed by Yamamoto [145] for a degraded wiretap channel that enables the use of a shared key in the construction. The random code construction for general keyed wiretap channel is proposed in [78]. This scheme is shown to satisfy the weak secrecy condition of (6.9). An alternative construction for the general keyed wiretap channel is proposed in [113]. The main idea of this construction is to use the secret key as a one-time pad to encrypt as much of the message as possible and use the wiretap random coding approach to protect the remaining part of the message. This idea has appeared in previous works including [5] but the security of the construction under strong secrecy condition is shown for the first time.

Explicit constructions of keyed wiretap channel codes (similar to regular wiretap codes) can be divided into modular and non-modular codes. The only explicit non-modular construction of a keyed wiretap channel is based on polar codes and is proposed in [141]. This construction satisfies strong secrecy condition and achieves the secrecy capacity of the keyed wiretap channel.

The only known modular keyed wiretap code is the **KHtE** (Keyed Hash then Encode) construction proposed in [117]. We review this construction in the following for the sake of completeness.

Let K be the shared key and D be a uniformly distributed random variable. The $\mathbf{KHtE}[\mathsf{h}_S, \mathsf{ECC}]$, with encoding and decoding function pairs $\mathsf{ECC.enc}$ and $\mathsf{ECC.dec}$, respectively, is defined as follows for encrypting message m.

1. *Encryption*:

$$\mathbf{KHtE.enc}(K, m) = \mathsf{ECC.enc}((\mathsf{h}_S(K) \oplus m) \| D).$$

2. *Decryption*: For a received vector Y:

$$\mathbf{KHtE.dec}(K, Y) = \mathsf{ECC.dec}(Y) \oplus \mathsf{h}_S(K).$$

The **KHtE** construction provides semantic security (in the sense of [12]), and achieves the secrecy capacity of degraded keyed weakly symmetric wiretap channel for a given key rate $R_K > 0$.

We note that the **KHtE** construction is based on the **HtE** construction, which is a modular semantic secure wiretap code, and so it is tempting to think one can straightforwardly construct a keyed version of other modular semantically secure wiretap codes. For example, in **ItE** construction in [9], one may use a key K to one-time pad part of the randomization message R (call it M_0) and treat M_0 as a secret message too[4]. This modified scheme may achieve the secrecy capacity, but will not provide semantic security because it does not satisfy the *message separable* condition that is required to imply distinguishing security (equivalently semantic security) from random message security [9, Lemma 5.6]. In other words, the above scheme is only secure for a uniformly distributed message space. Constructing other semantically secure keyed wiretap codes is an interesting research question.

6.3.5 Our work

The **KHtE** construction is the only known modular semantically secure keyed wiretap code. This construction requires a positive key rate to guarantee the secrecy of the encrypted block and is not applicable for conventional wiretap channels, where there is no shared key. Also the security of the **KHtE** construction is shown for weakly symmetric channels.

In this work, in contrast to [117] that only considers $0 < R_K$, we consider $0 \leq R_K$. This allows us to combine the conventional wiretap encoding schemes and OTP encryption using a single construction that is secure for $R_K = 0$ as well as $R_K > 0$.

In Section 6.4, we propose a new keyed wiretap coding scheme by a slight modification to the **KHtE** construction. The new construction is called **KHtE***. In both constructions, a random seed is transmitted reliably over a public channel to the receiver as part of the construction.

We prove the reliability, semantic security and capacity-achieving properties of this construction. Achieving the secrecy capacity is asymptotically possible by amortizing the cost of sending the seed. This is by using the same seed for encrypting many message blocks. This technique has been introduced in [11] to prove the capacity-achieving property of a seeded wiretap code. We use this technique to show that the **KHtE*** construction achieves the secrecy capacity of weakly symmetric wiretap channels.

[4]This was suggested by an anonymous referee of ITW 2019.

The **KHtE*** construction corresponds to the wiretap coding scheme **HtE** when the key rate is zero. The proof of Lemma 6.4 gives a *direct* security proof (without relying on the framework in [11]) for the **HtE** construction. Moreover, when the secrecy capacity of the wiretap channel is zero, the construction becomes an ϵ-secure OTP.

In Section 6.6, we analyze the application of the construction to finite-length messages and answer how the same seed can be used for encryption of finite number of message blocks. This is by introducing a t-resilient construction that allows the encryption of 2^t message blocks with a same seed while guaranteeing the security of each encrypted block.

In Appendix B.4, we also propose another wiretap construction with semantic security for splittable channels, called **KXtX**, and show it achieves the secrecy capacity of weakly symmetric channels. This scheme is the keyed version of the **XtX** construction that was proposed in [12], and while its semantic security was proven, its capacity achieving property was unknown. We show that the **XtX** construction, and its keyed version **KXtX**, achieve the secrecy capacity of weakly symmetric wiretap channels. This is possible because we choose the parameters of the construction based on tight bounds in Lemmas B.4.1 and B.4.2.

6.4 KHtE*: A new keyed wiretap encryption scheme

In this section, we consider the same communication setting as [78], that is a wiretap channel $\mathsf{WT}^n : \mathcal{X}^n \to \mathcal{Y}^n \times \mathcal{Z}^n$ with the main channel $\mathsf{T}^n : \mathcal{X}^n \to \mathcal{Y}^n$, the wiretapper's channel $\mathsf{W}^n : \mathcal{X}^n \to \mathcal{Z}^n$, and a shared key of rate R_K with the goal of secure and reliable transmission of the message $m \in \mathcal{M}$.

In a wiretap channel with shared key setting, the sender and receiver have two resources: the shared secret key, and the wiretap channel. A keyed wiretap construction uses the shared key in combination with channel randomness in an optimal way to completely hide the message m. However, the shared key is available at the sender and receiver before transmission, while the noise advantage is provided once the message is transmitted over the channel. The desired scheme should use the shared key at the sender for partially masking the message such that in combination with the extracted randomness from channel noise during transmission, the message is perfectly hidden from the wiretapper.

Definition 6.6. For a wiretap channel with a shared key as described above, an $(\mathcal{M}, n, \sigma(n), \epsilon(n))$ *keyed seeded encryption scheme* $(0 < \sigma(n), \epsilon(n) < 1)$ consists of a seeded encryption $\mathsf{KSEnc} : \mathcal{S} \times \mathcal{K} \times \mathcal{M} \to \mathcal{X}^n$, and a seeded decryption $\mathsf{KSDec} : \mathcal{S} \times \mathcal{K} \times \mathcal{Y}^n \to \mathcal{M}$ algorithms that satisfy the following reliability and distinguishing security properties:

Reliability.

$$\mathop{\mathbb{E}}_{S\in\mathcal{S}}\left[\max_{m\in\mathcal{M}}\Pr[\mathsf{KSDec}_S(\mathsf{T}^n(\mathsf{KSEnc}_S(K,m))\neq m]\right]<\sigma(n) \tag{6.11}$$

Distinguishing Security.

$$\begin{aligned}&Adv^{ds}(\mathsf{KSEnc};\mathsf{W})=\max_{m_0,m_1}\\&\mathbf{SD}\Big(\Big(S,\mathsf{W}^n\big(\mathsf{KSEnc}_S(m_0,k)\big)\Big);\Big(S,\mathsf{W}^n\big(\mathsf{KSEnc}_S(m_1,k)\big)\Big)\Big)<\epsilon(n)\end{aligned} \tag{6.12}$$

6.4.1 Overview

The $\mathbf{KHtE}^*$ construction uses bitwise XOR for encoding the message. Therefore, our analysis is for a binary alphabet setting. This simplifies the representation of parameters and entropies in bits as well[5].

We show the $\mathbf{KHtE}^*$ construction is reliably decryptable, provides distinguishing security and achieves the secrecy capacity of a degraded weakly symmetric channel.

- *Reliability:* For $\mathbf{KHtE}^*[\mathsf{h}_S,\mathsf{ECC}]$, reliability according to (6.11) is satisfied when ECC is a good error correcting code for T, the main channel. This is given in Theorem B.4.1.

- *Security:* The hash function at the heart of the construction extracts randomness from the shared key and channel's noise and effectively employs it to completely hide the message from the adversary's view. The available randomness from channel's noise is proportional to n, the number of channel uses for sending the encrypted block. In order to access enough randomness for masking the message from channel noise, we extend the length of the encrypted block by concatenating a randomness D to the masked message part of the encryption. This randomness is first concatenated with the key to be *hashed*, and then concatenated with the encrypted block to be *encoded* with an error correcting code. In Theorem 6.3, distinguishing security of $\mathbf{KHtE}^*[\mathsf{h}_S,\mathsf{ECC}]$ is proved using Lemma 6.4. This lemma is an extension of Lemma 6.3 given in [43] that enables randomness extraction from two independent randomness sources. As noted, here two sources of randomness are the random key and channel randomness.

- *Capacity-achieving:* We show that for a weakly symmetric wiretap channel (weakly symmetric main and wiretapper's channels), when the error correcting code in the $\mathbf{KHtE}^*$ construction is from families that achieve the capacity of the main channel T, and the length of random string D is sufficient (with respect to Theorem 6.4), the $\mathbf{KHtE}^*$ construction achieves the secrecy capacity given by (6.10).

[5]Note that in digital communication, messages are always represented as binary strings and this assumption doesn't force any limitation to the communication model in practice.

6.4.2 KHtE* construction

For a message space $\mathcal{M} = \{0,1\}^b$, a wiretap channel $\mathsf{WT} : \{0,1\}^\ell \to \{0,1\}^t \times \{0,1\}^w$, let $\mathcal{H} = \{\mathsf{h}_s | s \in \mathcal{S}\}$, where $\mathsf{h}_s : \{0,1\}^{d_1+d_2} \to \{0,1\}^b$, be a family of pairwise universal hash functions, and $\mathsf{ECC} : \{0,1\}^{b+d_1} \to \{0,1\}^{n.\ell}$ be a family of capacity-achieving error correcting codes for the main channel. Let a random secret key $K \in \{0,1\}^{d_2}$ be shared by the sender and the receiver and a random seed S be publicly available to the sender, receiver and the eavesdropper.

The $\mathbf{KHtE}^*[\mathsf{h}_S, \mathsf{ECC}]$, with encoding and decoding function pairs $\mathsf{ECC.enc}$ and $\mathsf{ECC.dec}$, respectively, is defined as follows.

1. Encryption:

$$\mathbf{KHtE}^*.\mathbf{enc}(K, m) = \mathsf{ECC.enc}\Big(\big(\mathsf{h}_S(K\|D) \oplus m\big)\|D\Big),$$

   where $D \xleftarrow{\$} \{0,1\}^{d_1}$.

2. Decryption: For a received vector Y^n:

$$\mathbf{KHtE}^*.\mathbf{dec}(K, Y^n) = \mathsf{ECC.dec}(Y^n) \oplus \mathsf{h}_S(K\|D).$$

In the following, we derive the relationship between parameters in the proposed encoding system so that the desired reliability and security requirements are satisfied. We then find the achievable rate of the encryption system and show it achieves the secrecy capacity of weakly symmetric wiretap channels.

Decryptability of KHtE*

Let $\mathsf{T} : \{0,1\}^\ell \to \{0,1\}^t$ with Shannon capacity C_T be the main channel and $\mathsf{ECC}^{(n)} : \{0,1\}^{b(n)+d_1(n)} \to \{0,1\}^{n.\ell_1}$ be a family of error correcting codes indexed by n for channel T, with decryption function $\mathsf{ECC.dec}^{(n)}$ and maximal decryption error $\sigma(n)$. The decryption algorithm applies the decoder of $\mathsf{ECC}^{(n)}$ to the received vector Y^n and parses the result into its first $b(n)$ bits $\mathsf{h}_S(K\|D) \oplus m$ and its last $d_1(n)$ bits D. Finally, message m is decrypted by the XOR of the first $b(n)$ bits with $\mathsf{h}_S(K\|D)$ using the shared key.

Theorem 6.2 (Reliability of $\mathbf{KHtE}^*$)**.** *Let the keyed seeded encryption function* $\mathsf{KSEnc}^{(n)} = \mathbf{KHtE}^*.\mathbf{enc}[\mathsf{h}_s, \mathsf{ECC}^{(n)}]$, *where* $\mathsf{ECC}^{(n)}$ *is described above. Then* $\mathsf{KSDec}_S = \mathbf{KHtE}^*.\mathbf{dec}[\mathsf{h}_s, \mathsf{ECC}^{(n)}]$ *is a decryption function for* KSEnc *with decryption error at most* $\sigma(n)$ *and there exist* $\mathsf{ECC}(n)$ *such that* $\lim_{n\to\infty} \sigma(n) = 0$

Proof. There always exists $\mathsf{ECC}^{(n)}$ achieving rates less than C_T, with maximal error probability approaching 0 as n grows. Such an ECC guarantees that $\big(\big(\mathsf{h}_S(K\|D) \oplus m\big)\|D$ is correctly recovered and the decryption

algorithm above can recover m. The maximal decryption error $\sigma(n)$ is upper-bounded by the maximal error probability of the ECC that goes to 0. Thus $\lim_{n\to\infty}\sigma(n)=0$. □

Distinguishing security of KHtE*

To prove security of **KHtE***, we bound Adv^{dsu} and use the relation $Adv^{ds}\leq 2Adv^{dsu}$. We interpret the channel as a source of randomness and use the maximum probability in the channel's transition matrix as an indication of the minimum randomness that the channel provides at its output for any input. We refer to this as *channel min-entropy* and denote it by $H_\infty(CH)$ for channel $\mathsf{CH}\langle\mathbf{CH},\{0,1\}^\ell,\{0,1\}^w\rangle$.

$$H_\infty(\mathsf{CH})=-\log\big(\max_{x\in\{0,1\}^\ell,y\in\{0,1\}^w}\mathbf{CH}(x,y)\big)$$

Consider a message space $\mathcal{M}=\{0,1\}^{b(n)}$, a shared secret key of rate $0\leq R_K\leq 1$, a wiretap channel WT with the main channel $\mathsf{T}:\{0,1\}^\ell\to\{0,1\}^t$, and the wiretapper's channel $\mathsf{W}:\{0,1\}^\ell\to\{0,1\}^w$, where $H_\infty(\mathsf{W})\geq\nu$. Let $\{\mathsf{h}_s|s\in\mathcal{S}\}$, for uniformly random s, be a family of pair-wise universal functions $\mathsf{h}_s:\{0,1\}^{d_1(n)+n.R_K}\to\{0,1\}^{b(n)}$ and $\mathsf{ECC}:\{0,1\}^{b(n)+d_1(n)}\to\{0,1\}^{n.\ell}$ be an arbitrary error correcting code for T. The following theorem shows the security of **KHtE*** construction.

Theorem 6.3. *[**Security of** **KHtE***] The keyed encryption scheme* $\mathsf{KSEnc}=\mathbf{KHtE}^*[\mathsf{h}_S,\mathsf{ECC}]$*, with key rate* R_K*,* h_S *and* ECC *related to the wiretap channel* WT *described above, provides* $2\epsilon(n)$*-distinguishing security, i.e.,* $Adv^{ds}(\mathsf{KSEnc};\mathsf{W}^n)\leq 2\epsilon(n)$*, assuming* $n.R_K+d_1(n)-2\log\frac{1}{\epsilon(n)}\leq b(n)$ *and*

$$n.\mathsf{R}_K+d_1(n)+n.\nu\geq n.w+2log(\frac{1}{\epsilon(n)}). \tag{6.13}$$

To prove Theorem 6.3, we use Lemma 6.4. Informally, this lemma shows that for an arbitrary injective function $\mathsf{F}(\cdot)$ and a uniform random variable $D\in\{0,1\}^{d_1}$, the output of a channel CH with an input $\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)$ is almost uniform over channel's output alphabet when the sum of the min-entropy of X, d_1 and channel min-entropy is almost equal to the output size of the channel. This lemma can be viewed as the channel version of the Leftover Hash Lemma in [77].

Lemma 6.4. *Let* $\{\mathsf{h}_s|s\in\mathcal{S}\}$ *be a family of pair-wise universal hash functions* $\mathsf{h}_s:\{0,1\}^{d_2}\to\{0,1\}^b$ *for uniform* s *and* $\mathsf{F}:\{0,1\}^{b+d_1}\to\{0,1\}^\ell$ *be an injective function* $(b+d_1\leq\ell)$*. For a channel* $\mathsf{CH}:\{0,1\}^\ell\to\{0,1\}^w$*, where* $H_\infty(\mathsf{CH})\geq\nu$*, a random variable* $X\in\{0,1\}^{d_2}$ *and uniform random variable* $D\in\{0,1\}^{d_1}$*,*

suppose $H_\infty(X) + d_1 - 2\log\frac{1}{\epsilon} \leq b$ *and* $H_\infty(X) + d_1 + \nu \geq w + 2\log(\frac{1}{\epsilon})$. *Then*

$$\mathbf{SD}\Big(\Big(S, \mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big)\Big); \Big(S, U_w\Big)\Big) \leq \epsilon. \tag{6.14}$$

Proof. According to [76, Claim 2], any distribution over a finite set Σ with collision probability at most $\frac{1+2\epsilon^2}{|\Sigma|}$ is ϵ-close to the uniform distribution. We bound the collision probability $\Pr[(S, \mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = (S^{'}, \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_{S'}(X')\|D'\big)\Big)]$, where $S^{'}$, $X^{'}$ and D' are sampled independently from the same distribution as S, X and D, respectively, and CH and CH' are the same channels but in different applications. We have

$$\begin{aligned}
&\Pr[\Big(S, \mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \Big(S^{'}, \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_{S'}(X')\|D'\big)\Big)] \\
&= \Pr[S = S^{'}] \cdot \Pr[D = D'] \cdot \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X')\|D\big)\Big)] \\
&= \frac{2^{-d_1}}{|\mathcal{S}|}\Big(\Pr[X = X'] \cdot \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big)] + \\
&\qquad \Pr[X \neq X'] \cdot \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X')\|D\big)\Big) | X \neq X']\Big).
\end{aligned} \tag{6.15}$$

Since

$$\begin{aligned}
\Pr[X = X'] &= \sum_{x \in \{0,1\}^{d_2}} \Pr[X = x].\Pr[X' = x] \\
&\leq 2^{-H_\infty(X)} \cdot \sum_{x \in \{0,1\}^{d_2}} \Pr[X' = x] = 2^{-H_\infty(X)},
\end{aligned}$$

and

$$\begin{aligned}
&\Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big)] \\
&\quad = \sum_{z \in \{0,1\}^w} \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = z] \cdot \Pr[\mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = z] \\
&\quad \leq 2^{-\nu} \cdot \sum_{z \in \{0,1\}^w} \Pr[\mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = z] = 2^{-\nu},
\end{aligned}$$

from (6.15),

$$\begin{aligned}
&\Pr[\Big(S, \mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \Big(S^{'}, \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_{S'}(X')\|D'\big)\Big)] \\
&\leq \frac{2^{-d_1}}{|\mathcal{S}|}\left(2^{-\nu - H_\infty(X)} + \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X')\|D\big)\Big) | X \neq X']\right).
\end{aligned} \tag{6.16}$$

Now we bound $\Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X')\|D\big)\Big) | X \neq X']$. Let $\mathcal{I}m_{\mathsf{F}}$ be the set of all the images of

$\{0,1\}^{b+d_1}$ in $\{0,1\}^{\ell}$ under the transform $\mathsf{F}(\cdot)$. Then because of the injective property of $\mathsf{F}(\cdot)$, $|\mathcal{I}m_{\mathsf{F}}| = 2^{b+d_1}$. We have

$$\begin{aligned}
&\Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(X')\|D\big)\Big)|X \neq X'] \\
&= \sum_{\substack{(x,x')\in\{0,1\}^{d_2}\times\{0,1\}^{d_2} \\ x\neq x'}} \Pr[X=x].\Pr[X'=x'] \cdot \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(x)\|D\big)\Big) = \mathsf{CH}'\Big(\mathsf{F}\big(\mathsf{h}_S(x')\|D\big)\Big)|x \neq x'] \\
&\leq \Big(\sum_{(y,y')\in\mathcal{I}m_{\mathsf{F}}\times\mathcal{I}m_{\mathsf{F}}} \Pr[\mathsf{F}\big(\mathsf{h}_S(x)\|D\big)=y].\Pr[\mathsf{F}\big(\mathsf{h}_S(x')\|D\big)=y']\cdot \\
&\qquad \Pr[\mathsf{F}\big(\mathsf{h}_S(x)\|D\big)=y \wedge \mathsf{F}\big(\mathsf{h}_S(x')\|D\big)=y'|x\neq x']\Big) \cdot \Big(\sum_{z\in\{0,1\}^w} \Pr[Z=z]\cdot\Pr[\mathsf{CH}(y)=\mathsf{CH}'(y')=z]\Big).
\end{aligned} \tag{6.17}$$

Since $\mathsf{F}(\cdot)$ is injective, $\Pr[\mathsf{F}\big(\mathsf{h}_S(x)\|D\big)=y \wedge \mathsf{F}\big(\mathsf{h}_S(x')\|D\big)=y'] = \Pr[\mathsf{h}_S(x)=\mathsf{F}^{-1}(y)|_b \wedge \mathsf{h}_S(x')=\mathsf{F}^{-1}(y')|_b]$, where the probability is over the choices of S, and since $\mathsf{h}_S(\cdot)$ is pairwise independent, for $x\neq x'$,

$$\Pr[\mathsf{h}_S(x)=\mathsf{F}^{-1}(y)|_b \wedge \mathsf{h}_S(x')=\mathsf{f}^{-1}(y')|_b] \leq 2^{-2b}. \tag{6.18}$$

Therefore, by using (6.18) to upper-bound (6.17):

$$\begin{aligned}
&\Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X')\|D\big)\Big)|X \neq X'] \\
&\leq 2^{-2b}\cdot\Big(\sum_{(y,y')\in\mathcal{I}m_{\mathsf{F}}\times\mathcal{I}m_{\mathsf{F}}} \sum_{z\in\{0,1\}^w} \\
&\qquad \Pr[Y=y]\cdot\Pr[Y'=y']\cdot\Pr[Z=z]\cdot\Pr[\mathsf{CH}(y)=\mathsf{CH}'(y')=z]\Big) &(6.19)\\
&\leq 2^{-2b}\cdot\Big(\sum_{(y,y')\in\mathcal{I}m_{\mathsf{F}}\times\mathcal{I}m_{\mathsf{F}}} \sum_{z\in\{0,1\}^w} \\
&\qquad \Pr[Y=y]\cdot\Pr[Y'=y']\cdot\Pr[Z=z]\cdot\mathbf{CH}(y,z)\cdot\mathbf{CH}(y',z)\Big) &(6.20)\\
&\leq 2^{-2b-\nu}\cdot\Big(\sum_{y'\in\mathcal{I}m_{\mathsf{F}}} \Pr[Y'=y']\cdot \sum_{y\in\mathcal{I}m_{\mathsf{F}}} \sum_{z\in\{0,1\}^w} \\
&\qquad \Pr[Y=y]\cdot\cdot\Pr[Z=z]\cdot\mathbf{CH}(y,z)\Big) &(6.21)\\
&\leq 2^{-2b-\nu} \sum_{y\in\mathcal{I}m_{\mathsf{F}}} \sum_{z\in\{0,1\}^w} \Pr[Y=y]\cdot\Pr[Z=z]\cdot\mathbf{CH}(y,z) &(6.22)\\
&= 2^{-2b-\nu}.2^{b+d_1} = 2^{-\nu-b+d_1}. &(6.23)
\end{aligned}$$

Here, (6.20) is obtained from (6.19) by using the transition probability matrix of the channel instead of $\Pr[\mathsf{CH}(y)=z]$ and $\Pr[\mathsf{CH}(y')=z]$. (6.21) is concluded from (6.20) since $\mathbf{CH}(y',z) \leq 2^{-\nu}$ and (6.22) is

obtained because $\sum_{y' \in \mathcal{I}m_{\mathsf{F}}} \Pr[Y' = y'] = 1$. For getting (6.23) from (6.22), we note that the sum of each row in a transition probability matrix of a channel is 1; that is $\sum_{z \in \{0,1\}^w} \Pr[Z = z] \cdot \mathbf{CH}(y, z) = 1$, and since $|\mathcal{I}m_{\mathsf{F}}| = 2^{b+d_1}$,

$$\sum_{y \in \mathcal{I}m_{\mathsf{F}}} \sum_{z \in \{0,1\}^w} \Pr[Y = y] \cdot \Pr[Z = z] \cdot \mathbf{CH}(y, z) = 2^{b+d_1}.$$

We then conclude from (6.16) and (6.23) that the collision probability is bounded as follows:

$$\begin{aligned} &\Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = \mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X')\|D\big)\Big)] \\ &\leq \tfrac{1}{|\mathcal{S}|2^w} \cdot \left(2^{-(d_1+H_\infty(X)+\nu-w)} + 2^{-(\nu+b-w)}\right). \end{aligned} \tag{6.24}$$

From the assumptions $H_\infty(X)+d_1+\nu \geq w+2\log\frac{1}{\epsilon}$, and $H_\infty(X)+d_1-2\log\frac{1}{\epsilon} \leq b$. Thus, $2^{-(H_\infty(X)+d_1+\nu-w)} \leq \epsilon^2$ and $2^{-(\nu+b-w)} \leq 1$, and the collision probability is bounded by $\frac{1+\epsilon^2}{|\mathcal{S}|2^w} \leq \frac{1+2\epsilon^2}{|\mathcal{S}|2^w}$ and the statistical distance is bounded by ϵ. Therefore,

$$\mathbf{SD}\left(\left(S, \mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big)\right); \left(S, U_w\right)\right) \leq \epsilon. \tag{6.25}$$

□

We use Lemma 6.4 to give a direct security proof for the security of $\mathbf{KHtE}^*$ construction in the wiretap setting.

Proof of Theorem 6.3. We bound Adv^{dsu} of the $\mathbf{KHtE}^*$ construction. Let $d_1(n)$ satisfy (6.13), that is

$$n.\mathsf{R}_K + d_1(n) + n.\nu \geq n.w + 2log(\frac{1}{\epsilon(n)}).$$

$K \in \{0,1\}^{d_2}$ is the key in the construction and its length is $d_2 = n.R_K$. Since the key is uniformly distributed, $n.R_K = H_\infty(K)$, and for the randomness $D \in \{0,1\}^{d_1}$, $H_\infty(K) \leq H_\infty(K\|D)$. Thus, $d_1(n)$ satisfies:

$$H_\infty(K\|D) + d_1(n) + n.\nu \geq w + 2log(\frac{1}{\epsilon(n)}),$$

and $n.R_K + d_1(n) - 2\log\frac{1}{\epsilon(n)} \leq b(n)$ from the assumption. Now from Lemma 6.4, and since $\mathsf{ECC}(\cdot)$ is an injective function

$$\mathbf{SD}\left(\left(S, \mathsf{W}^n\Big(\mathsf{ECC}\big(\mathsf{h}_S(K\|D)\|D\big)\Big)\right); \left(S, U_w^n\right)\right) \leq \epsilon(n).$$

For any $m \in \{0,1\}^{b(n)}$, if $\mathsf{h}_s(\cdot)$ is a pairwise UHF, so is $\mathsf{h}_s(\cdot) \oplus m$. Therefore,

$$Adv^{dsu}(\mathsf{KSEnc}; \mathsf{W}^n) = \mathbf{SD}\Big(\big(S, \mathsf{W}^n\big(\mathbf{KHtE}^*(K,m)\big)\big); \big(S, U_w^n\big)\Big) < \epsilon(n).$$

Finally, for any m_0 and m_1,

$$Adv^{ds}(\mathsf{KSEnc}; \mathsf{W}^n) \leq Adv^{dsu}(\mathsf{KSEnc}; \mathsf{W}^n) \leq 2\epsilon(n).$$

□

Achieving secrecy capacity in KHtE*

In the following, we show the **KHtE*** construction achieves the capacity of keyed wiretap channel as given in (6.10), for weakly symmetric main and wiretapper's channels.

Theorem 6.4. *Consider a keyed wiretap channel* WT *consisting of a weakly symmetric main channel* $\mathsf{T} : \{0,1\}^\ell \to \{0,1\}^t$ *with capacity* C_T*, the wiretapper's channel* $\mathsf{W}^n : \{0,1\}^\ell \to \{0,1\}^w$ *with capacity* C_W *and the shared secret key rate* $0 \leq R_K \leq 1$*, and an* $\mathsf{ECC}^{(n)} : \{0,1\}^{b(n)+d_1(n)} \to \{0,1\}^{n.\ell}$ *that achieves the capacity of the main channel. Then the secrecy capacity of the keyed wiretap setting is achievable by* $\mathsf{KSEnc} = \mathbf{KHtE}^*[\mathsf{h}_S, \mathsf{ECC}]$.

Proof. Suppose the output distribution of W for an arbitrary reference input y_r is P_V over $\{0,1\}^t$ and for $y \in \{0,1\}^\ell$, $y \neq y_r$ is P_Z over $\{0,1\}^t$. Since W is weakly symmetric, for any $v \in \{0,1\}^t$ there is a $z \in \{0,1\}^t$ such that $P_V(v) = P_Z(z)$. Let us define a permutation over $\{0,1\}^t$ called $\tau_y(\cdot)$, where $\tau_y(v) = z$ if $P_V(v) = P_Z(z)$ and for $y = y_r$, let $\tau_y(\cdot)$ be the identity function. Then, for V, a random variable vector with distribution P_{V^n},

$$\mathbf{W}(y,z) = \Pr[\mathsf{W}(y) = z] = \Pr[\big(\tau_y(V)\big) = z]. \tag{6.26}$$

Now let $y_r^n = (y_{r_1}, y_{r_2}, \ldots, y_{r_n}) \in \{0,1\}^{n.\ell}$ be the reference input vector for W^n, and P_{V^n} be the output distribution over $\{0,1\}^{n.t}$. Since W is a DMC, P_{V^n} is a distribution with n independent samples, and since W is weakly symmetric, so is W^n. Then, for $V^n = (V_1, V_2, \ldots, V_n)$, a random variable vector with distribution P_{V^n}. Form (6.26),

$$\mathbf{W}^{\otimes n}(y^n, z^n) = \Pr[\mathsf{W}^n(y^n) = z^n] = \Pr[\big(\tau_{y^n}(V^n)\big) = z^n]. \tag{6.27}$$

Suppose $V_{\epsilon(n)}$ is the random variable that achieves the ϵ-smooth min-entropy of V^n, that is,

$$H_\infty^{\epsilon(n)}(V^n) = \max_{V_{\epsilon(n)}: \mathbf{SD}(V^n, V_{\epsilon(n)}) \leq \epsilon(n)} H_\infty(V_{\epsilon(n)}).$$

From Lemma 6.1,

$$H_\infty(V_{\epsilon(n)}) = H_\infty^{\epsilon(n)}(V^n) \geq H(V^n) - n\delta(n), \tag{6.28}$$

where $\delta(n) = \log(2^\ell + 3).\sqrt{2log\frac{1}{\epsilon(n)}/n}$.

Now consider a virtual channel $\mathsf{W}_{\epsilon(n)} : \{0,1\}^{n.\ell} \to \{0,1\}^{n.w}$ as follows: the output distribution of $\mathsf{W}_{\epsilon(n)}$ for $y_r^n \in \{0,1\}^{n.\ell}$ is the distribution of $V_{\epsilon(n)}$, and for any $y^n \neq y_r^n$ the distribution is the distribution of $\tau_{y^n}(V_{\epsilon(n)})$. From the application of Theorem 6.3, $Adv^{dsu}(\mathsf{KSEnc}; \mathsf{W}_{\epsilon(n)}) \leq \epsilon(n)$ for any $d_1(n)$ satisfying

$$d_1(n) + n.R_K + H_\infty(V_{\epsilon(n)}) \geq n.w + 2log\epsilon(n),$$

and from (6.28), it is sufficient to have

$$d_1(n) \geq n.w - H(V^n) + \sqrt{n}.\log(2^\ell + 3).\sqrt{2log\frac{1}{\epsilon(n)}} - 2log\epsilon(n) - n.R_K. \tag{6.29}$$

In other words, for $d_1(n)$ satisfying (6.29),

$$Adv^{dsu}(\mathsf{KSEnc}; \mathsf{W}_{\epsilon(n)}) = \mathbf{SD}\Big(\Big(S, \mathsf{W}_{\epsilon(n)}\big(\mathbf{KHtE}^*(K,m)\big)\Big); \Big(S, U_w^n\Big)\Big) < \epsilon(n). \tag{6.30}$$

On the other hand, for any $y^n \in \{0,1\}^{n.\ell}$,

$$\mathbf{SD}(V^n; V_{\epsilon(n)}) \leq \epsilon(n) \overset{\text{Lemma } 6.2}{\Rightarrow} \mathbf{SD}\big(\tau_{y^n}(V^n); \tau_{y^n}(V_{\epsilon(n)})\big) \leq \epsilon(n),$$

and since from (6.26),

$$\Pr[\big(\tau_{y^n}(V^n)\big) = z^n] = \Pr[\mathsf{W}^n(y^n) = z^n],$$

and

$$\Pr[\big(\tau_{y^n}(V_{\epsilon(n)} = z^n] = \Pr[\mathsf{W}_{\epsilon(n)}(y^n) = z^n],$$

we have

$$\mathbf{SD}\Big(\big(\mathsf{W}^n\big(\mathbf{KHtE}^*(K,m); \big(\mathsf{W}_{\epsilon(n)}\big(\mathbf{KHtE}^*(K,m)\big)\Big) \leq \epsilon(n) \tag{6.31}$$

By the triangular inequality

$$\begin{aligned}
&\mathbf{SD}\Big(\big(S, \mathsf{W}^n\big(\mathbf{KHtE}^*(K,m)\big)\big); \big(S, U_w^n\big)\Big) \\
&\qquad \leq \mathbf{SD}\Big(\big(S, \mathsf{W}^n\big(\mathbf{KHtE}^*(K,m)\big)\big); \big(S, \mathsf{W}_{\epsilon(n)}\big(\mathbf{KHtE}^*(K,m)\big)\big)\Big) \\
&\qquad\quad + \mathbf{SD}\Big(\big(S, \mathsf{W}_{\epsilon(n)}\big(\mathbf{KHtE}^*(K,m)\big)\big); \big(S, U_w^n\big)\Big), \qquad (6.32)
\end{aligned}$$

where the first term on the right-hand side of the inequality is bounded by (6.31) and the second term is bounded by (6.30). Thus,

$$\mathbf{SD}\Big(\big(S, \mathsf{W}^n\big(\mathbf{KHtE}^*(K,m)\big)\big); \big(S, U_w^n\big)\Big) \leq 2\epsilon(n),$$

and for the $\mathbf{KHtE}^*$ construction with the given $d_1(n)$, $Adv^{ds}(\mathsf{KSEnc}; \mathsf{W}^n) \leq 2Adv^{dsu}(\mathsf{KSEnc}; \mathsf{W}^n) \leq 4\epsilon(n)$.

The achievable rate of the construction is $R = \lim_{n\to\infty} \frac{b(n)}{n}$. For $d_1(n)$ satisfying (6.29) and a capacity-achieving ECC,

$$\begin{aligned}
&\lim_{n\to\infty} \frac{b(n) + d_1(n)}{n} = \mathrm{C}_{\mathsf{T}} \\
&\Rightarrow \lim_{n\to\infty} \frac{b(n)}{n} = \mathrm{C}_{\mathsf{T}} - \lim_{n\to\infty} \frac{d_1(n)}{n}.
\end{aligned}$$

For $\mathrm{C}_{\mathsf{T}} \geq \mathrm{C}_{\mathsf{W}}$,

$$R \leq \mathrm{C}_{\mathsf{T}} - \mathrm{C}_{\mathsf{W}} + R_K.$$

From Shannon's coding theorem, $R \leq \mathrm{C}_{\mathsf{T}}$. Therefore,

$$R \leq \min\big([C_{\mathsf{T}} - C_{\mathsf{W}}] + R_K, \mathrm{C}_{\mathsf{T}}\big),$$

where the upper bound is achieved when $d_1(n)$ in (6.29) is set to its minimum.

For $\mathrm{C}_{\mathsf{T}} \leq \mathrm{C}_{\mathsf{W}}$,

$$R \leq \min\big(R_K, \mathrm{C}_{\mathsf{T}}\big).$$

This is discussed in Section 6.5.2.

□

6.4.3 Amortizing the seed

In seeded encryption systems, the seed must be sent reliably to the receiver. In the absence of additional channels, the seed must be encoded using an ECC and sent over the wiretap channel (no secrecy required). This incurs an extra cost for sending the seed that would affect the final rate of the system. In [11], the notion of *seed recycling* is introduced, which effectively means the seed can be used many times, without compromising security. Using seed recycling allows the cost of sending the seed to be amortized over multiple blocks, hence the final rate of the seeded encryption system approaches the secrecy capacity of the wiretap channel. Seed recycling is directly applicable to the **KHtE*** construction.

Lemma 6.5. *[9, Lemma 4.2] For $t \geq 1$, let $\mathsf{CH} = \mathsf{CH}_0 \| \mathsf{CH}_1^t$ be a channel such that $\mathsf{CH}_0 : \{0,1\}^{\ell_0} \to \{0,1\}^{w_0}$ and $\mathsf{CH}_1 : \{0,1\}^{\ell} \to \{0,1\}^{w}$. For a seeded encryption scheme $\mathsf{SEnc} : \mathcal{S} \times \{0,1\}^b \to \{0,1\}^\ell$ and an error correcting code $\mathsf{ECC}_0 : \mathcal{S} \to \{0,1\}^{\ell_0}$, the seed recycling encryption scheme $\mathsf{SR}_t[\mathsf{SEnc}, \mathsf{ECC}_0]$ uses SEnc to encrypt t blocks of b bits with the same random seed $S \in \mathcal{S}$, and concatenates $\mathsf{ECC}_0(S)$ to the encrypted block. Then*

$$Adv^{ds}(\mathsf{SR}_t; \mathsf{CH}) \leq t \cdot Adv^{ds}(\mathsf{SEnc}; \mathsf{CH}_1).$$

The rate of the encryption scheme $\mathsf{SR}_{t(n)}^{(n)}[\mathsf{SEnc}^{(n)}, \mathsf{ECC}_0^{(n)}]$ consisting of $\mathsf{SEnc}^{(n)} : \mathcal{S}^{(n)} \times \{0,1\}^{b(n)} \to \{0,1\}^{\ell(n)}$ and $\mathsf{ECC}_0^{(n)} : \mathcal{S}^{(n)} \to \{0,1\}^{\ell_0(n)}$, achieves the rate of $\mathsf{SR}^{(n)}$ asymptotically, by letting $\ell_0(n) = o(n \cdot t(n))$ and $t(n) = O(log(n))$.

Note that the above lemma, as well as Theorem 5.2, is in the form of averages over the choice of the seeds. In other words, for a given adversary's channel $\tilde{\mathsf{W}}$, there exists some seed s for which Adv^{ds} can't be bounded. This means the random seed in the construction should be chosen once the adversary's channel is fixed (because otherwise, the adversary can choose a view corresponding to $\tilde{\mathsf{W}}$ for a given s). Thus, a hard coded seed cannot be used in this construction.

6.5 Special cases

In the following, we consider two extreme cases: i) the wiretapper's channel is the only available resource, and ii) only a shared key is available to the communicants. We show that the **KHtE*** construction results in a capacity-achieving wiretap code with semantic security, and the traditional one-time-pad, in the two cases respectively.

6.5.1 Wiretap chanel construction: $R_K = 0$

The **KHtE*** reduces to the **HtE** wiretap code when the key rate is zero[6]. In [120], the security of the **HtE** construction is proved by using the framework of [11]. This framework consists of two steps: first the security of an encoded uniformly distributed message is proved when the wiretapper's channel is a BISC or an additive noise channel, and then using *message linear* and *separable* properties of the encryption systems, security for random message is shown to be equivalent to security for *any* message. We call this approach for proving security an *indirect* approach. The *direct* approach on the other hand, is to prove security for any message distribution in one step. The direct security proof of the **HtE** construction follows from Theorem 6.3 by letting $R_K = 0$. The security proof holds for a wide class of wiretapper's channels, namely, DMCs with binary alphabet input. This means the **HtE** construction is the first semantically secure wiretap code for such general DMCs.

Comparison

We compare the **HtE** construction (given the new security proof) with other existing modular wiretap constructions including two other seeded encryption systems, **XtX** (Extract then XOR) construction in [12] and **ItE** (Invert then Encode) construction in [11], and a construction by Hayashi and Matsumoto [66] that uses invertible universal hash functions to construct a modular wiretap code.

1. **Semantic security:** The **XtX** construction provides distinguishing security when the wiretap channel is splittable (See Appendix B.4.1 for the definition of splittable channels), that is the main channel is $\mathsf{T} = \mathsf{T}_1 \| \mathsf{T}_2$ and the wiretapper's channel is $\mathsf{W} = \mathsf{W}_1 \| \mathsf{W}_2$, and the first part of the wiretapper's channel W_1 is also splittable. **ItE** construction is semantic secure for BISCs and additive noise channels (it is unknown if RDS yields DS for a more general channel[7]). The construction in [66] achieves strong security defined as the total information leakage [90], and assumes uniformly distributed messages. In [67], the security of [66] is shown for more general distributions namely "weak asymptotically conditionally uniform" distributions. The channel in [67] is *regular* in the sense of [37] (See Appendix B.4.2 for definition and discussion on regular channels), and the proposed construction is over a binary alphabet. The **HtE** construction provides distinguishing security when the wiretapper's channel is a DMC with binary alphabet input of the form $\{0,1\}^\ell$.

2. **Capacity-achieving:** **XtX** is not capacity-achieving. The construction in [66] is capacity-achieving under certain conditions (if the distribution P_V on V realizing (6.6) also maximizes the mutual in-

[6]However, the hash function in the **HtE** construction belongs to an XOR-universal family of hash functions while the hash function in the **KHtE*** construction belongs to the more general family of pair-wise universal hash functions.

[7]It is likely that RDS yeilds DS for regular channels based on the proof method used in [12]

formation $I(V, Z|V)$). The **ItE** construction is capacity-achieving for degraded wiretap channels with symmetric main and wiretapper's channels in which uniform input to the wiretapper's channel generates uniform output. Using the channel upgrading technique in [131], the latter conditioned for the **ItE** construction is relaxed. The **HtE** construction is capacity-achieving for degraded wiretap channels with weakly symmetric main and wiretapper's channels and binary alphabet input of the form $\{0,1\}^{\ell}$.

3. **Error correcting code:** The required error correcting code for **ItE** is linear and message seperable. The error correcting code for **XtX** is systematic and the error correcting code for **HtE** and [66] is any good ECC.

Remark 6.2. *To have a fair comparison, we note that the definition of strong symmetric/symmetric channels in [11] (for **ItE** construction) is based on the definitions in [54], while the symmetric/weakly symmetric channels definitions in this work are from [30]. The definition of strong symmetric channels in [54] coincides with the definition of symmetric channels in [30]. However, according to [54], a channel with transition probability matrix* $\mathbf{CH}$ *is called symmetric if with appropriate indexing of the input and output alphabet, one can write* $\mathbf{CH}$ *in the form of* $[\mathbf{CH}[1] \ \cdots \mathbf{CH}[\ell]]$*, where each sub-matrix* $\mathbf{CH}[i]$ *is a transition probability matrix of a strongly symmetric channel. Theorem 6.4 is given for weakly symmetric channels according to the definition of [30]. However, the proof easily and without any change works for symmetric channels according to definitions of [54].*

6.5.2 One-Time Pad: $\mathbf{C}_s(\mathsf{WT}) = 0$

When the secrecy capacity of the wiretap channel is zero ($\mathrm{C}_{\mathsf{T}} \leq \mathrm{C}_{\mathsf{W}}$ for weakly symmetric channels), the shared key is the only accessible source for providing security. In this case, the classic one-time pad construction provides message security. However, we can also rely on the proposed constructions to provide security. Since the proposed construction provides ϵ-indistinguishability, we call the construction ϵ-secure OTP, which is the $\mathbf{KHtE}^{*}$ construction satisfying Theorem 6.3 for $\nu = 0$ (we set channel's min-entropy to zero because we cannot extract any randomness for secrecy from the channel noise when $\mathrm{C}_s = 0$) and denote it with $\mathbf{OTP}^{\epsilon}$.

For a message $m \in \{0,1\}^{b(n)}$, the key rate R_K, the random string $D \in \{0,1\}^{d_1(n)}$, the main channel T and the wiretapper's channel $\mathsf{W} : \{0,1\}^{\ell} \to \{0,1\}^{w}$, from Theorem 6.3, $Adv^{ds}(\mathsf{KSEnc}; \mathsf{W}^n) \leq 2\epsilon(n)$ if:

$$n.\mathsf{R}_K + d_1(n) \geq n.w + 2log(\frac{1}{\epsilon(n)}), \tag{6.33}$$

$$n.R_K + d_1(n) - 2\log\frac{1}{\epsilon(n)} \leq b(n). \tag{6.34}$$

On the other hand, for a weakly symmetric wiretap channel,

$$n.w \geq n.\mathrm{C}_{\mathsf{W}} \geq n.\mathrm{C}_{\mathsf{T}} \geq b(n) + d_1(n),$$

and from (6.33),

$$n.\mathsf{R}_K + d_1(n) \geq b(n) + d_1(n) + 2log(\frac{1}{\epsilon(n)})$$

$$\Rightarrow n.\mathsf{R}_K \geq b(n) + 2log(\frac{1}{\epsilon(n)}). \tag{6.35}$$

To satisfy (6.34) and (6.35) simultaneously, we should set $d_1(n) = 0$ and have

$$n.\mathsf{R}_K - 2log(\frac{1}{\epsilon(n)}) = b(n).$$

The resulting coding scheme is then

1. Encoding:

$$\mathbf{OTP}^{\epsilon}.\mathbf{enc}[\mathsf{h}_S, \mathsf{ECC}](m) = \mathbf{OTP}^{\epsilon}.\mathbf{enc}[\mathsf{h}_S, \mathsf{ECC}](m) = \mathsf{ECC}\big(m \oplus \mathsf{h}_S(K)\big);$$

2. Decoding:

$$\mathbf{OTP}^{\epsilon}.\mathbf{dec}(Y) = \mathbf{OTP}^{\epsilon}.\mathbf{dec}(Y) = \mathsf{ECC}.\mathsf{dec}(Y) \oplus \big(\mathsf{h}_S(K)\big).$$

The achievable rate of the construction is $\min(R_K, \mathrm{C}_{\mathsf{T}})$, where C_{T} is the capacity of the main channel.

6.6 Using the construction in practice

We discussed the asymptotic behaviour of the proposed construction in Section 6.4. We are also interested in finite-length behaviour of the construction in practice.

6.6.1 Single block encryption

The bounds in Theorems 6.3 and B.4.3 corresponding to (6.13) and (6.29) enable finite-length analysis of a single block encryption.

Example 6.1. *Consider a setting where* T *is noiseless and* W *is a BSC, with error probability 0.2. Suppose a shared key of rate* $R_K = 0.4$ *is available. Alice wants to send a message* m *of length 1000 bits to Bob with secrecy guarantee of* $\epsilon \leq 2^{-100}$*. When the main channel is noise-free, both constructions become the same.*

From (6.13) (or (B.15)),

$$n.R_k + d_1 + n.\nu \geq n.w + 2log\frac{1}{\epsilon} + 2.$$

For a BSC with error probability 0.2, $H_\infty(BSC) = -\log(1-0.2) = 0.32$ *and since the main channel is noise-free,* $w = b + d_1$*. Thus,*

$$0.4n + d_1 + 0.32n \geq 1000 + d_1 + 202$$

$$\Rightarrow 0.72n \geq 1202 \Rightarrow n \geq 1670 \quad and \quad d_1 \geq 670.$$

For Alice to send a message m of length b to Bob with perfect security, she can use Shannon's approach and use a OTP encryption algorithm to perfectly mask the message. Note that in the above example, the shared key for encrypting a 1000 bits message is at least $n.R_K \geq 0.4 \times 1670 = 668$ bits. By comparing this key length with the regular OTP that requires a key as long as the message, we can see that the required length of key is decreased by 332 bits due to the use of noise over the wiretap channel.

6.6.2 Encryption of 2^t blocks

To encrypt 2^t blocks for a fixed t, we can still use the seed recycling technique. However, Lemma 6.5 upper-bounds the distinguishing advantage of a group of 2^t encrypted blocks when the same seed is used for encryption. The distinguishing advantage of each encrypted block in this case is less than the bound in Lemma 6.5, which is 2^t times the advantage of a single encrypted block with a fresh seed. We are interested in a tighter guarantee on the security of each encrypted block when the same seed is used for encryption. We show such a tight bound can be found by making the construction of "t-resilient" extractor.

t-resilient extractors. Performance of strong extractors with respect to multiple given sources was investigated in [8], where the authors consider a true random number generator that is operating in a hostile environment where an adversary can influence the distribution to be one of the 2^t distributions. A t-resilient extractor is required to output almost uniform randomness with high probability, in this hostile environment, when the seed is chosen uniformly random.

Definition 6.7. [8] A seeded extractor is called a t-resilient extractor if its output is ϵ-close to uniform for 2^t pre-determined source distributions with probability at least $1 - \epsilon$, when the seed is chosen uniformly random.

Explicit constructions of t-resilient extractors from ℓ-wise independent UHF are given in [8]. We show for a range of parameters in **KHtE*** construction, the construction has *t-resilience* in the sense that each coded block is ϵ close to the uniform distribution with high probability. The construction can be interpreted

as a "two-source t-resilient extractor", which extracts from channel randomness as well as a second source that is the input to the channel. The 2^t pre-determined source distributions can be any combination of distributions over the channel's input and randomness. This construction of a two-source t-resilient extractor is of independent interest, for example, in the study of true random number generators.

Lemma 6.6. *Let $\{\mathsf{h}_s | s \in \mathcal{S}\}$ be a family of pair-wise universal hash functions $\mathsf{h}_s : \{0,1\}^{d_2} \to \{0,1\}^b$ for uniformly chosen s, and $\mathsf{F} : \{0,1\}^{b+d_1} \to \{0,1\}^\ell$ be an injective function ($\ell \geq b + d_1$). For a channel $\mathsf{CH} : \{0,1\}^\ell \to \{0,1\}^w$ with transition probability matrix $\mathbf{CH}$, where $H_\infty(\mathsf{CH}) \geq \nu$, a uniform random variable $D \in \{0,1\}^{d_1}$ and a random variable $X \in \{0,1\}^{d_2}$ such that $H_\infty(X) + d_1 \leq b$, with probability (over uniform random S) at least $1 - 2^{-u}$,*

$$\mathbf{SD}\Big(\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X) \| D\big)\Big); U_w\Big) \leq \epsilon, \tag{6.36}$$

where

$$u \geq H_\infty(X) + d_1\nu - w - 3\log(\frac{1}{\epsilon}) - 4. \tag{6.37}$$

In particular, $\mathsf{CH}\big(\mathsf{F}\big(\mathsf{h}_S(X)\big)$ is a two-source t-resilient extractor for

$$t \leq H_\infty(X) + d_1 + \nu - w - 4\log(\frac{1}{\epsilon}) - 4. \tag{6.38}$$

Proof. Let $z \in \{0,1\}^w$ be an output of $\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_s(X) \| D\big)\Big)$. An output z is called *light* if $\frac{1}{2^w} - \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_s(X) \| D\big)\Big) = z] \geq \frac{1}{2^w} \cdot \epsilon$. Then a hash function h_s is called *good* if the number of its light outputs is less than $2^w \cdot \epsilon$. More precisely, let $\mathcal{L}(\mathsf{h}_s)$ denote the set of light outputs of h_s. Then h_s is good if $|\mathcal{L}(\mathsf{h}_s)| < 2^w \cdot \epsilon$; otherwise, it is called *bad*. We can readily bound $\mathbf{SD}\Big(\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X) \| D\big)\Big); U_w\Big)$ for a good hash function h_s as

$$\mathbf{SD}\Big(\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X) \| D\big)\Big); U_w\Big) \leq 2^w(\frac{1}{2^w} \cdot \frac{\epsilon}{2}) + \frac{1}{2^w}(2^w \cdot \frac{\epsilon}{2}) = \epsilon.$$

We then proceed to bound $\Pr[\mathsf{h}_S \text{ is bad}]$. First, by Markov's inequality for the random variable $|\mathcal{L}(\mathsf{h}_S)|$,

$$\Pr[\mathsf{h}_S \text{ is bad}] = \Pr[|\mathcal{L}(\mathsf{h}_S)| \geq 2^w \cdot \frac{\epsilon}{2}] \leq \frac{\mathbb{E}_S\left(|\mathcal{L}(\mathsf{h}_s)|\right)}{2^w \cdot \frac{\epsilon}{2}}. \tag{6.39}$$

Denote

$$\Lambda(s,z) = \begin{cases} 1, & \text{if } \frac{1}{2^w} - \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_s(X) \| D\big)\Big) = z] \geq \frac{1}{2^w} \cdot \frac{\epsilon}{2}. \\ 0, & \text{otherwise.} \end{cases}$$

We have

$$\begin{aligned}\mathbb{E}_S\left(|\mathcal{L}(\mathsf{h}_S)|\right) &= \sum_{s\in\mathcal{S}} \Pr[S=s].\sum_{z\in\{0,1\}^w} \Lambda(s,z)\\ &= \sum_{z\in\{0,1\}^w}\sum_{s\in\mathcal{S}} \Pr[S=s].\Lambda(s,z)\\ &= \sum_{z\in\{0,1\}^w} \left(\Pr[\frac{1}{2^w} - \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big)=z] \geq \frac{1}{2^w}\cdot\frac{\epsilon}{2}\right).\end{aligned}$$

$\Pr[\frac{1}{2^w} - \Pr[\mathsf{CH}\Big(\mathsf{F}\big(\mathsf{h}_S(X)\|D\big)\Big) = z] \geq \frac{1}{2^w}\cdot\frac{\epsilon}{2}$ is bounded by the application of Chebychev's inequality as follows,

$$\begin{aligned}&\Pr\Big[\big(\frac{1}{2^w} - \Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D)) = z]\big) \geq \frac{1}{2^w}\cdot\frac{\epsilon}{2}\Big] \leq\\ &\qquad\frac{\mathbb{E}_S\left((\frac{1}{2^w} - \Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D)) = z])^2\right)}{\left(\frac{1}{2^w}\cdot\frac{\epsilon}{2}\right)^2}.\end{aligned} \tag{6.40}$$

The numerator is bounded as:

$$\mathbb{E}_S\big((\frac{1}{2^w} - \Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D) = z])^2\big) \tag{6.41}$$

$$= \frac{1}{2^{2w}} - \frac{2}{2^w}\cdot\mathbb{E}_S\big(\Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D) = z])\big) + \mathbb{E}_S\left(\Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D) = z]\right)^2 \tag{6.42}$$

$$\leq \frac{1}{2^{2w}} - \frac{2}{2^w} + \mathbb{E}_S\left(\Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D) = z]\right)^2 \tag{6.43}$$

$$\leq \mathbb{E}_S\left(\Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D) = z]\right)^2 \tag{6.44}$$

$$\leq \mathbb{E}_S\Pr[Z=z]\cdot\frac{1}{2^w}\cdot\left(2^{-(H_\infty(X)+d_1+\nu-w)} + 2^{-(\nu+b-w)}\right) \tag{6.45}$$

$$\leq \Pr[Z=z]\cdot\frac{2}{2^w}\cdot\mathbb{E}_S\left(2^{-(H_\infty(X)+d_1+\nu-w)}\right). \tag{6.46}$$

Here, (6.43) is obtained from (6.42) because $\mathbb{E}_S\big(\Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D) = z])\big) \leq 1$, where (6.42) is the expansion of (6.41). Since $\frac{1}{2^{2w}} - \frac{2}{2^w} < 0$, (6.44) holds, and then using (6.24) we obtain (6.45). Finally, (6.46) is concluded from (6.45) since $H_\infty(X) + d_1 \leq b$. Now as long as $H_\infty(X) + d_1 + \nu \geq w + 3\log(\frac{1}{\epsilon}) + u + 4$,

$$\mathbb{E}_S\big((\frac{1}{2^w} - \Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D) = z])^2\big) \leq \Pr[Z=z]\cdot\frac{2^{-u-3}\epsilon^3}{2^w},$$

which when substituted into (6.40) gives

$$\Pr[\frac{1}{2^w} - \Pr[\mathsf{CH}(\mathsf{F}(\mathsf{h}_S(X)\|D)) = z] \geq \frac{1}{2^w}\cdot\frac{\epsilon}{2}] \leq 2^{-u}\cdot\frac{\epsilon}{2},$$

which in turn, when substituted into (6.39), gives the desired bound:

$$\Pr[\mathsf{h}_S \text{ is bad}] \leq 2^{-u}.$$

From the union bound, in order to make the extractor t-resilient, one needs to have $2^{t-u} \leq \epsilon$, which gives $t \leq u - \log(\frac{1}{\epsilon})$.

□

Theorem 6.5. *For the keyed seeded encryption scheme* $\mathsf{KSEnc} = \mathbf{KHtE}^*[\mathsf{h}_S, \mathsf{ECC}]$ *in Section 6.4 satisfying* $n.\mathsf{R}_K + d_1(n) + \nu \geq w + t + 4log(\frac{1}{\epsilon(n)}) + 4$*, each encrypted block is* ϵ*-close to the uniform distribution with probability* $1 - \epsilon$*, and* $Adv^{ds}(\mathsf{KSEnc}; \mathsf{W}^n) \leq 4\epsilon(n) - 2\epsilon(n)^2$ *for* 2^t *pre-determined input distributions.*

Proof. The proof follows similar steps as the proof of Theorem 6.3. We first bound Adv^{dsu} of $\mathbf{KHtE}^*$, and then using $Adv^{ds} \leq 2Adv^{dsu}$, we can bound Adv^{dsu}. Parameters of $\mathbf{KHtE}^*$ construction satisfy (6.38). Therefore, the application of Lemma 6.6 immediately proves each encrypted block is $\epsilon(n)$-close to the uniform distribution with probability $1 - \epsilon(n)$, where the probability is over the choice of a random seed. By taking average over the choice of seed,

$$Adv^{dsu}(\mathsf{KSEnc}; \mathsf{W}^n) \leq \epsilon(n) \cdot (1 - \epsilon(n)) + 1 \cdot \epsilon(n) = 2\epsilon(n) - \epsilon^2(n)$$

$$\Rightarrow Adv^{ds}(\mathsf{KSEnc}; \mathsf{W}^n) \leq 4\epsilon(n) - 2\epsilon(n)^2.$$

□

The above theorem shows the same seed can be used for encrypting 2^t blocks (one can view each block as a shift to the input distributions of the extractor and therefore, using a same seed for 2^t messages means having 2^t pre-determined distributions), while each block is guaranteed to be ϵ-close to the uniform distribution with probability at least $1-\epsilon$ over the choice of seed. For the convenience of representation, when parameters of the $\mathbf{KHtE}^*$ construction satisfy Theorem 6.5, we denote it by $\mathbf{KHtE}^*_t$.

Remark 6.3. *It is possible to amortize the seed length in* $\boldsymbol{KHtE}^*$ *and achieve capacity when the number of blocks goes to infinity. For* $t \geq 1$*, let* $\mathsf{CH} = \mathsf{CH}_0 \| \mathsf{CH}_1^t$ *be a channel such that* $\mathsf{CH}_0 : \{0,1\}^{\ell_0} \to \{0,1\}^{w_0}$ *and* $\mathsf{CH}_1 : \{0,1\}^{\ell} \to \{0,1\}^{w}$*. The seed recycling encryption scheme* $\mathsf{KRSE}_{2^t}[\mathsf{KSEnc}, \mathsf{ECC}_0]$*, with* $\mathsf{KSEnc} = \mathbf{KHtE}^*_t[\mathsf{h}_S, \mathsf{ECC}_1, \mathsf{ECC}_2]$ *and* $\mathsf{ECC}_0 : \mathcal{S} \to \{0,1\}^{\ell_0}$*, uses* KSEnc *to encrypt* 2^t *blocks of* b *bits with a same random seed* $S \in \mathcal{S}$ *and concatenates* $\mathsf{ECC}_0(S)$ *to the encrypted block. Then by using the triangular inequality*

it follows that

$$Adv^{ds}(\mathsf{KRSE}_{2^t}; \mathsf{CH}) \leq 2^t \cdot Adv^{ds}(\mathsf{KSEnc}; \mathsf{CH}_1).$$

Let $t = O(\log n)$ *and* $R_{\mathsf{KRSE}_{2^t}}(n)$ *denote the rate of* KRSE_{2^t} *and* $R_{\mathsf{KSEnc}}(n)$ *the rate of* $R_{\mathsf{KRSE}_{2^t}}(n)$*, then* $\lim_{n\to\infty} R_{\mathsf{KRSE}_{2^t}}(n) = R_{\mathsf{KSEnc}}(n)$*, which shows we can amortize the cost of sending a seed over multiple usages of the channel. Note that when the parameters of* KSEnc *are chosen according to Theorem 6.5 instead of Theorem 6.3, still the capacity of a degraded weakly symmetric channel is achieved by the use of a capacity-achieving family of error correcting code. The difference between the length of* $d_1(n)$ *in Theorem 6.5 and Theorem 5.2, ignoring some constant terms, is the term "t", which can be seen as the price of achieving t-resilience. For* $t = O(\log n)$*,* $\lim_{n\to\infty} \frac{t}{n} = 0$*.*

6.7 Related works

Wiretap channel constructions

Hayashi and Matsumoto [66] used an invertible UHF to construct modular wiretap encryption systems satisfying strong secrecy requirement for random messages that are capacity-achieving under certain conditions. Bellare et al. [11] introduced the notion of semantic security for a wiretap channel and proposed a novel approach to construct a capacity-achieving scheme over a wide range of discrete symmetric wiretap channels using invertible extractors with semantic security. Their security proof has two steps and semantic security is guaranteed if the randomised encryption system is *message linear* and *separable* (See Definition [12, Section 4.6].). The construction in [11] uses a UHF (e.g., using finite field multiplication UHF), followed by a linear ECC, and satisfies these properties. Tal and Vardy [131] generalized this construction to a wider class of channels by using letter splitting method. Tyagi and Vardy [138] constructed semantically secure wiretap codes for Gaussian wiretap channels with infinite alphabet. This construction however, provides uniform message security only. An alternative efficient semantically secure wiretap code for discrete symmetric wiretap channels is given in [120]. The construction is called *Hash-then-Encode (***HtE***)* and uses universal hash functions. In Section 6.5.1, we gave a more detailed comparison of existing modular constructions.

An explicit construction using polar codes, with weak security, for BISCs (Binary Input Symmetric Channel) was proposed in [71]. In [87], a polar code based capacity-achieving construction with strong secrecy for BISC was given[8].

[8]Using the framework of [11] (relation between uniform message and any message security), the construction of [87] was later shown to have semantic security.

Wiretap channel with extra resources

Wiretap channels with extra resources are considered in a class of works. Public communication between the legitimate users is considered in [92] and it is shown that this extra resource increases the secrecy capacity of the setting. Lai et al. [82] consider a modulo-additive wiretap channel with noisy feedback, and characterize its capacity. The general wiretap channel with noisy feedback is studied in [60]. Ahlswede and Cai [1] characterized the secrecy capacity of the physically degraded wiretap channel with secure output feedback. An upper-bound for the secrecy capacity of general wiretap channel with secure feedback is given in [5]. For the case of physically degraded wiretap channel, it is shown that receiver can ignore what they receive and substitute secure "fresh" randomness (that plays the role of a secret key) with secure feedback. A wiretap channel with a shared secret key is studied in [145], where distortion is allowed at the receiver. Merhav [94] considered the same setting in presence of side information (correlated to the source), which is available both to the receiver and the wiretapper, and characterized the secrecy capacity for the degraded wiretap channel. In [78], the secrecy capacity of a general wiretap channel with a shared secret key of a given rate is derived. The construction uses random encoding, and is for uniformly distributed messages. The construction does not consider distortion or side information. Secure broadcasting with independent secret keys is studied in [113].

6.8 Concluding remarks

We proposed the first construction of modular keyed wiretap codes with semantic security, that reduces to wiretap code or an ϵ-OTP, if the key rate or the secrecy capacity of the wiretap channel is zero, respectively. The construction achieves the secrecy capacity of the wiretap channels with weakly symmetric main and wiretapper's channel. We compared our construction with other constructions that achieve similar properties and showed the advantages of our construction. Similar to other modular constructions, our construction requires a seed that must be reliably sent to the receiver. We discussed seed recycling where the same seed is used for the encryption of multiple blocks, allowing the seed length to be amortized over multiple blocks leading to a capacity-achieving construction. We proposed a stronger seed recycling approach where instead of security guarantee for a group of blocks, the guarantee is for individual message blocks. This seed recycling approach enables communication of finite-length messages with security guarantee for each individual block. Our analysis provides the first step towards finite-length analysis of the construction for a given level of reliability and secrecy. Another interesting direction for future works is to explore if the construction can achieve the secrecy capacity of other types of channels.

Part III

Information-Theoretic Secret Key Agreement

Chapter 7

A Capacity-Achieving One-Message Key Agreement With Finite Blocklength Analysis[1]

Abstract. Information-theoretic secret key agreement (SKA) protocols are a fundamental cryptographic primitive that are used to establish a shared secret key between two or more parties. In a two-party SKA in source model, Alice and Bob have samples of two correlated variables that are partially leaked to Eve, and their goal is to establish a shared secret key by communicating over a reliable public channel. Eve must have no information about the established key. In this chapter, we study the problem of one-message secret key agreement where the key is established by Alice sending a single message to Bob. We propose a one-message SKA (OM-SKA) protocol, prove that it achieves the one-way secret key capacity, and derive finite blocklength approximations of the achievable secret key length. We compare our results with existing OM-SKAs and show the protocol has a unique combination of desirable properties.

7.1 Introduction

Key agreement is a fundamental problem in cryptography: Alice wants to share a secret key with Bob that will be completely unknown to Eve. In this chapter, we consider information-theoretic secret key agreement (SKA) that uses physical layer assumptions to achieve security. Wyner [143] pioneered the use of physical layer properties, in his case noise in the channel, for secure message transmission. The approach has found significant attention because of its application to many wireless communication settings, and its information-theoretic security, which provides security even if a quantum computer exists. Information-theoretic secret key agreement was first proposed by Maurer, and Ahlswede and Csiszár independently [2, 92]. In the so-

[1]The content of this chapter is submitted to ISIT 2020 [122].

called *source model* of [2], Alice and Bob have samples of correlated random variables (RVs) X and Y, and want to agree on a secret key by exchanging messages over a public (authenticated and error free) channel that is visible to the eavesdropper Eve, who has initial side information Z about the correlated variables. The three variables X, Y, and Z have a joint distribution P_{XYZ} that is public.

In this chapter, we study *one-message secret-key agreement* (OM-SKA), where the key is established by Alice sending a single message to Bob. The problem is first studied by [74] and [73], and later, OM-SKA constructions based on polar codes were proposed in [105] and [29]. The problem is important in practice because it avoids interaction between Alice and Bob that would require stateful protocols with vulnerabilities in implementation. It is also interesting theoretically due to [74] because it is related to circuit polarization and immunization of public-key encryption, or it can be used for oblivious transfer [23].

Efficiency of an SKA is measured by the length ℓ of the established secret key. When Alice, Bob and Eve have n independent samples of their random variables, denoted by (X^n, Y^n, Z^n), the *rate of the secret key* is given by ℓ/n. The *secret key capacity* associated with a distribution P_{XYZ} is the highest achievable key rate when $n \to \infty$.

The secret key (SK) capacity $C_s(X, Y|Z)$ of a general distribution is a long-standing open problem. When the three variables form a Markov Chain $X - Y - Z$, the secret key capacity is given by $C_s(X, Y|Z) = I(X; Y|Z)$ [2].

The secret key capacity of a general distribution when the public communication channel is one-way (i.e., only Alice sending to Bob), is called *the one-way secret key (OW-SK) capacity*, and is denoted by $C_s^{ow}(X, Y|Z)$. This capacity, by definition, is a lower-bound to the SK capacity, that is $C_s^{ow}(X, Y|Z) \leq C_s(X, Y|Z)$ [2].

In a real life deployment of SKA protocols, n, the number of available initial samples to each party, is finite and the efficiency of a protocol is measured by ℓ. In [68], bounds on secret key length in finite blocklength regime are established using higher order approximations. The given lower-bound of [68], however, cannot be used for OM-SKA because the proposed SKA protocol is interactive and uses many ($\mathcal{O}(n)$) rounds of public communication.

The first explicit constructions of OM-SKA protocols are given in [73, 74]. The construction of [74] uses the concatenation of a random linear code with a Reed-Solomon code to allow Bob to recover the variable of Alice, and use that to derive a shared key. The protocol achieves the OW-SK capacity. There is no explicit finite blocklength analysis of this construction in [74], although as shown in Proposition 7.1, the work of [73] can be extended to obtain a lower-bound on the key length. Renes, Renner and Sutter [105], and Chou, Bloch and Abbe [29] proposed constructions of OM-SKA using polar codes. These constructions are capacity-achieving, but their finite blocklength analysis, which is not discussed in [29, 105], will be directly

related to the finite blocklength analysis of the underlying polar codes.

Our work. We propose a OM-SKA protocol, analyze its security and derive a finite blocklength lower-bound for the key length. The construction (and hence the bound) holds for the more general case that the n samples that are held by the parties are independent, but could be drawn from different distributions (this was called "independent experiments" in [108]). The construction achieves the OW-SK capacity and provides a finite blocklength lower-bound for one-way SKA. We compare the finite blocklength lower-bound of the protocol with the only other lower-bounds that we derived based on the constructions in [73], and show its superior performance. In particular, as we illustrate in a numerical example, the latter bound of [74] becomes positive only when n, the number of samples, is larger than a high threshold ($\sim 10^9$ bits), while our bound is positive for values of n starting from 10^3 bits (See Figure 7.1).

An important property of our OM-SKA protocol is that it gives an explicit finite blocklength upper-bound on the required public communication for achieving the OW-SK capacity. The bound only depends on n, P_{XYZ}, and key's secrecy and reliability properties. The full comparison of our protocol with all the known OM-SKA is given in Table 7.1.

Related works. Maurer [92] and Ahlswede and Csiszár [2] initiated the study of information-theoretic secret key agreement, and derived lower and upper-bounds on the secret key capacity of the source model. There have been many follow up works, most notably for our study, deriving upper and lower-bounds for the secret key length with matching (i.e., optimum) second order approximations [68], assuming the Markov chain $X - Y - Z$ holds.

One-way secret key (OW-SK) capacity was introduced by Ahlswede and Csiszár [2], who derived an expression to calculate OW-SK capacity. Holenstein and Renner [74] considered one-message SKA protocols and gave constructions that achieve OW-SK capacity. Their constructions have the computational complexity of $\mathcal{O}(n^2)$. In [105] and [29], two capacity-achieving OM-SKA constructions using polar codes are given. Although, these SKA protocols require specific construction of a polar code (i.e., computation of the index sets) for the underlying distribution, they can benefit from progresses in polar code constructions. These codes do not provide finite blocklength bounds for the key length.

Organization. The background is given in Section 7.2 and in Section 7.3 we discuss the OW-SK capacity. Our main results are in Section 7.4. We conclude this chapter in Section 7.5 by comparing our results with previous works.

7.2 Background

7.2.1 Notations and definitions

We denote random variables (RVs) with upper-case letters (e.g., X), and their realizations with lower-case letters, (e.g., x). Calligraphic letters show the alphabet of a random variable (e.g., $\mathcal{X}$). The probability mass function (p.m.f) of an RV X is denoted by $P_X(x) = \Pr(X = x)$.

Shannon entropy of an RV X over the alphabet $\mathcal{X}$ is $H(X) = -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x)$. The average conditional min-entropy is $\tilde{H}_\infty(X|Y) = -\log \mathbb{E}_{P_Y} \max_{x\in\mathcal{X}} P_{X|Y}(x|Y)$ [44]. The maximum number of extractable random bits from a random variable is given by its *smooth min-entropy* [107] defined as $H^\epsilon_\infty(X) = \max_{Y:SD(X,Y)\leq\epsilon} H_\infty(Y)$.

The *mutual information* between X and Y is $I(X;Y) = H(X) - H(X|Y)$. The conditional mutual information between X and Y given Z is $I(X;Y|Z) = H(X|Z) - H(X|Y,Z)$.

If for RVs (X,Y,Z) the Markov relation $X - Y - Z$ holds, i.e., $P_{XYZ}(x,y,z)P_Y(y) = P_{XY}(x,y)P_{YZ}(y,z)$ then, $I(X;Y|Z) = H(X|Z) - H(X|Y)$.

The *statistical distance* between two RVs X and Y with p.m.f's P_X and P_Y, defined over a common alphabet $\mathcal{W}$, is given by $\mathbf{SD}(X;Y) = \frac{1}{2}\sum_{w\in\mathcal{W}} |P_X(w) - P_Y(w)|$.

Lemma 7.1 (Berry-Esseen Inequality [18, 50])**.** *Let P_{W^n} be an IID distribution, then for any $-\infty < \alpha < \infty$*

$$\left| \Pr\left(\sum_{j=1}^{n} W_j \leq n\mu - \alpha\sqrt{\Delta n} \right) - Q(\alpha) \right| \leq \frac{3\rho}{\Delta^{3/2}\sqrt{n}},$$

where $\mu = \mathbb{E}\{W\}, \Delta = \mathbb{V}\mathrm{ar}\{W\}, \rho = \mathbb{E}\{|W-\mu|^3\}$, and $Q(\cdot)$ is the tail probability of the standard Gaussian distribution.

7.2.2 Universal Hash Functions

Definition 7.1 (2-Universal Hash Family (2-UHF)[25])**.** A family $\{h_s | s \in \mathcal{S}\}$ of functions $h_s : \mathcal{X} \to \mathcal{Y}$ is a 2-UHF if for any $x \neq x'$, $\Pr\{h_S(x) = h_S(x')\} \leq \frac{1}{|\mathcal{Y}|}$, where the probability is on the uniform choices over $\mathcal{S}$.

The *Leftover Hash Lemma* (LHL) [77] states that 2-UHFs extract randomness from a source with a lower-bound on its min-entropy [77]. The average-case version of LHL is given in [45].

7.2.3 SKA in source model

An information-theoretic key agreement protocol has two main steps [24]: *information reconciliation* where the goal is to arrive at a common string, and *privacy amplification* where the goal is to extract a secret key

from the shared string. Sometimes an initiation phase is included in the protocol during which protocol parameters and public values are determined. The following definitions for information-theoretic SKA are consistent with the corresponding ones in [74].

Definition 7.2 (See [68, 74, 139])**.** Let Alice and Bob be two parties with inputs X and Y and local independent randomness sources U_A and U_B, respectively. A random variable K over $\mathcal{K}$ is an (ϵ, σ)-Secret Key (in short (ϵ, σ)-SK), if there exists a protocol with public communication $\boldsymbol{F}$, and two functions $K_A(X, U_A, \boldsymbol{F})$ and $K_B(Y, U_B, \boldsymbol{F})$, that satisfy the following reliability and security properties:

$$\text{(reliability)} \quad \Pr\left(K_A = K_B = K\right) \geq 1 - \epsilon, \tag{7.1}$$

$$\text{(security)} \quad \mathbf{SD}\left((K, \boldsymbol{F}, Z); (U, \boldsymbol{F}, Z)\right) \leq \sigma, \tag{7.2}$$

where U is sampled uniformly from $\mathcal{K}$, and Z is a random variable corresponding to Eve's side information.

Efficiency of an SKA protocol is in terms of the secret key length that is obtained for a given set of variables.

Definition 7.3 ([68])**.** For a given source model (X, Y, Z) with joint distribution P_{XYZ}, and pair of reliability and secrecy parameters $(\epsilon, \sigma) \in [0, 1)^2$, the highest achievable key length is denoted by $S_{\epsilon,\sigma}(X, Y|Z)$, and is defined by the supremum of the key length $\log|\mathcal{K}|$ for all (ϵ, σ)-SKA protocols Π :

$$S_{\epsilon,\sigma}(X, Y|Z) = \sup_{\Pi}\{\log|\mathcal{K}| \mid K \text{ is } (\epsilon, \sigma)\text{-SK for } (X, Y, Z)\}.$$

7.3 One-way secret key capacity

Ahlswede and Csiszár [2] derived the "forward key capacity" (or what we call the one-way secret key capacity) of the source model. Let $X^n = (X_1, \ldots, X_n)$, $Y^n = (Y_1, \ldots, Y_n)$ and $Z^n = (Z_1, \ldots, Z_n)$ denote n IID samples of the distribution P_{XYZ} that is publicly known, and consider a protocol family indexed by n, achieving a secret key of length $\ell(n)$.

The *secret key rate* of the protocol, indexed by n, is given by $R(n) = \ell(n)/n$, and the achievable rate of the family is given by $R^* = \liminf_{n\to\infty} \ell(n)/n$. The secret key *capacity* is the supremum of the achievable key rate of all protocol families for the same setting. The following definition follows the definitions in [68].

Definition 7.4 (One-way Secret Key Capacity [2])**.** For a source model with distribution $P_{X^nY^nZ^n}$, the secret

[2] In some works including [73, 105, 108] the term "capacity" is reserved for physical channels, and for source model only "key rate" is used.

key capacity $C_s^{ow}(X,Y|Z)$ is defined by

$$C_s^{ow}(X,Y|Z) = \sup_{\Pi_n} \liminf_{n\to\infty} \frac{1}{n} S^{ow}_{\epsilon_n,\sigma_n}(X^n,Y^n|Z^n), \tag{7.3}$$

where the supremum is over all protocols Π_n with reliability and secrecy parameters ϵ_n, σ_n, such that $\lim_{n\to\infty}(\epsilon_n+\sigma_n)=0$ and $S^{ow}_{\epsilon_n,\sigma_n}(X^n,Y^n|Z^n)$ is the corresponding key length from the OW-SKA protocol Π_n.

It was shown [2, Theorem 1] that one-way secret key capacity is given by the supremum of $H(U|Z,V) - H(U|Y,V)$, where the supremum is over all distributions P_{UV} satisfying $V - U - X - YZ$. This result also follows from [34, Corollary 2]. Holenstein and Renner [74, Theorem 3] proved the supremum can be taken over all distributions $P_{UV|X}$ satisfying $X - U - V$, and that the supremum can always be achieved by a OM-SKA protocol [73, Theorem 3.3], and so we have the following theorem for OW-SKA capacity.

Theorem 7.1 (Theorem 1 of [74])**.** *For any given source model (X,Y,Z) with IID distribution $P_{X^nY^nZ^n}$, the OW-SK capacity is given by*

$$C_s^{ow}(X,Y|Z) = \max_{P_{UV|X}} H(U|Z,V) - H(U|Y,V), \tag{7.4}$$

where optimization is over joint distributions $P_{UV|X}$'s such that $X - U - V$ holds.

Finding explicit solution to (7.4) in general is not known. For some source models, the optimizing $P_{UV|X}$ can be analytically calculated [73, 74], and be used to construct OM-SKA that achieves the OW-SK capacity [74].

Corollary 7.1 (Corollary 4 of [105])**.** *For a source model with IID distribution $P_{X^nY^nZ^n}$ such that for any RV U satisfying $U - X - (Y,Z)$, we have $I(U;Y) \geq I(U;Z)$,*

$$C_s^{ow}(X,Y|Z) = H(X|Z) - H(X|Y). \tag{7.5}$$

A special case of Corollary 7.1 is when the Markov chain $X - Y - Z$ holds. In this case, the OW-SK capacity is equal to $C_s^{ow}(X,Y|Z) = H(X|Z) - H(X|Y) = I(X;Y|Z)$.

7.4 Π_{SKA}: A one-message SKA protocol

Consider the source model setting, and assume Alice, Bob and Eve have their corresponding n components of the source (X^n,Y^n,Z^n). Let the required secrecy and reliability parameters of the key be σ and ϵ, respectively. Alice and Bob choose two 2-UHFs $h_s : \mathcal{X}^n \to \{0,1\}^t$ and $\hat{h}_{s'} : \mathcal{X}^n \to \{0,1\}^\ell$, and share (over

Protocol 1: $\mathbf{\Pi}_{\text{SKA}}$: A Capacity-achieving SKA

Public Information: P_{XYZ}
Input: $n-$fold samples $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, ϵ, σ.
Output: Key estimates k_A and k_B.

`// Initiation Phase`

- Alice and Bob, (i) find and share λ, and ℓ and t for the hash functions $h_s : \mathcal{X}^n \to \{0,1\}^t$ and $\hat{h}_{s'} : \mathcal{X}^n \to \{0,1\}^\ell$, (ii) generate and share the seeds $s \in \mathcal{S}$ and $s' \in \mathcal{S}'$ for the hash function.

`// Information Reconciliation Phase`

1 Alice sends the hash value $v = h_s(x^n)$ to Bob.
2 Bob forms a list of guesses for x^n,

$$\mathcal{T}(X^n|y^n) = \{\hat{x^n} : -\log P_{X^n|y^n}(\hat{x^n}|y^n) \leq \lambda\}. \tag{7.6}$$

3 Bob finds, if exists, a unique $\hat{x^n} \in \mathcal{T}(X^n|y^n)$ such that $h_s(\hat{x^n}) = v$.
4 **if** *no* $\hat{x^n}$ *was found* ***or*** $\hat{x^n}$ *was not unique* **then**
  Abort the protocol.

`// Key Extraction Phase`

5 Alice computes $k_A = \hat{h}_{s'}(x^n)$.
6 Bob computes $k_B = \hat{h}_{s'}(\hat{x^n})$.

public channel) two uniformly random seeds $s \in \mathcal{S}$ and $s' \in \mathcal{S}'$ for the two families. (In the following we show how the values of t and ℓ will be determined.) In the rest of this paper, we use the multiplicative hash family (See Section 7.2) for the 2-UHF.

Our SKA protocol ($\mathbf{\Pi}_{\text{SKA}}$) works as follows: Alice uses $h_s(\cdot)$ to compute the hash value of her sample vector x^n, and sends it to Bob; Bob uses the received hash value, his sample vector y^n, and the known probability distribution of the source, to recover Alice's sample vector (*reconciliation*). The main idea behind the reconciliation technique of Protocol 1, used by Bob, is to divide the range of $P_{X^n|Y^n=y^n}$ values into two parts, and search in only the main part to find Alice's vector. This reduces search complexity at the cost of increased error. By choosing an appropriate value for t, Bob can bound the reconciliation error to ϵ. The transmitted hash value will also be used in conjunction with their vector z^n to learn about the key, and so longer key hash values (reduced error probability) will result in shorter keys. Alice and Bob will estimate the total leaked information about their common strings, and remove it during the *privacy amplification* (key extraction) phase that is implemented by using a second 2-UHF hash function $\hat{h}_{s'}$.

The security and reliability of the protocol, and the choice of the hash functions' parameters that result in an (ϵ, σ)- SKA are given in Theorem 7.2. We prove the theorem for the case that the distribution $P_{X^nY^nZ^n} = \Pi_j P_{X_jY_jZ_j}$ is due to independent experiments that are not necessarily identical. Corollary 7.2 shows that the resulting bound from the theorem can be tightened for IID case.

Theorem 7.2. *Let the source model* (X^n, Y^n, Z^n) *be described by a joint distribution* $P_{X^nY^nZ^n} = \Pi_j P_{X_jY_jZ_j}$.

For any pair of real numbers (ϵ, σ) *where* $0 < \epsilon, \sigma < 1$, Π_{SKA} *Protocol 1 gives an* (ϵ, σ)*-SK with maximum key length of,*

$$\max(\ell_{\epsilon,\sigma}^{\mathbf{\Pi}_{\text{SKA}}}) = H(X^n|Z^n) - H(X^n|Y^n) - \sqrt{n} f_{\epsilon,\sigma}(|\mathcal{X}|) - \log \frac{4n^3}{\epsilon\sigma^2} + \mathcal{O}(\frac{1}{\sqrt{n}}), \tag{7.7}$$

where $f_{\epsilon,\sigma}(|\mathcal{X}|) = \sqrt{2}\log(|\mathcal{X}| \ + \ 3)\left(\sqrt{\log 1/\epsilon} + \sqrt{\log 2/\sigma}\right)$.

Proof. Reliability. Bob's recovery algorithm searches the set $\mathcal{T}(X^n|y^n)$ for vector(s) that their hash value match the received hash value, and fails in two cases: (i) x is not in the set, and (ii) there are more than one vector in the set whose hash value matches the received hash value v. Bob's failure probability $P_e = \Pr(K_A \neq K_B)$ is upper-bounded by finding the probabilities of the above two events. Each event corresponds to the possible samples of Alice, as shown below.

$$\begin{aligned}
\xi_1 &= \{x^n : -\log P_{X^n|Y^n}(x^n|y^n) > \lambda\} \\
\xi_2 &= \{x^n \in \mathcal{T}(X^n|y^n) : \exists\ \hat{x^n} \in \mathcal{T}(X^n|y^n) \text{ s.t.} \\
&\qquad\qquad h_S(\hat{x^n}) = h_S(x^n)\}.
\end{aligned}$$

To bound $\Pr(\xi_1)$, we use the result of [75, Theorem 2], for n-IID samples of a joint distribution that states:

$$\Pr[-\log P_{X^n|Y^n}(x^n|y^n) > H(X^n|Y^n) + n\delta\}] \leq \beta.$$

for $\beta = 2^{-\frac{n\delta^2}{2\log^2(|X|+3)}}$. By choosing

$$\lambda = H(X^n|Y^n) + n\delta_1, \tag{7.8}$$

where δ_1 satisfies $\epsilon_1 = 2^{\frac{-n(\delta_1)^2}{2\log^2(|\mathcal{X}|+3))}}$ for some chosen value of $\epsilon_1 \leq \epsilon$, we have $\xi_1 = \{x^n : -\log P_{X^n|Y^n}(x^n|y^n) > H(X^n|Y^n) + n\delta_1\}$, and $\Pr(\xi_1) \leq \epsilon_1$.

To bound $\Pr(\xi_2)$, we note that for a $\hat{x^n} \in \mathcal{T}(X^n|y^n)$, the collision probability with any other $x^n \in \mathcal{X}^n$ is bounded by $\Pr\left(h_S(\hat{x^n}) = h_S(x^n)\right) \leq 2^{-t}$ (Definition 7.1), and so the total probability that some element $\mathcal{T}(X^n|y^n)$ collides with an element in $\mathcal{X}^n$ is $|\mathcal{T}(X^n|y^n)| \cdot 2^{-t}$. That is

$$\Pr(\xi_2) \leq |\mathcal{T}(X^n|y^n)| \cdot 2^{-t}.$$

On the other hand, since the probability of each element of $\mathcal{T}$ is bounded by $2^{-\lambda}$, we have $2^{-\lambda}|\mathcal{T}(X^n|y^n)| \leq \Pr(\mathcal{T}(X^n|y^n))) \leq 1$, and we have $|\mathcal{T}(X^n|y^n)| \leq 2^{\lambda}$. Let $t = \lambda - \log\epsilon_2$ for some chosen value of $\epsilon_2 \leq \epsilon$. Then

we have $\Pr(\xi_2) \leq \epsilon_2$. That is

$$t = H(X^n|Y^n) + n\delta_1 - \log \epsilon_2 \tag{7.9}$$

The above shows that the choice of ϵ_1 determines δ_1, and then λ, which together with the choice of ϵ_2, determines t. Finally, $\epsilon = \epsilon_1 + \epsilon_2$ and $P_e \leq \epsilon$. Equation (7.9) clearly shows the relation between t and the error probability: smaller ϵ_1 and ϵ_2 give larger t. This is expected since larger t provides more information about X^n to Bob for reconciliation. We also note that larger information about X^n reduces achievable key length of the protocol.

Key secrecy. To show the secrecy of the key, we need to bound the statistical distance of the joint distribution of the derived key and the adversary's information, from the joint distribution of the uniform distribution and the adversary's information.

According to Lemma B.5.1 in Appendix B.5, we have

$$\begin{aligned}&\mathbf{SD}((\hat{h}_{S'}(X^n), h_S(X^n), S', S, Z^n);\\ &(U_\ell, h_S(X^n), S', S, Z^n)) \leq 2\epsilon' + \frac{1}{2}\sqrt{2^{t+\ell-\tilde{H}_\infty^{\epsilon'}(X^n|Z^n)}},\end{aligned} \tag{7.10}$$

We now note the following:

(ii) The relation between the smooth average min-entropy and the smooth conditional min-entropy is given in [45, Appendix B], and states $\tilde{H}_\infty^{\epsilon'}(X^n|Z^n) \geq H_\infty^{\epsilon'}(X^n|Z^n)$.

(iii) Using [75, Theorem 1], we have $H_\infty^{\epsilon'}(X^n|Z^n) \geq H(X^n|Z^n) - n\delta'$, with $\epsilon' = 2^{\frac{-n\delta'^2}{2\log^2(|\mathcal{X}|+3)}}$. Therefore, we can substitute $\tilde{H}_\infty^{\epsilon'}(X^n|Z^n)$ in (7.10) with $H(X^n|Z^n) - n\delta'$:

$$\begin{aligned}&\mathbf{SD}((\hat{h}_{S'}(X^n), h_S(X^n), S', S, Z^n);\\ &\quad(U_\ell, h_S(X^n), S', S, Z^n)) \leq 2\epsilon' + \frac{1}{2}\sqrt{2^{t+\ell-H(X^n|Z^n)+n\delta'}},\end{aligned}$$

where $\epsilon' = 2^{\frac{-n\delta'^2}{2\log^2(|\mathcal{X}|+3)}}$ and thus $\delta' = \sqrt{\frac{(\log\frac{1}{\epsilon'})(2\log^2(|\mathcal{X}|+3))}{n}}$. To satisfy σ-secrecy of the key agreement protocol, it is sufficient to have $2\epsilon' + \frac{1}{2}\sqrt{2^{t+\ell-H(X^n|Z^n)+n\delta'}} \leq \sigma$. Thus, the maximum achievable key length of the protocol must satisfy,

$$\begin{aligned}&\sqrt{2^{t+\ell-H(X^n|Z^n)+n\delta'}} \leq 2(\sigma - 2\epsilon')\\ &\quad\Rightarrow \ell \leq H(X^n|Z^n) - n\delta' - t + 2 + 2\log(\sigma - 2\epsilon')\end{aligned}$$

To have error probability bounded by ϵ, we will use t from (7.9) and obtain the maximum achievable key

length with (ϵ, σ) parameters, as

$$\begin{aligned}\ell \leq & H(X^n|Z^n) - H(X^n|Y^n) + 2 + \log \epsilon_2(\sigma - 2\epsilon')^2 \\ & - \sqrt{2n}\log(|\mathcal{X}|+3)(\sqrt{(\log \frac{1}{\epsilon'})} + \sqrt{(\log \frac{1}{\epsilon_1})}).\end{aligned} \tag{7.11}$$

We will then optimize the bound by choosing appropriate values for ϵ', ϵ_1 and ϵ_2.

ϵ' is the smoothing parameter and can be chosen arbitrarily subject to satisfying $\epsilon' \leq \frac{\sigma}{2}$. The effect of ϵ' on the upper-bound (7.11) appears in two terms: larger values of ϵ', in $\log(\sigma - 2\epsilon')$ reduce the RHS of the bound, and as part of the coefficient of the term $-\sqrt{n}$, increase the RHS of the bound. However the effect of the latter will be multiplied by the $\sqrt{n}$, and so we will choose $\epsilon' = \frac{n-1}{2n}\sigma$.

For ϵ_1 and ϵ_2 we have $\epsilon_1 + \epsilon_2 \leq \epsilon$. In the bound (7.11) $(\log \frac{1}{\epsilon_1})$ is the coefficient of $\sqrt{n}$, and its larger values correspond to larger value of the RHS of the bound. ϵ_2 however appears within a constant term. We thus choose $\epsilon_1 = \frac{n-1}{n}\epsilon$ and $\epsilon_2 = \frac{\epsilon}{n}$. These are reasonable choices for bounding error probabilities of ξ_1 and ξ_2: ξ_1 is the error of x^n being outside of $\mathcal{T}(X^n|y^n)$, while ξ_2 is related to the collision probability of the hash function, and is expected to be much smaller than ξ_1. Using these substitutions, we have

$$\begin{aligned}\max(\ell^{\mathbf{\Pi}_{\text{SKA}}}_{\epsilon,\sigma}) = & H(X^n|Z^n) - H(X^n|Y^n) + 2 + \log \frac{\epsilon\sigma^2}{n^3} \\ & - \sqrt{2n}\log(|\mathcal{X}|+3)\big(\sqrt{\log \frac{n}{(n-1)\epsilon}} + \sqrt{\log \frac{2n}{(n-1)\sigma}}\big).\end{aligned} \tag{7.12}$$

Since $\sqrt{\log \frac{an}{(n-1)b}} = \sqrt{\log \frac{a}{b}} + \mathcal{O}(1/n)$, we have

$$\begin{aligned}\max(\ell^{\mathbf{\Pi}_{\text{SKA}}}_{\epsilon,\sigma}) = & H(X^n|Z^n) - H(X^n|Y^n) \\ & - \sqrt{n} f_{\epsilon,\sigma}(|\mathcal{X}|) - \log \frac{4n^3}{\epsilon\sigma^2} + \mathcal{O}(\frac{1}{\sqrt{n}}),\end{aligned} \tag{7.13}$$

which completes the proof. □

Remark 7.1. *The third order term of these bounds can be further improved by choosing ϵ_1, ϵ_2, and ϵ' differently. For example, let $\epsilon' = \frac{\sqrt[4]{n}-1}{2\sqrt[4]{n}}\sigma$, $\epsilon_1 = \frac{\sqrt{n}-1}{2\sqrt{n}}\epsilon$, and $\epsilon_2 = \frac{\epsilon}{\sqrt{n}}$. Then*

$$\begin{aligned}\max(\ell^{\mathbf{\Pi}_{\text{SKA}}}_{\epsilon,\sigma}) = & H(X^n|Z^n) - H(X^n|Y^n) \\ & - \sqrt{n} f_{\epsilon,\sigma}(|\mathcal{X}|) - \log n + \mathcal{O}(1),\end{aligned} \tag{7.14}$$

which follows from the fact that

$$\sqrt{\log \frac{a\sqrt{n}}{(\sqrt{n}-1)b}} = \sqrt{\log \frac{a}{b}} + \frac{1}{2\ln 2\sqrt{n \log \frac{a}{b}}} + \mathcal{O}(\frac{1}{n}).$$

Theorem 7.2 gives the maximum achievable key length $\ell_{\epsilon,\sigma}^{\mathbf{\Pi}_{\text{SKA}}}$ of the protocol and provides a lower-bound on the maximum key length of OW-SKA protocols. That is, $S_{\epsilon,\sigma}^{ow}(X^n, Y^n|Z^n) \geq \max(\ell_{\epsilon,\sigma}^{\mathbf{\Pi}_{\text{SKA}}})$. Next corollary tightens the lower-bound for IID sources, using Berry-Esseen inequality [18, 50].

Corollary 7.2. *For any source model described by IID distribution $P^n = \Pi_j P_{X_j Y_j Z_j}$ we have*

$$S_{\epsilon,\sigma}^{ow}(X^n, Y^n|Z^n) \geq n(H(X|Z) - H(X|Y)) - \sqrt{n} g_{\epsilon,\sigma} - \frac{3}{2}\log n + \mathcal{O}(1), \tag{7.15}$$

where

$$g_{\epsilon,\sigma} = Q^{-1}(\epsilon)\sqrt{\Delta_{X|Y}} + Q^{-1}(\frac{\sigma}{2})\sqrt{\Delta_{X|Z}},$$

and $\Delta_{U|V} = \mathbb{V}\text{ar}\left\{-\log P_{U|V}\right\}$.

Proof. We revisit the proof of Theorem 7.2. For reliability, we bound the probability of these two events:

$$\xi_1 = \{x^n : -\log P_{X^n|Y^n}(x^n|y^n) > \lambda\}$$
$$\xi_2 = \{x^n \in \mathcal{T}(X^n|y^n) : \exists\ \hat{x^n} \in \mathcal{T}(X^n|y^n) \text{ s.t. } h_S(\hat{x^n}) = h_S(x^n)\}.$$

Let $W_i = -\log P_{X_i|Y_i}$ and $\lambda = nH(X|Y) + \sqrt{nV_{X|Y}}Q^{-1}(\epsilon - \theta_n)$, where $\Delta_{X|Y} = \mathbb{V}\text{ar}\left\{-\log P_{X|Y}\right\}$, and $\theta_n = \frac{1}{\sqrt{n}} + \frac{3\rho}{V_{X|Y}^{3/2}\sqrt{n}}$. Then by Lemma 7.1, $\Pr(\xi_1) \leq \epsilon - \frac{1}{\sqrt{n}}$. By choosing $t = \lambda - \log\frac{1}{\sqrt{n}}$, we will get $\Pr(K_A \neq K_B) \leq \Pr(\xi_1) + \Pr(\xi_2) \leq \epsilon$.

For the secrecy constraint, we use Lemma B.5.1. By this lemma, and noting the fact that $\tilde{H}_\infty^{\epsilon'}(X^n|Z^n) \geq H_\infty^{\epsilon'}(X^n|Z^n)$, we have $\sqrt{2^{t+\ell-H_\infty^{\epsilon'}(X^n|Z^n)}} \leq 2(\sigma - 2\epsilon')$, for any ϵ'. This implies that for $\eta_n = \frac{2}{\sqrt{n}}$ we get:

$$\ell \leq H_\infty^{\frac{\sigma-\eta_n}{2}}(X^n|Z^n) - t + \log 4\eta_n^2.$$

From [65], we know that for IID distribution $P_{X^nZ^n}$,

$$H_\infty^\delta(X^n|Z^n) = nH(X|Z) - Q^{-1}(\delta)\sqrt{n\Delta_{X|Z}} + \mathcal{O}(1),$$

where $\Delta_{X|Z} = \mathbb{V}\mathrm{ar}\left\{-\log P_{X|Z}\right\}$. Thus,

$$\begin{aligned}\ell \leq & n(H(X|Z) - H(X|Y)) \\ & \sqrt{n}\left(Q^{-1}(\epsilon - \theta_n)\sqrt{\Delta_{X|Y}} + Q^{-1}(\frac{\sigma - \eta_n}{2})\sqrt{\Delta_{X|Z}}\right) \\ & - \frac{3}{2}\log n + \mathcal{O}(1),\end{aligned}$$

and thus the proof is complete by using Taylor expansions to remove θ_n and η_n. □

Corollary 7.3 (OW-SK Capacity)**.** *For IID distribution $P_{X^nY^nZ^n}$, Protocol $\mathbf{\Pi}_{\mathrm{SKA}}$ achieves the OW-SK capacity.*

Proof. If variables U and V can be found for a given source model (X, Y, Z) with distribution P_{XYZ}, such that $X - U - V$ holds and $P_{UV|X}$ maximizes $H(U|Z, V) - H(U|Y, V)$, then the protocol $\mathbf{\Pi}_{\mathrm{SKA}}$ achieves $C_s^{ow}(X, Y, Z)$, i.e., the OW-SK capacity. To prove this, first note that $\mathbf{\Pi}_{\mathrm{SKA}}$ achieves the SK rate of $R = H(X|Z) - H(X|Y)$ for any given source model (X, Y, Z). Due to this protocol, parties first reconcile on X^n and then extract the key from X^n knowing that the adversary has access to a correlated variable Z^n. Assume for a given source model (X, Y, Z) the optimal variables U and V can be calculated such that $X - U - V$ holds, and $C_s^{ow}(X, Y, Z) = H(U|Z, V) - H(U|Y, V)$. In the IID regime, parties observe IID variables (X^n, Y^n, Z^n). Thus, in the first step, Alice, who has access to X^n, generates U^n and V^n. Then she broadcasts V^n over the public channel. Note that now Eve also has access to both side information variables Z^n and V^n. After these initial steps, Alice and Bob run Protocol $\mathbf{\Pi}_{\mathrm{SKA}}$ to reconcile on U^n. For the reconciliation step Bob uses his side information, i.e., (Y^n, V^n) to find U^n. To extract the key from U^n, parties know that Eve has access to (Z^n, V^n), thus by performing the appropriate key extraction the final SK rate will be $H(U|Z, V) - H(U|Y, V)$, which is equal to $C_s^{ow}(X, Y, Z)$. Hence, the proof is complete. This proof is due to [2], Section IV. Also see [105], Section III.B. □

In Figure 7.1, we compare the two lower-bounds of (7.15) and the lower-bound given in (7.14) for a source model where X is a uniformly distributed binary variable, $Y = \mathrm{BSC}_p(X)$, and $Z = \mathrm{BSC}_q(Y)$ are obtained as the output of binary symmetric channels on X and Y, respectively, and $\mathrm{BSC}_p(\cdot)$ denotes a binary symmetric channel with crossover probability p. For this example, the OW-SK capacity is $C_s^{ow} = h_2(p*q) - h_2(p)$, where $p * q = p(1-q) + (1-p)q$, and $h_2(\cdot)$ is the binary entropy given by $h_2(p) = -p\log p - (1-p)\log(1-p)$. For $p = 0.02$, $q = 0.15$, and $\epsilon = \sigma = 0.05$ we have $C_s^{ow} = 0.5$. The maximum secret key length by $\mathbf{\Pi}_{\mathrm{SKA}}$ achieves this OW-SK capacity. The finite blocklength bounds of (7.15) and (7.14) are converted to key rate (divided by n), and are depicted for this example in Figure 7.1. The graph shows the bound of (7.15) is tighter than

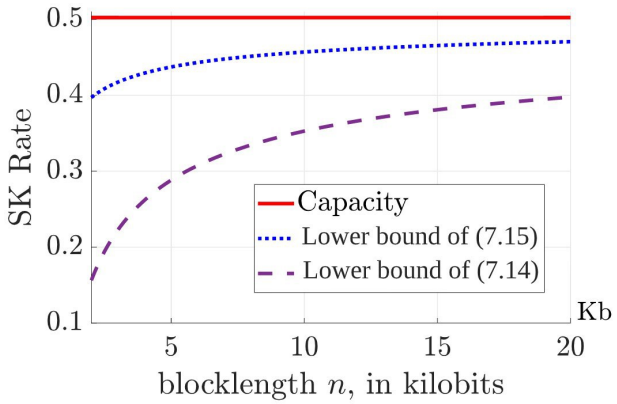

Figure 7.1: Comparing the finite-length bounds of (7.15) and (7.14). Here, $P_{X^nY^nZ^n}$ is IID, X is binary uniform, $Y = \mathrm{BSC}_{0.02}(X)$, $Z = \mathrm{BSC}_{0.15}(Y)$, reliability and secrecy parameters are $\epsilon = \sigma = 0.05$, and the secret key capacity is 0.5. The sample's length $n \in [2000, 20000]$. For this range of n, the bounds of (7.18) and (7.19) give SK rate of 0. In this example, bounds of (7.18) and (7.19) are positive only for $n > 10^7$, and $n > 1.1 \times 10^9$, respectively.

the bound of (7.14), and is closer to the capacity. In Section 7.5, we derive the bounds associated with the constructions in [73]. These bounds will not have positive values for the range of n used in Figure 7.1 and so are not included.

Corollary 7.4 (Public communication cost)**.** *For the source model described by distribution* $P_{X^nY^nZ^n} = \Pi_j P_{X_jY_jZ_j}$*, let* $F^{om}_{\epsilon,\sigma}$ *denote the* least *communication cost (in bits) that is needed for a OM-SKA* $S^{ow}_{\epsilon,\sigma}(X^n, Y^n|Z^n)$*. Then*

$$F^{ow}_{\epsilon,\sigma} \leq H(X^n|Y^n) + \sqrt{n}B^{\epsilon}_1(|\mathcal{X}|) + \frac{1}{2}\log n + \mathcal{O}(1), \tag{7.16}$$

where $B^{\epsilon}_1(|\mathcal{X}|) = \sqrt{2}\log(|\mathcal{X}|+3)\sqrt{\log\frac{1}{\epsilon}}$*. Moreover, for the case of IID source distributions we have*

$$F^{ow}_{\epsilon,\sigma} \leq nH(X|Y) + \sqrt{n}B^{\epsilon}_2 + \frac{1}{2}\log n + \mathcal{O}(1), \tag{7.17}$$

where $B^{\epsilon}_2 = Q^{-1}(\epsilon)\sqrt{\Delta_{X|Y}}$*.*

7.5 Comparison with related protocols

We compare Protocol 1 with other known OM-SKA protocols. We compare the protocols based on the type of reconciliation, SK length, public communication cost, and the computational complexity of the protocol for Alice and Bob, individually. A summary of this comparison is given in Table 7.1. We list these protocols in the following:

HR05 Holenstein and Renner proposed a key agreement method in [74] that achieves the OW-SK capacity of *a general distribution*. The reconciliation message uses linear codes. We derive two finite blocklength lower-bounds for the two variations of their SKA [73], one using a random linear code, and the second a concatenation of a linear code with a Reed-Solomon code. The bounds given in Theorem 3.13, and Theorem 3.15 of [73], are re-derived in the following proposition as functions of ϵ and σ. In [73], the bounds are expressed in the form of $B(n) = n(C_s^{ow} - f_B(\kappa_1, \kappa_2))$, where $n\kappa_1 = \log(1/\epsilon)$ and $n\kappa_2 = \log(1/\sigma)$.

Proposition 7.1. *For any source model with IID distribution P_{XYZ}, let $R_n = H(X^n|Z^n) - H(X^n|Y^n)$. Then for large enough n and any $\epsilon, \sigma < 1/4$ we have*

$$S^{ow}_{\epsilon,\sigma}(X^n, Y^n|Z^n) \geq [R_n - \sqrt{n} f'_{\epsilon,\sigma}]^+, \tag{7.18}$$

$$S^{ow}_{\epsilon,\sigma}(X^n, Y^n|Z^n) \geq [R_n - \sqrt[4]{n^3} g''_{\epsilon,\sigma} - \sqrt{n} f''_{\epsilon,\sigma}]^+, \tag{7.19}$$

where $[a]^+ = \max\{0, a\}$, and

$$\begin{aligned} f'_{\epsilon,\sigma} &= 90 \log(|\mathcal{X}||\mathcal{Y}|)(\sqrt{\log 1/\epsilon} + \sqrt{\log 1/\sigma}), \\ g''_{\epsilon,\sigma} &= \sqrt[4]{2^{22} \log(1/\epsilon) \log^2(|\mathcal{X}|) \log^2(|\mathcal{X}||\mathcal{Y}|)}, \\ f''_{\epsilon,\sigma} &= 8 \log(|\mathcal{X}|) \sqrt{\log(1/\sigma)}. \end{aligned}$$

The first bound (7.18) corresponds to random linear codes and second bound is due to concatenated codes. For both lower-bounds (7.18) and (7.19), the SKA protocol uses $\mathcal{O}(n^2)$ bits of communication. The computational complexity of Alice corresponding to both bounds is $\mathcal{O}(n^2)$. The computational complexity of Bob is $\mathcal{O}(n^2)|\mathcal{X}|^n$ and $\mathcal{O}(n^2)$, respectively corresponding to (7.18) and (7.19). As mentioned in [74, 105], the computational complexity of (7.19) for Alice and Bob is *efficient* (i.e., in $\mathcal{O}(n^d)$) but it is not *practically efficient* (i.e., it is not in $\mathcal{O}(n)$ or $\mathcal{O}(n \log n)$).

We note that our derived finite-length bounds in (7.15) and (7.14) are far closer to the capacity upper-bound than the finite-length bounds of HR05. For instance, considering the same setting and parameters of the example given for Fig 7.1, the rate associated with (7.19) (i.e., bound of (7.19) divided by n) will be positive $n > 1.1 \times 10^9$.

RRS13 Renes et al. proposed an SKA protocol that used polar codes for both reconciliation and privacy amplification [105]. The implementation cost of the protocol is $\mathcal{O}(n \log n)$ for both Alice and Bob, but the code construction for any given distribution might not be straighforward. The protocol uses a single message of length $\mathcal{O}(n)$. Their analysis of the protocol does not provide finite-length approximation of the key length.

Protocol	HR05	RRS13 & CBA15	$\mathbf{\Pi}_{\text{SKA}}$
Coding Method	linear codes	polar codes	universal hashes
Comm Cost	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	$\mathcal{O}(n)$
Comp A	$\mathcal{O}(n^2)$	$\mathcal{O}(n \log n)^{(**)}$	$\mathcal{O}(n \log \log n)$
Comp B	$\mathcal{O}(n^2)^{(*)}$	$\mathcal{O}(n \log n)^{(**)}$	$\mathcal{O}(2^{n.H(X\|Y)})$
FL Bound	yes	no	yes

Table 7.1: The comparison of Protocol 1 with other protocols. Comm cost refers to the public communication bits required for the protocol. Comp A and Comp B refer to the computational complexity of implementation for Alice and Bob, respectively. FL bound stands for finite-length lower (achievability) bounds. (*) For the lower-bound given in (7.18) this computational complexity is $\mathcal{O}(2^n)$. (**) Note that for SKAs using polar codes, parties need to compute the index sets that are required for code construction. The exact computational complexity of this step should be considered in addition to the implementation costs.

CBA15 In [29], authors propose an SKA protocol using polar codes. The reconciliation and privacy amplification is combined in one step polar coding, and the protocol requires a small pre-shared secret seed of length $\mathcal{O}(2^{-a.n})$. The public communication cost of this protocol in terms of bits is $\mathcal{O}(n)$, and the analysis of [29] does not give any finite-length approximations for the final key length.

$\mathbf{\Pi}_{\text{SKA}}$ (Protocol 1) This protocol uses universal hash functions for both reconciliation and privacy amplification. This protocol is very efficient in terms of public communication because it uses a single message of length $\mathcal{O}(nH(X|Y))$ (See Corollary 7.4). This protocol gives achievable finite-length bounds as given in (7.14) and (7.15). The computation cost of Alice is practically efficient; i.e., $\mathcal{O}(n \log \log n)$ (computing a single hash value). However, unfortunately for Bob, the computation cost is in $\mathcal{O}(2^{n.H(X|Y)})$; i.e., the implementation is not efficient.

7.6 Conclusion

We studied OM-SKA protocols in source model. These protocols are important for practical reasons because they do not require any interaction. They are also important from theoretical viewpoint since they can achieve the secret key capacity of one-way SKA, and also are related to problems in computational cryptography. Our construction uses a reconciliation method that is inspired by information spectrum analysis of [68]. Interesting open questions are providing efficient decoding algorithm for Bob, and refine the reconciliation to improve the lower-bound. Obtaining finite blocklength bounds for SKA using polar coding is also an interesting open question for future work.

Acknowledgement: This research is in part supported by Natural Sciences and Engineering Research Council of Canada, Discovery Grant program.

Chapter 8

Secret Key Agreement using a Virtual Wiretap Channel[1]

Abstract. Key agreement using the physical layer properties of communication channels is a well-studied problem. iJam is a physical layer key agreement protocol that achieves security by creating a "virtual" wiretap channel for the adversary through a subprotocol between the sender and the receiver that uses self-jamming by the receiver. The protocol was implemented and its security was shown through extensive experiments. The self-jamming subprotocol of iJam was later modelled as a wiretap channel and used for designing a secure message transmission protocol with provable security. We use the same wiretap model of the subprotocol to design secret key agreement protocols with provable security. We propose two protocols that use the wiretap channel once from Alice to Bob, and a protocol that uses two wiretap channels, one from Alice to Bob, and one in the opposite direction. We provide the security proof and efficiency analysis for the protocols. The protocols effectively give physical layer security protocols that can be implemented and have provable security. We discuss our results and propose directions for future research.

8.1 Introduction

Wireless communication provides flexibility for mobile users and with the increasing number of sensors and growth of the Internet of Things, may soon become the dominant form of communication. A major drawback of wireless communication is its vulnerability to passive eavesdropping. Wireless signals can be intercepted from afar, and so wireless communication is considered completely insecure.

[1]The content of this chapter is published as a paper [118] in proceedings of INFOCOM 2017.

Wyner [143] proposed an ingenious model for secure communication in presence of an eavesdropper, that is particularly suited for securing wireless communication. In Wyner wiretap channel model, a sender is connected to a receiver over a *main channel*, and the transmission to the receiver is eavesdropped by an eavesdropper Eve, through a second channel that is referred to as the *wiretapper's channel*. A wiretap code is a randomized code that is used by the sender to encode the message before transmission over the main channel. Wyner proved that as long as the wiretapper's channel is noisier than the main channel, there exists an encoding that provides perfect secrecy for the communication. Wiretap channels have been used for secure message transmission and secret key agreement. The two problems, although related, may achieve different levels of efficiency.

In [59], an innovative secret key agreement protocol, called iJam, was proposed that uses interaction between the sender and the receiver, to establish a shared key between the sender and the receiver over a noiseless channel. The basic subprotocol that is used for providing secure communication, and we refer to it as *Basic iJam Tranmission (BiT)*, uses cooperative self-jamming by the receiver to create uncertainty for the eavesdropper. The BiT protocol was experimentally evaluated. The authors considered the best adversarial strategies to measure the information leakage to the adversary, and showed that by careful choices of the modulation and the coding systems by the sender and receiver, BiT can create uncertainty for the eavesdropper about the transmitted information, and this can be used to establish a secret shared key. The protocol analysis was experimental.

In [119], BiT was modelled as a *virtual wiretap* channel, where "virtual" meant that the wiretap channel was not because of the physical noise in the environment, but was created effectively by using friendly jamming of the receiver that created a noisy view for the eavesdropper, while the receiver enjoyed an error-free communication. This model was then used to construct a one-way protocol for secure message transmission. As noted earlier, iJam and BiT were implemented and analyzed for the setting that the channel from Alice to Bob was noise-free, and running BiT created the eavesdropper's uncertain view of the communication. Sharifian et al. [119] showed that by running BiT over a physical wiretap channel between Alice, Bob and Eve, and the interpretation of BiT as a virtual wiretap channel, one can effectively "make Eve's channel noisier".

Our work

The goal of this paper is to use BiT to construct key agreement protocols with provable security. As noted earlier, execution of BiT enables Alice and Bob to communicate over a wiretap channel. The transition matrix of this channel is determined by the *Bit Error Rate (BER)* of Eve for the transmitted message and

as a result of using BiT for message transmission.

Assuming adversary's BER can be estimated, we have a setting that Alice and Bob are connected by a wiretap channel with known parameters, and the goal is to establish a shared secret key. One can also use the plain communication channel between Alice and Bob as a *public discussion (PD)* channel: a channel that can be perfectly eavesdropped by Eve.

We recall the formal security and efficiency definitions of information-theoretic Secret Key Agreement (SKA) problem when there is a wiretap channel from Alice to Bob, together with a public discussion channel that can be used in both directions (Alice to Bob and vice versa), and design three protocols with provable security in this model.

C1 The first protocol uses the wiretap channel from Alice to Bob created by BiT (one-way) together with the public discussion (PD) channel in the same direction, and is a direct application of the message transmission protocol with semantic security that was proposed in [119]. For the secret key agreement protocol, Alice chooses a random string and uses the message transmission system to send it to Bob. Intuitively, security of the resulting shared key follows from the semantic security of the message transmission system.

C2 The second protocol is a pure key agreement protocol: Alice chooses a random string and sends it through the virtual wiretap channel (invoking BiT protocol) to Bob. Bob receives the string with perfect reliability. However, the string is partially leaked to the adversary and the amount of leakage can be estimated using the parameters of the virtual wiretap channel. Alice and Bob then use a seeded extractor to extract the available randomness in the string and thus obtain a shared key. The seed of the extractor is sent from Alice to Bob over PD.

C3 The above two protocols assume Eve's BER is known and the parameters of the wiretap channel can be correctly estimated. To relax these assumptions, we will use a protocol that uses two invocations of BiT: one by Alice and one by Bob. Using two invocations provides some level of robustness in the sense that, assuming a fixed adversary, if BER for one direction is under-estimated, it will be over-estimated in the opposite direction. We use a novel way (Lemma 8.4) of extracting randomness from two independent sources to generate the final secret key, and use it to allow Alice and Bob to extract a shared key.

We will provide formal analysis and security proofs for all these protocols.

Related works

Modelling iJam as a wiretap channel was first considered in [119] where the model was used to construct a secure message transmission system with perfect secrecy. Our work focuses on key agreement problem. The two problems are related, but the highest achievable rate of the two problems, for the same communication setting, could be different. For example, in Section 8.3 we have two one-way protocols: the first one using the wiretap code in [11] and the second using a direct key agreement protocol. Both of these protocols achieve the same asymptotic secret key rate. However, the second protocol in Section 8.3 cannot be directly used for message transmission.

It has been known that cooperative jamming could be used for physical layer security by mixing a jamming signal in the eavesdropper's view [81, 86, 132]. Wiretap channels have been used to model and analyze these systems. In a general cooperative jamming system, a trusted third party sends a jamming signal that is partially known to the legitimate communicants, while completely unknown to the adversary. This type of jamming is referred to as "helper" [144], "cooperative" [81], or "friendly" [62] jamming. iJam [59] uses a variation of friendly jamming where the role of the trusted third party is given to the legitimate receiver.

The rest of this chapter is organized as follows. In Section 8.2, we provide an overview of iJam self-jamming subprotocol, and how it was modelled by a virtual wiretap channel. We also provide the required background for secure message transmission over wiretap channels. In Section 8.3, we give two one-way secret key agreement protocols and prove their security and capacity-achieving properties. In Section 8.4, we give a two-way SKA protocol and prove its security. In Section 8.5, we propose some alternative self-jamming strategies, and Section 8.6 concludes the paper.

8.2 Preliminaries

We use uppercase letters X to denote random variables and bold lowercase letters to denote their corresponding realization. By $\Pr[X = \mathbf{x}]$ we mean probability of $X = \mathbf{x}$. We also use $P_X(\mathbf{x})$ as an alternative notation for $\Pr[X = \mathbf{x}]$. The calligraphic letters $\mathcal{X}$ denote sets, and $|\mathcal{X}|$ denotes the number of elements in a set. We write $X \in \mathcal{U}$ to denote a random variable that is defined over the set $\mathcal{U}$. For two random variables X and Y, P_{XY}, $P_{X|Y}$ and P_X denote their joint distribution, conditional distribution, and the marginal distribution of X, respectively. All logarithms are in base 2, and $\mathbf{x} \parallel \mathbf{y}$ denotes concatenation of two binary strings $\mathbf{x}$ and $\mathbf{y}$.

Shannon entropy of a random variable $X \in \mathcal{X}$ is given by

$$H(X) = -\sum_{\mathbf{x}\in\mathcal{X}} P_X(\mathbf{x}) \log P_X(\mathbf{x}),$$

and its min-entropy is given by

$$H_\infty(X) = -\log(\max_{\mathbf{x}}(P_X(\mathbf{x}))).$$

For two random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ with joint and conditional distributions $P_{XY}(\mathbf{x}, \mathbf{y})$ and $P_{X|Y}(\mathbf{x}|\mathbf{y})$, respectively, the *conditional entropy* $H(X|Y)$ is defined as follows:

$$H(X|Y) = -\sum_{\mathbf{x}\in\mathcal{X}} \sum_{\mathbf{y}\in\mathcal{Y}} P_{XY}(\mathbf{x}, \mathbf{y}) \log P_{X|Y}(\mathbf{x}|\mathbf{y}).$$

The *mutual information* between two random variables is:

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X),$$

and the *average conditional min-entropy* [44] is given by

$$\tilde{H}_\infty(X|Y) = -\log \mathbb{E}_{\mathbf{y}\in\mathcal{Y}} \max_{\mathbf{x}\in\mathcal{X}} P_{X|Y}(\mathbf{x}|\mathbf{y}).$$

The *statistical distance* of two variables $X, Y \in \mathcal{U}$ is given by

$$\mathbf{SD}(X, Y) \triangleq \frac{1}{2} \sum_{\mathbf{u}\in\mathcal{U}} |Pr(X = \mathbf{u}) - Pr(Y = \mathbf{u})|.$$

Min-entropy and statistical distance are related through the definition of *smooth min-entropy*.

Definition 8.1. [107] For a random variable $X \in \mathcal{X}$, the smooth min-entropy is:

$$H^\epsilon_\infty(X) \triangleq \max_{Y\in\mathcal{X}:SD(X,Y)\leq\epsilon} H_\infty(Y).$$

The following lemma states that Shannon entropy and smooth min-entropy almost behave the same when the experiment is repeated independently a large number of times.

Lemma 8.1. *[107] Let $X_1, X_2, ..., X_\ell$ be ℓ independent random variables over $\mathcal{X}$ with probability distribution $P_X(\mathbf{x})$, then we have*

$$H^\epsilon_\infty(X_1, ..., X_\ell) \geq \ell(H(X) - \delta),$$

where $\delta > 0$ *and* $\epsilon = 2^{\frac{-\ell\delta^2}{2\log^2(|\mathcal{X}|+3)}}$.

A physical communication channel, such as a wire, provides an environment through which information signal is sent from a sender to a receiver. Channels can be probabilistic or adversarial. A noisy channel modifies the transmitted signal probabilistically as it travels through it. A noisy communication channel can be modelled by a randomized function $\mathsf{W} : \mathcal{X} \rightarrow \mathcal{Y}$ that is specified by a transition probability matrix $\mathbf{W}$, where the element $\mathbf{W}[x, y]$ is the probability that input x generates output y. Let the channel input be a random variable $X \in \mathcal{X}$; then the output random variable $Y \in \mathcal{Y}$ will be $\mathsf{W}(X) = Y$. A channel is called *strongly symmetric* if the rows of the transition matrix are permutations of one another, and so is the case for the columns. The channel $\mathsf{W}(\cdot)$ is *symmetric* if there exists a partition of the output set $\mathcal{Y} = \mathcal{Y}_1 \cup \cdots \cup \mathcal{Y}_n$, such that for all i the sub-matix $\mathbf{W}_i = \mathbf{W}[\cdot, \mathcal{Y}_i]$ is strongly symmetric.

We denote ℓ times independent applications of the channel on ℓ independently sampled inputs by $\mathsf{W}^\ell(\cdot)$.

8.2.1 Randomness extractors

An important building block of our constructions is a randomness extractor.

Definition 8.2. [44] A function $\mathsf{EXT} : Sds \times \{0,1\}^n \rightarrow \{0,1\}^\ell$ is a (d, ϵ)-strong, average-case extractor if, $SD((\mathsf{EXT}(S, X), Z, S); (U, Z, S)) \leq \epsilon$ for all pairs of correlated random variables (X, Z) over $\{0,1\}^n \times \{0,1\}^*$, assuming $\tilde{H}_\infty(X|Z) \geq d$.

A well-known construction of randomness extractors is from (2-) *Universal Hash Families* (UHFs).

Definition 8.3. A family $\{h_s | s \in \mathcal{S}\}$ of functions $h_s : \mathcal{X} \rightarrow \mathcal{Y}$ is a UHF if for any $x \neq x^{'}$,

$$\Pr[h_s(x) = h_s(x^{'})] \leq \frac{1}{|\mathcal{Y}|},$$

where S denotes a random seed chosen uniformly from $\mathcal{S}$.

The construction uses the so called *Leftover Hash Lemma* (LHL) [77]. The following average-case version of LHL is given in [44].

Lemma 8.2. *Let* $\{h_s | s \in Sds\}$ *be a UHF with* $h_s : \{0,1\}^n \rightarrow \{0,1\}^\ell$. *Let* X *and* Z *be random variables over* $\{0,1\}^n$ *and* $\{0,1\}^*$, *respectively. Then*

$$\mathbf{SD}\big((S, Z, h_S(X)); (S, Z, U_\ell)\big) \leq \frac{1}{2}\sqrt{2^{\ell - \tilde{H}_\infty(X|Z)}},$$

where S *denotes a random seed chosen uniformly from the set* Sds.

Using Definition 8.2, the lemma says that UHF is an average-case $(\ell - 2 - 2\log\varepsilon, \varepsilon)$-strong extractor.

Definition 8.4. A family $\{h_s | s \in Sds\}$ of functions $h_s : \mathcal{X} \to \mathcal{Y} = \{0,1\}^\ell$ is an XOR-UHF if for any $\mathbf{x} \neq \mathbf{x}'$,

$$\Pr[h_S(\mathbf{x}) \oplus h_S(\mathbf{x}') = \mathbf{a}] \leq \frac{1}{|\mathcal{Y}|}, \text{ for all } \mathbf{a} \in \{0,1\}^\ell,$$

where S denotes a random seed chosen uniformly from Sds.

Lemma 8.3. *[43] Let $\{h_s | s \in Sds\}$ be a family of XOR-universal hash functions $h_s : \{0,1\}^n \to \{0,1\}^\ell$. If random variables A over $\{0,1\}^n$ and B over $\{0,1\}^\ell$ are independent. Then*

$$\mathbf{SD}\big((S, h_S(A) \oplus B); (S, U_\ell)\big) \leq \varepsilon,$$

as long as $H_\infty(A) + H_\infty(B) \geq \ell + 2\log(\frac{1}{\varepsilon}) + 1$.

8.2.2 Wiretap codes

In Wyner wiretap model, the sender is connected to the receiver through a channel W_1, referred to as the *main channel* that maps input $X \in \mathcal{X}$ to output $Y \in \mathcal{Y}$, and to the eavesdropper through a second channel W_2 called the *wiretapper's channel* that maps $X \in \mathcal{X}$ to $Z \in \mathcal{Z}$, such that the Markov chain $X \to Y \to Z$ holds. In the following, we will denote a wiretap channel by $\{\mathsf{WT} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}\}$. This original Wyner wiretap model assumes that W_2 is a *physically degraded* version of the channel W_1. This definition was extended to a *broadcast channel* where the above Markov chain does not necessarily hold.

The goal of wiretap coding is to provide secrecy and reliability for message transmission. A wiretap code C is specified by a tuple $(\mathcal{M}, N, \mathcal{X}, \epsilon, \delta)$, denoting the message space, code length, alphabet set, and upper-bounds on the secrecy loss and the error probability, respectively. When other parameters are clear from the context, we refer to the code as an (ϵ, δ) code. The *rate* of a wiretap code is defined by the number of secure transmitted bits in each application of the channel; that is, $R = \frac{\log|\mathcal{M}|}{N}$. An (ϵ, δ) wiretap code family is a family $\{C^N\}$ of (ϵ, δ) wiretap codes, indexed by the code length N. The rate R_0 is achievable by an (ϵ, δ) wiretap code family, if for any sufficiently small $\xi > 0$, there exists an integer N_0 such that for all $N \geq N_0$ we have $R(C^N) \geq R_0 - \xi$, the secrecy requirement satisfies $\epsilon \leq \xi$, and the decoding error probability satisfies $\delta \leq \xi$. The *secrecy capacity* of a wiretap channel is the highest achievable rate of all (ϵ, δ) wiretap code families for the channel and is denoted by C_s. This secrecy capacity is for transmission of secure messages.

Theorem 8.1. *[84] The secrecy capacity of Wyner wiretap channel when W_1 and W_2 are symmetric is given*

by

$$C_s = C_{\mathsf{W}_1} - C_{\mathsf{W}_2},$$

where C_{W_1} *and* C_{W_2} *are (reliability) channel capacities of* W_1 *and* W_2*, respectively.*

To achieve the secrecy capacity, one must consider security and reliability requirements together. This is because error-correction reduces noise over both of the main and the adversary's channels. The first construction of capacity-achieving wiretap codes in [87] used specific error correcting codes. *Modular constructions of wiretap codes* separate coding for security and reliability, and can be used with a much larger class of (reliability) capacity-achieving error correcting codes.

The modular construction in [11] uses *invertible extractors.* A function $\mathsf{INV} : \{0,1\}^r \times Sds \times \{0,1\}^b \to \{0,1\}^n$ is an inverter for the extractor $\mathsf{EXT}(\cdot,\cdot)$ in Definition 8.2, if for a uniform $R \in \{0,1\}^r$ and for all $S \in Sds$ and $Y \in \{0,1\}^b$, the random variable $\mathsf{INV} : (S, R, Y)$ is uniformly distributed on all preimages of Y under $\mathsf{EXT}(S,\cdot)$

Definition 8.5. [11] Let $S \in Sds$ be a uniformly distributed random seed that is chosen by the encryptor, and sent to the decryptor over a public channel. For an arbitrarily distributed message space $\{0,1\}^b$, the seeded encryption function $\mathcal{SE} : Sds \times \{0,1\}^b \to \{0,1\}^n$, outputs a ciphertext $\mathcal{SE}(S, M)$ for a message $M \in \{0,1\}^b$. The corresponding seeded decryption function is $\mathbf{SD} : Sds \times \{0,1\}^n \to \{0,1\}^b$, where for all $S \in Sds$ and $M \in \{0,1\}^b$ we have $\mathcal{SD}(S, \mathcal{SE}(S, M)) = M$.

Let $Sds = \{0,1\}^n \backslash 0^n$. For inputs $S \in Sds$ and $X \in \{0,1\}^n$ and $n > b$, the function $\mathsf{EXT} : Sds \times \{0,1\}^n \to \{0,1\}^b$ is defined as:

$$\mathsf{EXT}(S, X) = (S \odot X)|_b,$$

where $\odot$ denotes multiplication over $\mathbb{F}_2^n = \{0,1\}^n$, and $X|_b$ is the first b bits of X.

An efficient inverter for $\mathsf{EXT}(S, X)$ is given by $\mathsf{INV}(S, R, M) = S^{-1} \odot (M \| R)$, where S^{-1} denotes the multiplicative inverse of S in $\mathbb{F}_2^n$, and R is uniformly distributed over $\{0,1\}^{(n-b)}$. For the message block $M \in \{0,1\}^b$, $S \in Sds$, and $R \xleftarrow{\$} \{0,1\}^r$, the seeded encryption function $\mathcal{SE}(S, M)$ is defined as follows:

$$X = \mathcal{SE}(S, M) = \mathsf{INV}(S, R, M) = S^{-1} \odot (M \| R)$$

The encrypted message is transmitted over the wiretap channel, and the seed is sent reliably to the receiver over the public channel.

The *Mutual Information Security (MIS)* advantage associated with an encoding function $\mathcal{E} : \{0,1\}^b \to$

$\{0,1\}^n$ and a wiretapper's channel W is defined by:

$$\mathbf{Adv}^{\text{mis}}(\mathcal{E};\mathsf{W}) = \max_{P_M} I(M;\mathsf{W}(\mathcal{E}(M))), \tag{8.1}$$

where the maximum is over all random variable $M \in \{0,1\}^b$. It is shown in [11] that this metric of measuring security is equivalent to Goldwasser and Micali's *semantic security (SS)* [58]. Furthermore, if W is symmetric and $\mathcal{E}$ satisfies the so-called "separable" and "message linear" properties (satisfied by the above construction), the MIS metric is equivalent to the following *mutual information security-random message (MIS-R)* metric [11].

$$\mathbf{Adv}^{\text{mis-r}}(\mathcal{E};\mathsf{W}) = I(U_b;\mathsf{W}(\mathcal{E}(U_b))),$$

where U_b denotes uniform b-bit string.

8.2.3 iJam and BiT protocol

In [59], a physical layer secret key agreement protocol called *iJam* was proposed and experimentally evaluated. iJam uses the Basic iJam Transmission (BiT) protocol that employs OFDM (Orthogonal Frequency-Division Multiplexing) with 2^q-QAM (Quadrature Amplitude Modulation) and works as follows: The sender generates a uniformly random string of length Nq bits and divides it into N blocks of q-bit each. The blocks are modulated into a sequence of N complex numbers $A_1, \cdots, A_N$ using 2^q-QAM, and each A_i is transmitted over a carefully selected frequency (N frequencies in total) of the OFDM signal. The next step is to apply Inverse Fast Fourier Transform (IFFT) on the N frequencies to obtain N time samples: $a_k = \sum_{n=0}^{N} A_n e^{\frac{i2\pi kn}{N}}$, $k = 1, \cdots, N$. Each time sample x_k is a linear combination of N random values A_i, and so by the central limit theorem, a_k will have approximately a Gaussian distribution. This property is used to create uncertainty for the eavesdropper.

In the BiT protocol, Alice transmits each OFDM time sample twice: $(a_1, \cdots, a_N) \parallel (a_1, \cdots, a_N)$. The receiver (i.e., jammer) Bob randomly jams one of the pairs, a_i or its repetition, using a random sample that is drawn from the same Gaussian distribution of a_k. Since the sum of the two Gaussian distributions is a Gaussian distribution, it is difficult for the eavesdropper to distinguish a clean sample (unjammed) and a jammed sample. The (jammer) receiver, however, obtains the unjammed samples, stitches them together and obtains the original OFDM signal. The eavesdropper's uncertainty in distinguishing the jammed sample and the clean sample is measured in terms of their Bit Error Rate (BER). In [59], various strategies of the attacker to recover the original signal is considered, and it was shown that BER of the adversary is maximised when the power ratio of the signal from the jammer to the signal from the sender at Eve's receiver is between

1 and 9. This power ratio depends on factors such as the sender transmission power, the jamming signal power, and the eavesdropper's location.

8.2.4 Modelling BiT as a wiretap channel

In [119], the BiT protocol described above was interpreted as creating a virtual wiretap channel with noiseless main channel and a noisy wiretapper's channel $\mathsf{W} : \{0,1\}^{Nq} \to \{0,1\}^{Nq}$.

Let η, $0 < \eta < 1$, denote the probability that the eavesdropper (correctly detects all the transmitted time samples and) outputs the correct OFDM signal, and recovers the correct message block. For Eve's view Z and the transmitted sequence X, the conditional probability distribution $Z|X$ is given by:

$$P(Z = i|X = i) \simeq \eta,$$
$$P(Z = i|X \neq i) \simeq \frac{1-\eta}{2^{Nq}}.$$

We also refer to this as a $\mathrm{BiT}^N_{\eta,q}$. The virtual wiretap channel is defined as follows:

Definition 8.6. [119] Let η be the probability that all the N clean time samples are distinguishable from their jammed counterparts. The BiT protocol approximation of the wiretap channel, denoted by $\mathrm{BiT}^N_{\eta,q}$, is defined by a noiseless main channel and a wiretapper's channel $\mathsf{W} : \{0,1\}^{Nq} \to \{0,1\}^{Nq}$ with the following transition probability matrix:

$$\mathbf{W} = \begin{bmatrix} \eta & \frac{1-\eta}{2^{Nq}-1} & \cdots & \frac{1-\eta}{2^{Nq}-1} \\ \frac{1-\eta}{2^{Nq}-1} & \eta & \cdots & \frac{1-\eta}{2^{Nq}-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1-\eta}{2^{Nq}-1} & \frac{1-\eta}{2^{Nq}-1} & \cdots & \eta \end{bmatrix}.$$

The following follows from Theorem 1.

Corollary 8.1. *[119] The secrecy capacity of $BiT^N_{\eta,q}$ is given as follows:*

$$C_s(BiT^N_{\eta,q}) = -\left(\eta \log \eta + (1-\eta) \log \frac{1-\eta}{2^{Nq}-1}\right). \tag{8.2}$$

Remark 8.1. *To interpret an execution of BiT as creating a virtual wiretap channel, we need the following assumptions.*

1. *Message blocks of size q should be IID to ensure the central limit theorem is applicable, and the distribution of each OFDM time sample can be approximated by Gaussian.*

2. *Jamming signal should be taken from a Gaussian distribution with appropriate parameter so that the jammed samples and the original ones become indistinguishable.*

3. *The jammer must transmit at a relatively high rate to avoid the joint decoding.*

8.2.5 Using $\text{BiT}_{\eta,q}^{N}$ to provide security for message transmission

In [119], the wiretap coding method of [11] was used to construct a message transmission protocol over $\text{BiT}_{\eta,q}^{N}$.

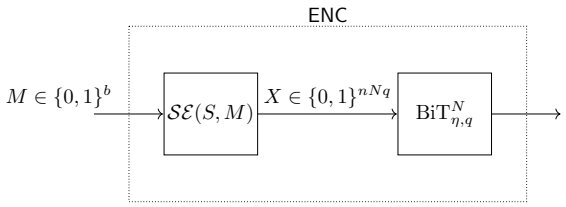

Figure 8.1: Secure message transmission using $\text{BiT}_{\eta,q}^{N}$

The construction is shown in Figure 8.1. ENC consists of two modules:

1. A seeded wiretap encryption block $\mathcal{SE} : Sds \times \{0,1\}^b \to \{0,1\}^{nNq}$ that encrypts a message block of length b bits to a codeword of length nNq bits.

2. The $\text{BiT}_{\eta,q}^{N}$ block that breaks the codeword into qN-bit units, copies each unit, and sends the original unit together with its copy over the channel using OFDM over 2^q-QAM.

The efficiency of the message transmission protocol is measured by the number of secret bits transmitted per usage of BiT.

Definition 8.7. [119] The rate of the message transmission protocol over $\text{BiT}_{\eta,q}^{N}$ (see Figure 8.1) is $R = \frac{b}{n}$.

Theorem 8.2. *[119] The rate of the message transmission protocol over $BiT_{\eta,q}^{N}$ (see Figure 8.1) is asymptotically $C_s(BiT_{\eta,q}^{N})$.*

8.3 Key agreement

One of the fundamental problems in cryptography is establishing a shared secret key between two parties. Once such a secret key is established, through one-time-pad, we immediately have a secure message transmission protocol. Secret key agreement protocols in information-theoretic setting have been widely studied in [2, 92, 108].

Definition 8.8. A Secret Key Agreement (SKA) protocol with respect to a wiretap channel $\{\mathsf{WT} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}\}$ is defined as follows: Alice chooses a random variable $X \in \mathcal{X}$. Alice samples X for n times, and transmits the samples across the wiretap channel to generate $(Y^n, Z^n) = \mathsf{WT}(X^n)$, where Bob receives Y^n and Eve receives Z^n. Alice and Bob can communicate through a public discussion channel, where we assume that Alice sends messages $C_1, C_3, C_5, \cdots$, and Bob sends messages $C_2, C_4, C_6, \cdots$, Each message can depend on the sender's entire view of the protocol and possibly on privately generated random bits. After the communication phase, Alice and Bob each either accepts or rejects the protocol execution, depending on whether they believe to be able to generate a shared secret key. If Alice accepts, she generates a key K_A depending on her view of the protocol. Similarly, if Bob accepts, he generates a key K_B depending on his view of the protocol. Even if a party does not accept, they may generate a key.

Let $C = C_1, C_2, C_3, \cdots$, denote the total communication during the communication phase. A *secret key rate* R_{sk} is achievable if, for every $\varepsilon > 0$ and sufficiently large n, there exists a SKA protocol (as described above) that uses the wiretap channel n times and satisfies:

$$\Pr[K_A \neq K_B] < \varepsilon, \tag{8.3}$$

$$\frac{1}{n} H(K) > R_{sk} - \varepsilon, \tag{8.4}$$

$$I(K; Z^n, C) < \varepsilon, \tag{8.5}$$

$$H(K) > \log |\mathcal{K}| - \varepsilon. \tag{8.6}$$

The largest achievable secret key rate is called the *secret key capacity* C_{sk}.

Remark 8.2. *In Definition 8.8, requirement (8.3) captures reliability, requirement (8.4) is on the secret key rate, and the requirements (8.5) and (8.6) capture secrecy and randomness of the key. These two latter conditions can be replaced by:*

$$\mathbf{SD}(Z^n, C^t, K; Z^n, C^t, U_{\mathcal{K}}) < \varepsilon, \tag{8.7}$$

where $U_{\mathcal{K}}$ is uniformly distributed over $\mathcal{K}$. See [105] for further discussion.

We propose two one-way key agreement protocols that use $\mathrm{BiT}_{\eta,q}^N$ to create a virtual wiretap channel for Eve.

SKA-I

This protocol uses the message transmission protocol in [119]. Alice and Bob are connected by a two-way noiseless channel. Alice can either directly transmit (without Bob's jamming) over the channel or use $\mathrm{BiT}^N_{\eta,q}$ with Bob's contribution, creating the virtual wiretap channel WT in Definition 8.6. The protocol is given in Figure 8.2:

Figure 8.2: SKA-I

1. Alice does the following:
   – Samples a uniform seed $S \in Sds$ and directly transmit to Bob.
   – Generates a random string $K \in \{0,1\}^b$, and encrypts it using the wiretap code in [11], $\mathsf{SE}(\mathsf{S},\mathsf{K}) = X^n \in \{0,1\}^{nNq}$.
   – Sends X^n to Bob using $\mathrm{BiT}^N_{\eta,q}$: X^n is divided into n blocks of Nq bits: $X_1, X_2, ..., X_n$. Each $X_i \in \{0,1\}^{Nq}$ is transmitted using $\mathrm{BiT}^N_{\eta,q}$.
2. Key derivation:
   - Alice outputs K;
   - Bob receives $Y^n = X^n = X_1, X_2, ..., X_n$, decodes X^n using the decryption block $\mathsf{SDE}(S, X^n)$ and recovers the key K.

Theorem 8.3. *The protocol SKA-I is an SKA with respect to $BiT^N_{\eta,q}$ that achieves the rate $C_s(BiT^N_{\eta,q})$.*

Proof. -**Correctness of the key:** it follows from the reliability of the message transmission scheme, that follows from the fact that the main channel of the virtual wiretap channel is noiseless.

-**Security of the key:** We use definitions (8.5) and (8.6). First, according to the MIS metric of the message transmission scheme, we have (8.1), which implies (8.5). Second, (8.6) follows from the fact that K is sampled uniformly.

-**Secret key rate:** Here, the secret key rate is equal to the rate of the message transmission scheme, which was shown to achieve $\frac{1}{2Nq} C_s(\mathrm{BiT}^N_{\eta,q})$ [119]. □

SKA-II

Using the same setting in this protocol, Alice sends a random string to Bob over a $\mathrm{BiT}^N_{\eta,q}$ that will be partially leaked to Eve. She will also send the seed for an extractor that is used by both of them. Both use the seed to extract a shared key. Figure 8.3 shows the protocol:

Theorem 8.4. *SKA-II is an SKA with respect to $BiT^N_{\eta,q}$ and achieves the rate $C_s(BiT^N_{\eta,q})$.*

Figure 8.3: SKA-II

1. Alice does the following:
   – Samples a uniform seed $S \in Sds$. S is directly transmitted.
   – For $i = 1, \cdots, n$, Alice chooses a vector X_i that is uniformly distributed over $\{0,1\}^{Nq}$, and sends it to Bob using $\mathrm{BiT}^N_{\eta,q}$.
2. Key derivation:
   Let $\mathsf{EXT} : Sds \times \{0,1\}^{nNq} \to \{0,1\}^b$ be a strong average-case extractor in Definition 8.2 from a UHF (see Lemma 8.2), where b is chosen according to the value of n, η and the security parameter ϵ (see (8.9)).
   - Alice computes $K_A = \mathrm{EXT}(X^n)$, where $X^n = X_1, X_2, ..., X_n$;
   - Bob receives $Y^n = X^n = X_1, X_2, ..., X_n$ and computes $K_B = \mathrm{EXT}(Y^n)$.

Proof. -**Correctness of the key:** The correctness follows from the fact that transmissions are over noiseless channel and $Y^n = X^n$.

-**Security of the key:** To prove the secrecy and the randomness of the key we use security definition given by the inequality (8.7), which, for the proposed protocol, becomes

$$\mathbf{SD}((K, Z^n, S); (U_{\mathcal{K}}, Z^n, S)) \leq \epsilon, \tag{8.8}$$

where $U_{\mathcal{K}}$ is a uniform distribution over $\mathcal{K}$. We need to show that for any $\epsilon > 0$, there exists sufficiently big n such that:

$$\mathbf{SD}((\mathsf{EXT}(S, X^n), Z^n, S); (U_{\mathcal{K}}, Z^n, S)) \leq \epsilon.$$

According to the probability matrix of the wiretapper's channel W of $\mathrm{BiT}^N_{\eta,q}$, we have $Z = W(X) = X \oplus \Delta$, where $\Delta \in \{0,1\}^{Nq}$ has the following distribution:

$$\Pr[\Delta = \alpha] = \begin{cases} \eta, & \text{if } \alpha = 0^{Nq}; \\ \frac{1-\eta}{2^{Nq}-1}, & \text{otherwise.} \end{cases}$$

Let $\epsilon' = \frac{\epsilon}{4}$. Suppose $\Delta_{\epsilon'}$ is a random variable with ϵ'-smooth min-entropy with respect to Δ. According to Lemma 8.1, we have

$$H^{\epsilon'}_{\infty}(\Delta_1, ..., \Delta_n) \geq n(H(\Delta) - \delta),$$

for $\delta > 0$ satisfying $\epsilon' = 2^{\frac{-n\delta^2}{2\log^2(|\mathcal{Z}|+3)}}$. Let ${Z_{\epsilon'}}^n = X^n \oplus \Delta_{\epsilon'}^n$. We then have,

$$\begin{aligned}
&\tilde{H}_\infty(X^n|{Z_{\epsilon'}}^n) \\
&= -\log\Big(\textstyle\sum_{{z_{\epsilon'}}^n \in \mathcal{Z}^n} \Pr[{Z_{\epsilon'}}^n = {z_{\epsilon'}}^n] \cdot \\
&\qquad\qquad \max_{x^n \in \mathcal{X}^n} \Pr[X^n = x^n | {Z_{\epsilon'}}^n = {z_{\epsilon'}}^n]\Big) \\
&\overset{(i)}{=} -\log\Big(\textstyle\sum_{{z_{\epsilon'}}^n \in \mathcal{Z}^n} \max_{x^n \in \mathcal{X}^n} \Pr[X^n = x^n] \cdot \\
&\qquad\qquad \Pr[{Z_{\epsilon'}}^n = {z_{\epsilon'}}^n | X^n = x^n]\Big) \\
&= -\log\Big(\textstyle\sum_{{z_{\epsilon'}}^n \in \mathcal{Z}^n} \frac{1}{|\mathcal{X}^n|} \max_{x^n \in \mathcal{X}^n} \Pr[x^n \oplus \Delta_{\epsilon'}^n = z_{\epsilon'}]\Big) \\
&\overset{(ii)}{\geq} -\log\Big(\textstyle\sum_{{z_{\epsilon'}}^n \in \mathcal{Z}^n} \frac{1}{|\mathcal{X}^n|} \cdot 2^{-n(H(\Delta)-\delta)}\Big) \\
&= n(H(\Delta) - \delta),
\end{aligned}$$

where (i) follows from uniform distribution of X^n and (ii) is because $\Pr[x^n \oplus \Delta_{\epsilon'}^n = z_{\epsilon'}] = \Pr[\Delta_{\epsilon'}^n = x^n \oplus z_{\epsilon'}] \leq 2^{H_\infty(\Delta^n)} = 2^{-n(H(\Delta)-\delta)}$.

Let $\mathsf{EXT}(S, X) = h_S(X)$ where $\{h_s | s \in Sds\}$ is a UHF with $h_s : \{0,1\}^{nNq} \to \{0,1\}^b$ and

$$\begin{aligned}
b &= n(H(\Delta) - \delta) + 2\log\epsilon \\
&= n(\eta\log\eta + (1-\eta)\log\frac{1-\eta}{2^{Nq}-1} - \delta) + 2log\epsilon
\end{aligned} \tag{8.9}$$

Relation (8.9) relates b to η, which is the channel's parameter because $H(\Delta) = -\Big(\eta\log\eta + (1-\eta)\log\frac{1-\eta}{2^{Nq}-1}\Big)$.

Let X^n be the input to $h_s(\cdot)$. Then, for the pair of correlated random variables $(X^n, {Z_{\epsilon'}}^n)$, Lemma 8.2 implies:

$$\mathbf{SD}((\mathsf{EXT}(S, X^n), {Z_{\epsilon'}}^n, S); (U_{\mathcal{K}}, {Z_{\epsilon'}}^n, S)) \leq \frac{\epsilon}{2}.$$

Since $SD(Z; Z_{\epsilon'}) \leq \epsilon'$ and $Z_1, \ldots, Z_n$ are independent, then $SD(Z^n; {Z_{\epsilon'}}^n) \leq \epsilon'$. We have

$$\begin{aligned}
&SD((\mathsf{EXT}(S, X^n), Z^n, S); (U_{\mathcal{K}}, Z^n, S)) \\
&\leq SD((\mathsf{EXT}(S, X^n), Z^n, S); (\mathsf{EXT}(S, X^n), {Z_{\epsilon'}}^n, S)) \\
&+SD((\mathsf{EXT}(S, X^n), Z_{\epsilon'}, S); (U_{\mathcal{K}}, {Z_{\epsilon'}}^n, S)) \\
&+SD((U_{\mathcal{K}}, Z^n, S); (U_{\mathcal{K}}, {Z_{\epsilon'}}^n, S)) \leq \epsilon' + \frac{\epsilon}{2} + \epsilon' = \epsilon.
\end{aligned}$$

That is the required condition (8.8) for security of the key.

-**Secret key rate:** b is the length of the extracted key. The achievable rate of the construction is then:

$$R_{sk} = \frac{b}{n} = \frac{\tilde{H}_\infty(X^n|{Z_{\epsilon'}}^n) - 2\log\frac{1}{\epsilon}}{n}.$$

When $n \to \infty$, we have

$$\begin{aligned}
\lim_{n\to\infty} R_{sk} &= \lim_{n\to\infty} \frac{\tilde{H}_\infty(X^n|{Z_{\epsilon'}}^n) - 2\log\frac{1}{\epsilon}}{n} \\
&\geq \lim_{n\to\infty} \frac{n(H(\Delta) - \delta) - 2\log\frac{1}{\epsilon}}{n} \\
&= H(\Delta) - \lim_{n\to\infty}\frac{\delta}{n} - \lim_{n\to\infty}\frac{2\log\frac{1}{\epsilon}}{n} \\
&= H(\Delta) = C_s(\mathrm{BiT}^N_{\eta,q}).
\end{aligned}$$

□

Remark 8.3. *According to [2, Corollary 2], if the wiretap channel* $\{\mathsf{WT} : \mathcal{X} \to \mathcal{Y}\times\mathcal{Z}\}$ *satisfies the condition* $\mathsf{WT}(y,z|x) = \mathsf{W}_1(y|x)\cdot\mathsf{W}_2(z|x)$*, then the secret key capacity is equal to the secrecy capacity of the wiretap channel. So SKA-I and SKA-II are both capacity-achieving.*

8.4 Two-way SKA over a pair of wiretap channels

The above two SKA's assume that a good estimation of η that is directly related to Eve's BER, is available. For fixed receiver device for Eve, and transmission and jamming signal power, η is primarily a function of the location of Eve. To provide some level of independence to Eve's location, we consider a two-way protocol where Alice and Bob invoke BiT^A_q initiated by Alice and BiT^B_q initiated by Bob, respectively, and the final key is a combination of the two shared strings that are obtained through this invocation. The authors in [59] pointed out (and verified in their experiment) that for a fixed static (not moving) adversary, in most cases, at least one of BiT^A_q or BiT^B_q gives the eavesdropper a corrupted view.

A direct approach to constructing a key from the two shared partially leaked strings is to apply an extractor on each individually, and then concatenate the results of the two. In the following, we use a novel way (Lemma 8.4) of extracting randomness from two independent sources, corresponding to the two strings generated by Alice and Bob, to generate the secret key. Intuitively, as long as the *combined entropy* of the two sources is sufficient, the secret key will be secure. This allows the key to remain secure in the situation when increasing the entropy of one source implies decreasing the entropy of the other source, which is typically the case in our two-way SKA. The source here is a uniform string conditioned on the eavesdropper's view of

Figure 8.4: SKA-III

1. Alice does the following.
   –Samples a uniform seed $S \in Sds$. S is directly transmitted to Bob.
   – For each $i = 1, \cdots, n$, Alice chooses a vector X_i that is uniformly distributed over $\{0,1\}^{Nq}$, and sends to Bob using BiT_q^A .
2. Bob does the following.
   –For each $i = 1, \cdots, n'$, Bob chooses a vector Y_i' that is uniformly distributed over $\{0,1\}^{Nq}$, and transmit to Bob using BiT_q^B .
3. Key derivation:
   - Alice computes $K_A = \mathsf{h}_S(X^n) \oplus Y'^{n'}$;
   - Bob computes $K_B = \mathsf{h}_S(Y^n) \oplus X'^{n'}$,

   where $(Y^n, Z^n) = \mathsf{WT}^n(X^n)$, $(X'^{n'}, Z'^{n'}) = \mathsf{WT}'^{n'}(Y'^{n'})$ and $\mathsf{h}_S : \{0,1\}^{nNq} \to \{0,1\}^{n'Nq}$ is an XOR-universal hash function. Suppose $\mathrm{BiT}_q^A = \mathrm{BiT}_{\eta,q}^N$ and $\mathrm{BiT}_q^B = \mathrm{BiT}_{\eta',q}^N$. The parameters n and n' should satisfy the relation $\frac{n}{n'} > \frac{1-C_s(\mathrm{BiT}_{\eta',q}^N)}{C_s(\mathrm{BiT}_{\eta,q}^N)}$.

the string, which in the case when the jamming power is fixed depends on the eavesdropper's location.

We abuse the notion of SKA with respect to a wiretap channel a little bit to allow a pair of wiretap channels $\{\mathsf{WT} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}\}$ and $\{\mathsf{WT}' : \mathcal{Y} \to \mathcal{X} \times \mathcal{Z}\}$. In particular, Alice uses the wiretap channel WT for n times and Bob uses the wiretap channel WT' for n' times. The public discussion phase together with the rest of the definition remain the same (see Definition 8.8). We then call it a two-way[2] SKA over a pair of wiretap channels. Our protocol in this model is given in Figure 8.4.

We need the following lemma for the security proof of our two-way SKA protocol. The lemma proves a generalization of the two-source extractor in Lemma 8.3, when both sources are all conditioned on other random variables. An intermediate generalization of Lemma 8.3 to the case when only one source is conditioned on another random variable was shown in [120].

Lemma 8.4. *Let $\{h_s | s \in Sds\}$ be a family of XOR-Universal hash functions $h_s : \{0,1\}^n \to \{0,1\}^\ell$. Let A be a random variable over $\{0,1\}^n$ and B be a random variable over $\{0,1\}^\ell$. Assume A are B are independent. Let V_A and V_B be random variables, possibly dependent on A and B, respectively. V_A is independent of B*

[2]Note that the term "one-way" and "two-way" were used to refer to the public discussions in some papers. Here we refer to the wiretap channels.

and V_B is independent of A. Then

$$\begin{aligned}&\mathbf{SD}((S, V_A, V_B, h_S(A) \oplus B); (S, V_A, V_B, U_\ell))\\ &\leq \sqrt{2^{-(\tilde{H}_\infty(A|V_A)+\tilde{H}_\infty(B|V_B)-\ell-1)}},\end{aligned}$$

or equivalently,

$$\mathbf{SD}((S, V_A, V_B, h_S(A) \oplus B); (S, V_A, V_B, U_\ell)) \leq \varepsilon,$$

if $\tilde{H}_\infty(A|V_A) + \tilde{H}_\infty(B|V_B) \geq \ell + 2\log(\frac{1}{\varepsilon}) + 1$.

Proof. Consider the fixed values $V_A = \mathbf{v}_A,\ V_B = \mathbf{v}_B$, and apply Lemma 8.3 to $A|V = \mathbf{v}_A$ and $B|V = \mathbf{v}_B$. We will have,

$$\begin{aligned}&\mathbf{SD}\left((S, h_S((A|V = \mathbf{v}_A) \oplus (B|V = \mathbf{v}_B)); (S, U_\ell)\right)\\ &\leq \sqrt{2^{-(H_\infty(A|V=\mathbf{v}_A)+H_\infty(B|V=\mathbf{v}_B)-\ell-1)}}.\end{aligned}$$

Taking expectation over $\mathbf{v}_A,\ \mathbf{v}_B$ on both sides yields,

$$\begin{aligned}&\mathbf{SD}\left((S, V_A, V_B, h_S(A) \oplus B); (S, V_A, V_B, U_\ell)\right)\\ &\leq \mathbb{E}_{\mathbf{v}_A,\ \mathbf{v}_B}\left(\sqrt{2^{-(H_\infty(A|V=\mathbf{v}_A)+H_\infty(B|V=\mathbf{v}_B)-\ell-1)}}\right)\\ &\leq \sqrt{\mathbb{E}_{\mathbf{v}_A,\ \mathbf{v}_B}\left(2^{-(H_\infty(A|V=\mathbf{v}_A)+H_\infty(B|V=\mathbf{v}_B)-\ell-1)}\right)}\\ &= \sqrt{2^{-(\tilde{H}_\infty(A|V_A)+\tilde{H}_\infty(B|V_B)-\ell-1)}},\end{aligned}$$

where the second inequality follows from applying Jensen's inequality to the function $f(x) = \sqrt{x}$, and the equality follows directly from the definition of conditional min-entropy. ■

An instantiation of the XOR-UHF Let $\mathcal{X} = \{0,1\}^n$ and $\mathcal{Y} = \{0,1\}^{n'}$. Let $Sds = \{0,1\}^n$ if $n \geq n'$ and $Sds = \{0,1\}^{n'}$, otherwise. Let $h_s : \mathcal{X} \to \mathcal{Y}$ be defined as follows.

$$h_s(\mathbf{x}) = \begin{cases} (s \odot \mathbf{x})|_{n'}, & \text{if } n \geq n' \\ s \odot (\mathbf{x}||0^{n'-n}), & \text{otherwise,} \end{cases} \tag{8.10}$$

where $\odot$ is the finite field multiplication and $|_{n'}$ denotes the first n' bits of the vector representation of a finite field element.

Theorem 8.5. *Two-way SKA protocol is an SKA as long as* $\frac{n}{n'} > \frac{1-C_s(BiT^N_{\eta',q})}{C_s(BiT^N_{\eta,q})}$.

Proof. The correctness of the derived key is straightforward as Alice receives $X'^{n'} = Y'^{n'}$ from Bob and Bob

receives $Y^n = X^n$ and S from Alice. They both are able to derive the shared key as follows:

$$K = K_A = K_B = \mathsf{h}_S(X^n) \oplus Y'^{n'} = \mathsf{h}_S(Y^n) \oplus X'^{n'}.$$

To prove the secrecy of the key we show the following:

$$SD(S, Z^n, Z'^{n'}, K; S, Z^n, Z'^{n'}, U_{\mathcal{K}}) \leq \epsilon, \tag{8.11}$$

where $U_{\mathcal{K}}$ is uniformly distributed over $\mathcal{K}$. This is using condition (8.7) for proving the security of the scheme.

Let $\beta = C_s(\mathrm{BiT}^N_{\eta,q})$ and $\beta' = C_s(\mathrm{BiT}^N_{\eta',q})$. According to the construction, the numbers of random bits transmitted through virtual wiretap channels in both directions, nNq from Alice to Bob and $n'Nq$ bits from Bob to Alice, should satisfy

$$\frac{n}{n'} > \frac{1-\beta'}{\beta}.$$

Assume $\frac{n}{n'} = \frac{1-\beta'}{\beta} + \xi$, where $\xi > 0$. We now want to show that for any security parameter $\varepsilon > 0$, (8.11) holds for large n. Let $\varepsilon' = \frac{\varepsilon}{8}$ be the smooth entropy parameter for both Z and Z', and denote the corresponding smoothed distributions $Z^{\varepsilon'}$ and $Z'^{\varepsilon'}$. By replacing Z with $Z^{\varepsilon'}$ and Z' with $Z'^{\varepsilon'}$, $\frac{\varepsilon}{8} \times 4 = \varepsilon/2$ is lost. Finally, since the secret key $K = \mathsf{h}_S(X^n) \oplus Y'^{n'}$ is the output of the two source extractor in Lemma 8.4, (8.11) holds as long as

$$\tilde{H}(X^n|Z^{\varepsilon' n}) + \tilde{H}(Y'^{n'}|Z'^{\varepsilon' n'}) \geq n'Nq + 2\log\frac{1}{\varepsilon/2} + 1. \tag{8.12}$$

It was shown in the proof of Theorem 8.4 that

$$\frac{\tilde{H}(X^n|Z^{\varepsilon' n})}{nNq} \to \beta \text{ (also } \frac{\tilde{H}(Y'^{n'}|Z'^{\varepsilon' n'})}{n'Nq} \to \beta').$$

We simply write

$$\tilde{H}(X^n|Z^{\varepsilon' n}) = nNq\beta - o(n)$$
$$\tilde{H}(Y'^{n'}|Z'^{\varepsilon' n'}) = n'Nq\beta' - o(n').$$

Substituting $\frac{n}{n'} = \frac{1-\beta'}{\beta} + \xi$, we then have

$$\tilde{H}(X^n|Z^{\varepsilon' n}) + \tilde{H}(Y'^{n'}|Z'^{\varepsilon' n'}) = n'Nq\left(\tfrac{n\beta}{n'} + \beta'\right) - o(n) = n'Nq + n'Nq\xi\beta' - o(n),$$

where the right hand side can be made bigger than the right hand side of (8.12) for large n. This concludes the proof. □

8.5 Discussion of the self-jamming strategies

In this section, we examine different self-jamming strategies to see possibilities of improving the achievable effective rate of the message transmission systems using them. More concretely, we ask the following question: are there jamming strategies other than the "repeat-and-jam-one of the two" strategy used in BiT that can improve the communication rate. BiT enables secret transmission by giving the receiver one correct time sample while giving the eavesdropper two time samples, one correct, and one jammed, such that with careful choice of system parameters, distinguishing the correct sample has small probability. This is realized by the "repeat-and-jam-one of the two" strategy. Repeating the sent signal allows the receiver to obtain one correct sample left for the receiver, and jamming one generates uncertainty for the eavesdropper. A direct generalization of this strategy suggests a jamming strategy where three copies of the signal is sent, and two of them jammed by the receiver. More generally, one may consider the case that the information, instead of being repeated multiple times, be coded into a string of n components such that recovery of k components by the receiver will recover the information. Note that since the receiver is the jammer and so can identify the correct components, recovery will be equivalent to erasure decoding. However, for Eve, who will receive the n components through a noisy channel, decoding of the n components and recovering k correct ones, will be with high uncertainty. Implementing such strategies and experimental results on the BER of the eavesdropper is an interesting direction for future research.

8.6 Conclusion

Concluding remarks

Physical layer security is a promising direction for providing secure communication. Protocols using this approach are commonly evaluated using extensive experiments. While such results could provide a good level of assurance for some settings, providing formal models and analysis can provide a deeper understanding of important parameters of the system, and suggest novel constructions. Our abstraction of BiT allowed us to propose three secret key agreement protocols with provable security. It also suggested new jamming strategies that could improve the rate of communication.

In our constructions, we obtained asymptotic rates and assumed that communication cost of seed is amortized over long length of key. Finding the effective key rate for finite-length key, and taking into account the transmission cost of the seed, is our future work.

Future work

Our results suggest a number of interesting directions for the future work.

- Although asymptotic performance of the two one-way protocols in C1 and C2 are the same, an interesting question is the comparison of the actual cost of establishing an ℓ-bit key. Such a cost must take into account the cost of reliable transmission of an extractor seed to the receiver. We will leave this as an open question.

- Eve's BER is determined by (i) the transmitter power level, (ii) reception device of Eve and (iii) the location of Eve. Considering strategies that can be used to reduce the dependence of the security guarantee on the actual value of BER is an interesting direction of future work.

- In our work, we started from an implementation of a physical layer security system, devised a formal model for it, and developed protocols for key agreement with provable security. The resulting protocols are practical in the sense that the underlying mechanism has already been implemented and studied and the proposed protocols use this mechanism as a black box and relate the final security to the properties of this box. In Section 8.5, we propose some alternative strategies of jamming. These strategies need to be implemented and evaluated in practice (similar to the evaluation of iJam). The interaction between theoretical and experimental systems is an exciting direction for future work.

Chapter 9

Conclusion and Future Work

Information-theoretic security provides secrecy guarantee for information communication systems without any computational assumption. In these systems, the noise over communication channels and the secret key shared by communicating parties are the primary resources that provide information-theoretic security. The main focus of this thesis was on secure communication using these two resources. In this context, three research problems were studied. In the first problem, secure message transmission using only noise over communication channels was studied. In the closely associated second problem, the shared secret key and the noise over channels both contribute to providing security for message transmission. In the third research problem of this thesis, the establishment of a shared key was questioned. The established information-theoretic secret key can be used for secure message transmission individually or coupled with noise (as in the second problem).

In the following, results of studying the above three main problems are summarized and open questions and future directions to pursue are pointed out.

9.1 Modular semantically secure wiretap encoding

In this thesis, the wiretap channel model is employed to study secure message transmission using noisy channels. A wiretap encoding scheme exploits the noise over the communication channel and provides secrecy for the message transmission. The secrecy notion of message encoding over the wiretap channel has been strengthened by the introduction of *semantic security* for wiretap channels by Bellare et al. [11] who also proposed a modular construction of wiretap encoding systems with semantic security that achieves the secrecy capacity of binary input discrete memoryless channels.

In Chapter 2, a new modular construction of wiretap codes called **HtE** is proposed. The construction

is a seeded encoding system that uses a public channel for sharing a random seed. This construction outperforms the computational efficiency of previously proposed modular semantically secure constructions, and has lower public transmission cost of encoding in comparison to other seeded encryption schemes due to using an essentially shorter random seed for encoding. In Chapter 3, a concrete framework for comparing the transmission efficiency of seeded wiretap encoding schemes in a finite-length regime is proposed.

The security proof of the construction in Chapter 2 is indirect and follows the framework of [11] by first proving the security for uniformly distributed message space and then concluding security for any message distribution when the encoding is separable and message linear. This results in showing the semantic security and capacity-achieving properties of the **HtE** construction for similar channels as the ones in [11]. The **HtE** construction is revisited in Chapter 6 as a special case of the more general keyed construction. Using this chapter's results, semantic security and capacity-achieving of the **HtE** construction are proved for a wider class of channels. In particular, the semantic security of the construction for DMCs over binary alphabets, and the capacity-achieving property for weakly symmetric wiretap channels are shown.

A practical physical layer security protocol with provable security is studied in Chapter 4, where a wiretap channel is realized. An already implemented cooperative jamming protocol in [59] is abstractly modelled as a wiretap channel and referred to as a virtual wiretap channel. Subsequently, channel parameters of the abstract model are estimated, the secrecy capacity is derived, and a secure message transmission protocol with provable semantic security for secure message transmission over the channel is introduced.

Open questions and challenges. This work creates a number of questions and challenges that remain to be answered.

- *Deterministic semantically secure wiretap codes:* Wiretap constructions considered here are seeded constructions. Although the seed value is public and its secrecy is not a concern for the encoding scheme, reliable transmission of the seed is costly. The proposed construction in this thesis requires the shortest seed length and consequently the least cost for transmitting the random seed among all wiretap seeded encryption systems. A direction for future research is exploring deterministic wiretap codes that don't use a random seed but still have other attractive properties of the seeded wiretap codes including modularity, semantic security and capacity-achieving. A good start in this direction is the modular deterministic wiretap code in [66] that is only shown to provide the strong security and not the semantic security.

- *Active adversary:* In this thesis, a passive adversary that only eavesdrops on the communication channel is studied. It is fair to ask if it is possible to transmit a message reliably and securely over a wiretap

channel in the presence of an active adversary. An active adversary for a wiretap channel needs to be carefully modelled to reflect the real-world capabilities and limitations of communication devices. For example, an active adversary in the wiretap channel model may have to choose between eavesdropping or jamming the communication in different time slots because most wireless devices cannot transmit and receive simultaneously.

- *Wiretap channel creation:* A self-jamming technique as a special type of cooperative jamming for realizing a wiretap channel is considered here. The framework of using practical physical layer communication techniques to realize a wiretap channel and design protocols with strong (in particular, information-theoretic) security guarantees can be considered in future research.

9.2 Modular semantically secure keyed wiretap encoding

In an information-theoretic context, using the shared secret key and the noise over the eavesdropper's channel for secure message transmission immediately results in the combined model of Wyner [143] and Shannon [116], known as the keyed wiretap channel model. The security of message encryption in this model has been defined for uniformly distributed message space, and the general secrecy capacity is derived in [78]. The only explicit construction of a keyed wiretap encryption scheme was the polar code-based construction of [141]. In Chapter 5, for the first time, semantic security is defined for the keyed wiretap channel encryption, and a modular construction named **KHtE** is proposed that provides semantic security and achieves the secrecy capacity of weakly symmetric wiretap channels. This construction cannot guarantee security in the absence of a shared key. The construction is improved in Chapter 6 to ensure that message encryption is secure as long as at least one of the two security contributors (shared key or noise over the wiretapper's channel) is available in the communication setting. The new construction is called **KHtE*** and shown to provide semantic security for any DMC with an arbitrary binary alphabet, and achieves the secrecy capacity of weakly symmetric wiretap channels.

Open questions and challenges. The open questions of this work are listed below:

- *Keyed wiretap codes for other types of channels:* Proposed constructions in this thesis are for DMCs. It is interesting to explore keyed wiretap codes for other types of channels such as Gaussian wiretap channels. Moreover, achieving the capacity of general DMCs still remains open. Showing the **KHtE*** construction, or any other explicit construction, achieves the general secrecy capacity of a keyed wiretap channel is an interesting open question for future work.

- *Finite-length analysis of existing keyed wiretap codes:* The finite-length analysis of keyed wiretap codes is a step toward evaluating their efficiency in practice. Bounds on the achievable rate of the **KHtE*** construction follow from the proof of semantic security. However, accurate approximation of second order terms, finding finite-length converse bounds and comparing the achievable and converse bounds is a direction for future research. This kind of analysis can also be considered for the polar code-based construction of [141].

9.3 Information-theoretic secret key agreement

Secret key agreement using physical layer assumptions is a desirable candidate for providing long-term security. Using the one-time-pad (OTP) encryption method, or any other symmetric key encryption scheme, a key agreement scheme can be directly converted into an encryption scheme. In Chapter 7 of this thesis, physical layer properties are abstracted in the source model, and information-theoretic secret key agreement in this model is considered. An OM-SKA protocol is proposed that achieves the OW-SK capacity of $n-$IID sources. The protocol uses the concept of information spectrum to design the information reconciliation phase of the protocol such that it achieves a close to optimal key length. The protocol also provides an upper-bound on the public communication cost (in terms of the transmitted bits) of the protocol in the finite-length regime.

Physical layer properties of the communication medium can be exploited by self-jamming techniques. The abstract "virtual" wiretap channel model of Chapter 4 is used in Chapter 8 to propose key agreement protocols using this technique and to suggest effective self-jamming strategies. Using this abstraction, the proposed key agreement protocols in this chapter are shown to be information-theoretically secure and their efficiency is formally analysed.

Open questions and challenges. This work raises many questions and directions for future works.

- *Efficient OM-SKA protocols:* A close investigation of the OM-SKA protocol in Chapter 7 shows that despite the relatively simple computation of the reconciliation phase, the protocol computation quickly becomes unwieldy. The construction of polar code-based OM-SKA protocols is also not efficient in practice. Modifications to the OM-SKA protocol of this thesis, or finding new efficient OM-SKA protocols that achieve the OW-SK capacity of the source model remains open for future research.

- *Tighter bounds on the achievable OM-SKA length:* Hayashi et al. [68] give a tight finite-length lower-bound (that matches a finite-length upper-bound up to the second order term in $\mathcal{O}(\sqrt{n})$) using an interactive protocol for the source model SKA. The achievable lower-bound of the proposed OM-SKA

protocol in this thesis does not match this tight bound. Any refinement of the protocol to improve its achievable bound or showing the impossibility of achieving tighter bounds with OM-SKA protocols can be a subject for future work.

- *Information-theoretic KEM:* The key encapsulation mechanism (KEM) is a public-key encryption scheme that generates the encryption of a random key that is decryptable by the receiver. The information flow in source model OM-SKA is aligned with the one-way information flow from the encapsuler to the decapsuler in KEM. Making a direct connection between a KEM and a one-message secret key agreement protocol is an interesting direction of future work. This study is initiated in Appendix C of this thesis.

- *Information-theoretic SKA in a network:* OM-SKA protocols are desired in networks, where interaction adds an extra layer of complexity to the network design. Information-theoretic key agreement for multiple terminals is studied in [56]. Studying OM-SKA protocols in networks with multiple terminals is subject to future researches.

- *SKA with Feedback:* The role of a feedback channel in improving the secrecy rate of a wiretap channel has been considered in works such as [83] and [5]. Abstracting a cooperative jamming or a self-jamming system by a wiretap channel with a feedback model enables the study of such systems from an information-theoretic viewpoint.

Bibliography

[1] R. Ahlswede and N. Cai, "Transmission, Identification and Common Randomness Capacities for Wire-Tape Channels with Secure Feedback from the Decoder," in *General Theory of Information Transfer and Combinatorics*. Springer, 2006, pp. 258–275.

[2] R. Ahlswede and I. Csiszar, "Common Randomness in Information Theory and Cryptography. I. Secret Sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul 1993.

[3] W. Aiello, M. Bellare, G. Di Crescenzo, and R. Venkatesan, "Security Amplification by Composition: The Case of Doubly-iterated, Ideal Ciphers," in *Annual International Cryptology Conference*. Springer, 1998, pp. 390–407.

[4] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange: A new hope," in *Proceedings of the 25th USENIX Conference on Security Symposium*, ser. SEC'16. USA: USENIX Association, 2016, p. 327–343.

[5] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap Channel With Secure Rate-Limited Feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, Dec 2009.

[6] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, Jul 2009.

[7] C. Asmuth and G. Blakley, "An Efficient Algorithm for Constructing a Cryptosystem which is Harder to Break than Two Other Cryptosystems," *Computers & Mathematics with Applications*, vol. 7, no. 6, pp. 447–450, 1981.

[8] B. Barak, R. Shaltiel, and E. Tromer, "True Random Number Generators Secure in a Changing Envi-

ronment," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2003, pp. 166–180.

[9] M. Bellare and S. Tessaro, "Polynomial-Time, Semantically-Secure Encryption Achieving the Secrecy Capacity," *arXiv preprint arXiv:1201.3160*, Jan 2012. [Online]. Available: http://arxiv.org/abs/1201.3160

[10] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," in *Annual International Cryptology Conference*. Springer, 1998, pp. 26–45.

[11] M. Bellare, S. Tessaro, and A. Vardy, "Semantic Security for the Wiretap Channel," in *Annual Cryptology Conference*. Springer, 2012, pp. 294–311.

[12] M. Bellare, S. Tessaro, and A. Vardy, "A Cryptographic Treatment of the Wiretap Channel," *arXiv preprint arXiv:1201.2205*, Jan 2012. [Online]. Available: http://arxiv.org/abs/1201.2205

[13] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy Amplification by Public Discussion," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, Apr 1988.

[14] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[15] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized Privacy Amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[16] K. Bentahar, P. Farshim, J. Malone-Lee, and N. P. Smart, "Generic Constructions of Identity-Based and Certificateless KEMs," *Journal of Cryptology*, vol. 21, no. 2, pp. 178–199, Apr 2008.

[17] P. Bergmans, "Random Coding Theorem for Broadcast Channels with Degraded Components," *IEEE Transactions on Information Theory*, vol. 19, no. 2, pp. 197–207, Mar 1973.

[18] A. C. Berry, "The Accuracy of the Gaussian Approximation to the Sum of Independent Variates," *Transactions of the American Mathematical Society*, vol. 49, no. 1, p. 122, Jan 1941.

[19] M. R. Bloch and J. N. Laneman, "Strong Secrecy From Channel Resolvability," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8077–8098, Dec 2013.

[20] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "Frodo," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, ACM. New York, New York, USA: ACM Press, 2016, pp. 1006–1018.

[21] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE. IEEE, Apr 2018, pp. 353–367.

[22] X. Boyen, Q. Mei, and B. Waters, "Direct Chosen Ciphertext Security from Identity-Based Techniques," in *Proceedings of the 12th ACM conference on Computer and communications security - CCS '05*, ACM. New York, New York, USA: ACM Press, 2005, p. 320.

[23] G. Brassard and C. Crépeau, "Oblivious Transfers and Privacy Amplification," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1997, pp. 334–347.

[24] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *Advances in Cryptology — EUROCRYPT '93*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 410–423.

[25] J. L. Carter and M. N. Wegman, "Universal Classes of Hash Functions (Extended Abstract)," in *Proceedings of the ninth annual ACM symposium on Theory of computing - STOC '77*. New York, New York, USA: ACM Press, 1977, pp. 106–112.

[26] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post-Quantum Cryptography," *Talk given at PQCrypto*, vol. 16, Apr 2016.

[27] Y. Chen, L. Chen, and Z. Zhang, "CCA Secure IB-KEM from the Computational Bilinear Diffie-Hellman Assumption in the Standard Model," in *International Conference on Information Security and Cryptology*. Springer, 2012, pp. 275–301.

[28] M. Cheraghchi, F. Didier, and A. Shokrollahi, "Invertible Extractors and Wiretap Protocols," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1254–1274, Feb 2012.

[29] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar Coding for Secret-Key Generation," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6213–6237, Nov 2015.

[30] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley, Sep 2005.

[31] R. Cramer and V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack," *SIAM Journal on Computing*, vol. 33, no. 1, pp. 167–226, Jan 2003.

[32] R. Cramer, G. Hanaoka, D. Hofheinz, H. Imai, E. Kiltz, R. Pass, A. Shelat, and V. Vaikuntanathan, "Bounded CCA2-Secure Encryption," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2007, pp. 502–518.

[33] R. Cramer, I. B. Damgård, N. Döttling, S. Fehr, and G. Spini, "Linear Secret Sharing Schemes from Error Correcting Codes and Universal Hash Functions," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2015, pp. 313–336.

[34] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[35] I. Csiszar and P. Narayan, "Common Randomness and Secret Key Generation with a Helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, Mar 2000.

[36] L. De Feo, "Mathematics of Isogeny Based Cryptography," *arXiv preprint arXiv:1711.04062*, Nov 2017. [Online]. Available: http://arxiv.org/abs/1711.04062

[37] P. Delsarte and P. Piret, "Algebraic Constructions of Shannon Codes for Regular Channels," *IEEE Transactions on Information Theory*, vol. 28, no. 4, pp. 593–599, Jul 1982.

[38] A. W. Dent, "A Designer's Guide to KEMs," in *IMA International Conference on Cryptography and Coding*. Springer, 2003, pp. 133–151.

[39] K. Dickerson, "Microsoft lab Predicts we'll have a working 'hybrid' quantum computer in 10 years," Oct 2015. [Online]. Available: https://www.businessinsider.com/microsoft-hybrid-quantum-computer-2015-10

[40] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov 1976.

[41] J. Ding, X. Xie, and X. Lin, "A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem." *IACR Cryptology ePrint Archive*, vol. 2012, p. 688, 2012.

[42] Y. Dodis and J. Katz, "Chosen-Ciphertext Security of Multiple Encryption," in *Theory of Cryptography Conference*. Springer, 2005, pp. 188–209.

[43] Y. Dodis and A. Smith, "Entropic Security and the Encryption of High Entropy Messages," in *Theory of Cryptography Conference*. Springer, 2005, pp. 556–577.

[44] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," in *SIAM Journal on Computing*, vol. 38. Springer, Jan 2004, pp. 523–540.

[45] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, Jan 2008.

[46] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, and A. Smith, "Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets," in *IEEE Transactions on Information Theory*, vol. 58. Springer, Sep 2012, pp. 6207–6222.

[47] D. Dolev, C. Dwork, and M. Naor, "Nonmalleable Cryptography," *SIAM Review*, vol. 45, no. 4, pp. 727–784, Jan 2003.

[48] G. Dueck, "Maximal Error Capacity Regions are Smaller than Average Error Capacity Regions for Multi-User Channels," *Problems of Control and Information Theory*, vol. 7, no. 1, pp. 11–19, 1978.

[49] C. Dwork and S. Naor, "Method for Message Authentication from Non-malleable Crypto Systems," 1996.

[50] C. G. Esseen, "Fourier Analysis of Distribution Functions. A Mathematical Study of the Laplace-Gaussian Law," *Acta Mathematica*, vol. 77, pp. 1–125, 1945.

[51] S. Even and O. Goldreich, "On the Power of Cascade Ciphers," *Advances in Cryptology*, vol. 3, no. 2, pp. 43–50, 1984.

[52] A. Freier, P. Karlton, and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0," Aug 2011. [Online]. Available: https://www.rfc-editor.org/info/rfc6101

[53] D. Galindo, "Chosen-Ciphertext Secure Identity-Based Encryption from Computational Bilinear Diffie-Hellman," in *International Conference on Pairing-Based Cryptography*. Springer, 2010, pp. 367–376.

[54] R. Gallager, "A Simple Derivation of the Coding Theorem and Some Applications," *IEEE Transactions on Information Theory*, vol. 11, no. 1, pp. 3–18, Jan 1965.

[55] F. Giacon, F. Heuer, and B. Poettering, "KEM Combiners," in *IACR International Workshop on Public Key Cryptography*. Springer, 2018, pp. 190–218.

[56] A. A. Gohari and V. Anantharam, "Information-Theoretic Key Agreement of Multiple Terminals—Part I," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3973–3996, aug 2010. [Online]. Available: http://ieeexplore.ieee.org/document/5508611/

[57] A. Goldsmith, *Wireless Communications*. Cambridge University Press, Aug 2005.

[58] S. Goldwasser and S. Micali, "Probabilistic Encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, Apr 1984.

[59] S. Gollakota and D. Katabi, "Physical Layer Wireless Security Made Fast and Channel Independent," in *2011 Proceedings IEEE INFOCOM*, IEEE. IEEE, Apr 2011, pp. 1125–1133.

[60] D. Gunduz, D. R. Brown, and H. V. Poor, "Secret Communication with Feedback," in *2008 International Symposium on Information Theory and Its Applications*, IEEE. IEEE, Dec 2008, pp. 1–6.

[61] V. Guruswami, "Bridging Shannon and Hamming: List Error-correction with Optimal Rate," in *Proceedings of the International Congress of Mathematicians 2010 (ICM 2010)*, World Scientific. Published by Hindustan Book Agency (HBA), India. WSPC Distribute for All Markets Except in India, Jun 2011, pp. 2648–2675.

[62] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical Layer Security Game: Interaction between Source, Eavesdropper, and Friendly Jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 452907, Dec 2010.

[63] K. Haralambiev, T. Jager, E. Kiltz, and V. Shoup, "Simple and Efficient Public-Key Encryption from Computational Diffie-Hellman in the Standard Model," in *International Workshop on Public Key Cryptography*. Springer, 2010, pp. 1–18.

[64] D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen, "On Robust Combiners for Oblivious Transfer and Other Primitives," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2005, pp. 96–113.

[65] M. Hayashi, "Semi-Finite Length Analysis for Secure Random Number Generation," in *2019 IEEE International Symposium on Information Theory (ISIT)*. IEEE, Jul 2019, pp. 952–956.

[66] M. Hayashi and R. Matsumoto, "Construction of Wiretap Codes from Ordinary Channel Codes," *2010 IEEE International Symposium on Information Theory*, pp. 2538–2542, Jun 2010.

[67] M. Hayashi and R. Matsumoto, "Secure Multiplex Coding with Dependent and Non-uniform Multiple Messages," *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, vol. 62, no. 5, pp. 954–959, Oct 2012.

[68] M. Hayashi, H. Tyagi, and S. Watanabe, "Secret Key Agreement: General Capacity and Second-Order Asymptotics," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3796–3810, Jul 2016.

[69] J. Herranz, D. Hofheinz, and E. Kiltz, "Some (in)sufficient conditions for secure hybrid encryption," *Information and Computation*, vol. 208, no. 11, pp. 1243–1257, Nov 2010.

[70] A. Herzberg, "On Tolerant Cryptographic Constructions," in *Cryptographers' Track at the RSA Conference*. Springer, 2005, pp. 172–190.

[71] E. Hof and S. Shamai, "Secrecy-Achieving Polar-Coding," in *2010 IEEE Information Theory Workshop*, IEEE. IEEE, Aug 2010, pp. 1–5.

[72] D. Hofheinz and D. Unruh, "On the Notion of Statistical Security in Simulatability Definitions," in *International Conference on Information Security*. Springer, 2005, pp. 118–133.

[73] T. Holenstein, "Strengthening Key Agreement using Hard-core Sets," Ph.D. dissertation, ETH Zurich, 2006.

[74] T. Holenstein and R. Renner, "One-Way Secret-Key Agreement and Applications to Circuit Polarization and Immunization of Public-Key Encryption," in *Advances in Cryptology – CRYPTO 2005*, V. Shoup, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 478–493.

[75] T. Holenstein and R. Renner, "On the Randomness of Independent Experiments," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1865–1871, Apr 2011.

[76] R. Impagliazzo and D. Zuckerman, "How to Recycle Random Bits," in *30th Annual Symposium on Foundations of Computer Science*, IEEE. IEEE, 1989, pp. 248–253.

[77] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-Random Generation from One-Way Functions," in *Proceedings of the twenty-first annual ACM symposium on Theory of computing - STOC '89*, ACM. New York, New York, USA: ACM Press, 1989, pp. 12–24.

[78] W. Kang and N. Liu, "Wiretap Channel with Shared Key," in *2010 IEEE Information Theory Workshop*, IEEE. IEEE, Aug 2010, pp. 1–5.

[79] B. Kanukurthi and L. Reyzin, "Key Agreement from Close Secrets over Unsecured Channels," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2009, pp. 206–223.

[80] G. Karagiannidis and A. Lioumpas, "An Improved Approximation for the Gaussian Q-Function," *IEEE Communications Letters*, vol. 11, no. 8, pp. 644–646, Aug 2007.

[81] L. Lai and H. El Gamal, "The Relay–Eavesdropper Channel: Cooperation for Secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep 2008.

[82] L. Lai, H. El Gamal, and H. V. Poor, "The Wiretap Channel With Feedback: Encryption Over the Channel," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059–5067, Nov 2008.

[83] L. Lai, H. El Gamal, and H. V. Poor, "The Wiretap Channel With Feedback: Encryption Over the Channel," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059–5067, Nov 2008.

[84] S. Leung-Yan-Cheong, "On a Special Class of Wiretap Channels (Corresp.)," *IEEE Transactions on Information Theory*, vol. 23, no. 5, pp. 625–627, Sep 1977.

[85] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wire-tap Channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[86] Lun Dong, Zhu Han, A. P. Petropulu, and H. V. Poor, "Cooperative Jamming for Wireless Physical Layer Security," in *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*, IEEE. IEEE, Aug 2009, pp. 417–420.

[87] H. Mahdavifar and A. Vardy, "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, Oct 2011.

[88] U. Maurer and S. Wolf, "Secret-Key Agreement over Unauthenticated Public Channels-Part I: Definitions and a Completeness Result," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 822–831, Apr 2003.

[89] U. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2000, pp. 351–368.

[90] U. M. Maurer, "The Strong Secret Key Rate of Discrete Random Triples," in *Communications and Cryptography*. Boston, MA: Springer US, 1994, pp. 271–285.

[91] U. M. Maurer and J. L. Massey, "Cascade Ciphers: The Importance of Being First," *Journal of Cryptology*, vol. 6, no. 1, pp. 55–61, Mar 1993.

[92] U. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[93] U. Maurer and S. Wolf, "Unconditionally Secure Key Agreement and the Intrinsic Conditional Information," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 499–514, Mar 1999.

[94] N. Merhav, "Shannon's Secrecy System With Informed Receivers and its Application to Systematic Coding for Wiretapped Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2723–2734, Jun 2008.

[95] Microsoft, "Understand Azure IoT Hub quotas and throttling — microsoft docs," Aug 2019. [Online]. Available: https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-quotas-throttling

[96] Y. Minsky, A. Trachtenberg, and R. Zippel, "Set Reconciliation with Nearly Optimal Communication Complexity," *IEEE Transactions on Information Theory*, vol. 49, no. 9, pp. 2213–2218, Sep 2003.

[97] A. Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct 2015.

[98] J. Muramatsu and S. Miyake, "Construction of Wiretap Channel Codes by using Sparse Matrices," in *2009 IEEE Information Theory Workshop*, IEEE. IEEE, 2009, pp. 105–109.

[99] N. Nisan and D. Zuckerman, "Randomness is Linear in Space," *Journal of Computer and System Sciences*, vol. 52, no. 1, pp. 43–52, Feb 1996.

[100] L. H. Ozarow and A. D. Wyner, "Wire-Tap Channel II," *Advances in Cryptology*, vol. 63, no. 10, pp. 33–50, 1984.

[101] C. Peikert, "Lattice Cryptography for the Internet," in *international workshop on post-quantum cryptography*. Springer, 2014, pp. 197–219.

[102] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel Coding Rate in the Finite Blocklength Regime," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[103] O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, Sep 2009.

[104] O. Regev, "The Learning with Errors Problem (Invited Survey)," *2010 IEEE 25th Annual Conference on Computational Complexity*, vol. 7, pp. 191–204, Jun 2010.

[105] J. M. Renes, R. Renner, and D. Sutter, "Efficient One-Way Secret-Key Agreement and Private Channel Coding via Polarization," in *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, ser. Lecture Notes in Computer Science, K. Sako and P. Sarkar, Eds., vol. 8269. Springer, 2013, pp. 194–213.

[106] R. Renner and S. Wolf, "The Exact Price for Unconditionally Secure Asymmetric Cryptography," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2004, pp. 109–125.

[107] R. Renner and S. Wolf, "Smooth Renyi Entropy and Applications," in *International Symposium on-Information Theory, 2004. ISIT 2004. Proceedings.*, IEEE. IEEE, 2004, pp. 232–232.

[108] R. Renner and S. Wolf, "Simple and Tight Bounds for Information Reconciliation and Privacy Amplification," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2005, pp. 199–216.

[109] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," *RFC 8446*, Aug 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8446

[110] S. Ross, *A First Course in Probability*. Pearson, Aug 1980, vol. 48.

[111] R. Safavi-Naini and S. Sharifian, "Generalized KEM and its Combiners," *ITC*, 2020, manuscript submitted for review.

[112] A. Sari and M. Karay, "Comparative Analysis of Wireless Security Protocols: WEP vs WPA," *International Journal of Communications, Network and System Sciences*, vol. 08, no. 12, pp. 483–491, Dec 2015.

[113] R. F. Schaefer, A. Khisti, and H. V. Poor, "Secure Broadcasting Using Independent Secret Keys," *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 644–661, Feb 2018.

[114] H. Schulze and C. Lüders, *Theory and Applications of OFDM and CDMA*. Wiley, Jul 2005.

[115] C. E. Shannon, "Communication Theory of Secrecy Systems*," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

[116] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul 1948.

[117] S. Sharifian and R. Safavi-Naini, "A Modular Semantically Secure Wiretap Code with Shared Key for Weakly Symmetric Channels," in *2019 IEEE Information Theory Workshop (ITW)*. IEEE, Aug 2019, pp. 1–5.

[118] S. Sharifian, F. Lin, and R. Safavi-Naini, "Secret Key Agreement using a Virtual Wiretap Channel," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. IEEE, May 2017, pp. 1–9.

[119] S. Sharifian, R. Safavi-Naini, and F. Lin, "A Virtual Wiretap Channel for Secure Message Transmission," in *International Conference on Cryptology in Malaysia*. Springer, 2017, pp. 171–192.

[120] S. Sharifian, F. Lin, and R. Safavi-Naini, "Hash-then-Encode: A Modular Semantically Secure Wiretap Code," in *Proceedings of the 2nd Workshop on Communication Security (WCS 2017)*. Springer, 2018, pp. 49–63.

[121] S. Sharifian, R. Safavi-Naini, and F. Lin, "Post-Quantum Security using Channel Noise," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: ACM, Oct 2018, pp. 2288–2290.

[122] S. Sharifian, A. Poostindouz, and R. Safavi-Naini, "A One-Round Key Agreement Protocol with Information-Theoretic Security," *ISIT*, 2020, manuscript submitted for review. [Online]. Available: http://arxiv.org/abs/1905.04280

[123] S. Sharifian, R. Safavi-Naini, and F. Lin, "Semantically Secure Keyed Wiretap Encoding Schemes," *Journal of Cryptology*, 2020, manuscript submitted for review.

[124] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct 1997.

[125] V. Shoup, "On Formal Models for Secure Key Exchange," Cryptology ePrint Archive, Report 1999/012, 1999.

[126] V. Shoup, "Using Hash Functions as a Hedge against Chosen Ciphertext Attack," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2000, pp. 275–288.

[127] V. Shoup, "A proposal for an ISO standard for public key encryption (version 2.1)," *IACR e-Print Archive*, vol. 112, 2001.

[128] T. Simonite, "NSA Says It 'Must Act Now' Against the Quantum Computing Threat," Feb 2016. [Online]. Available: https://www.technologyreview.com/s/600715/nsa-says-it-must-act-now-against-the-quantum-computing-threat/

[129] D. Stebila, S. Fluhrer, and S. Gueron, "Design issues for hybrid key exchange in TLS 1.3," Internet-Draft draft-stebila-tls-hybrid-design-01, Internet Engineering Task, Tech. Rep., 2019.

[130] M. Strasser, B. Danev, and S. Čapkun, "Detection of Reactive Jamming in Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 7, no. 2, pp. 1–29, Aug 2010.

[131] I. Tal and A. Vardy, "Channel Upgrading for Semantically-Secure Encryption on Wiretap Channels," in *2013 IEEE International Symposium on Information Theory*, IEEE. IEEE, Jul 2013, pp. 1561–1565.

[132] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference Assisted Secret Communication," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[133] E. Tekin and A. Yener, "Achievable Rates for the General Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy," *arXiv preprint cs/0612084*, Dec 2006. [Online]. Available: http://arxiv.org/abs/cs/0612084

[134] E. Tekin and A. Yener, "The Gaussian Multiple Access Wire-tap Channel: Wireless Secrecy and Cooperative Jamming," in *2007 Information Theory and Applications Workshop*, IEEE. IEEE, Jan 2007, pp. 404–413.

[135] E. Tekin and A. Yener, "The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, Jun 2008.

[136] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC Codes to the Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, Aug 2007.

[137] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, May 2005.

[138] H. Tyagi and A. Vardy, "Explicit Capacity-Achieving Coding Scheme for the Gaussian Wiretap Channel," *2014 IEEE International Symposium on Information Theory*, pp. 956–960, Jun 2014.

[139] H. Tyagi and S. Watanabe, "A Bound for Multiparty Secret Key Agreement and Implications for a Problem of Secure Computing," in *Adv. Cryptol. – EUROCRYPT 2014*, ser. Lecture Notes in Computer Science, P. Q. Nguyen and E. Oswald, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, vol. 8441, pp. 369–386.

[140] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. River Publishers, 2013.

[141] H. Wang, X. Tao, N. Li, and Z. Han, "Polar Coding for the Wiretap Channel With Shared Key," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1351–1360, Jun 2018.

[142] M. N. Wegman and J. Carter, "New Hash Functions and Their Use in Authentication and Set Equality," *Journal of Computer and System Sciences*, vol. 22, no. 3, pp. 265–279, Jun 1981.

[143] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[144] Xiaojun Tang, Ruoheng Liu, P. Spasojevic, and H. V. Poor, "The Gaussian Wiretap Channel with a Helping Interferer," in *2008 IEEE International Symposium on Information Theory*, IEEE. IEEE, Jul 2008, pp. 389–393.

[145] H. Yamamoto, "Rate-distortion Theory for the Shannon Cipher System," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[146] T. Ylonen and C. lo, "The Secure Shell (SSH) Protocol Architecture," pp. 1–30, Jan 2006. [Online]. Available: https://www.rfc-editor.org/info/rfc4251https://www.rfc-editor.org/info/rfc4254

[147] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key Generation From Wireless Channels: A Review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[148] R. Zhang, G. Hanaoka, J. Shikata, and H. Imai, "On the Security of Multiple Encryption or CCA-Security+CCA-Security=CCA-Security?" in *International Workshop on Public Key Cryptography*. Springer, 2004, pp. 360–374.

Appendix A

Contributions to Co-authored Papers

In this appendix, an overview of my contributions to the papers with more than two authors (myself and Dr. Reihaneh Safavi-Naini) is explained.

1. S. Sharifian, F. Lin, and R. Safavi-Naini, "Hash-then-Encode: A Modular Semantically Secure Wiretap Code," in *Proceedings of the 2nd Workshop on Communication Security (WCS 2017)*. Springer, 2018, pp. 49–63

   My main contribution in this paper was proposing the new modular wiretap code. I actively was involved in proving the security of the wiretap code and comparing it with the existing codes. All the authors were equally contributed in writing and submitting the paper.

2. S. Sharifian, R. Safavi-Naini, and F. Lin, "Post-Quantum Security using Channel Noise," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: ACM, Oct 2018, pp. 2288–2290

   My main contribution was to compare the finite length rate of the two wiretap constructions based on the proposed comparison framework by other authors. I was in charge of writing the first draft which was revised by my co-authors and I presented this work in a form of a poster at CCS 2018 conference.

3. S. Sharifian, R. Safavi-Naini, and F. Lin, "A Virtual Wiretap Channel for Secure Message Transmission," in *International Conference on Cryptology in Malaysia*. Springer, 2017, pp. 171–192

   My main contribution in this paper was in estimating the parameters for the virtual wiretap channel. I also contributed in capacity calculation and designing the secure message protocol. I provided the first draft of this paper which was revised and improved by my co-authors so that we could successfully submit it to a conference. I attended the conference for presenting our work.

4. S. Sharifian, F. Lin, and R. Safavi-Naini, "Secret Key Agreement using a Virtual Wiretap Channel," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. IEEE, May 2017, pp. 1–9

   My main contribution in this paper was in the security proof and efficiency analysis of the protocols. Dr. Lin and I worked equally on the first draft of this paper. The draft was revised and improved a lot by Dr. Safavi-Naini to be submitted to INFOCOM conference.

5. S. Sharifian, R. Safavi-Naini, and F. Lin, "Semantically Secure Keyed Wiretap Encoding Schemes," *Journal of Cryptology*, 2020, manuscript submitted for review.

   My contribution in this paper was proposing two new keyed wiretap schemes and proving their security and capacity achieving. The idea of making the construction t-resiliant was initiated by Dr. Safavi-Naini and developed by Dr.Lin for a wiretap construction. I used the same proof technique for showing the t-resiliency. I was in charge of writing this paper which was revised and improved a lot by Dr. Safavi-Naini to be submitted to the Journal of Cryptology.

Appendix B

Appendices of Chapters

B.1 Appendix of Chapter 2

Proof of Lemma 2.4

Proof. According to Lemma 2.3, we only need to show that $\{h_{\mathbf{s}}|\mathbf{s} \in \mathcal{S}\}$ is XOR-Universal, which is easily verified.

- When $r \geq b$, $h_{\mathbf{s}}(\mathbf{x}) \oplus h_{\mathbf{s}}(\mathbf{x}^{'}) = \mathbf{a}$ if and only if there exists an $\mathbf{e} \in \{0,1\}^{r-b}$ satisfying $s \odot (\mathbf{x} \oplus \mathbf{x}^{'}) = (\mathbf{a}||\mathbf{e})$. Since we assume $\mathbf{x} \neq \mathbf{x}^{'}$, $\mathbf{s} = (\mathbf{a}||\mathbf{e}) \odot (\mathbf{x} \oplus \mathbf{x}^{'})^{-1}$ is uniquely determined by the right hand side. The number of s satisfying $h_{\mathbf{s}}(\mathbf{x}) \oplus h_{\mathbf{s}}(\mathbf{x}^{'}) = \mathbf{a}$ is exactly the number of $\mathbf{e} \in \{0,1\}^{r-b}$, which is 2^{r-b}. The total number of seeds $|\mathcal{S}|$ in this case is 2^r. Hence $\Pr[h_{\mathbf{s}}(\mathbf{x}) \oplus h_{\mathbf{s}}(\mathbf{x}^{'}) = \mathbf{a}] \leq \frac{1}{2^b}$ for any $\mathbf{x} \neq \mathbf{x}^{'} \in \mathcal{X}$ and $\mathbf{a} \in \mathcal{Y}$.

- When $r < b$, $h_{\mathbf{s}}(\mathbf{x}) \oplus h_{\mathbf{s}}(\mathbf{x}^{'}) = \mathbf{a}$ if and only if $s \odot (\mathbf{x} \oplus \mathbf{x}^{'}||0^{b-r}) = \mathbf{a}$. Since we assume $\mathbf{x} \neq \mathbf{x}^{'}$, $\mathbf{s} = \mathbf{a} \odot (\mathbf{x} \oplus \mathbf{x}^{'}||0^{b-r})^{-1}$ is uniquely determined by the right hand side. The number of s satisfying $h_{\mathbf{s}}(\mathbf{x}) \oplus h_{\mathbf{s}}(\mathbf{x}^{'}) = \mathbf{a}$ is exactly 1. The total number of seeds $|\mathcal{S}|$ in this case is 2^b. Hence $\Pr[h_{\mathbf{s}}(\mathbf{x}) \oplus h_{\mathbf{s}}(\mathbf{x}^{'}) = \mathbf{a}] \leq \frac{1}{2^b}$ for any $\mathbf{x} \neq \mathbf{x}^{'} \in \mathcal{X}$ and $\mathbf{a} \in \mathcal{Y}$.

□

B.2 Appendix of Chapter 3

Proof of Theorem 3.1

To prove Theorem 3.1, we first prove a lemma.

Lemma B.2.1. *Let $\{h_s|s \in \mathcal{S}\}$ be a family of XOR-Universal hash functions $h_s : \mathcal{X} \to \mathcal{Y} = \{0,1\}^\ell$. Let A and B be two independent random variables over $\mathcal{X}$ and $\mathcal{Y}$, respectively. Let V be a third variable that is independent of B but is possibly dependent on A. Then*

$$\mathbf{SD}((S, V, h_S(A) \oplus B); (S, V, U_\ell)) \leq \sqrt{2^{-(\tilde{H}_\infty(A|V)+H_\infty(B)-\ell-1)}}.$$

Equivalently,

$$\mathbf{SD}((S, V, h_S(A) \oplus B); (S, V, U_\ell)) \leq \varepsilon, \text{ if } \tilde{H}_\infty(A|V) + H_\infty(B) \geq \ell + 2\log(\frac{1}{\varepsilon}) + 1.$$

Proof. Consider a fixed value $V = \mathbf{v}$ and apply Lemma 3.6 in [43] to the two variables, $A|(V = \mathbf{v})$ and B.

$$\mathbf{SD}\left((S, h_S((A|V = \mathbf{v}) \oplus B); (S, U_\ell)\right) \leq \sqrt{2^{-(H_\infty(A|V=\mathbf{v})+H_\infty(B)-\ell-1)}}.$$

Taking expectation over $\mathbf{v}$ on both sides yields

$$\begin{aligned}
\mathbf{SD}\left((S, V, h_S(A) \oplus B); (S, V, U_b)\right) &\leq \mathbb{E}_{\mathbf{v}}\left(\sqrt{2^{-(H_\infty(A|V=\mathbf{v})+H_\infty(B)-\ell-1)}}\right) \\
&\leq \sqrt{\mathbb{E}_{\mathbf{v}}\left(2^{-(H_\infty(A|V=\mathbf{v})+H_\infty(B)-\ell-1)}\right)} \\
&= \sqrt{2^{-(\tilde{H}_\infty(A|V)+H_\infty(B)-\ell-1)}},
\end{aligned}$$

where the second inequality follows from applying Jensen's inequality to the function $f(x) = \sqrt{x}$, and the equality follows directly from the definition of conditional min-entropy $\tilde{H}_\infty(A|V)$. □

Proof of Theorem 3.1. When the main channel is noise-free, $\mathbf{HtE}(K, S, \mathbf{m}) = K \| h_S(K) \oplus \mathbf{m}$, where $\mathbf{m} \in \{0,1\}^b$, $K \in \{0,1\}^k$ is a uniformly distributed random string and $S \in \mathcal{S}$ is a uniformly random seed of an XOR-universal hash family $\{h_s|s \in \mathcal{S}\}$. The distinguishing advantage of the seeded encryption scheme is defined as:

$$Adv^{\mathrm{ds}} = \max_{\mathbf{m}_0, \mathbf{m}_1 \in \mathcal{M}} \left\{\mathbf{SD}\left((S, V_K, V_{S,\mathbf{m}_0}); (S, V_K, V_{S,\mathbf{m}_1})\right)\right\}.$$

Here V_K is the wiretapper's view of the random string K appended to the encrypted message, and $V_{S,\mathbf{m}}$ is the wiretapper's view of $h_S(K) \oplus \mathbf{m}$. When the wiretapper's channel W is BSC_p used for n times, the effect of the channel can be given by a random variable $N \in \{0,1\}^n$ (that is n IID samples of a Bernoulli random variable with $\Pr[X = 1] = p$), added to channel's input. Therefore, $V_K = K \oplus N_K$ and $V_{S,\mathbf{m}} = h_S(K) \oplus \mathbf{m} \oplus N_M$, where N_K and N_M denote two independent variables denoting channel noise added to the two parts of the transmission. The first part of the transmission is V_K, which does not contain any direct information

about the message, but is useful when it is used together with $V_{S,\mathbf{m}}$, which is the message $\mathbf{m}$ masked by a random string $h_S(K) \oplus N_M$. Using Lemma B.2.1, the string $h_s(K) \oplus N_M$, can be seen as the output of an average-case two-source (seeded) extractor, and so have (close to) uniform distribution. Thus, from the viewpoint of the wiretapper the message is protected by an almost uniform pad. This intuition is formalized as follows.

$$
\begin{aligned}
&\mathbf{SD}\left((S, V_K, V_{S,\mathbf{m}_0}); (S, V_K, V_{S,\mathbf{m}_1})\right) \\
&= \mathbf{SD}\left((S, V_K, \mathbf{m}_0 \oplus h_S(K) \oplus N_M); (S, V_K, \mathbf{m}_1 \oplus h_S(K) \oplus N_M)\right) \\
&\leq \mathbf{SD}\left((S, V_K, \mathbf{m}_0 \oplus h_S(K) \oplus N_M); (S, V_K, \mathbf{m}_0 \oplus U_b)\right) \\
&\quad + \mathbf{SD}\left((S, V_K, \mathbf{m}_0 \oplus U_b); (S, V_K, \mathbf{m}_1 \oplus U_b)\right) \\
&\quad + \mathbf{SD}\left((S, V_K, \mathbf{m}_1 \oplus U_b); (S, V_K, \mathbf{m}_1 \oplus h_S(K) \oplus N_M)\right) \\
&= 2\mathbf{SD}\left((S, V_K, h_S(K) \oplus N_M); (S, V_K, U_b)\right),
\end{aligned}
$$

which holds for any pair of messages $\mathbf{m}_0$ and $\mathbf{m}_1$. We then have

$$
Adv^{\mathrm{ds}} \leq 2\mathbf{SD}\left((S, V_K, h_S(K) \oplus N_M); (S, V_K, U_b)\right). \tag{B.1}
$$

Now Lemma B.2.1 yields the following bound.

$$
Adv^{\mathrm{ds}} \leq 2\sqrt{2^{-(\tilde{H}_\infty(K|V_K)+H_\infty(N_M)-b-1)}}, \tag{B.2}
$$

that implies semantic security.

For the code to be capacity-achieving we need to further bound Adv^{ds} in terms of smooth entropy. Let N_M^ε be a random variable that is sampled from a distribution that achieves the ε-smooth min-entropy of the distribution of N_M, that is, $H_\infty(N_M^\varepsilon) \geq b(h_2(p) - \delta_M)$, where $\delta_M = \log 5 \cdot \sqrt{\frac{2\log(\frac{1}{\varepsilon})}{b}}$. Similarly, denote $V_K = K \oplus N_K$ and let N_K^ε be sampled from a distribution achieving the ε-smooth min-entropy of the distribution of N_K, namely, $H_\infty(N_K^\varepsilon) \geq k(h_2(p) - \delta_K)$, where we have $\delta_K = \log 5 \cdot \sqrt{\frac{2\log(\frac{1}{\varepsilon})}{k}}$. Write

$V_K^\varepsilon = K \oplus N_K^\varepsilon$. Now

$$\begin{aligned}
\tfrac{1}{2}Adv^{\mathrm{ds}} &\leq \mathbf{SD}\left((S, V_K, h_S(K) \oplus N_M); (S, V_K, U_b)\right) \\
&\leq \mathbf{SD}\left(S, V_K, h_S(K) \oplus N_M; S, V_K^\varepsilon, h_S(K) \oplus N_M\right) \\
&\quad + \mathbf{SD}\left(S, V_K^\varepsilon, h_S(K) \oplus N_M; S, V_K^\varepsilon, \mathsf{h}_S(K) \oplus {N_M}^\varepsilon\right) \\
&\quad + \mathbf{SD}\left((S, V_K^\varepsilon, h_S(K) \oplus {N_M}^\varepsilon); (S, V_K^\varepsilon, U_b)\right) \\
&\quad + \mathbf{SD}\left((S, V_K^\varepsilon, U_b); (S, V_K, U_b)\right) \\
&\leq \varepsilon + \varepsilon + \mathbf{SD}\left((S, V_K^\varepsilon, h_S(K) \oplus {N_M}^\varepsilon); (S, V_K^\varepsilon, U_b)\right) + \varepsilon \\
&\leq 3\varepsilon + \sqrt{2^{-(\tilde{H}_\infty(K|V_K^\varepsilon) + H_\infty({N_M}^\varepsilon) - b - 1)}},
\end{aligned}$$

where the last inequality follows from Lemma B.2.1. The next step is to bound $\sqrt{2^{-\left(\tilde{H}_\infty(K|V_K^\varepsilon) + H_\infty({N_M}^\varepsilon) - b - 1\right)}}$. From Lemma 2.1, we have $H_\infty({N_M}^\varepsilon) \geq b(h_2(p) - \delta_M)$, where $h_2(p)$ is the binary entropy function given by $h_(p) = -p\log p - (1-p)\log(1-p)$. We have yet to bound $\tilde{H}_\infty(K|V_K^\varepsilon)$:

$$\begin{aligned}
\tilde{H}_\infty(K|V_K^\varepsilon) &= -\log\left(\textstyle\sum_{\mathbf{v}^\varepsilon \in \{0,1\}^k} \Pr[V_K^\varepsilon = \mathbf{v}^\varepsilon] \max_{\mathbf{k} \in \{0,1\}^k} \Pr[K = \mathbf{k} | V_K^\varepsilon = \mathbf{v}^\varepsilon]\right) \\
&= -\log\left(\textstyle\sum_{\mathbf{v}^\varepsilon \in \{0,1\}^k} \max_{\mathbf{k} \in \{0,1\}^k} \Pr[K = \mathbf{k}] \cdot \Pr[V_K^\varepsilon = \mathbf{v}^\varepsilon | K = \mathbf{k}]\right) \\
&= -\log\left(\textstyle\sum_{\mathbf{v}^\varepsilon \in \{0,1\}^k} \frac{1}{2^k} \max_{\mathbf{k} \in \{0,1\}^k} \Pr[\mathbf{k} \oplus N_K^\varepsilon = \mathbf{v}^\varepsilon]\right) \\
&\geq -\log\left(\textstyle\sum_{\mathbf{v}^\varepsilon \in \{0,1\}^k} \frac{1}{2^k} \cdot 2^{-k(h_2(p) - \delta_K)}\right) = k(h_2(p) - \delta_K).
\end{aligned}$$

We then have $Adv^{\mathrm{ds}} \leq 8\varepsilon$ if

$$\sqrt{2^{-(\tilde{H}_\infty(K|V_K^\varepsilon) + H_\infty({N_M}^\varepsilon) - b - 1)}} \leq 2^{-\frac{(k+b)h_2(p) - k\delta_K - b\delta_M - b - 1}{2}} \leq \epsilon.$$

In particular, $Adv^{\mathrm{ds}} \leq \varepsilon$ holds if

$$\frac{(k+b)h_2(p) - \log 5 \cdot \left(\sqrt{2k\log(\frac{8}{\varepsilon})} + \sqrt{2b\log(\frac{8}{\varepsilon})}\right) - b - 1}{2} = \log(\frac{8}{\varepsilon}).$$

Finally (3.1) follows by substituting $\log(\frac{1}{\varepsilon}) = \sigma$.

□

B.3 Appendices of Chapter 4

B.3.1 Achievable Transmission Rate using $\mathrm{BiT}^N_{q,\eta}$

For a noise free main channel, the secrecy capacity of $\mathrm{BiT}^N_{q,\eta}$ is given by:

$$C_s(\mathrm{BiT}^N_{\eta,q}) = -\{\eta \log \eta + (1-\eta) \log \frac{1-\eta}{(2^{Nq}-1)}\}.$$

Figure B.1 shows the rate of communication when, the information block length is Nq bits, $q = 2, 3$ and 4, and $N = 64$. The graphs show the achievable rates for $\sigma = 128$ semantic security, and $\eta = 0.2$ (upper graph) and $\eta = 0.4$ (lower graph). The figures show that the achievable secrecy rate and secrecy capacity decreases as η grows. This is expected because higher η means that the adversary has a better chance of correctly decoding the jammed signal.

B.3.2 BiT over Noisy Receiver's Channel — An Example

In this section we derive a sufficient relation between P_b and η so that the virtual wiretap channel is a stochastically degraded broadcast channel. Following Section 4.3, the transition matrix of the virtual wiretapper's channel W for $q = 2$ is given by:

$$\mathbf{P}_{\mathsf{W}} = \begin{bmatrix} \eta & \frac{1-\eta}{3} & \frac{1-\eta}{3} & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \eta & \frac{1-\eta}{3} & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \frac{1-\eta}{3} & \eta & \frac{1-\eta}{3} \\ \frac{1-\eta}{3} & \frac{1-\eta}{3} & \frac{1-\eta}{3} & \eta \end{bmatrix},$$

where $u = \frac{1-\eta}{3}$, and $v = \eta - \frac{1-\eta}{3} = \frac{4\eta-1}{3}$. Note that the sum of each row is $4u + v = 1$. On the other hand, we can compute:

$$\mathbf{P}^{-1}_{\mathsf{M}} = \frac{1}{(1-2P_b)^2} \cdot \begin{pmatrix} (1-P_b)(1-P_b) & -P_b(1-P_b) & -P_b(1-P_b) & P_b^2 \\ -P_b(1-P_b) & (1-P_b)(1-P_b) & P_b^2 & -P_b(1-P_b) \\ -P_b(1-P_b) & P_b^2 & (1-P_b)(1-P_b) & -P_b(1-P_b) \\ P_b^2 & -P_b(1-P_b) & -P_b(1-P_b) & (1-P_b)(1-P_b) \end{pmatrix}.$$

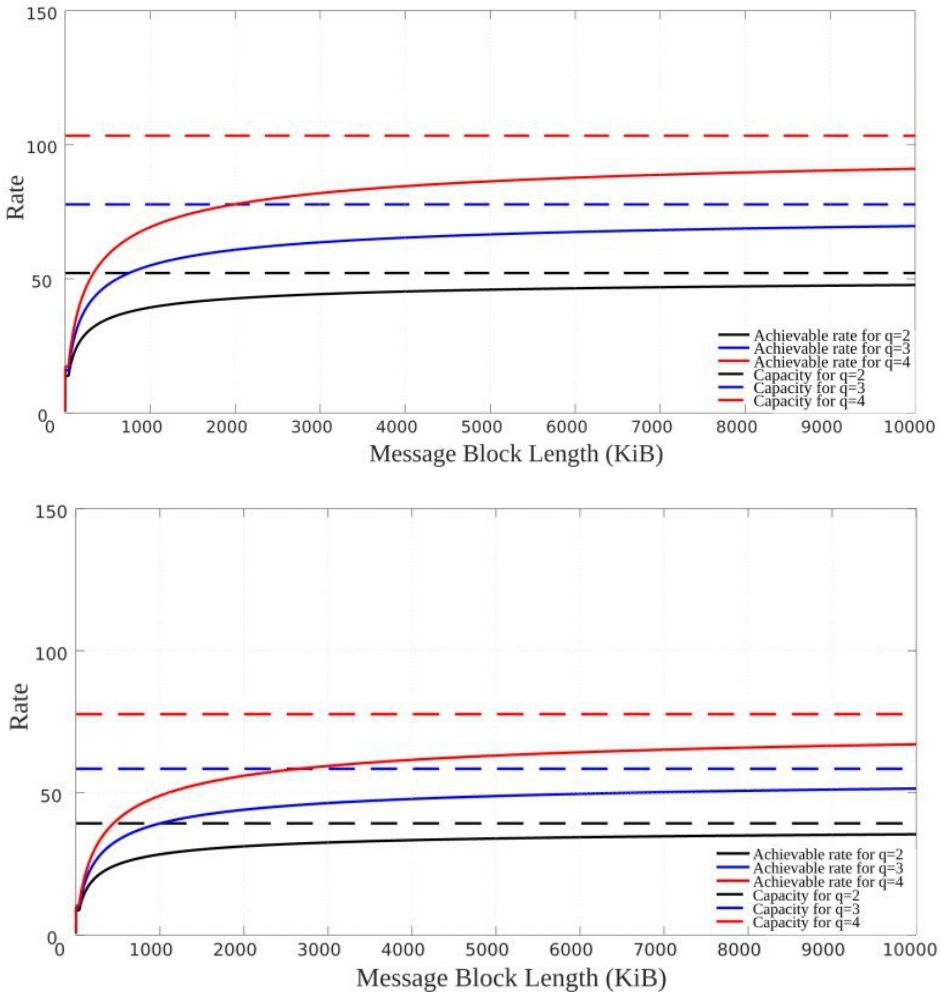

Figure B.1: The secrecy rate and capacity (bits per channel use) of BiT for $N = 64$ and different values of q for $\eta = 0.2$ (upper graph) and $\eta = 0.4$ (lower graph).

Let $a = 1 - P_b$ and $b = P_b$. The above matrix can be written as:

$$\mathbf{P}_{\mathsf{M}}^{-1} = \frac{1}{(a-b)^2} \cdot \begin{pmatrix} a^2 & -ab & -ab & b^2 \\ -ab & a^2 & b^2 & -ab \\ -ab & b^2 & a^2 & -ab \\ b^2 & -ab & -ab & a^2 \end{pmatrix}.$$

The sum of entries of each row is given by, $\frac{1}{(a-b)^2}(a^2 - 2ab + b^2) = 1$. The following is used to prove the required relation.

Lemma B.3.1. *Let there be two matrices*

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}, B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix}.$$

If $\sum_{j=1}^{n} a_{ij} = 1$ *and* $\sum_{j=1}^{n} b_{ij} = 1$ *for any* $i \in [n]$*, then* $\sum_{j=1}^{n} (AB)_{ij} = 1$*, for any* $i \in [n]$*.*

Proof. For any $i \in [n]$,

$$\begin{aligned} \textstyle\sum_{j=1}^{n} (AB)_{ij} &= \textstyle\sum_{j=1}^{n} \left(\sum_{k=1}^{n} a_{ik} b_{kj}\right) \\ &= \textstyle\sum_{k=1}^{n} a_{ik} \cdot \left(\sum_{j=1}^{n} b_{kj}\right) \\ &= \textstyle\sum_{k=1}^{n} a_{ik} \\ &= 1. \end{aligned}$$

□

Lemma B.3.2. *The virtual wiretap channel is a stochastically degraded broadcast channel if* $P_b \leq \frac{1-\sqrt{\frac{4\eta-1}{3}}}{2}$ *and* $\eta > \frac{1}{4}$*.*

Proof. The virtual wiretap channel is a stochastically degraded broadcast channel if there exists a matrix $\mathbf{R}$ such that $\mathbf{P}_{\mathsf{W}} = \mathbf{P}_{\mathsf{M}} \times \mathbf{R}$, and $\mathbf{R}$ is a channel transition matrix; that is, has non-negative entries and each

row sums to 1. Using the matrices $\mathbf{P}_{\mathsf{M}}$ and $\mathbf{P}_{\mathsf{W}}$ above, we have:

$$\begin{aligned}\mathbf{R} &= \mathbf{P}_{\mathsf{W}} \times \mathbf{P}_{\mathsf{M}}^{-1} \\ &= \tfrac{1}{(a-b)^2} \begin{bmatrix} u(a-b)^2+va^2 & u(a-b)^2-vab & u(a-b)^2-vab & u(a-b)^2+vb^2 \\ u(a-b)^2-vab & u(a-b)^2+va^2 & u(a-b)^2+vb^2 & u(a-b)^2-vab \\ u(a-b)^2-vab & u(a-b)^2+vb^2 & u(a-b)^2+va^2 & u(a-b)^2-vab \\ u(a-b)^2+vb^2 & u(a-b)^2-vab & u(a-b)^2-vab & u(a-b)^2+va^2 \end{bmatrix}.\end{aligned}$$

Using Lemma B.3.1, entries in each row of $\mathbf{R}$ sum to 1.

To ensure entries of $\mathbf{R}$ are all non-negative, we first note that $u(a-b)^2+va^2 > 0$ and $u(a-b)^2+vb^2 > 0$. So the virtual wiretap channel is a stochastically degraded broadcast channel if $u(a-b)^2 - vab \geq 0$ and so:

$$\begin{aligned} u(a-b)^2 - vab \geq 0 &\Leftrightarrow ua^2+ub^2-(2u+v)ab \geq 0 \\ &\Leftrightarrow ua^2+ub^2-(2u+1-4u)ab \geq 0 \\ &\Leftrightarrow ua^2+ub^2-(1-2u)ab \geq 0 \\ &\Leftrightarrow u(a+b)^2-ab \geq 0 \\ &\Leftrightarrow u-ab \geq 0 \\ &\Leftrightarrow P_b^2-P_b+u \geq 0, \end{aligned}$$

where $4u+v=1$ and $a+b=1$ are repeatedly invoked to simplify the expressions. The solution to the above inequality depends on the determinant $1-4u$. When $1-4u>0$, we have

$$\begin{aligned} P_b^2-P_b+u \geq 0 &\Leftrightarrow \left(P_b-\tfrac{1-\sqrt{1-4u}}{2}\right)\left(P_b-\tfrac{1+\sqrt{1-4u}}{2}\right) \geq 0 \\ &\Leftrightarrow \left(P_b-\tfrac{1-\sqrt{v}}{2}\right)\left(P_b-\tfrac{1+\sqrt{v}}{2}\right) \geq 0 \\ &\Leftrightarrow \left(P_b-\tfrac{1-\sqrt{\frac{4\eta-1}{3}}}{2}\right)\left(P_b-\tfrac{1+\sqrt{\frac{4\eta-1}{3}}}{2}\right) \geq 0 \\ &\Leftrightarrow P_b \leq \tfrac{1-\sqrt{\frac{4\eta-1}{3}}}{2} \text{ or } P_b \geq \tfrac{1+\sqrt{\frac{4\eta-1}{3}}}{2}. \end{aligned}$$

By assumption, $P_b \in [0, \frac{1}{2}]$ and so $P_b \leq \frac{1-\sqrt{\frac{4\eta-1}{3}}}{2} = \frac{1}{2} - \sqrt{\frac{4\eta-1}{12}}$. □

Example B.1. *Let $P_b = 0.1$ and Let $\eta = 0.55$. Therefore,*

$$\mathbf{P}_{\mathsf{M}} = \begin{bmatrix} 0.81 & 0.09 & 0.09 & 0.01 \\ 0.09 & 0.81 & 0.01 & 0.09 \\ 0.09 & 0.01 & 0.81 & 0.09 \\ 0.01 & 0.09 & 0.09 & 0.81 \end{bmatrix}$$

and

$$\mathbf{P}_{\mathsf{W}} = \begin{bmatrix} 0.55 & 0.15 & 0.15 & 0.15 \\ 0.15 & 0.55 & 0.15 & 0.15 \\ 0.15 & 0.15 & 0.55 & 0.15 \\ 0.15 & 0.15 & 0.15 & 0.55 \end{bmatrix}.$$

Therefore

$$\mathbf{R} = \mathbf{P}_{\mathsf{W}} \times \mathbf{P}_{\mathsf{M}}^{-1} = \begin{bmatrix} 0.66 & 0.094 & 0.094 & 0.156 \\ 0.094 & 0.66 & 0.156 & 0.094 \\ 0.094 & 0.156 & 0.66 & 0.094 \\ 0.156 & 0.094 & 0.094 & 0.66 \end{bmatrix}.$$

$\mathbf{R}$ *is the transition probability matrix of a virtual channel that confirms* $\mathbf{P}_{\mathsf{W}}$ *is degraded with respect to* $\mathbf{P}_{\mathsf{M}}$. *The secrecy capacity in this example is*

$$C_s = C_{\mathsf{M}} - C_{\mathsf{W}} = (2 - 0.7624) - (2 - 1.1515) = 0.3891.$$

B.4 Appendices of Chapter 6

B.4.1 KXtX: The Second Keyed Wiretap Construction

The **KXtX** construction is the keyed version of the **XtX** construction proposed in [12]. The choice of parameters in [12] for the **XtX** construction are such that the construction does not achieve the secrecy capacity of a BSC. We show with the appropriate choice of parameters (according to Theorem B.4.2), the **KXtX** construction achieves the secrecy capacity of a keyed wiretap channel with shared key for a weakly symmetric splittable wiretap channel (weakly symmetric splittable main and wiretapper's channels). As a special case of the **KXtX** construction with key rate equal to zero, our proof also shows the **XtX** construction achieves the secrecy capacity of weakly symmetric splittable wiretap channels.

Splittable channels are defined in [12]. A channel $\mathsf{CH} : \{0,1\}^{\ell_1+\ell_2} \to \mathcal{Y}_1 \times \mathcal{Y}_2$ is (ℓ_1, ℓ_2)-splittable if there are channels $\mathsf{CH}_1 : \{0,1\}^{\ell_1} \to \mathcal{Y}_1$ and $\mathsf{CH}_2 : \{0,1\}^{\ell_2} \to \mathcal{Y}_2$ such that for all $x_1 \in \{0,1\}^{\ell_1}$ and $x_2 \in \{0,1\}^{\ell_2}$ we have $\mathsf{CH}(x_1 \| x_2) = \mathsf{CH}_1(x_1) \| \mathsf{CH}_2(x_2)$. In these channels the application of the channel on an input of length $\ell_1 + \ell_2$ can be written as independent applications of two channels with input length ℓ_1 and ℓ_2 respectively. In this case, for the ease of representation we write $\mathsf{CH} = \mathsf{CH}_1 \| \mathsf{CH}_2$. BSC channels for inputs of length ℓ are (ℓ_1, ℓ_2)-splittable for all non-negative integers ℓ_1 and ℓ_2 with $\ell_1 + \ell_2 = \ell$ (this is because the application of channel on each input bit is independent from other inputs).

Suppose CH is a (ℓ_1, ℓ_2)-splittable channels, where $\mathsf{CH} = \mathsf{CH}_1 \| \mathsf{CH}_2$ and $\mathsf{CH}_1 : \{0,1\}^{\ell_1} \to \mathcal{Y}_1$ and $\mathsf{CH}_2 : \{0,1\}^{\ell_1} \to \mathcal{Y}_2$. Then there always exist families of codes with encoders $\mathsf{Enc}_1 : \mathcal{M}_1^{(n)} \to \{0,1\}^{n.\ell_1}$ and $\mathsf{Enc}_2 : \mathcal{M}_2^{(n)} \to \{0,1\}^{n.\ell_2}$ and achievable rates $R_1 \leq \mathrm{C}_{\mathsf{CH}_1}$ and $R_2 \leq \mathrm{C}_{\mathsf{CH}_2}$ respectively that achieve the capacity of CH when used together for encoding over CH[1].

The only assumption made about the wiretap channel for the **KXtX** construction is that it is (ℓ_1, ℓ_2)-splittable (in the sense of [12]). A (ℓ_1, ℓ_2)-splittable wiretap channel is denoted as $\mathsf{WT} : \{0,1\}^{\ell_1+\ell_2} \to \{0,1\}^{t_1+t_2} \times \{0,1\}^{w_1+w_2}$ (both receiver $\mathsf{T} : \{0,1\}^{\ell_1+\ell_2} \to \{0,1\}^{t_1+t_2}$ and adversary channels $\mathsf{W} : \{0,1\}^{\ell_1+\ell_2} \to \{0,1\}^{w_1+w_2}$). For a message space $\mathcal{M} = \{0,1\}^b$, an (ℓ_1, ℓ_2)-splittable wiretap channel, and a shared key K of d_2 bits, let $\{\mathsf{h}_s | s \in \mathcal{S}\}$ be a family of pair-wise Universal hash functions where $\mathsf{h}_s : \{0,1\}^{d_1+d_2} \times \to \{0,1\}^b$ for uniformly random seed s. Let $\mathsf{ECC}_1 : \{0,1\}^{d_1} \to \{0,1\}^{\ell_1}$ and $\mathsf{ECC}_2 : \{0,1\}^b \to \{0,1\}^{\ell_2}$ be appropriate error correcting codes for satisfying reliability for the legitimate receiver channel. For unifirmly selected public seed S, the $\mathbf{KXtX}[\mathsf{h}_S, \mathsf{ECC}_1, \mathsf{ECC}_2]$ construction consists of an encoding and decoding functions as follows

1. Encryption:

$$\mathbf{KXtX}.\mathbf{enc}[\mathsf{h}_S, \mathsf{ECC}_1, \mathsf{ECC}_2](K, m) = \mathsf{ECC}_1(D) \| \mathsf{ECC}_2\big(m \oplus \mathsf{h}_S(D \| K)\big),$$

   where $D \xleftarrow{\$} \{0,1\}^{d_1}$.

2. Decryption: The received block Y is parsed to obtain (Y_1, Y_2).

$$\mathbf{KXtX}.\mathbf{dec}(K, Y) = \mathsf{ECC}_2.\mathsf{dec}(Y_2) \oplus \big(\mathsf{h}_S(\mathsf{ECC}_1.\mathsf{dec}(Y_1) \| K)\big).$$

- *Reliability:* Suppose the receiver channel splits as $\mathsf{T} : \mathsf{T}_1 \| \mathsf{T}_2$. If ECC_1 is a good ECC for T_1 and ECC_2 is a good ECC for T_2 then $\mathbf{KXtX}[\mathsf{h}_S, \mathsf{ECC}_1, \mathsf{ECC}_2]$ is decryptable. This is given in Theorem B.4.1.

- *Security:* In the **KXtX** construction, the adversary channel splits as $\mathsf{W} : \mathsf{W}_1 \| \mathsf{W}_2$. The randomness D is first *encoded* over W_1 (this is for collecting randomness from W_1), and then concatenated with the key and *hashed* to encrypt the message which will be encoded over W_2. This part collects randomness from the channel proportional to its length. The construction combines the key randomness with the collected randomness from W_1 and W_2 to hides the message. Lemma B.4.1 captures how much randomness is collected by sending random D over W_1. Distinguishing security of $\mathbf{KXtX}[\mathsf{h}_S, \mathsf{ECC}_1, \mathsf{ECC}_2]$ is proved in Theorem B.4.2 using lemma B.4.2 that is the average-case version of Lemma 5.1 and

[1]The achievable rate of such a combined code is $R_1 + R_2$. On the other hand, by the application of chain rule for mutual information in the definition of capacity, one can show the capacity of such a channel is upper bounded by $\mathrm{C}_{\mathsf{CH}} = \mathrm{C}_{\mathsf{CH}_1} + \mathrm{C}_{\mathsf{CH}_2}$. Therefore, it is always possible to find $R_1 \leq \mathrm{C}_{\mathsf{CH}_1}$ and $R_2 \leq \mathrm{C}_{\mathsf{CH}_2}$ such that $R_1 + R_2 = \mathrm{C}_{\mathsf{CH}}$.

enables conditioning on view of the adversary from the encoded block over W_1. The two sources of randomness in this construction are channel randomness from W_1 concatenated with the random key, (which means this source is itself concatenation of two randomness sources) and W_2 randomness.

- *Capacity Achieving:* We show that the **KXtX** construction achieves the capacity of the keyed wiretap channel with weakly symmetric channels when error correcting codes are from families that achieve the capacity of the main channel T and the length of random string D is sufficient (with respect to Theorems B.4.3.

In the following we describe the choice of parameters in the proposed encoding system to meet the desired reliability and security requirements. We then find the achievable rate of the encryption system and show it achieves the secrecy capacity of weakly symmetric splittable wiretap channels.

Decryptability of KXtX

Consider a receiver channel T of the form $\mathsf{T} = \mathsf{T}_1 \| \mathsf{T}_2$ where $\mathsf{T}_1 : \{0,1\}^{\ell_1} \to \{0,1\}^{t_1}$ with Shannon capacity $\mathrm{C}_{\mathsf{T}_1}$, and $\mathsf{T}_2 : \{0,1\}^{\ell_2} \to \{0,1\}^{t_2}$ with Shannon capacity of $\mathrm{C}_{\mathsf{T}_2}$. Let $\mathsf{ECC}_1^{(n)} : \{0,1\}^{d_1(n)} \to \{0,1\}^{n.\ell_1}$ be a family of error correcting codes indexed by n for channel T_1, with decryption function $\mathsf{ECC_1.dec}^{(n)}$ and decryption error $\sigma_1(n)$ and $\mathsf{ECC}_2^{(n)} : \{0,1\}^{b(n)} \to \{0,1\}^{n.\ell_2}$ be a family of error correcting codes indexed by n for channel T_2, with decryption function $\mathsf{ECC_2.dec}^{(n)}$ and decryption error $\sigma_2(n)$.

The decryption algorithm parses the received ciphertext into its first $n.t_1$ bits Y_1, and its last $n.t_2$ bits Y_2. The decoder of $\mathsf{ECC}_1^{(n)}$ decodes D from Y_1, and the decoder of $\mathsf{ECC}_2^{(n)}$ decodes $m \oplus \mathsf{h}_S(D\|K)$ from Y_2. Finally, message m is obtained from the XOR of the two parts. Note that K is the shared key and known by the receiver.

Theorem B.4.1 (Reliability of **KXtX**). *Let* $\mathsf{KSEnc}_S^{(n)} = \mathbf{KXtX.enc}[\mathsf{h}_s, \mathsf{ECC}_1^{(n)}, \mathsf{ECC}_2^{(n)}]$ *be a keyed seeded encryption function, where* $\mathsf{ECC}_1^{(n)}$ *and* $\mathsf{ECC}_2^{(n)}$ *are described above. Then the decryption function for* KSEnc *is* $\mathsf{KSDec}_S = \mathbf{KXtX.dec}[\mathsf{h}_s, \mathsf{ECC}_1^{(n)}, \mathsf{ECC}_2^{(n)}]$ *with decryption error at most* $\sigma_1(n)+\sigma_2(n)$ *and* $\lim_{n\to\infty} \sigma_1(n)+\sigma_2(n) = 0$

Proof. Using the union bound, the decryption error is bounded by bounded by $(\sigma_1(n) + \sigma_2(n))$, where $\lim_{n\to\infty} \sigma_1(n) = \lim_{n\to\infty} \sigma_2(n) = 0$ for (reliability) capacity-achieving codes $\mathsf{ECC}_1^{(n)}$ and $\mathsf{ECC}_2^{(n)}$. □

Distinguishing security of KXtX

Consider a message space $\mathcal{M} = \{0,1\}^{b(n)}$, a shared secret key of rate $0 \le R_K \le 1$ and a wiretap channel with an (ℓ_1, ℓ_2)-splittable main channel $\mathsf{T} = \mathsf{T}_1 \| \mathsf{T}_2$ and wiretapper's channel $\mathsf{W} = \mathsf{W}_1 \| \mathsf{W}_2$, such that

$\mathsf{T}_1 : \{0,1\}^{\ell_1} \to \{0,1\}^{t_1}$, $\mathsf{T}_2 : \{0,1\}^{\ell_2} \to \{0,1\}^{t_2}$, $\mathsf{W}_1 : \{0,1\}^{\ell_1} \to \{0,1\}^{w_1}$ and $\mathsf{W}_2 : \{0,1\}^{\ell_2} \to \{0,1\}^{w_2}$, where $H_\infty(\mathsf{W}_1) \geq \nu_1$ and $H_\infty(\mathsf{W}_2) \geq \nu_2$. Let $\{\mathsf{h}_s | s \in \mathcal{S}\}$ for a uniformly random S, be a family of pair-wise universal functions $\mathsf{h}_s : \{0,1\}^{d_1(n)+n.R_K} \to \{0,1\}^{b(n)}$, and $\mathsf{ECC}_1 : \{0,1\}^{d_1(n)} \to \{0,1\}^{n.\ell_1}$ and $\mathsf{ECC}_2 : \{0,1\}^{b(n)} \to \{0,1\}^{n.\ell_2}$ be error correcting codes for T_1 and T_2 respectively. The following theorem shows the security of the **KXtX**.

Theorem B.4.2. *[**Security of KXtX**] For the described setting above, the keyed encryption scheme* $\mathsf{KSEnc} = \mathbf{KXtX}[\mathsf{h}_S, \mathsf{ECC}_1, \mathsf{ECC}_2]$*, provides* $\epsilon(n)$*-distinguishing security, i.e.,*$Adv^{ds}(\mathsf{KSEnc}; \mathsf{W}^n) \leq 2\epsilon(n)$ *when parameters satisfy*

$$n.R_K + d_1(n) + n.\nu_1 + n.\nu_2 \geq n.w_1 + n.w_2 + 2log(\frac{1}{\epsilon(n)}).$$

To prove Theorem B.4.2, we need to prove two lemmas. In Lemma B.4.1 we find a lowerbound on the average conditional min-entropy of a uniformly distributed random variable X given $\mathsf{CH}\big(\mathsf{F}(X)\big)$, where $\mathsf{CH}(\cdot)$ is the probabilistic map of the channel, and $\mathsf{F}(\cdot)$ is an arbitrary injective function. In the proposed construction, $\mathsf{F}(\cdot)$ will be realized by an error correcting code and X will be realized by a uniformly random variable that is transmitted over the channel to collect randomness from it for hiding the message. The intuition is that sending a string over the channel results in a noisy version of the string that has some min-entropy related to the channel's randomness (i.e., channel's min-entropy). This min-entropy however is partially leaked. The remaining min-entropy can be extracted and used in hiding the message. Lemma B.4.1 gives a lower-bound on the amount of this remaining min-entropy.

In Lemma B.4.2, we prove the average case version of Lemma 5.1 for a null randomness and, bound the statistical distance of $\mathsf{CH}\big(\mathsf{F}(X)\big)$ with uniform distribution conditioned on a third random variable V dependant on X. In the proposed construction, V is realized by the view of the wiretapper from the transmitted dummy message.

Lemma B.4.1. *Let* $\mathsf{F} : \{0,1\}^d \to \{0,1\}^\ell$ *be an injective function for* $d < \ell$ *and* $X \in \{0,1\}^d$ *be an independent uniformly distributed random variable. For a channel* $\mathsf{CH} : \{0,1\}^\ell \to \{0,1\}^w$ *with* $H_\infty(\mathsf{CH}) \geq \nu$*, let* $Z = \mathsf{CH}(\mathsf{F}(X))$*, then the* average conditional min-entropy *of* $X|Z$ *is bounded as*

$$\tilde{H}_\infty(X|Z) \geq d + \nu - w.$$

Proof. We start with the definition of average conditional min-entropy of $X|Z$.

$$\tilde{H}_\infty(X|Z) = -\log \mathbb{E}_z \max_x \Pr[X = x|Z = z] \tag{B.3}$$

$$= -\log \mathbb{E}_z \max_x \frac{\Pr[X = x] \cdot \mathbf{CH}(\mathsf{F}(x), z)}{\Pr[Z = z]} \tag{B.4}$$

$$= -\log \mathbb{E}_z \max_x \frac{\Pr[X = x] \cdot \mathbf{CH}(\mathsf{F}(x), z)}{\mathbf{CH}(\mathsf{F}(X), z)} \tag{B.5}$$

$$= -\log \mathbb{E}_z \max_x \frac{\Pr[X = x] \cdot \mathbf{CH}(\mathsf{F}(x), z)}{\sum\limits_{x \in \{0,1\}^d} \Pr[X = x].\mathbf{CH}(\mathsf{F}(x), z)} \tag{B.6}$$

$$\geq -\log 2^{-\nu} \mathbb{E}_z \frac{1}{\sum\limits_{x \in \{0,1\}^d} \mathbf{CH}(\mathsf{F}(x), z)} \tag{B.7}$$

$$= -\log 2^{-\nu} \sum_{z \in \{0,1\}^w} \frac{\Pr[Z = z]}{\sum\limits_{x \in \{0,1\}^d} \mathbf{CH}(\mathsf{F}(x), z)} \tag{B.8}$$

$$= -\log 2^{-\nu} \sum_{z \in \{0,1\}^w} \frac{\mathbf{CH}(\mathsf{F}(X), z)}{\sum\limits_{x \in \{0,1\}^d} \mathbf{CH}(\mathsf{F}(x), z)} \tag{B.9}$$

$$= -\log 2^{-\nu} \sum_{z \in \{0,1\}^w} \frac{\sum\limits_{x \in \{0,1\}^d} \Pr[X = x] \cdot \mathbf{CH}(\mathsf{F}(x), z)}{\sum\limits_{x \in \{0,1\}^d} \mathbf{CH}(\mathsf{F}(x), z)} \tag{B.10}$$

$$= -\log 2^{-\nu-d} \sum_{z \in \{0,1\}^w} 1 \tag{B.11}$$

$$= -\log 2^{-\nu-d+w} = \nu + d - w \tag{B.12}$$

where (B.4) follows from (B.3) using the Bayes rule. Subsequently (B.5) is obtained from (B.4) by substituting $\Pr[Z = z]$ with $\mathbf{CH}(\mathsf{F}(X), z)$. Next in (B.6), $\mathbf{CH}(\mathsf{F}(X), z)$ in the denominator is expanded to $\sum\limits_{x \in \{0,1\}^d} \Pr[X = x] \cdot \mathbf{CH}(\mathsf{F}(x), z)$. Since X is uniformly distributed, $\Pr[X = x] = 2^{-d}$ which cancels from the denominator and nominator and since $\max\limits_{y,z} \mathbf{CH}(y, z) \leq 2^{-\nu}$, we have (B.7). The average probability over Z is calculated in (B.8). Then $\Pr[Z = z]$ is replaced by $\mathbf{CH}(\mathsf{F}(X), z)$ in (B.9) and then expanded to $\sum\limits_{x \in \{0,1\}^d} \Pr[X = x] \cdot \mathbf{CH}(\mathsf{F}(x), z)$ in (B.10). Finally, we get (B.12) by using $\Pr[X = x] = 2^{-d}$ and $\sum\limits_{z \in \{0,1\}^w} 1 = 2^w$. □

Lemma B.4.2. *Let $\{\mathsf{h}_s | s \in \mathcal{S}\}$ be a family of pair-wise Universal hash functions $\mathsf{h}_S : \{0,1\}^d \to \{0,1\}^b$ for uniform S and $\mathsf{F} : \{0,1\}^b \to \{0,1\}^\ell$ be an injective function ($\ell \geq b$). For channel $\mathsf{CH} : \{0,1\}^\ell \to \{0,1\}^w$, where $H_\infty(\mathsf{CH}) \geq \nu$, a random variable, $X \in \{0,1\}^d$, and a random variable $V \in \{0,1\}^*$ possibly dependent*

on X and not dependent on the channel, suppose $\tilde{H}_\infty(X|V) + \nu \geq w + 2\log(\frac{1}{\epsilon})$ and $b \geq \tilde{H}_\infty(X|V)$. Then

$$\mathbf{SD}\Big(\Big(S, V, \mathsf{CH}\big(\mathsf{F}\big(\mathsf{h}_S(X)\big)\big)\Big); \Big(S, V, U_w\Big)\Big) \leq \epsilon. \tag{B.13}$$

Proof. From Lemma 5.1, by letting $D = null$ and $d_1 = 0$, for $H_\infty(X) + \nu \geq w + 2\log(\frac{1}{\epsilon})$ and $b \geq H_\infty(X)$, we have

$$\mathbf{SD}\Big(\Big(S, \mathsf{CH}\big(\mathsf{F}\big(\mathsf{h}_S(X)\big)\big); \Big(S, U_w\Big)\Big) \leq \epsilon, \tag{B.14}$$

To prove (B.13), consider an arbitrary value $V = v$ and apply the above result for random variable $X|(V = v)$ instead of X, we have

$$\mathbf{SD}\Big(\Big(S, \mathsf{F}\big(\mathsf{h}_S(X|V = v)\big)\Big); \Big(S, U_w\Big)\Big) \leq \sqrt{2^{-H_\infty(X|V=v)-\nu+w}}.$$

Taking expectation over v on both sides yields

$$\begin{aligned}
\mathbf{SD}\Big(\Big(S, \mathsf{F}\big(\mathsf{h}_S(X|V = v)\big)\Big); \Big(S, U_w\Big)\Big) &\leq \mathbb{E}_v\left(\sqrt{2^{-H_\infty(X|V=v)-\nu+w}}\right) \\
&\leq \sqrt{\mathbb{E}_{\mathbf{v}}\left(2^{-H_\infty(X|V=v)-\nu+w}\right)} \\
&= \sqrt{2^{-H_\infty(X|V=v)-\nu+w}} \\
&\leq \epsilon
\end{aligned}$$

where the second inequality follows from applying Jensen's inequality to the function $f(x) = \sqrt{x}$, and the equality follows directly from the definition of conditional min-entropy $\tilde{H}_\infty(X|V)$.

□

We use Lemma B.4.1 and Lemma B.4.2 to give a direct security proof for the **KXtX** construction in the wiretap setting.

Proof of Theorem B.4.2. Let

$$\Delta(m_0, m_1) = \mathbf{SD}\Big(\Big(S, \mathsf{W}^n\big(\mathsf{KSEnc}_S(m_0, k)\big)\Big); \Big(S, \mathsf{W}\big(\mathsf{KSEnc}_S(m_1, k)\big)\Big)\Big),$$

and

$$\Gamma(m) = \mathbf{SD}\Big(\Big(S, \mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big), \mathsf{W}_2^n\big(\mathbf{KXtX}(K, m)\big)\Big); \Big(S, \mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big), U_{w_2}^n\Big)\Big).$$

Then

$$Adv^{ds}(\mathsf{KSEnc}; \mathsf{W}^n) = \max_{m_0, m_1} \Delta(m_0, m_1),$$

and

$$\begin{aligned}\Delta(m_0,m_1) &= \mathbf{SD}\Big(\Big(S,\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big),\mathsf{W}_2^n\big(\mathbf{KXtX}(m_0,k)\big)\Big);\\ &\qquad\qquad\Big(S,\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big),\mathsf{W}_2^n\big(\mathbf{KXtX}(m_1,k)\big)\Big)\Big)\\ &\le \mathbf{SD}\Big(\Big(S,\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big),\mathsf{W}_2^n\big(\mathbf{KXtX}(m_0,k)\big)\Big);\Big(S,\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big),U_{w_2}^n\Big)\Big)\\ &+ \mathbf{SD}\Big(\Big(S,\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big),U_{w_2}^n\Big);\Big(S,\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big),\mathsf{W}_2^n\big(\mathbf{KXtX}(m_1,k)\big)\Big)\Big)\\ &= 2\Gamma(m).\end{aligned}$$

Now we bound $\Gamma(m)$. In the described setting, the eavesdropper receives $\mathsf{W}_1^n(\mathsf{ECC}_1(D))$ through its channel. From Lemma B.4.1

$$\tilde{H}_\infty\big(D|\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big)\big) \ge d_1(n) + n.\nu_1 - n.w_1.$$

The independent random key K of rate R_K is concatenated to D, and so

$$\tilde{H}_\infty\big((D\|K)|\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big)\big) \ge n.R_K + d_1(n) + n.\nu_1 - n.w_1.$$

Now since $d_1(n)$ satisfies

$$n.R_K + d_1(n) + n.\nu_1 + n.\nu_2 \ge n.w_1 + n.w_2 + 2log(\frac{1}{\epsilon(n)}) + 2 \tag{B.15}$$

$$\Rightarrow \tilde{H}_\infty\big((D\|K)|\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big)\big) + n.\nu_2 \ge n.w_2 + 2log(\frac{1}{\epsilon(n)}) + 2. \tag{B.16}$$

From Lemma B.4.2 for any message m

$$\mathbf{SD}\Big(\Big(S,\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big),\mathsf{W}_2^n\big(\mathbf{KXtX}(K,m)\big)\Big);\Big(S,\mathsf{W}_1^n\big(\mathsf{ECC}_1(D)\big),U_{w_2}^n\Big)\Big) < \epsilon(n)/2.$$

Therefore, for any m_0 and m_1,

$$\Delta(m_0,m_1) \le 2\Gamma(m) \le \epsilon(n).$$

□

Achieving secrecy capacity using KXtX

In the following we show **KXtX** construction is capacity-achieving for keyed wiretap channels with weakly symmetric main and wiretapper's channels.

Theorem B.4.3. *In the described (ℓ_1, ℓ_2)-splittable wiretap channel* WT *with the shared secret key of rate* $0 \leq R_K \leq 1$*, suppose an injective* $\mathsf{ECC}_1^{(n)} : \{0,1\}^{d_1(n)} \to \{0,1\}^{n.\ell_1}$ *and* $\mathsf{ECC}_2^{(n)} : \{0,1\}^{d_2(n)} \to \{0,1\}^{n.\ell_2}$ *in the* **KXtX** *construction achieve rates R_1 and R_2 respectively such that $R_1 + R_2 = C_{\mathsf{T}}$. For degraded weakly symmetric* T *and* W*, the secrecy capacity of the keyed wiretap setting is achievable by* $\mathsf{KSEnc} = \mathbf{KXtX}^*[\mathsf{h}_S, \mathsf{ECC}_1, \mathsf{ECC}_2]$

Proof of Theorem B.4.3. From the definition of weakly symmetric channels (see Section 6.2), it is easy to see that when $\mathsf{W} = \mathsf{W}_1 \| \mathsf{W}_2$ is a weakly symmetric channel, then each of W_1 and W_2 is a weakly symmetric (suppose one of W_1 or W_2 is not weakly symmetric, then W cannot be symmetric). Suppose the distribution of W_1^n for a reference vector $y_r^n \in \{0,1\}^{n.\ell_1}$ is V^n, and the distribution of W_2^n for a reference vector $\hat{y}_r^n \in \{0,1\}^{n.\ell_2}$ is $\hat{V}^n$. Since W_1 and W_2 are weakly symmetric, then W_1^n and W_2^n are weakly symmetric. Then the output of the two channels for any input $y^n \neq y_r^n$ $\hat{y}^n \neq \hat{y}_r^n$ is a permutation of V^n and $\hat{V}^n$, say $\tau_{y^n}(V^n)$ and $\tau_{\hat{y}^n}(\hat{V}^n)$, respectively. Since the channels are DMCs, V^n, and $\hat{V}^n$ are vectors of n independent random variables. Moreover, $H(V^n) = n \cdot H(V)$ and $H(\hat{V}^n) = n \cdot H(\hat{V})$. Suppose $V_{\epsilon_1(n)}$ is the random variable that achieves the ϵ_1-smooth min-entropy of V^n and $\hat{V}_{\epsilon_2(n)}$ is the random variable that achieves the ϵ_2-smooth min-entropy of $\hat{V}^n$ i.e.,

$$H_\infty^{\epsilon_1(n)}(V^n) = \max_{V_{\epsilon_1(n)}:\mathbf{SD}(V^n, V_{\epsilon_1(n)}) \leq \epsilon_1(n)} H_\infty(V_{\epsilon_1(n)}),$$

and

$$H_\infty^{\epsilon_2(n)}(\hat{V}^n) = \max_{\hat{V}_{\epsilon_2(n)}:\mathbf{SD}(\hat{V}^n, \hat{V}_{\epsilon(n)}) \leq \epsilon_2(n)} H_\infty(\hat{V}_{\epsilon_2(n)}).$$

From Lemma 6.1 we have

$$H_\infty(V_{\epsilon_1(n)}) = H_\infty^{\epsilon_1(n)}(V^n) \geq n.H(V) - n\delta_1(n), \tag{B.17}$$

where $\delta_1(n) = \log(2^{\ell_1} + 3).\sqrt{2log\frac{1}{\epsilon_1(n)}/n}$ and

$$H_\infty(\hat{V}_{\epsilon_2(n)}) = H_\infty^{\epsilon_2(n)}(\hat{V}^n) \geq n.H(\hat{V}) - n\delta_2(n), \tag{B.18}$$

where $\delta_2(n) = \log(2^{\ell_2} + 3).\sqrt{2log\frac{1}{\epsilon_2(n)}/n}$.

Now consider a virtual channels $\mathsf{W}_{\epsilon_1(n)} : \{0,1\}^{n.\ell_1} \to \{0,1\}^{n.w_1}$ and $\hat{\mathsf{W}}_{\epsilon_2(n)} : \{0,1\}^{n.\ell_2} \to \{0,1\}^{n.w_2}$ as

follows: the output distribution of W_1 for ${y_r}^n \in \{0,1\}^{n.\ell_1}$ is $V_{\epsilon_1(n)}$ and for any $y^n \neq y_r^n$ the distribution is $\tau_{y^n}(V_{\epsilon_1(n)})$ and the output distribution of W_2 for $\hat{y}_r^n \in \{0,1\}^{n.\ell_2}$ is $\hat{V}_{\epsilon_2(n)}$ and for any $\hat{y}^n \neq \hat{y}_r^n$ the distribution is $\tau_{\hat{y}^n}(\hat{V}_{\epsilon_2(n)})$. The virtual channels $\mathsf{W}_{\epsilon_1(n)}$ and $\hat{\mathsf{W}}_{\epsilon_2(n)}$ are weakly symmetric channel by definition.

Now let $d_1(n)$ satisfy

$$n.\mathsf{R}_K + d_1(n) + H_\infty(V_{\epsilon_1(n)}) + H_\infty(\hat{V}_{\epsilon_2(n)}) \geq n.w_1 + n.w_2 + 2log(\frac{1}{\epsilon(n)}) + 2. \tag{B.19}$$

Since W_1 and W_2 are weakly symmetric, $\mathrm{C}_{\mathsf{W}_1} = w_1 - H(V_1)$ and $\mathrm{C}_{\mathsf{W}_2} = w_2 - H(V_2)$. Therefore, from (B.17) and (B.18), To satisfy (B.19), it is sufficient for $d_1(n)$ to satisfy the bound (B.20) below,

$$\begin{aligned} d_1(n) \geq n.C_{\mathsf{W}} - \sqrt{n}\left[\log(2^{\ell_1}+3).\sqrt{2log\frac{1}{\epsilon_1(n)}} + \log(2^{\ell_2}+3).\sqrt{2log\frac{1}{\epsilon_2(n)}}\right] \\ - 2log\epsilon_1(n).\epsilon_2(n) - n.\mathsf{R}_K + 2. \end{aligned} \tag{B.20}$$

The application of Theorem B.4.2 and triangular inequality yeilds that the **KXtX** construction with the given choice of $d_1(n)$ gives $Adv^{ds}(\mathsf{KSEnc}; \mathsf{W}^n) \leq 2\epsilon(n)$.

The corresponding rates of ECC_1 and ECC_2 are R_1 and R_2 respectively, where $R_1 + R_2 = \mathrm{C}_{\mathsf{T}}$. The achievable rate of the construction is $R = R_2 = \lim_{n\to\infty} \frac{b(n)}{n}$. By substituting $d_1(n)$ from (B.20) we have

$$\begin{aligned} &\lim_{n\to\infty} \frac{d(n)}{n} \geq \mathrm{C}_{\mathsf{W}} - R_K \\ &\Rightarrow R_1 \geq \mathrm{C}_{\mathsf{W}} - R_K \\ &\Rightarrow \mathrm{C}_{\mathsf{T}} - R_2 \geq \mathrm{C}_{\mathsf{W}} - R_K \\ &\Rightarrow R_2 \leq \mathrm{C}_{\mathsf{T}} - \mathrm{C}_{\mathsf{W}} + R_K. \end{aligned}$$

From Shannon's coding theorem we have $R \leq \mathrm{C}_{\mathsf{T}}$. The combination of the latter two inequalities completes the proof,

$$R \leq \min\left([C_{\mathsf{T}} - C_{\mathsf{W}}] + R_K, \mathrm{C}_{\mathsf{T}}\right)$$

where the upper bound is achieved when $d_1(n)$ in (B.20) is set to its minimum. □

The XtX construction.

The **KXtX** construction reduces to the **XtX** construction for $R_K = 0$.

1. Encoding:

$$\mathbf{XtX}.\mathbf{enc}[\mathsf{h}_S, \mathsf{ECC}_1, \mathsf{ECC}_2](m) = \mathsf{ECC}_1(D) \| \mathsf{ECC}_2\big(m \oplus \mathsf{h}_S(D)\big),$$

where $D \xleftarrow{\$} \{0,1\}^{d_1}$.

2. Decoding: In the **XtX** construction the received block Y is parsed to obtain (Y_1, Y_2).

$$\mathbf{KXtX}.\mathbf{dec}(Y) = \mathsf{ECC}_2.\mathsf{dec}(Y_2) \oplus \big(\mathsf{h}_S(\mathsf{ECC}_1.\mathsf{dec}(Y_1))\big).$$

The security of this wiretap construction follows from Theorem B.4.2 by letting $R_K = 0$. Note that since the security proof of Theorem B.4.2 holds for *any* (ℓ_1, ℓ_2)-splittable DMC, this special case is a semantically secure modular wiretap encoding scheme for *any* (ℓ_1, ℓ_2)-splittable DMC. The asymptotic achievable rate of this construction for a splittable wiretap channel with weakly symmetric main and wiretapper's channels, according to Theorem B.4.3 and letting $R_k = 0$, is $\mathrm{C}_\mathsf{T} - \mathrm{C}_\mathsf{W}$ which is the secrecy capacity of a degraded wiretap channel with weakly symmetric main and wiretapper's channels.

B.4.2 Regular Channels

Suppose $|\mathcal{X}| = q$ is a prime power. This allows one to endow $|\mathcal{X}|$ with the structure of the Galois field $GF(q)$. The additive group of $GF(q)$ acts on $\mathcal{Y}$ as a permutation; that is each element $x \in \mathcal{X}$ defines a permutation τ_x on the set $\mathcal{Y}$ with the property

$$\tau_x(\tau'_x(y)) = \tau_{x+x'}(y)$$

for all $x \in \mathcal{X}$, $x' \in \mathcal{X}$, $y \in \mathcal{Y}$. Then the channel is called *regular* if the probability $\Pr(y|x)$ depends only on $\tau_x(y)$.

Remark B.4.1. *It turns out that regular channels are symmetric [37]. But, no all symmetric channels are regular as the input size of a regular channel is always a prime power while symmetric channels' input size is arbitrary. However, a (weakly) symmetric channel on a binary alphabet is a regular channel.*

Lemma B.4.3. *Let* $\mathsf{CH} : \{0,1\}^b \to \{0,1\}^\ell$ *be a symmetric channel and let* $\mathbf{W}$ *be the transition probability matrix of* CH. *Then there exists a family* $\{\tau_m\}_{m \in \{0,1\}^b}$ *of functions* $\tau_m : \{0,1\}^\ell \to \{0,1\}^\ell$ *such that* τ_{0^b} *is the identity permutation on* $\{0,1\}^\ell$, *and for all* $m, m' \in \{0,1\}^b$, *and* $y \in \{0,1\}^\ell$,

$$\tau_{m \oplus m'}(y) = \tau_m(\tau_{m'}(y)),$$

Proof. Since the channel is symmetric, all rows are permutations of the first row. Then for any pair of

$m, m' \in \{0,1\}^b$ and $y \in \{0,1\}^\ell$, there exists a $y' \in \{0,1\}^\ell$ such that $\mathbf{W}(m,y) = \mathbf{W}(m',y')$. We define the family $\{\tau_m\}_{m\in\{0,1\}^b}$ of functions $\tau_m : \{0,1\}^\ell \to \{0,1\}^\ell$ as follows:

$$\tau_{m\oplus m'}(y) = y'.$$

Since $\mathbf{W}(m,y) = \mathbf{W}(m,y)$, then $\tau_{m\oplus m}(y) = \tau_{0^b}(y) = y$. Moreover, $\tau_m(\cdot)$ is self-inverse, that is, $\tau_m(\tau_m(y)) = y$.

For any m' and y, there exists y' such that $\mathbf{W}(0^b,y) = \mathbf{W}(m',y')$ and therefore $\tau_{m'}(y) = y'$ and $\tau_{m'}(y') = y$ which implies $\mathbf{W}(m',y) = \mathbf{W}(0^b,y')$.

From the symmetry of the channel, for any m, y', there exists y^* such that $\mathbf{W}(0^b,y') = \mathbf{W}(m,y^*)$. This implies $y^* = \tau_m(y')$ (due to the definition of $\tau(\cdot)$) and since $y' = \tau_{m'}(y)$,

$$y^* = \tau_m(\tau_{m'}(y))$$

On the other hand, for any m, m' and y, there exists $\bar{y}$ such that $\mathbf{W}(m',y) = \mathbf{W}(m,\bar{y})$ then $\bar{y} = \tau_{m\oplus m'}(y)$ and since $\mathbf{W}(m',y) = \mathbf{W}(0^b,y') = \mathbf{W}(m,y^*)$. Then $y^* = \bar{y}$ and therefore $\tau_{m\oplus m'}(y) = \tau_m(\tau_{m'}(y))$. □

B.5 Appendix of Chapter 7

B.5.1 LHL for Average Smooth Min-entropy

Lemma B.5.1. *Let family $\{h_s | s \in \mathcal{S}\}$ of functions $h_s : \{0,1\}^n \to \{0,1\}^\ell$ be a 2-UHF. Then for possibly correlated random variables $X \in \{0,1\}^n$, $V \in \{0,1\}^t$ and $Z \in \{0,1\}^*$,*

$$\mathbf{SD}((S,Z,V,h_S(X)); (S,Z,V,U_\ell)) \le 2\epsilon + \frac{1}{2}\sqrt{2^{\ell+t-\tilde{H}^\epsilon_\infty(X|Z)}}.$$

Proof. From the average-case version of LHL in [45, Lemma 2.3] we have

$$\mathbf{SD}((S,Z,V,h_S(X)); (S,Z,V,U_\ell)) \le 2\epsilon + \frac{1}{2}\sqrt{2^{\ell-\tilde{H}_\infty(X|Z,V)}},$$

and then for $V \in \{0,1\}^t$ from [45, Lemma 2.2(b)] we have

$$\tilde{H}_\infty(X|Z,V) \ge \tilde{H}_\infty(X|Z) - t,$$

and therefore

$$\mathbf{SD}((S,Z,V,h_S(X));(S,Z,V,U_\ell)) \leq 2\epsilon + \frac{1}{2}\sqrt{2^{\ell+t-\tilde{H}_\infty(X|Z)}}.$$

Since $\tilde{H}^\epsilon_\infty(X|Z) = \max_{(\hat{X},\hat{Z}):\mathbf{SD}((X,Y);(\hat{X},\hat{Z}))\leq\epsilon} \tilde{H}_\infty(\hat{X}|\hat{Z})$, we have $\mathbf{SD}(Z;\hat{Z}) \leq \epsilon$ and $\mathbf{SD}(X;\hat{X}) \leq \epsilon$ and therefore, $\mathbf{SD}(h_S(X);h_S(\hat{X})) \leq \epsilon$. We have

$$\begin{aligned}
&\mathbf{SD}((S,Z,h_S(X));(S,Z,U_\ell)) \\
&\quad\leq \mathbf{SD}((S,Z,h_S(X));(S,Z,h_S(\hat{X}))) \\
&\qquad + \mathbf{SD}((S,Z,h_S(\hat{X}));(S,\hat{Z},h_S(\hat{X})) \\
&\qquad + \mathbf{SD}((S,\hat{Z},h_S(\hat{X}));(S,Z,U_\ell)) \\
&\quad\leq 2\epsilon + \frac{1}{2}\sqrt{2^{\ell-\tilde{H}_\infty(\hat{X}|\hat{Z})}}.
\end{aligned}$$

□

Appendix C

Generalized KEM and its Combiners

Abstract. Public-key encryption systems have restricted message spaces. A hybrid encryption system uses a public key part known as *key encapsulation mechanism (KEM)*, and a symmetric key part known as *data encapsulation mechanism (DEM)*, to obtain a public-key encryption system for arbitrary length messages: KEM establishes a shared key between the sender and the receiver, which is used by the symmetric key part to encrypt the actual message. KEM/DEM paradigm is widely used for securing the Internet communication.

In this paper we make a direct connection between a KEM and a one-message secure key establishment protocol, and initiate the study of *information theoretic KEM, or iKEM* for short. We introduce the framework of *generalized KEMs (gKEM)* that includes iKEM and computational KEM as special cases, and define its security. We construct an iKEM and prove its security with respect to the iKEM specialization of the gKEM framework. Finally, we define *gKEM combiners* that combine an iKEM and a traditional KEM, and guarantee that the security of the final combined gKEM will hold if one of the two ingredient gKEMs remains secure. We also give two black-box constructions of such combiners, and prove their security.

iKEMs significantly expand the range of available KEMs that provide post-quantum security, by constructing iKEMs from information theoretic and quantum theoretic secure key establishment protocols. The combination of iKEM with computational KEMs give an elegant approach to improving robustness of computational KEMs that rely on new and less scrutinized computational assumptions. We discuss our results and directions for future work.

C.1 Introduction

Public-key encryption (PKE) schemes were proposed in the seminal paper of Diffie and Hellman [40], and are one of the essential cryptographic primitives for securing the Internet.

Security of encryption schemes in general is defined against *chosen plaintext attack (CPA)* and *chosen ciphertext attack (CCA)*, and is modelled as security against an adversary with access to two types of oracles, *encryption oracle* that allows the adversary to query messages of their choice and receive the corresponding ciphetexts, and *decryption oracle* that allows the adversary to sample and query points in the ciphertext space, and see the corresponding message, or receive an error symbol if the sampled point does not correspond to a valid ciphertext. The security goal is commonly formulated as the probability of distinguishing the ciphertext of two messages that are chosen by the adversary with access to one or both of the oracles above, at the end of playing the indistinguishability game (See Figure C.1). In the case of PKE schemes, the adversary has access to the public key and so can see the ciphertext of any message of its choice. A widely accepted notion of security in this case is *security against adaptive chosen ciphertext attack* (CCA2 security) which gives the adversary access to the decryption oracle, before and after the challenge ciphertext is presented to the adversary. An adaptive adversary chooses each query using their previous queries and their corresponding responses. Chosen-ciphertext security is essential for providing security against active adversaries in protocols for authentication [47, 49] and key exchange [125]. (In symmetric key encryption schemes both types of queries are considered extra capability for the adversary.)

Hybrid encryption and KEM/DEM framework. A PKE scheme is defined for a restricted message space that depends on the security parameter and the public key. In practice however, message sizes are unrestricted and one needs to extend the domain of the encryption function while maintaining strong security. One way of achieving this goal is by using a *hybrid encryption scheme* that, loosely speaking, uses a public key component to establish a shared key between Alice and Bob, and then use the key to encrypt the message using a symmetric key encryption system. These two parts are called *key encapsulation mechanism (KEM)*, and data encapsulation mechanism (DEM), respectively. Cramer and Shoup formalized security of a hybrid encryption scheme [31]. They noted that the *key encapsulation mechanism (KEM)* is a public-key encryption scheme, where the goal of the encryption algorithm is to generate the encryption of a random key k that is decryptable by the receiver. The KEM outputs are a key k, that is stored locally (and is computable by the receiver), and a ciphertext c that is sent to the receiver to allow them to recover k. Data Encapsulation mechanism (DEM) is a highly efficient symmetric key algorithm that uses the established key to encrypt the message.

Cramer et al. defined the required security notions for KEM and DEM and proved ([31, Theorem 5])

that if KEM and DEM are secure against adaptive CCA attacks, then so will be the resulting hybrid PKE (sufficient condition). DEM in practice is implemented using an efficient and secure block cipher such as AES. The KEM/DEM paradigm provides a neat way of constructing efficient and practical public-key encryption schemes for arbitrary length messages, and so has received significant attention in recent years. Because of their simplicity and modular approach they have been incorporated into standards for encryption (see, e.g., [129], and numerous KEM schemes have been proposed in literature [22, 31, 38, 126, 127]).

KEM combiners. Cryptographic combiners have been used to combine multiple cryptographic primitives (called *ingredient* or *component* primitives) that have the same functionality, into a single system that provides the same functionality, with the property that the security of the combined scheme holds, if at least one of the ingredient schemes is secure. The main motivation for using combiners is providing robustness against possible insecurity of the ingredient primitive, and gives a prudent approach toward providing robust security. Another strong motivation for using combiner stems from the challenging task of choosing among multiple schemes that provide the same functionality, but use different computational assumptions and/or ideal objects in their security proof. By using a combiner to combine the primitives, one will avoid the need for making such a decision. The combiners however increase the cost of a protocol because of the redundancy of running multiple protocols with the same functionality.

Combiners have been used for combining encryption systems and message authentication codes [3, 42, 70], and more recently for combining KEMs [55], which is a very well motivated application of combiners because KEM has been widely used for securing communication over the Internet but recent advances in quantum technologies has rendered all the widely used encryption algorithms such as RSA, and the KEM constructions that are based on them, insecure. Furthermore, existing proposals for quantum-safe KEM schemes rely on new and less understood computational assumptions such as isogenies [36] and Ring Learning with Error [104]. Using KEM combiners provides an elegant method of adding robustness to quantum-safe KEMs and allowing security of the combined KEM to rely on more than one computational assumption. Giacon, Heuer and Pottering [55] proposed efficient black-box constructions for KEM combiners that combine multiple ingredient KEMs into a single KEM, such that the resulting KEM provides CCA security as long as at least one of the ingredient KEMs is CCA secure.

Information Theoretic KEM. A KEM uses a pair of encapsulation and decapsulation algorithms to establish a shared key between Alice and Bob: $\mathsf{KEM.enc}$ algorithm generates the pair (c, k), where k is the shared key that will be held by Alice, and will be recovered by Bob by applying $\mathsf{KEM.dec}$ algorithm to c. Security of the key is defined using an indistinguishability game where the adversary's goal is to distinguish the key k from a random string, against a polynomially bounded attacker with oracle access to $\mathsf{KEM.dec}$

algorithm. KEM is a public key primitive and so access to KEM.enc is free.

We ask, (i) if KEM functionality can be defined in information theoretic setting with security against a computationally unbounded adversary, and (ii) in the case of affirmative answer to (i), if one can combine an iKEM with traditional computational KEMs. We refer to an *information theoretic KEM, as iKEM.*

Our main insight in answering the first question is by connecting the KEM functionality to the well-studied problem of *two-party key establishment* with security against a computationally unbounded adversary.

Information theoretic Secure Key Agreement (SKA). A KEM can be seen as a one message public key establishment protocol: Alice uses public key of Bob to send a message to him that establishes a shared key between the two parties. Information theoretic SKA has been widely studied in a number of settings [2, 44, 92]. Maurer showed [92] that information theoretic key agreement is possible only if Alice and Bob hold correlated variables X and Y, about which Eve may have partial information Z. This is also intuitive as without any correlated variable, and in absence of any computation bound, Eve can always simulate the view of Bob. The initial correlation is usually provided through a physical process, such as each party having access to the output of a noisy channel. SKA protocols use message transmission over public channel to convert this initial correlation into a shared secret key that is indistinguishable from a random value to the adversary. The adversary can be passive, in which case the public channel is authenticated [2, 92], or active [46, 79, 88] in which the adversary can tamper with the communication. A one message SKA has the functionality of a KEM, staring with an initial setup where Alice and Bob (and Eve) has samples of correlated variables, instead of KEM where Bob has a public and private key pair, and the public component is known by Alice and Eve. The KEM.enc and KEM.dec are the explict computation of Alice and Bob in this one message SKA. In this paper we generalize KEM definition to gKEM that includes iKEM and computational KEM as special cases and allows us to treat both of them similarly, design an iKEM and prove its security, and construct KEM combiners that combine an iKEM and a computational KEM.

Making a clean connection between KEM and information theoretic SKA significantly expands the range of available KEMs with post-quantum security and allows iKEMs that are based on physical layer assumptions (including SKA that use quantum theoretic assumption to generate the initial correlation) to be considered in the combiner. It also elegantly addresses the following challenges.

1. The initial correlation in Information theoretic SKA is usually obtained through physical layer processes. For example Maurer [92] considered a setting where a random sequence is broadcasted by a satellite, and received by Alice, Bob and Eve, through their own respective noisy channels. A similar setting has been used in a wireless local area network where a beacon transmits the sequence. The correlation in these cases is modelled by a sequence of independent samples of a public probability

distribution P_{XYZ}. This modelling of physical process of correlation generation effectively assumes that, in addition to Alice's and Bob's receptions, the Eve's reception of the broadcasted signal can be correctly estimated. Although Alice's and Bob's channels can be accurately modelled, correct estimation of Eve's channel could raise challenges. A secure combiner for iKEM and a computational KEM guarantees that the final key will be at least protected by a computational assumption.

2. SKA with information theoretic security provides security against *offline attack*. An off-line attacker can store all the communications and attempt to recover the message at a later time, either by applying sufficient computation, or leaving it for a future time when such computation becomes available. A computationally secure KEM/DEM will allow this attacker to find the key that is established by the KEM and decrypt the message that is encrypted by DEM. Using iKEM, as long as the initial correlation is correctly modelled, capturing transcript of the protocol will not allow such an offline attack. This follows from the security definition of SKA that requires the protocol transcript to be (statistically) independent from the final derived key. Using iKEM effectively forces Eve to break the symmetric key part of DEM.

C.1.1 Contributions

We define gKEM (Generalized KEM) for a generalized initial setup defined by public and private keys for Alice and Bob, and partial leakage of private keys to Eve, against a general adversary that can be computationally unbounded or bounded. We allow the adversary to query a $\mathsf{KEM.enc}$ and/or a $\mathsf{KEM.dec}$ oracle. Our general definition can be specialized to iKEM and computational KEM. We give the construction of an iKEM that satisfies our security definition of gKEM when specialized to the information theoretic setting. We define gKEM combiners and give two black-box combiners for gKEM, *XOR combiner* and *PRF-then-XOR combiner*, and prove their security.

Defining gKEM. A gKEM $\mathsf{gK} = (\mathsf{gK.gen}, \mathsf{gK.enc}, \mathsf{gK.dec})$, consists of three algorithms, where $\mathsf{gK.gen}$ is a randomized algorithm that takes a security parameter, and a second input Θ which is the description of a process that will use the security parameter and outputs a triplet of "correlated" random strings (r_A, r_B, r_E) that will be privately given to Alice, Bob and Eve, respectively. We allow Alice and Bob to publish (randomized) functions of their private inputs. If there is no initial leakage to Eve, we have $r_E = 0$. In a traditional KEM, Θ is the description of the $\mathsf{KEM.Gen}(\cdot)$ algorithm and uses the security parameter to generate $r_A = pk_B$, $r_B = (sk_B, pk_B)$, and $r_E = (sk'_B)$, where (sk_B, pk_B) are the public and private keys of Bob, assuming the $\mathsf{gK.enc}$ will be used by Alice, and sk'_b models possible initial leakage of Bob's private key to Eve which will be set to 0 if Bob's private key is perfectly secret (this is what is assumed in computational

KEM). Bob will publish pk_B).

In information theoretic setting Θ will be the description of a family of mathematical models of probabilistic physical processes that will depend on the iKEM. For the iKEM in Section C.3.2 the physical process can be modelled by taking repeated independent samples of a public distribution P_{XYZ}, where the number of samples will depend on the security parameter. Another widely studied initial setup for SKA is known as *fuzzy extractors* where the correlation is expressed as *distance* between vectors. The randomized algorithm $\mathsf{gK.enc}$ and deterministic algorithm $\mathsf{gK.dec}$ are defined similar to the corresponding algorithms in computational KEMs, using the private inputs of Alice and Bob, as well as the published values.

Security of gKEM is defined by an indistinguishability game where the attacker must distinguish between a key that is the encoded key using $\mathsf{gK.enc}$, and a random string of the same length, and is measured by using the advantage of the adversary in the game. In the computational setting, the adversary algorithm is computationally bounded (polynomially), while in information theoretic setting there is no computational bound on the adversary's computation. The adversary's power is defined by their access to $\mathsf{gK.enc}$ and $\mathsf{gK.dec}$ oracles. In information theoretic setting the two oracles hold Alice's and Bob's private inputs, respectively. We refer to an attack with access to the encapsulation oracle by *EnA* and with access to the decapsulation oracle by *CCA* in this setting. In computational setting however, $\mathsf{gK.enc}$ uses Bob's public key and so access to it will be free, and adversary's oracle access will be to $\mathsf{gK.dec}$.

A Secure iKEM. In Section C.3.2, we construct an iKEM where Θ describes a family of a public distributions $\mathcal{P}_{XYZ}$, and $\mathsf{gK.gen}$ chooses an appropriate member for a given security parameter. This results in a setting where Alice, Bob and Eve have private random variables X, Y and Z, respectively, correlated according to a public distribution P_{XYZ}. The iKEM uses two families of strongly universal hash functions $\mathcal{H} = \{\mathsf{h}_s\}_{s\in\mathcal{S}}$ and $\mathcal{H}' = \{\mathsf{h}'_{s'}\}_{s'\in\mathcal{S}'}$, with appropriate parameters. The $\mathsf{gK.enc}(x)$ algorithm selects a random string and assigns it to the key k that is stored locally, and uniformly selects two seeds s and s' for the hash functions, $\mathsf{h}_s(\cdot)$ and $\mathsf{h}'_{s'}(\cdot)$, respectively. The ciphertext c, that will be sent to the receiver, is given by $c = (s, s', \mathsf{h}'_{s'}(k))$. The receiver will use $\mathsf{gK.dec}(c, y)$ to recover the key. Theorem C.1 proves the correctness, and Theorems C.2,C.3 and C.4 prove security against three types of adversaries distinguished by their oracle accesses: an adversary that does not have any oracle access, an adversary that can query the encapsulation oracle q_e times, and an adversary that can query the decapsulation oracle q_c times, respectively.

The proofs show that the achievable length of the secret key reduces as the number of queries grow and approach zero after certain number of queries. This is expected as each query reveals part of the private information of Alice and Bob to Eve.

For a key length ℓ, Theorems C.3 and C.4 also show that if correctness error is smaller than $2^{-\ell}$ the

achievable secure key length for q encapsulation queries is the same as q decapsulation queries. This is also intuitive because the key length uses the common entropy of Alice's and Bob's samples.

Combiners for gKEM. A gKEM combiner combines two gKEMs with the goal of guaranteeing that the security for the combined gKEM will be at least the security of the ingredient KEMs. We define gKEM combiners such that when all gKEMs are computational, it becomes identical to the definition of KEM combiners in [55].

We give two black-box combiners for gKEMs: the *XOR combiner* that combines the output keys of the ingredient gKEMs by XORing them together, and the *PRF-then-XOR combiner* that uses the established key of each gKEM as the key to a PRF that is applied on the concatenation of ciphertexts of all gKEMS, and XORs the results. These combiners were studied in Giacon et al. for a computational setting.

The combination of ν computational gKEMs follows the results of Giacon et al: the XOR combiner retains the CPA security of the computational gKEM (this is when the adversary does not have access to decryption oracle), and the PRF-then-XOR construction retains the CCA security of the computational gKEM. (Giacon et al. also proposed an split-key construction that provides CCA security and can be used here.)

If at least one of the ν gKEMs is information theoretic, the final security will depend on the security of the iKEM. Theorem C.5 shows that if the iKEM is secure against q_e-bounded encapsulation queries (EnA secure), the XOR combiner will retain this security. If the q_e-bounded EnA security does not hold, the combined gKEM will have the CPA security of the computational gKEM [55, Lemma 1]. Theorem C.6 shows that If the iKEM is q_c-bounded CCA secure, then the PRF-then-XOR combiner retains this security as much as *the PRF that is used in the construction allows.* That is for the combined KEM K, the iKEM iK, and the PRF $\mathsf{F}(\cdot)$ is the construction of Theorem C.6.

$$Adv^{kind\text{-}q_c\text{-}cca}_{\mathsf{K},\mathsf{A}} \leq Adv^{kind\text{-}cca}_{\mathsf{iK},\mathsf{B}} + Adv^{PRF}_{\mathsf{F},\mathsf{C}}$$

If the q_c-bounded CCA security does not hold, then the CCA security of the computational gKEMs will be retained [55, Theorem 3]

We leave tight bounds on security of the combined gKEM if more than one iKEM exists, for future works.

C.2 Preliminaries

Notations: We denote random variables (RVs) with upper-case letters, (e.g., X), and their realizations with lower-case letters, (e.g., x). Calligraphic letters are to denote sets. If $\mathcal{S}$ is a set then $|\mathcal{S}|$ denotes its size. $U_{\mathcal{X}}$ denotes a random variable with uniform distribution over $\mathcal{X}$ and U_ℓ denotes a random variable with uniform distribution over $\{0,1\}^\ell$.

Functions are denoted with sanserif fonts e.g., $\mathsf{f}(\cdot)$. We use the symbol '$\leftarrow$', to assign a constant value (on the right-hand side) to a variable (on the left-hand side). Similarly, we use, '$\xleftarrow{\$}$', to assign to a variable either a uniformly sampled value from a set or the output of a randomized algorithm. We denote by $x \xleftarrow{r} \mathrm{P}_X$ the assignment of a fresh sample from P_X to the variable x. We write $\mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2,\cdots}(.)$ to denote an A that has access to to oracles $\mathsf{O}_1, \mathsf{O}_2, ...$, and by $u \leftarrow \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2,\cdots}(x, y, \cdots)$ denoting the algorithm taking inputs $x, y, \cdots$, and generating output u.

We use n as the security parameter. A non-negative function $\mathsf{f}(n)$ is called negligible, if for any polynomial $\mathsf{p}(\cdot)$, there exists an integer N such that for all integers $n > N$ we have $\mathsf{f}(n) < 1/\mathsf{p}(n)$.

Probability notations and relations. The probability mass function (p.m.f) of an RV X is denoted by P_X and $\mathrm{P}_X(x) = \Pr(X = x)$. For two random variables X and Y, P_{XY} denotes their joint distribution, and $\mathrm{P}_{X|Y}$ denotes their conditional distribution. The conditional probability of a random variable X given that Y takes a value y with $\mathrm{P}_Y(y) > 0$, is denoted by $\mathrm{P}_{X|Y}(x|y)$ and is given by: $\mathrm{P}_{X|Y}(x|y) = \frac{\mathrm{P}_{XY}(x,y)}{\mathrm{P}_Y(y)}$. The expected value of a random variable X is denoted by $\mathbb{E}(X)$ and is given by $\mathbb{E}(X) = \sum_{x \in \mathcal{X}} x\Pr(X = x)$. Let X be a non-negative random variable and suppose that $\mathbb{E}(X)$ exists. For any $a > 0$, the *Markov's inequality*[110, Proposition 2.1] holds, that is

$$\Pr(X > a) \leq \frac{\mathbb{E}(X)}{a}. \tag{C.1}$$

Definition C.1. The *statistical distance* between two probability distributions P_X and P_Y, or equivalently between two corresponding RVs X and Y defined over a common alphabet $\mathcal{T}$, is given by,

$$\mathbf{SD}(X;Y) = \max_{\mathcal{W} \subset \mathcal{T}} (\Pr_{t \xleftarrow{r} \mathrm{P}_X}(t \in \mathcal{W}) - \Pr_{t \xleftarrow{r} \mathrm{P}_Y}(t \in \mathcal{W}))$$

C.2.1 A public-key Encryption

A public-key encryption scheme Π is given by a triple of algorithms, $\Pi = (\Pi.\mathsf{Gen}, \Pi.\mathsf{Enc}, \Pi.\mathsf{Dec})$, where

- $\Pi.\mathsf{Gen}(1^n)$, the key generation algorithm, is a probabilistic algorithm that takes a security parameter n and outputs a pair (pk, sk) of matching public and secret keys, where $p_k \in \mathcal{PK}$ and $s_k \in \mathcal{SK}$.

- $\Pi.\mathsf{Enc}(pk, m)$, the encryption algorithm, is a probabilistic algorithm that takes a public key pk and a message m from a message space, and produces a ciphertext $c \in \mathcal{C}$.
- $\Pi.\mathsf{Dec}(sk, c)$ the decryption algorithm, is a deterministic algorithm which takes a secret key sk and ciphertext c, and produces either a message m, or $\perp$, where $\perp$ indicates that the ciphertext was invalid. We denote the decryption of ciphertext c under the secret key sk with $\mathsf{Dec}(sk, c)$.

Security of public-key encryption schemes. A secure encryption system provides confidentiality for encrypted messages. This is formalized by an *indistinguishability* game between the attacker and a challenger (See Figure C.1) who may have access to a decryption oracle. The goal of the adversary is to distinguish if the challenge ciphertext c^* is the encryption of one of the two messages $m^b, b \in \{0, 1\}$. The game models different types of attacks, distinguished by the access of the adversary to the decryption oracle. In chosen plaintext attack (CPA) the adversary does not have access to decryption oracle; we refer to this as 0-query attack also. The *non-adaptive chosen-ciphertext attack* (CCA1), and *adaptive chosen-ciphertext attack* (CCA2) allow the adversary to have access to the decryption oracle before seeing the challenge ciphertext, and before and after seeing the challenge ciphertext, respectively. We use the definitions in [10], and define the indistinguishability game as follows.

Definition C.2. Let $\Pi = (\Pi.\mathsf{Gen}, \Pi.\mathsf{Enc}, \Pi.\mathsf{Dec})$ be an encryption scheme and let $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ be an adversary. For $atk \in \{cpa, cca1, cca2\}$

$$Adv^{ind\text{-}atk}_{\Pi,\mathsf{A}}(n) \triangleq |\Pr[\mathrm{IND}^{atk\text{-}0}_{\Pi,\mathsf{A}}(n) = 1] - \Pr[\mathrm{IND}^{atk\text{-}1}_{\Pi,\mathsf{A}}(n) = 1]|, \tag{C.2}$$

where the distinguishing game $\mathrm{IND}^{atk\text{-}b}_{\Pi,\mathsf{A}}$ for $b \in \{0, 1\}$ is defined in Figure C.1.

Game $\mathrm{IND}^{atk\text{-}b}_{\Pi,\mathsf{A}}(n)$

1: $(pk, sk) \xleftarrow{\$} \Pi.\mathsf{Gen}(1^n)$
2: $(st, m_1, m_0) \xleftarrow{\$} \mathsf{A}_1^{\mathsf{O}_1(\cdot)}(pk)$
3: $c^* \xleftarrow{\$} \Pi.\mathsf{Enc}(pk, m_b)$
4: $b' \xleftarrow{\$} \mathsf{A}_2^{\mathsf{O}_2(\cdot)}(c^*, st, m_1, m_0)$
5: Return b'

Oracles O_1 and O_2

atk	$\mathsf{O}_1(\cdot)$	$\mathsf{O}_2(\cdot)$
cpa	ε	ε
$cca1$	$\Pi.\mathsf{Dec}(sk, c)$	ε
$cca2$	$\Pi.\mathsf{Dec}(sk, c)$	$\Pi.\mathsf{Dec}(sk, c)$

Figure C.1: Security game $\mathrm{IND}^{atk\text{-}0}_{\Pi,\mathsf{A}}$, where $b \in \{0, 1\}$ and $atk \in \{cpa, cca1, cca2\}$ for defining indistinguishability of an encryption scheme. Here $\mathsf{O}_i = \varepsilon$, where $i \in \{1, 2\}$, means O_i returns the empty string ε. In the case of A_2 we require that a decryption query c to satisfy $c \neq c^*$.

A public-key encryption scheme is said to be *indistinguishable against a CPA (CCA1, CCA2) attack* if the advantage function in (C.2) is negligible for all adversaries A.

C.2.2 Hybrid Encryption and KEM

A *hybrid encryption* system uses a special public-key encryption scheme, known as KEM, to establish a shared key between Alice and Bob, and uses a symmetric key encryption schemes, known as DEM, to encrypt an arbitrarily long message. Cramer et al [31, 127] formalised *KEM/DEM paradigm* for hybrid encryption schemes, defined adaptive CCA security (CCA2) for KEM and DEM, and proved that if both KEM and DEM are CCA2 secure, the resulting hybrid encryption will be CCA2 secure. The focus of this paper is on KEM.

A key encapsulation mechanism $\mathsf{K} = (\mathsf{K.Gen}, \mathsf{K.Enc}, \mathsf{K.Dec})$ for a finite session key space $\mathcal{K}$, private and public key spaces $\mathcal{SK}$ and $\mathcal{PK}$, respectively, and a ciphertext space $\mathcal{C}$, is a triple of algorithms defined as follows.

1. $\mathsf{K.Gen}(1^n)$ is a randomized key generation algorithm that takes the security parameter $n \in \mathbb{N}$ returns a public and secret-key pair (pk, sk), where $pk \in \mathcal{PK}$ and $sk \in \mathcal{SK}$.

2. $\mathsf{K.Enc}(pk)$ takes a public key pk and outputs a ciphertext $c \in \mathcal{C}$, and a key $k \in \mathcal{K}$.

3. $\mathsf{K.Dec}(sk, c)$ is a deterministic decapsulation algorithm that takes a secret key sk and a ciphertext c, and returns a key $k \in \mathcal{K}$, or $\perp$ that denotes failure.

A KEM K is $\epsilon(n)$-*correct* if for all $(sk, pk) \leftarrow \mathsf{K.Gen}(1^n)$ and $(c, k) \leftarrow \mathsf{K.Enc}(pk)$, it holds that $\Pr[\mathsf{K.Dec}(sk, c) \neq k] \leq \epsilon(n)$, where probability is over the choices of (sk, pk) and the randomness of $\mathsf{K.Enc}(\cdot)$, and $\epsilon(n)$ is a negligible function in n. We say the *KEM is correct if* $\epsilon(n) = 0$. Correctness with $\epsilon(n) = 0$ is called *consistency* in [72].

CPA, CCA1 and CCA2 security of KEM are defined in [69] with CCA2 security matching the corresponding definition in [31].

Definition C.3. Let $\mathsf{K} = (\mathsf{K.Gen}, \mathsf{K.Enc}, \mathsf{K.Dec})$ be a KEM and $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ denote an adversary. For $atk \in \{cpa, , cca1, cca2\}$, the key indistinguishability (kind) advantage of K is defined as

$$Adv^{kind\text{-}atk}_{\mathsf{K},\mathsf{A}}(n) \triangleq |\Pr[\mathrm{KIND}^{atk\text{-}0}_{\mathsf{K},\mathsf{A}}(n) = 1] - \Pr[\mathrm{KIND}^{atk\text{-}1}_{\mathsf{K},\mathsf{A}}(n) = 1]|, \tag{C.3}$$

where the distinguishing game $\mathrm{KIND}^{atk\text{-}b}_{\mathsf{K},\mathsf{A}}$ for $b \in \{0, 1\}$ is defined in Figure C.2.

A key encapsulation mechanism is said to be *indistinguishable against CPA (CCA1 and CCA2) attack* if for all polynomial-time adversaries A that corresponds to $atk = cpa$ ($atk = cca1$ and $atk = cca2$, respectively), the advantage function in (C.3) is negligible (in n). In this paper, for an adversary who has access

Game $\mathrm{KIND}^{atk\text{-}b}_{\mathsf{K},\mathsf{A}}(n)$

1: $(pk, sk) \xleftarrow{\$} \mathsf{K.Gen}(1^n)$
2: $st \xleftarrow{\$} \mathsf{A}_1^{\mathsf{O}_1(\cdot)}(pk)$
3: $(k^*, c^*) \xleftarrow{\$} \mathsf{K.Enc}(pk)$
4: $k_0 \leftarrow k^*$; $k_1 \xleftarrow{\$} \mathcal{K}$
5: $b' \xleftarrow{\$} \mathsf{A}_2^{\mathsf{O}_2(\cdot)}(c^*, st, k_b)$
6: Return b'

Oracles O_1 and O_2

atk	$\mathsf{O}_1(\cdot)$	$\mathsf{O}_2(\cdot)$
cpa	ε	ε
$cca1$	$\mathsf{K.Dec}(sk, c)$	ε
$cca2$	$\mathsf{K.Dec}(sk, c)$	$\mathsf{K.Dec}(sk, c)$

Figure C.2: Security game $\mathrm{KIND}^{atk\text{-}b}_{\mathsf{K},\mathsf{A}}$, where $b \in \{0,1\}$ and $atk \in \{cpa, cca1, cca2\}$, for defining indistinguishability of a KEM. The adversary A_2 cannot ask O_2 to decrypt c^*.

to decapsulation oracle we only consider CCA2 security, and refer to it as "CCA" security. We also consider CPA security which corresponds to zero decapsulation query.

KEM Combiners [55].

Let $\mathsf{K}_1, \ldots, \mathsf{K}_i, \ldots, \mathsf{K}_\nu$ be (ingredient) key-encapsulation mechanisms, where KEM $\mathsf{K}_i = (\mathsf{K}_i.\mathsf{Gen}, \mathsf{K}_i.\mathsf{Enc}, \mathsf{K}_i.\mathsf{Dec})$ has session-key space $\mathcal{K}_i$, public-key space $\mathcal{PK}_i$, secret-key space $\mathcal{SK}_i$, and ciphertext space $\mathcal{C}_i$. Let $\mathcal{K}^* = \mathcal{K}_1 \times \cdots \times \mathcal{K}_i \times \cdots \times \mathcal{K}_\nu$ and $\mathcal{PK} = \mathcal{PK}_1 \times \cdots \times \mathcal{PI} \times \cdots \times \times \mathcal{PK}_\nu$ and $\mathcal{SK} = \mathcal{SK}_1 \times \cdots \times \mathcal{SI} \times \cdots \times \mathcal{SK}_\nu$ and $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_i \times \cdots \times \mathcal{C}_\nu$. Let $\mathcal{K}$ be an auxiliary finite session-key space. A *core function* is used to derive a combined session key from a vector of session keys and a vector of ciphertexts: $\mathsf{W} : \mathcal{K}^* \times \mathcal{C} \to \mathcal{K}$. The KEM combination with respect to W is a KEM with session key space $\mathcal{K}$, and consists of the algorithms $\mathsf{K.Gen}, \mathsf{K.Enc}, \mathsf{K.Dec}$ specified in Figure C.3.

Algo $\mathsf{K.Gen}$
For $i \leftarrow 1$ to ν
  $(pk_i, sk_i) \xleftarrow{\$} \mathsf{K.Gen}_i(1^n)$
$\mathbf{pk} \leftarrow (pk_1, \ldots, pk_\nu)$
$\mathbf{sk} \leftarrow (sk_1, \ldots, sk_\nu)$
Return$(\mathbf{pk}, \mathbf{sk})$

Algo $\mathsf{K.Enc}$
$(pk_1, \ldots, pk_\nu) \leftarrow \mathbf{pk}$
For $i \leftarrow 1$ to ν
  $(c_i, k_i) \xleftarrow{\$} \mathsf{K.Enc}_i(pk_i)$
$\mathbf{c} \leftarrow (c_1, ..., c_\nu)$
$k \leftarrow \mathsf{W}(k_1, \ldots, k_\nu, \mathbf{c})$
Return$(k, \mathbf{c})$

Algo $\mathsf{K.Dec}$
$(sk_1, \ldots, sk_\nu) \leftarrow \mathbf{sk}$
$(c_1, \ldots, c_\nu) \leftarrow \mathbf{c}$
For $i \leftarrow 1$ to ν
  $k_i \leftarrow \mathsf{K.Dec}_i(sk_i, c_i)$
  If $k_i = \perp$: Return $\perp$
$k \leftarrow \mathsf{W}(k_1, \ldots, k_\nu, \mathbf{c})$
Return k

Figure C.3: KEM Combiner

C.2.3 Secret Key Agreement from Correlated Randomness

Maurer [93] and Ahlswede et al. [2] independently considered a model of secret key agreement where Alice and Bob have samples of correlated random variables (RVs) X and Y, and Eve has side information Z. The correlation between variables X, Y, and Z is specified by a public distribution P_{XYZ}. Alice and Bob want

to share a secret key by communicating over a public authenticated and error free channel that is visible to Eve. This model is called a *two-party secret key agreement (SKA) in source model*.

Let $\boldsymbol{F}$ denote the set of messages that are communicated over the public channel. Eve sees $\boldsymbol{F}$. A random variable K over $\mathcal{K}$ is an(ϵ, σ)-*Secret Key Agreement (in short* (ϵ, σ)-*SKA),* if there exists a protocol with public communication $\boldsymbol{F}$, and two (possibly random) functions $\mathsf{K}_x(X, \boldsymbol{F})$ and $\mathsf{K}_y(Y, \boldsymbol{F})$ outputting K_x and K_y respectively, satisfying the following reliability and security properties:

$$\text{(reliability)} \quad \Pr[K_x = K_y = K] \geq 1 - \epsilon, \tag{C.4}$$

$$\text{(security)} \quad \mathbf{SD}\left((K, \boldsymbol{F}, Z); (U_{\mathcal{K}}, \boldsymbol{F}, Z)\right) \leq \sigma, \tag{C.5}$$

where ϵ and σ are small non-negative numbers.

To achieve these bounds for arbitrarily small values of ϵ and σ one needs to make additional assumptions about the probability distribution. A commonly used assumption is that the experiment that generates the distribution P_{XYZ} is repeated independently N times. This assumption is well motivated when the distribution is generated by independent discrete memoryless channels.

Randomness Extraction.

The *min-entropy* $H_\infty(X)$ of random variable $X \in \mathcal{X}$ with distribution P_X where $\mathrm{P}_X(x) \in [0, 1], x \in \mathcal{X}$, is defined by $H_\infty(X) = -\log(\max_x(\mathrm{P}_X(x)))$. The *average conditional min-entropy* [44] is commonly defined as,

$$\tilde{H}_\infty(X|Y) = -\log \mathbb{E}_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}} \mathrm{P}_{X|Y}(x|y).$$

Randomness extractors map a random variable with a guaranteed entropy, to a random variable from a smaller set that is statistically close (in terms of the statistical distance) to a uniform random variable. See [99] and references therein for more details. One of the well known constructions for randomness extractors is by using *(Strong)Universal Hash Families* (UHF) via the so called *Leftover Hash Lemma* (LHL) [77].

Definition C.4 (Strong Universal Hash Family[142])**.** A family of functions $\{\mathsf{h}_s : \mathcal{X} \to \mathcal{Y}\}_{s \in \mathcal{S}}$ is a Strong Universal Hash Family if for any $x \neq x^{'}$ and any $a, b \in \mathcal{Y}$,

$$\Pr\{h_S(x) = a \wedge h_S(x^{'}) = b\} = \frac{1}{|\mathcal{Y}|^2},$$

where the probability is over the uniform choices over $\mathcal{S}$.

We will use a variation of the LHL [77], called the *generalized* LHL [45, Lemma 2.4] later in this paper.

Lemma C.1 (Generalized LHL)**.** *For two possibly dependant random variables $A \in \mathcal{X}$ and $B \in \mathcal{Y}$, applying a universal hash function (UHF) $\{\mathsf{h}_s : \mathcal{X} \to \{0,1\}^\ell\}_{s\in\mathcal{S}}$ on A can extract a uniformly random variable whose length ℓ will be bounded by the average min-entropy of A, given B, and the required closeness to the uniform distribution. That is:*

$$\mathbf{SD}(B, S, (h_S(A)); (B, S, U_\ell)) \leq \frac{1}{2}\sqrt{2^{\ell - \tilde{H}_\infty(A|B)}},$$

where S is the randomly chosen seed of the hash function family, and the average conditional min-entropy is defined above.

C.3 gKEM

To define iKEM our first step is to define gKEM as a generalization of KEM such that it can be specialized to KEM and iKEM for computational and information theoretic security, respectively. We define a gKEM where Alice and Bob both have private inputs, and may publish a randomized function of their input as their public value. The adversary may have partial information about the private inputs of the parties, modelling possible leakages of these values to the adversary.

Let Alice and Bob be the parties who use the encapsulation and the decapsulation functions of the gKEM, respectively, and let Eve denote the adversary.

Definition C.5 (gKEM)**.** A gKEM $\mathsf{gK} = (\mathsf{gK.Gen}, \mathsf{gK.Enc}, \mathsf{gK.Dec})$ is a triplet of polynomial-time algorithms, where $n \in \mathbb{N}$ is the security parameter, and the algorithms are defined as below.

1. $\mathsf{gK.Gen}(1^n, \Theta)$, the generation algorithm, is a randomized algorithm that takes a security parameter n and Θ which is the description of a probabilistic algorithm, and outputs a triplet of correlated random strings (r_A, r_B, r_E), that will be given privately to Alice, Bob and Eve, respectively. Bob may publish a (randomized) function of their strings. Let pub_B denote Bob's published string.

2. $\mathsf{gK.Enc}(r_A, pub_B)$, the encapsulation algorithm, is a probabilistic algorithm that takes as input the sender's random string r_A and Bob's public string pub_B, and outputs a key/ciphertext pair (c, k).

3. $\mathsf{gK.Dec}(r_B, c)$, the decapsulation algorithm, is a deterministic algorithm that takes as input the receiver's random string r_B and the ciphertext c, and outputs a key $\hat{k}$ or special symbol $\perp$ ($\perp$ shows that the ciphertext has been invalid).

Θ is the description of a probabilistic algorithm that takes the security parameter as an input. The $\mathsf{gK.Gen}$ algorithm uses the security parameter and Θ to generate the private inputs of the parties.

In computational setting, Θ is the description of the generation algorithm of a KEM: it receives the security parameter of the gKEM and generates private and public keys of Bob. In information theoretic setting, Θ specifies a probabilistic experiment that generates correlated samples of the parties. The $\mathsf{gK.Gen}$ algorithm uses the security parameter and Θ, and selects the appropriate "index" of the experiment to generate the private inputs of the parties. Here we use the term "index" in an informal sense, and make it more precise for a particular probabilistic setting. A widely studied case of correlated inputs for SKA is when the private inputs of Alice, Bob and Eve are related by a joint probability distribution $\mathrm{P}_{X,Y,Z}$ that is public, and its N independent runs of the underlying experiment [92]. Let the correlation be described by a family of distributions $\mathcal{P}_{R_A R_B R_E} = \{\mathrm{P}^{(n')}_{R_A R_B R_E} | n' \in \mathbb{N}\}$. For a given security parameter n, the $\mathsf{gK.Gen}$ will use an appropriate n' (that achieves the required security) from $\mathcal{P}_{R_A R_B R_E}$ to generate the private samples of the parties.

A second widely studied case for Θ [44] is when R_A and R_B are samples of a random variable with sufficient min-entropy, and satisfy certain "distance" condition. For example $\mathsf{d}(r_A, r_B) \leq t$ where $\mathsf{d}(.,.)$ is a distance function. In practice such samples can be generated by multiple readings of a user biometric data. The iKEM construction in Section ... is for the former

Correctness of gKEM. Let $\epsilon(n)$ denote a non-negative function $\epsilon : \mathbb{N} \to [0, 1)$ A gKEM gK is $\epsilon(n)$-correct if for all $n \in \mathbb{N}$ and $(c, k) \xleftarrow{\$} \mathsf{gK.Enc}(r_A)$, it holds that $\Pr[\mathsf{gK.Dec}(r_B, c) \neq k] \leq \epsilon(n)$, where the probability is taken over all choices $(r_A, r_B, r_C) \leftarrow \mathsf{gK.Gen}(1^n, \Theta)$, and the coins of the encapsulation and decapsulation algorithm. The gKEM is *correct* if $\epsilon(n) = 0$.

Security of a gKEM. In gKEM, Alice and Bob both can have private inputs that will be used to establish the shared key and the adversary may interact with each of the parties to learn their secret input and the final shared key. We thus, consider three types of attacks, *Chosen Plaintext Attack (CPA)*, *Encapsulation Attack (EnA)* and *Chosen Ciphertext Attack (CCA)*, modelled by the adversary's access to two types of oracles, $\mathsf{gK.Enc}(r_A)$ and $\mathsf{gK.Dec}(r_B)$, respectively. The CPA attack for gKEM (similar to the traditional KEM) is just a technical term to refer to an attack without any oracle access for the adversary and it doesn't literally means "choosing a plaintext" since there is no plaintext in a gKEM (KEM) structure. A query to $\mathsf{gK.Enc}(r_A)$ does not have any input, and outputs a pair (c, k) where k and c are a key and the corresponding ciphertext that is obtained by using the secret input of Alice and other system's public information. is the key and c is the ciphertext that is obtained A query to $\mathsf{gK.Dec}(r_B)$ is a chosen ciphertext c, and will result in $\mathsf{gK.Dec}(r_B)$ to output either a key k, or $\perp$, indicating that $\mathsf{gK.Dec}$ can/cannot generate a valid key for the presented c.

Definition C.6. Let $\mathsf{gK} = (\mathsf{gK.Gen}, \mathsf{gK.Enc}, \mathsf{gK.Dec})$ be a gKEM and let $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ be an adversary. The

Game $\text{gKIND}^{atk\text{-}b}_{\mathsf{gK,A}}(n)$

1: $(r_A, r_B, r_E) \xleftarrow{\$} \mathsf{gK.Gen}(\Theta)$
2: $st_1 \xleftarrow{\$} \mathsf{A_1}^{\mathsf{O}_0, \mathsf{O}_1(\cdot)}(r_E)$
3: $(k^*, c^*) \xleftarrow{\$} \mathsf{gK.Enc}(r_A)$
4: $k_0 \leftarrow k^*$; $k_1 \xleftarrow{\$} \mathcal{K}$
5: $b' \xleftarrow{\$} \mathsf{A_2}^{\mathsf{O}_2(\cdot)}(c^*, st_1, k_b)$
6: Return b'

Oracles O_0, O_1 and O_2

atk	O_0	$\mathsf{O}_1(\cdot)$	$\mathsf{O}_2(\cdot)$
cpa	ε	ε	ε
ena	$\mathsf{gK.Enc}(r_A)$	ε	ε
cca	$\mathsf{gK.Enc}(r_A)$	$\mathsf{gK.Dec}(r_B, c)$	$\mathsf{gK.Dec}(r_B, c)$

Figure C.4: Key indistinguishability game: is defined by the security game $\text{gKIND}^{atk\text{-}b}_{\mathsf{K,A}}$, where $b \in \{0,1\}$ and $atk \in \{cpa, ena, cca\}$. For computational KEM, $atk \in \{cpa, cca\}$, and for iKEM $atk \in \{cpa, ena, cca\}$. The adversary $\mathsf{A_2}$ does not ask its oracle to decrypt c^* in $atk = cca$.

gKEM's key indistinguishability advantage (gkind) for $atk \in \{cpa, ena, cca\}$ is defined as follows.

$$Adv^{gkind\text{-}atk}_{\mathsf{gK,A}}(n) \triangleq |\Pr[\text{gKIND}^{atk\text{-}0}_{\mathsf{gK,A}}(n) = 1] - \Pr[\text{gKIND}^{atk\text{-}1}_{\mathsf{gK,A}}(n) = 1]|, \tag{C.6}$$

where the distinguishing game $\text{gKIND}^{atk\text{-}b}_{\mathsf{gK,A}}$ for $b \in \{0,1\}$ is defined in Figure C.4.

The adversary A may be, (i) computationally bounded, or (ii) computationally unbounded. The advantage is bounded by $\sigma(n)$, a function of n, that goes to zero as n increases. For a computational adversary, this function must be negligible in n. For computationally unbounded adversary (iKEM), $\sigma(n)$ is a "small function" of n. That is for any small $\hat{\sigma} > 0$, there is a $\hat{n}$ where for all $n > \hat{n}$, we have $\sigma(n) < \hat{\sigma}$. For the security parameter n let $\sigma(n)$ be such a function. Then the gKEM is $\sigma(n)$-*indistinguishable against EnA (or CCA) attacks* when (C.6) is upper bounded by $\sigma(n)$ for $atk = ena$ (or $atk = cca$).

A traditional computational KEM is a gKEM with $\mathsf{gK.Gen}$ generating a pair (sk, pk) for Bob, and making pk available to Alice, and key indistinguishability (See Definition C.3) is against a polynomially bounded adversary. In this case r_A is a public value and so access to $\mathsf{gK.Enc}(r_A)$ is free for the adversary. This is why EnA security is not applicable to the computatinal KEM. For iKEM r_A is private and encapsulation algorithm is a randomized algorithm and each query to $\mathsf{gK.Enc}(r_A)$ will result in a different pairs of (k, c) with overwhelming probability.

C.3.1 iKEM

We define an iKEM $\mathsf{iK} = (\mathsf{iK.Gen}, \mathsf{iK.Enc}, \mathsf{iK.Dec})$ as a gKEM where (i) $\mathsf{iK.Gen}$ takes the security parameter and a publicly known family of distributions in the form of $\mathcal{P}_{R_A R_B R_E}$ or $\mathcal{P}_{R_A R_B}$), and provides private inputs to Alice and Bob, and possibly Eve, and (ii) in the key indistinguishability game, the adversary A is computationally unbounded (Definition C.6).

This models a setting that is known as the so called *satellite setting* [92], where a satellite (or a beacon) broadcasts a sequence of uniformly random bits that will be received by Alice, Bob and Eve through three distinct noisy channels. Alice and Bob use communication over a public authenticated channel to arrive at a shared key k.

Expected correctness of iKEM.

$\mathsf{iK.Enc}(\cdot)$ outputs a pair (c, k) of key and ciphertext. Let $\mathsf{iK.Enc}.key = k$ and $\mathsf{iK.Enc}.ctxt = c$. Then the correctness of iKEM for a given pair of samples (r_A, r_B) is defined as $\Pr[\mathsf{iK.Dec}(r_B, c) \neq \mathsf{iK.Enc}(r_A).key] \leq \epsilon_n$ where the probability is over all the random coins of $\mathsf{iK.Enc}$, $\mathsf{iK.Dec}$ and $\mathsf{iK.Gen}$.

Note that the $\mathsf{iK.Gen}$ samples a probability distribution and so the above probability is the expected correctness as defined below,

$$\tilde{\mathrm{P}}_e = \mathbb{E}_{r_A, r_B \xleftarrow{r} \mathrm{P}^{(n')}_{R_A R_B R_E}} \Pr[\mathsf{iK.Dec}(r_B, c) \neq \mathsf{iK.Enc}.key]. \tag{C.7}$$

An iKEM is ϵ_n-correct if (C.7) is bounded by $\epsilon(n)$, where $\epsilon : \mathbb{N} \to [0, 1)$ is a small function in n.

Security of iKEM.

Security of an iKEM can be defined by bounding the distinguishing advantage of an adversary in $\mathrm{gKIND}^{atk\text{-}b}_{\mathsf{gK},\mathsf{A}}$ games of Definition C.6 for $atk \in \{cpa, ena, cca\}$ and $b \in \{0, 1\}$.

In computational setting the adversary may have access to polynomially bounded ciphertext queries. Cramer et al. [32, Definition2] also defined q-bounded CCA security (IND-q-CCA security) where the adversary can have access to constant (q) number of queries.

In information theoretic setting the established key will use the entropy of the correlated variables (R_A, R_B, R_E), which with every query reduces. We thus consider two query bounded attackers: an attacker with access to q_e encapsulation queries, and an attacker has access to q_c ciphertext (decryption/decapsulation) queries. The attackers model q_e-bounded EnA and q_c-bounded CCA (decapsulation) attack, and denote them as q_e-ena and q_c-cca respectively.

For $atk \in \{cpa, q_e\text{-}ena, q_c\text{-}cca\}$, an iKEM is σ_n-indistinguishable if for all adversaries we have

$$Adv^{gkind\text{-}atk}_{\mathsf{iK},\mathsf{A}}(n) = |\Pr[\mathrm{gKIND}^{atk\text{-}0}_{\mathsf{iK},\mathsf{A}}(n) = 1] - \Pr[\mathrm{gKIND}^{atk\text{-}1}_{\mathsf{iK},\mathsf{A}}(n) = 1]| \leq \sigma_n, \tag{C.8}$$

where $\sigma(n)$ is a small function of n.

The following lemmas show that the advantage in the indistinguishability game is bounded by the the statistical distance of the adversary's view of the game and its outcome. The proofs are given in Appendix A.

Lemma C.2. *Let $\mathbf{v}^{q_e\text{-}ena}_{\mathsf{A}} = (v^{ena}_1, \cdots, v^{ena}_{q_e})$ for $v^{ena}_i \in \mathcal{K} \times \mathcal{C}$ denote the encapsulation oracle's responses to adversary A's queries in the q_e-bounded EnA attack. The iKEM is σ_n-indistinguishable against q_e-bounded EnA, if and only if for all adversaries A we have*

$$\mathbf{SD}\big((R_E, C^*, K^*, \mathbf{v}^{q_e\text{-}ena}_{\mathsf{A}}); (R_E, C^*, U_{\mathcal{K}}, \mathbf{v}^{q_e\text{-}ena}_{\mathsf{A}})\big) \leq \sigma_n. \tag{C.9}$$

where random variables R_E, C^* and K^* correspond to r_E, the initial correlated random string received by the adversary an the challenge ciphertext and key pair in the game $\mathrm{gKIND}^{q_e\text{-}ena\text{-}b}_{\mathsf{gK},\mathsf{A}}(n)$ respectively.

Lemma C.3. *Let $\mathbf{qr}^{q_c\text{-}cca}_{\mathsf{A}} = (qr^{cca}_1, \cdots, qr^{cca}_{q_e})$ for $qr^{cca}_i \in \mathcal{K}$ denote an adversary A's queries to the decapsulation oracle in the CCA attack and $\mathbf{v}^{q_c\text{-}cca}_{\mathsf{A}} = (v^{cca}_1, \cdots, v^{cca}_{q_e})$ for $v^{cca}_i \in \mathcal{C} \cup \{\perp\}$ denote decapsulation oracle to A's queries in the CCA attack. An iKEM is σ_n-indistinguishable against q_c-bounded CCA attack if for all adversaries A we have*

$$\mathbf{SD}\big((R_E, C^*, K^*, \mathbf{v}^{q_c\text{-}cca}_{\mathsf{A}}, \mathbf{qr}^{q_c\text{-}cca}_{\mathsf{A}}); (R_E, C^*, U_{\mathcal{K}}, \mathbf{v}^{q_c\text{-}cca}_{\mathsf{A}}, \mathbf{qr}^{q_c\text{-}cca}_{\mathsf{A}})\big) \leq \sigma_n. \tag{C.10}$$

where random variables R_E, C^* and K^* correspond to r_E, the initial correlated random string received by the adversary an the challenge ciphertext and key pair in the game $\mathrm{gKIND}^{q_c\text{-}cca\text{-}b}_{\mathsf{gK},\mathsf{A}}(n)$ respectively.

C.3.2 An iKEM with provable security

In the following, we introduce an iKEM that starts with a correlated randomness given by a joint distribution P_{XYZ} that is public, and uses a single message from Alice to Bob to establish a shared secret key between them.

The iKEM iK. The iKEM $\mathsf{iK} = (\mathsf{iK.Gen}, \mathsf{iK.Enc}, \mathsf{iK.Dec})$ will have the following algorithms.

Initialization: Let $\{\mathsf{h}_s : \mathcal{X} \to \{0,1\}^t\}_{s \in \mathcal{S}}$ and $\{\mathsf{h}'_{s'} : \mathcal{X} \to \{0,1\}^\ell\}_{s' \in \mathcal{S}'}$ be two strong universal hash families (UHFs). Also let $\mathcal{C} = \{0,1\}^t \times \mathcal{S} \times \mathcal{S}'$ and $\mathcal{K} = \{0,1\}^\ell$ denote the set of ciphertexts and keys.

Theorem C.1 shows how to determine t and Theorems C.2 to C.4 show how to determine ℓ for the required levels of correctness and security, respectively, knowing the correlation among the variables.

- $\mathsf{iK.Gen}(1^n, \mathcal{P}_{XYZ})$: The generation algorithm chooses an appropriate $\mathrm{P}_{XYZ}^{n'}$ from $\mathcal{P}_{XYZ} = \{\mathrm{P}_{XYZ}^{n'} | n' \in \mathbb{N}\}$ according to n, and samples the distribution to output the triplet x, y and z of correlated samples[1], and privately gives them to Alice, Bob and Eve, respectively. That is

$$(x, y, z) \xleftarrow{\$} \mathsf{iK.Gen}(1^n, \mathcal{P}_{XYZ}).$$

- $\mathsf{iK.Enc}(x)$: The encapsulation algorithm $\mathsf{iK.Enc}(\cdot)$ samples $s' \xleftarrow{\$} \mathcal{S}'$ and $s \xleftarrow{\$} \mathcal{S}$ for the seed of the strongly universal hash functions, and generates the key $k = \mathsf{h'}_{s'}(x)$ and the ciphertext $c = (\mathsf{h}_s(x), s', s)$, Thus

$$(c, k) = \big((\mathsf{h}_s(x), s', s), \mathsf{h'}_{s'}(x)\big) \xleftarrow{\$} \mathsf{iK.Enc}(x).$$

- $\mathsf{iK.Dec}(y, c)$: The decapsulation mechanism $\mathsf{iK.Dec}(y, c)$ takes the private input of Bob, y, and the ciphertext $\mathsf{h}_s(x), s', s$ as inputs, and outputs the key $h_{s'}(x)$ or $\perp$. We have

$$k = (\mathsf{h'}_{s'}(x)) \leftarrow \mathsf{iK.Dec}\big(y, (\mathsf{h}_s(x), s', s)\big).$$

  The decapsulation algorithm works as follows:

  1. Parses the received ciphertext to (g, s', s), where g is a t-bit string.
  2. Define the set,

$$\mathcal{T}(X|y) \triangleq \{x : -\log \mathrm{P}_{X|Y}^{n'}(x|y) \leq \lambda\}, \tag{C.11}$$

     For each vector $x \in \mathcal{T}(X|y)$, check $g \stackrel{?}{=} \mathsf{h}_s(x)$.
  3. Output $\hat{x}$ if it is the unique value of x that satisfies $g = \mathsf{h}_s(\hat{x})$; Else output $\perp$.

  The value of λ depends on the correlation of x and y: higher correlation corresponds to smaller λ, and smaller set of candidates (see Theorem C.1 for the precise relationship).

  If successful, the decapsulation algorithm outputs a key $k = \mathsf{h'}_{s'}(\hat{x})$; otherwise it outputs $\perp$.

The intuition behind the construction iK is as follows. Alice encapsulation algorithms extracts a key from its private input x, and by sending sufficient information to Bob aims to enable Bob to recover x, and

[1] We use x, y and z instead of r_A, r_B and r_E to stay consistent with the conventional information theoretic notations.

extract the same key. The ciphertext to Bob thus includes the required information to recover x, and the seeds of the hash functions that are used for key extraction and also generating the data for reconcilliation. Eve has her own sample of side information z that leaks partial information about Alice's and Bob's samples, and also sees the ciphertext. that leaks information about Alice's samples. Alice and Bob will estimate the total leaked information about their shared string, and remove it by the application of $\mathsf{h}'_{s'}(\cdot)$ on x (by Alice) and its estimate $\hat{x}$ (by Bob).

Correctness and Security of iK. In the following we prove for appropriate choices of the hash functions and their parameters, iK can achieve $\epsilon(n)$-correctness and $\sigma(n)$-indistinguishability against $atk \in \{cpa, q_e\text{-}ena, q_c\text{-}cca\}$. To satisfy security requirement of an iKEM, $\sigma(n)$ should be a small function of n. In other words, for every small $\hat{\sigma} > 0$, there exists an $\hat{n}$ such that for all $n > \hat{n}$, the expression (C.8) holds. In the following, we show the error probability and distinguishing advantage can be bounded for the proposed iK construction. We prove this for concrete values of ϵ, σ, and P_{XYZ}, and omit the parametrization for simplicity. Theorem C.1 shows that expected error probability of iK can be bounded by ϵ when sufficient information for reconciliation is sent (according to (C.17)). In Theorem C.2 we prove σ-indistinguishablity of iK against an adversary without access to encapsulation or decapsulation queries. Finally in Theorem C.3 and Theorem C.4 we prove q_e-bounded EnA security and q_c-bounded CCA security of iK.

We note that the security definition of gKEM allows the adversary to use both oracles. The above theorems however consider each type of queries separately.

Theorem C.1. *In the iKEM* iK*, to achieve average error probability at most ϵ, the output length of the hash function* $\mathsf{h}_s(.)$ *denoted by t must satisfy, $t \geq 2\tilde{H}_\infty(X|Y)/\epsilon - \log\epsilon - 1$.*

Proof. The decapsulation algorithm in iK searches the set $\mathcal{T}(X|y)$ for x values such that $h_s(x) = g$ where g is the received hash value. The algorithm fails in two cases: (i) x is not in the set, and (ii) there are more than one vector in the set whose hash value is equal to g, and so the KEM's expected probability of failure, $\tilde{\mathrm{P}}_e = \mathbb{E}_{x,y}\mathrm{Pr}[\mathsf{iK.Dec}(y,c) \neq \mathsf{iK.Enc}(x).key]$, is upper bounded by the sum of the probabilities of the above two events, where the probability is over the randomness of encapsulation, and the average is over all sample pairs (x, y). The two events correspond to cases that Alice's sample are in the sets below.

$$\xi_1 = \{x : -\log \mathrm{P}_{X|Y}(x|y) > \lambda\}$$
$$\xi_2 = \{x \in \mathcal{T}(X|y) : \exists\ \hat{x} \in \mathcal{T}(X|y) \text{ s.t. } h_S(\hat{x}) = h_S(x)\}.$$

We use Markov's inequality (C.1) to bound the average probability of ξ_1 ($\tilde{\mathrm{Pr}}(\xi_1)$) as follows. Let $g(X, Y) =$

$-\log \mathrm{P}_{X|Y}(X|Y)$. Then using the Markov inequality

$$\Pr(g(X,Y) \geq \lambda) \leq \frac{\mathbb{E}(g(X,Y))}{\lambda}.$$

Let $\lambda = 2\tilde{H}_\infty(X|Y)/\epsilon$. We have

$$\Pr(-\log \mathrm{P}_{X|Y}(X|Y) \geq \frac{2\tilde{H}_\infty(X|Y)}{\epsilon}) \leq \frac{\mathbb{E}_{x,y}(-\log \mathrm{P}_{X|Y}(x|y))}{2\tilde{H}_\infty(X|Y)/\epsilon} \tag{C.12}$$

$$= \frac{\mathbb{E}_{x,y}(-\log \mathrm{P}_{X|Y}(x|y))}{(2/\epsilon)\big(-\log \mathbb{E}_y \max_x \mathrm{P}_{X|Y}(x|y)\big)} \tag{C.13}$$

$$\leq \frac{-\log(\mathbb{E}_{x,y}\mathrm{P}_{X|Y}(x|y))}{(2/\epsilon)\big(-\log \mathbb{E}_y \max_x \mathrm{P}_{X|Y}(x|y)\big)} \tag{C.14}$$

$$\leq \frac{-\log(\mathbb{E}_y \max_x \mathrm{P}_{X|Y}(x|y))}{(2/\epsilon)\big(-\log \mathbb{E}_y \max_x \mathrm{P}_{X|Y}(x|y)\big)} \tag{C.15}$$

$$\Rightarrow \tilde{\Pr}(\xi_1) \leq \frac{\epsilon}{2}. \tag{C.16}$$

In above, (C.13) is by substituting the definition of conditional min-entropy, (C.14) is by using the Jensen's inequality [2], and finally (C.15) is by using $\max_x(\cdot)$ instead of $\mathbb{E}_x(\cdot)$.

To bound the average probability of ξ_2, $(\tilde{\Pr}(\xi_2))$, we note that for any $x' \in \mathcal{T}(X|y)$, the collision probability with any $x \in \mathcal{X}$, such that $x' \neq x$, is bounded by $\Pr[h_S(\hat{x}) = h_S(x)] \leq 2^{-t}$ (Definition C.2), and so the total probability that some element in $\mathcal{T}(X|y)$ collides with an element in $\mathcal{X}^n$ is $|\mathcal{T}(X|y)| \cdot 2^{-t}$. That is

$$\Pr(\xi_2) \leq |\mathcal{T}(X|y)| \cdot 2^{-t}.$$

On the other hand, since the probability of each element of $\mathcal{T}$ is bounded by $2^{-\lambda}$, we have $|\mathcal{T}(X|y)|.2^{-\lambda} \leq \Pr[\mathcal{T}(X|y))] \leq 1$, and we have $|\mathcal{T}(X|y)| \leq 2^{\lambda}$. By letting $t \geq \lambda - \log \frac{\epsilon}{2}$, we have

$$t \geq 2\tilde{H}_\infty(X|Y)/\epsilon - \log \epsilon - 1. \tag{C.17}$$

Thus, $\Pr(\xi_2) \leq \frac{2}{\epsilon}$ which implies $\tilde{\Pr}(\xi_2) \leq \frac{2}{\epsilon}$. Finally, we have $\tilde{\mathrm{P}}_e = \tilde{\Pr}(\xi_1) + \tilde{\Pr}(\xi_2) \leq \epsilon$. ■

Theorem C.1 relates the length of the ciphertext to the expected error probability of the protocol (ϵ) and the correlation of random strings x and y that is measured by the average conditional min-entropy of X given Y. Equation (C.17) clearly shows the relation between t and the average error probability: smaller ϵ gives larger t. This is expected as larger t provides more information about X to Bob for decapsulation.

The following theorem gives the maximum number of key bits that can be established using iK when the

[2] If X is a random variable and $\mathsf{f}(\cdot)$ is a convex function, then $\mathsf{f}\big(\mathbb{E}(X)\big) \leq \mathbb{E}\big(\mathsf{f}(X)\big)$.

adversary is not allowed to make any queries (encapsulation or decapsulation oracles), in order to bound its advantage by σ_0 for any computatinally unbounded adversary. The upperbound on the key lenngth is given by the correlation between the random strings x and z measured by $\tilde{H}_\infty(X|Z)$, t the output length of the hash function $\mathsf{h}_s(\cdot)$ and σ_0.

Theorem C.2. *Any established key using the iKEM* iK*, with the length of* $\ell \leq \tilde{H}_\infty(X|Z) - t + 2\log\sigma_0 + 2$ *is* σ_0*-indistinguishable against an adversary that does not have access to any encapsulation or decapsulation queries (*σ_0 *CPA secure).*

Proof. We show that in the key indistinguishability game of iKEM, the key that is generated by the protocol satisfies (C.9). Note that here $\mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena} = null$. We use Lemma C.1 and noting that a strongly universal hash function is also a UHF. Then for X and Z generated by $\mathsf{iK.Gen}$, we have

$$\mathbf{SD}\left(\Big((S, \mathsf{h}_S(X), Z), S', \mathsf{h}'_{S'}(X)\Big); \Big((S, \mathsf{h}_S(X), Z), S', U_\ell\Big)\right) \leq \frac{1}{2}\sqrt{2^{\ell - \tilde{H}_\infty(X|Z)}},$$

In using [45, lemma 2.2(b)], since the range of $\mathsf{h}_S(\cdot)$ has at most 2^t elements, we have

$$\tilde{H}_\infty(X|\mathsf{h}_S(X), Z) \geq \tilde{H}_\infty(X|Z) - t.$$

Therefore, by applying the Lemma C.1 we have

$$\begin{aligned}\mathbf{SD}\big((Z, \mathsf{h}_S(X), S, S', (\mathsf{h}'_{S'}(X));\\ (Z, \mathsf{h}_S(X), S, S', U_\ell)\big) \leq \frac{1}{2}\sqrt{2^{t+\ell-\tilde{H}_\infty(X|Z)}}.\end{aligned} \tag{C.18}$$

Thus, for $\ell \leq \tilde{H}_\infty(X|Z) - t + 2\log\sigma_0 + 2$, we have

$$\frac{1}{2}\sqrt{2^{t+\ell-\tilde{H}_\infty(X|Z)}} \leq \sigma_0, \tag{C.19}$$

and finally,

$$\mathbf{SD}((Z, C^*, K); (Z, C^*, U_{\mathcal{K}})) \leq \sigma_0. \ \blacksquare \tag{C.20}$$

We next consider a stronger computationally unbounded adversary that has access to q_e encapsulation queries (EnA), and derive maximum achievable key length from iK to bound the adversary's advantage in the corresponding distinguishing game by σ_e.

Theorem C.3. *Any established key using the iKEM* iK*, with the length of* $\ell \leq \frac{2+2\log\sigma_e+\tilde{H}_\infty(X|Z)}{q_e+1} - t$ *is* σ_e*-indistinguishable against an adversary with access to* q_e *encapsulation queries (*q_e*-bounded EnA).*

Proof. Each query to the encapsulation oracle gives a pair of matching key and ciphertext (c, k) to the adversary. The vector $\mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena} = (v_1^{ena}, \cdots, v_{q_e}^{ena})$ is the vector of adversary's received responses to their EnA queries, and reveal information about X to them. The remaining uncertainty about X that can be used for key extraction is $H_\infty(X|V_i^{ena} = v_i^{ena})$, where $v_i^{ena} = (c_i, k_i)$ and $c_i = (c_{0i}, s_i, s_i')$. Let the values of S and S' (in $\mathsf{h}_S(X)$ and $\mathsf{h}'_{S'}(X)$) in the i^{th} query's response, $c_i = (c_{0i}, s_i, s_i')$, be s_i and s_i'.

$$H_\infty(X|V_i^{ena} = v_i^{ena}) = H_\infty(X|C_i = c_i, K_i = k_i) \tag{C.21}$$

$$= -\log \max_x \Pr(X = x|, \mathsf{h}_{s_i}(X) = c_{0i}, \mathsf{h'}_{s_i'}(X) = k_i) \tag{C.22}$$

$$= -\log \max_x \frac{\Pr(X = x).\Pr(\mathsf{h}_{s_i}(x) = c_0, \mathsf{h'}_{s_i'}(x) = k)}{\Pr(\mathsf{h'}_{s_i'}(X) = k_i, \mathsf{h}_{s_i}(X) = c_{0i})} \tag{C.23}$$

$$\geq -\log \frac{2^{-H_\infty(X)}}{\Pr(\mathsf{h}_{s_i}(X) = c_{0i}, \mathsf{h'}_{s_i'}(X) = k_i)} \tag{C.24}$$

$$\geq -\log \frac{2^{-H_\infty(X)}}{\Pr(\mathsf{h}_{s_i}(X) = c_{0i}).\Pr(\mathsf{h'}_{s_i'}(X) = k_i)} \tag{C.25}$$

$$= -\log \frac{2^{-H_\infty(X)}}{2^{-t-\ell}} = H_\infty(X) - t - \ell \tag{C.26}$$

In above, (C.23) follows from (C.21) since $\Pr(\hat{\mathsf{h}}_{s_i'}(x) = k_i, \mathsf{h}_{s_i}(x) = c_{0i})$ is either 1 (for those x that satisfy the expression), or 0 (for those x that not satisfy the expression), so to maximize the probability, the value of x must satisfy the expression and therefore, $\Pr\big(\mathsf{h}_{s_i}(x) = c_{0i}, \mathsf{h'}_{s_i'}(x) = k_i\big) = 1$; (C.24) is obtained from (C.23) by replacing $\Pr(X = x)$ with $2^{-H_\infty(X)}$, the maximum probability; (C.25) follows from (C.24) by using the multiplicative inequality ($\Pr(AB) \geq \Pr(A).\Pr(B)$); and finally, (C.26) in obtained from (C.25) by using the strong universality of the hashes. When Z is also given, using a similar argument we have, $\tilde{H}_\infty(X|Z, C_i = c_i, K_i = k_i) \geq \tilde{H}_\infty(X|Z) - t - \ell$.

This is adversary's maximum uncertainty about X after making a query to the encapsulation oracle, and so each query decreases the remaining min-entropy of X by at most by $t + \ell$. Thus, after q_e queries we have $\tilde{H}_\infty(X|Z, \mathbf{V}_{\mathsf{A}}^{q_e\text{-}ena} = \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) \geq \tilde{H}_\infty(X|Z) - q_e(t + \ell)$. Now from (C.18) we have

$$\mathbf{SD}\bigg(\Big(Z, S, S', \mathsf{h}_S(X), \mathsf{h}'_{S'}(X), \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}\Big); \Big(Z, S, S', \mathsf{h}_S(X), U_\ell, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}\Big)\bigg) \leq \frac{1}{2}\sqrt{2^{(q_e+1)(t+\ell)-\tilde{H}_\infty(X|Z)}}.$$

Since $\ell \leq \frac{2+2\log\sigma_e+\tilde{H}_\infty(X|Z)}{q_e+1} - t$, we have,

$$\mathbf{SD}\Big(\Big(Z, S, S', \mathsf{h}_S(X), \mathsf{h}'_{S'}(X), \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}\Big); \Big(Z, S, S', \mathsf{h}_S(X), U_\ell, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}\Big)\Big) \leq \sigma_e,$$

and finally for $C^* = (h_S(X), S', S)$, the inequality (C.9) is satisfied . That is we have σ_e-indistinguishability against q_e EnA. ■

Theorem C.4. *Any established key using the iKEM* iK*, with the length of* $\ell \leq \min\{\frac{2+2\log\sigma_c+\tilde{H}_\infty(X|Z)}{q_c+1} - t, \log\frac{1}{\epsilon}\}$ *is* σ_c*-indistinguishable against an adversary with access to* q_c *decapsulation queries (*q_c*-bounded CCA).*

Proof. Consider the adversary $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ in the distinguishing game. Let $\mathbf{qr}_{\mathsf{A}_1}^{q_c\text{-}cca} = (qr_1^{cca}, \cdots, qr_j^{cca})$ and $\mathbf{v}_{\mathsf{A}_1}^{q_c\text{-}cca} = (v_1^{cca}, \cdots, v_j^{cca})$ denote A_1's queries and the corresponding responses. Similarly, let $\mathbf{qr}_{\mathsf{A}_2}^{q_c\text{-}cca} = (qr_{j+1}^{cca}, \cdots, qr_{q_c}^{cca})$ and $\mathbf{v}_{\mathsf{A}_2}^{q_c\text{-}cca} = (v_{j+1}^{cca}, \cdots, v_{q_c}^{cca})$ denote A_2's queries and responses, respectively.

For a decapsulation query $qr_i^{cca} = c_i = (c_{0i}, s_i, s'_i)$, the decapsulation oracle answers $v_i^{cca} = k_i$, which a key value, with probability $1-\epsilon$, and $v_i^{cca} =\perp$' with probability ϵ. If the decapsulation oracle outputs k_i, from (C.25) we have

$$H_\infty(X|V_i^{cca} = v_i^{cca}, QR_i^{cca} = qr_i^{cca}) = H_\infty(X|C_i = c_i, K_i = k_i) \geq H_\infty(X) - t - \ell$$

When the decapsulation oracle outputs $\perp$, from (C.26) we have

$$H_\infty(X|C_i = c_i, K_i =\perp) \geq -\log\frac{2^{-H_\infty(X)}}{\Pr(\mathsf{h}_{s_i}(X) = c_{0i}).\Pr(K =\perp)} = H_\infty(X) - t + \log\epsilon.$$

Thus, conditioned on Z, and after j queries by A_1,

$$\tilde{H}_\infty\big(X|Z, \mathbf{v}_{\mathsf{A}_1}^{q_c\text{-}cca}, \mathbf{qr}_{\mathsf{A}_1}^{q_c\text{-}cca}\big) \geq \tilde{H}_\infty(X|Z) - j.\big(t - \min(\ell, \log\frac{1}{\epsilon})\big).$$

After j queries, the challenge ciphertext $C^* = c^*$ is given. We have

$$\tilde{H}_\infty\big(X|Z, c^*, \mathbf{v}_{\mathsf{A}_1}^{q_c\text{-}cca}, \mathbf{qr}_{\mathsf{A}_1}^{q_c\text{-}cca}\big) \geq \tilde{H}_\infty(X|Z, c^*) - j.\big(t - \min(\ell, \log\frac{1}{\epsilon})\big),$$

and q_c-j new queries are made by A_2. They also reduce the uncertainty by $(q_c - j).\big(t - \min(\ell, \log\frac{1}{\epsilon})\big)$. We

Algo gK.Gen	**Algo** gK.Enc	**Algo** gK.Dec
For $i \leftarrow 1$ to ν	$(r_{A1}, \ldots, r_{A\nu}) \leftarrow \mathbf{r_A}$	$(r_{B1}, \ldots, r_{B\nu}) \leftarrow \mathbf{r_B}$
$(r_{Ai}, r_{Bi}, r_{Ei}) \xleftarrow{\$} \mathsf{gK.Gen}_i(\Theta)$	For $i \leftarrow 1$ to ν	$(c_1, \ldots, c_\nu) \leftarrow \mathbf{c}$
$\mathbf{r_A} \leftarrow (r_{A1}, \ldots, r_{A\nu})$	$(c_i, k_i) \xleftarrow{\$} \mathsf{gK.Enc}_i(r_{Ai})$	For $i \leftarrow 1$ to ν
$\mathbf{r_B} \leftarrow (r_{B1}, \ldots, r_{B\nu})$	$\mathbf{c} \leftarrow (c_1, ..., c_\nu)$	$k_i \leftarrow \mathsf{gK.Dec}_i(r_{Bi}, c_i)$
$\mathbf{r_E} \leftarrow (r_{E1}, \ldots, r_{E\nu})$	$k \leftarrow \mathsf{W}(k_1, \ldots, k_\nu, \mathbf{c})$	If $k_i = \perp$: Return $\perp$
Return$(\mathbf{r_A}, \mathbf{r_B}, \mathbf{r_E})$	Return$(k, \mathbf{c})$	$k \leftarrow \mathsf{W}(k_1, \ldots, k_\nu, \mathbf{c})$
		Return k

Figure C.5: gKEM Combiner

have

$$\tilde{H}_\infty\big(X|Z, c^*, \mathbf{qr}_{\mathsf{A}}^{q_c\text{-}cca}, \mathbf{v}_{\mathsf{A}}^{q_c\text{-}cca}\big) \geq \tilde{H}_\infty(X|Z, c^*) - q_c.\big(t - \min(\ell, \log\frac{1}{\epsilon})\big),$$

where $\mathbf{qr}_{\mathsf{A}}^{q_c\text{-}cca} = (\mathbf{qr}_{\mathsf{A}_1}^{q_c\text{-}cca}, \mathbf{qr}_{\mathsf{A}_2}^{q_c\text{-}cca})$ and $\mathbf{v}_{\mathsf{A}}^{q_c\text{-}cca} = (\mathbf{v}_{\mathsf{A}_1}^{q_c\text{-}cca}, \mathbf{v}_{\mathsf{A}_2}^{q_c\text{-}cca})$ and in using [45, lemma 2.2(b)] we have

$$\tilde{H}_\infty\big(X|Z, C^*, \mathbf{qr}_{\mathsf{A}}^{q_c\text{-}cca}, \mathbf{v}_{\mathsf{A}}^{q_c\text{-}cca}\big) \geq \tilde{H}_\infty(X|Z) - q_c.\big(t - \min(\ell, \log\frac{1}{\epsilon})\big) - t.$$

Finally, since $\ell \leq \min\{\frac{2+2\log\sigma_c + \tilde{H}_\infty(X|Z)}{q_c+1} - t, \log\frac{1}{\epsilon}\}$ and by using (C.18) we have

$$\mathbf{SD}\Big(\Big(Z, \mathbf{qr}_{\mathsf{A}}^{q_c\text{-}cca}, \mathbf{v}_{\mathsf{A}}^{q_c\text{-}cca}, S, S', \mathsf{h}_S(X), \mathsf{h}'_{S'}(X)\Big); \Big(Z, \mathbf{qr}_{\mathsf{A}}^{q_c\text{-}cca}, \mathbf{v}_{\mathsf{A}}^{q_c\text{-}cca}, S, S', \mathsf{h}_S(X), U_\ell\Big)\Big) \leq \sigma_c,$$

and for $C^* = (h_S(X), S', S)$, the inequality (C.9) is satisfied . That is we have σ_c-indistinguishability against q_c CCA. ■

C.4 gKEM combiners

Let for $i \in \{1, 2, \ldots, \nu\}$, $\mathsf{K}_i = (\mathsf{gK}_i.\mathsf{Gen}, \mathsf{gK}_i.\mathsf{Enc}, \mathsf{gK}_i.\mathsf{Dec})$ be a gKEM that has the session-key space $\mathcal{K}_i$, the triple of correlated random string sets $\mathcal{R}_{\mathcal{A}i}, \mathcal{R}_{\mathcal{B}i}$ and $\mathcal{R}_{\mathcal{E}i}$, and the ciphertext space $\mathcal{C}$. Suppose (R_{Ai}, R_{Bi}, R_{Ei}) is the triple of correlated random strings for each K_i, and each triple is independent of all the other triples. Let $\mathcal{K}^* = \mathcal{K}_1 \times \cdots \times \mathcal{K}_i \times \cdots \times \mathcal{K}_\nu$, and $\mathcal{R}_{\mathcal{A}} = \mathcal{R}_{\mathcal{A}1} \times \cdots \times \mathcal{R}_{\mathcal{A}i} \times \cdots \times \mathcal{R}_{\mathcal{A}\nu}$, $\mathcal{R}_{\mathcal{B}} = \mathcal{R}_{\mathcal{B}1} \times \cdots \times \mathcal{R}_{\mathcal{B}i} \times \cdots \times \mathcal{R}_{\mathcal{B}\nu}$, $\mathcal{R}_{\mathcal{E}} = \mathcal{R}_{\mathcal{E}1} \times \cdots \times \mathcal{R}_{\mathcal{E}i} \times \cdots \times \mathcal{R}_{\mathcal{E}\nu}$ and $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_i \times \cdots \times \mathcal{C}_\nu$. Let further $\mathcal{K}$ be an auxiliary finite session-key space.

Using Giason et al.'s approach [55] we define a *core function* $\mathsf{W} : \mathcal{K}^* \times \mathcal{C} \to \mathcal{K}$ for combining gKEMs: the gKEM combination with respect to W is a gKEM with session key space $\mathcal{K}$ that consists of the algorithms $\mathsf{gK.Gen}, \mathsf{gK.Enc}, \mathsf{gK.Dec}$ specified below.

The combiner must be secure if at least one of its components is. The challenge of gKEM combiner is that the ingredient gKEMs may be computational or iKEM, and the key indistinguishability in the two cases is against two different types of adversaries: computational and information theoretic, respectively, and one needs to consider this difference in the security of the resulting key. We consider the combination of ingredient gKEMs in the following cases:

1. All gKEMs are computationally secure.

2. One gKEM is information theoretically secure.

Case 1 is addressed in the work of [55] as gKEM definition when specialized to computational security, is identical to that of the KEM definition (Definition C.3). In the following we consider case 2. The case that there are multiple ingredient iKEMs, can be studied as case 2 with one of the iKEMs. Tighter bounds on the security of the combined gKEM will be our future work.

C.4.1 Combiners for iKEM and computational gKEMs

Consider a gKEM combiner for ν gKEMs, and without loss of generality, assume $\mathsf{K}_1 = (\mathsf{iK}_1.\mathsf{Gen}, \mathsf{iK}_1.\mathsf{Enc}, \mathsf{iK}_1.\mathsf{Dec})$ is an iKEM and $\mathsf{K}_i = (\mathsf{gK}_i.\mathsf{Gen}, \mathsf{gK}_i.\mathsf{Enc}, \mathsf{gK}_i.\mathsf{Dec})$ for $2 \leq i \leq \nu$ are computational gKEMs. We assume the iKEM and gKEMs produce the same length keys. Then the resulting key will have the following properties,

- If iKEM is secure (i.e. the initial correlation is correctly specified), then the combiner should result in an information theoretic secure key establishment protocol.

- If iKEM is not secure, the resulting key will be computationally secure as long as at least one of gKEM ingredients is computationally secure

The security of the final established key will depend on the security of the ingredient gKEMs, and in particular the number of queries of the two types, EnA and CCA, for each.

We first introduce a combiner which maintains security of ingredient gKEMs, assuming their security are against adversaries with access to decapsulation queries. That is the iKEM has security against a q_e-bounded EnA, and the computational gKEMs are CPA secure. The combiner will retain q_e-bounded EnA security of iKEM, and CPA security of the computational KEM, if the iKEM is not secure.

The XOR combiner.

Assume $\mathcal{K}_1 = \cdots = \mathcal{K}_\nu = \{0,1\}^\kappa$ are the corresponding key spaces for an iKEM K_1 and gKEMs K_2 to K_ν . The combiner with an XOR core function W, outputs the following key:

$$\mathsf{W}(k_1, \ldots, k_\nu) = \oplus_{i=1}^{\nu} k_i, \quad k_1, \ldots, k_\nu \in \{0,1\}^\kappa$$

Theorem C.5. *The XOR combiner that is used for combining an iKEM and a number of computational gKEMs, retains the CPA security of the gKEMs and the q_e-bounded EnA security of the iKEM.*

Proof. The proof that the combiner retains the CPA security of the gKEMs follows from [55, Lemma 1].

To show that the combiner retains the q_e-bounded EnA security of the iKEM, we use contradiction. Suppose there is an adversary $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ who breaks the q_e-bounded EnA security of the key $k = \oplus_{i=1}^{\nu} k_i$. Then we define an adversary $\mathsf{B} = (\mathsf{B}_1, \mathsf{B}_2)$ who uses A as a subroutine and breaks the q_e-bounded security of the iKEM. B_1 receives r_{E_1} and on its encapsulation queries receives $\mathbf{v}_{\mathsf{B}}^{q_e\text{-}ena} = \big((c_{1,1}, k_{1,1}), \ldots, (c_{1,q_e}, k_{1,q_e})\big)$. Then, for $2 \leq i \leq \nu$, B_1uses $\mathsf{gK.Gen}_i$ to generate (r'_{A_2}, r'_{E_2}) to (r'_{A_ν}, r'_{E_ν}) (generating r'_{B_i} is not necessary) and uses $\mathsf{gK.Enc}_i$ on each r'_{A_i} for q_e times to generate $\mathbf{v'}_i^{q_e\text{-}ena} = \big((c'_{i,1}, k'_{i,1}), \ldots, (c'_{i,q_e}, k'_{i,q_e})\big)$

B_1 then gives $\mathbf{r}_E = (r_{E_1}, r'_{E_2}, \ldots, r'_{E_\nu})$ to A_1 and on encapsulation queries of A_1 returns

$$\mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena} =$$
$$\big((c_{1,1}, \ldots, c'_{i,1}, \ldots, c'_{\nu,1}, k_{1,1} \oplus_{i=2}^{\nu} k'_{i,1}), \ldots, (c_{1,1}, \ldots, c'_{i,1}, \ldots, c'_{\nu,q_e}, k_{1,q_e} \oplus_{i=2}^{\nu} k'_{i,q_e})\big).$$

A_1 outputs st_1. Then B_2 receives (c_1^*, k_1^*) and sends st_1, $\mathbf{c}^* = (c_1^*, c'^*_2, \ldots, c'^*_\nu)$ and $k^* = k_1^* \oplus_{i=2}^{\nu} k'^*_i$ to A_2, where $(c'^*_i, \ldots, c'^*_\nu, k'^*_i)$ for $2 \leq i \leq \nu$ is obtained by the application of $\mathsf{gK.Enc}_i$ by B_2. Finally, B_2 outputs b' equal to A_2's output. The advantage of A and B are equal because k^* is a sample from uniform distribution only if k_1^* be a sample from uniform distribution. Since we assumed A breaks the q_e-bounded security of the combined gKEM then B can breaks the q_e-bounded security of the iKEM which is a contradiction. ■

PRF-then-XOR combiner.

The XOR combiner cannot maintain CCA security of the ingredient gKEMs. Giacon et al. [55] gave constructions of KEM combiners that retain CCA security of the ingredient KEMs. In the following we show the "PRF-then-XOR combiner" can be used for combining an iKEM and computational gKEMs. The resulting key will retain the CCA security of the computational gKEMs, and q_c-bounded CCA security of iKEM against a computational adversary. We first recall the definition of Pseudo-Random Functions (PRFs).

Pseudorandom functions. A function $\mathsf{F} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, for a finite key space $\mathcal{K}$, an input space $\mathcal{X}$, a finite

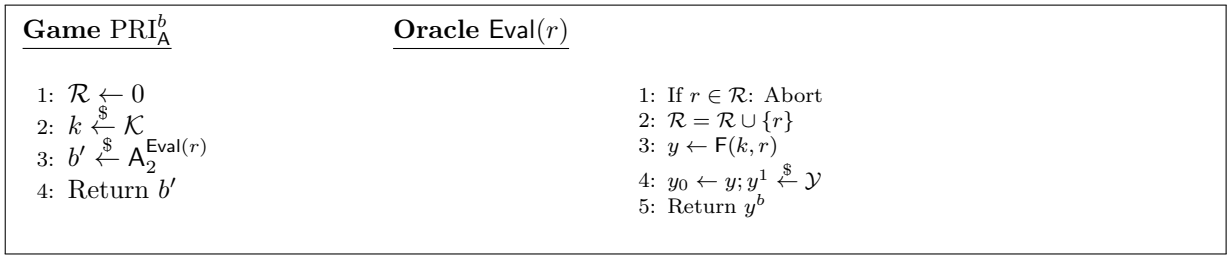

Figure C.6: A PRF distinguishing game

output space $\mathcal{Y}$, is a PRF if all practical adversaries A achieve a negligible advantage Adv^{PRF} defined as

$$Adv^{PRF}_{\mathsf{F},\mathsf{A}} \triangleq |\Pr[\mathrm{PRI}^0_{\mathsf{A}} = 1] - \Pr[\mathrm{PRI}^1_{\mathsf{A}} = 1]|,$$

where the games PRI^b for $b \in \{0, 1\}$ is defined in Figure C.6.

The PRF-then-XOR construction works as follows: for $i \in \{1, 2, \ldots, \nu\}$, let K_i be the ingredient gKEMs, with the corresponding session key space $\mathcal{K}_i$ and ciphertext space $\mathcal{C}_i$, and let $\mathcal{C}^i = \mathcal{C}_1 \times \cdots \times \mathcal{C}_{i-1} \times \mathcal{C}_{i+1} \times \cdots \times \mathcal{C}_\nu$ and $\mathcal{K}^i = \mathcal{K}_1 \times \cdots \times \mathcal{K}_{i-1} \times \mathcal{K}_{i+1} \times \cdots \times \mathcal{K}_\nu$. Further, assume $\mathsf{F}_i : \mathcal{K}_i \times \mathcal{C}^i \to \mathcal{K}$ be a (pseudorandom) function for all i. Then the core combiner function W is defined as follows

$$\mathsf{W}(k_1, \ldots, k_\nu, c_1..c_\nu) = \oplus_{i=1}^n \mathsf{F}_i(k_i, c_1..c_{i-1}c_{i+1}..c_\nu).$$

In the following we show that the above PRF-then-XOR combiner results in a CCA secure gKEM. The combiner retains the CCA security of its ingredient gKEMs, and reduces the q_c-bounded CCA security of the iKEM to the security of the PRF that is used in the combiner.

Theorem C.6. *Let $\mathsf{F}_i : \mathcal{C}^i \times \mathcal{K}_i \to \{0,1\}^r$ be PRFs, and the above PRF-then-XOR combiner is used for combining the iKEM K_1 and gKEMs K_i (for $2 \le i \le \nu$) to a single gKEM K. Then for adversaries A, B and C, for the combiner (information theoretic), iKEM (information theoretic) and PRF (computational), respectively, we have*

$$Adv^{kind\text{-}q_c\text{-}cca}_{\mathsf{K},\mathsf{A}} \le 2\big(Adv^{kind\text{-}cca}_{\mathsf{K}_i,\mathsf{B}} + Adv^{PRF}_{\mathsf{F}_i,\mathsf{C}}\big) \tag{C.27}$$

and

$$Adv^{kind\text{-}q_c\text{-}cca}_{\mathsf{K},\mathsf{A}} \le Adv^{kind\text{-}q_c\text{-}cca}_{\mathsf{K}_1,\mathsf{B}} + Adv^{PRF}_{\mathsf{F}_1,\mathsf{C}} \tag{C.28}$$

Proof. We define four games to prove the security of the PRF-then-XOR construction, namely Game^0, Game^1, Game^2 and Game^3. In these game Game^0 is indeed gKEM's distinguishing game when the challenge key is generated from the combiner and Game^3 is the distinguishing game when the challenge key is sampled

uniformly. In our proof Game^1 and Game^2 are the intermediate games that enable us to bound the final advantage of the adversary. Game^1 is obtained by substituting the iKEM's key with a uniformly random key and Game^2 is by replacing the output of the PRF function that takes the iKEM's key as an input with a uniformly random value.

The PRF-then-XOR construction for an iKEM K_1 and gKEM K_i works as follows

$$k = \mathsf{F}_1(k_1, c_2..c_\nu) \oplus_{i=2}^{\nu} \mathsf{F}_i(k_i, c_1..c_{i-1}c_{i+1}..c_\nu),$$

where k_1 and c_1 are corresponding key/ciphers from the iKEM K_1 and k_i and c_i are corresponding key/ciphers from the gKEM K_i.

From [55, Theorem 3], for $i \leq 2$ we have

$$Adv^{kind\text{-}cca}_{\mathsf{K},\mathsf{A}} \leq 2\big(Adv^{kind\text{-}cca}_{\mathsf{K}_i,\mathsf{B}} + Adv^{PRF}_{\mathsf{F}_i,\mathsf{C},}\big)$$

For security against q_c-bounded CCA, we define the following sequence of games. Note that $c^1 = c_2..c_\nu$ and $c^i = c_1..c_{i-1}c_{i+1}..c_\nu$. In each game the total number of q_c queries is allowed.

Claim C.1. $\Pr[\text{gKIND}^{q_c\text{-}cca-0}_{\mathsf{A}} = 1] = \Pr[\text{Game}^0_{\mathsf{A}} = 1]$.

This is straightforward from the definition of gKIND$^{q_c\text{-}cca-0}$.

Claim C.2. $|\Pr[\text{Game}^0_{\mathsf{A}} = 1] - \Pr[\text{Game}^1_{\mathsf{A}} = 1]| \leq Adv^{kind\text{-}q_c\text{-}cca}_{\mathsf{B},\mathsf{K}_1}$.

The only difference between Game^0 and Game^1 is that line 8 in Game^0 is replaced by lines 8 and 9 in Game^1, where the k_1 from $\mathsf{iK.Enc}$ is replaced by k_1 sampled uniformly random. The advantage of distinguishing between these two cases (while making q queries) is $Adv^{kind\text{-}q_c\text{-}cca}_{\mathsf{B},\mathsf{K}_1}$. Thuse, $|\Pr[\text{Game}^0_{\mathsf{A}} = 1] - \Pr[\text{Game}^1_{\mathsf{A}} = 1]| \leq Adv^{kind\text{-}q_c\text{-}cca}_{\mathsf{K}_1,\mathsf{B}}$.

Claim C.3. $|\Pr[\text{Game}^1_{\mathsf{A}} = 1] - \Pr[\text{Game}^2_{\mathsf{A}} = 1]| \leq Adv^{PRF}_{\mathsf{F}_1,\mathsf{C}}$.

The difference between these two games is that $\mathsf{F}_1(k_1, c^1)$ (with k_1 uniformly sampled) is replaced by f_1 sampled from the uniform distribution. The advantage of distinguishing between $\mathsf{F}_1(k_1, c^1)$ and f_1 is the advantage of the PRF F_1 that is $Adv^{PRF}_{\mathsf{C},\mathsf{F}_1}$. So the distinguishing advantage of two games is upper-bounded by $Adv^{PRF}_{\mathsf{C},\mathsf{F}_1}$.

Claim C.4. $\Pr[\text{Game}^2_{\mathsf{A}} = 1] = \Pr[\text{Game}^3_{\mathsf{A}} = 1]$.

The difference between two games is that k^* in Game^2 is $f_1 \oplus_{i=2}^{n} \mathsf{F}_i(k_i, c^i)$ while k^* is sampled uniformly random in Game^3. However, since f_1 in Game^2 is sampled uniformly random, then k^* in Game^2 is uniform and two games become the same.

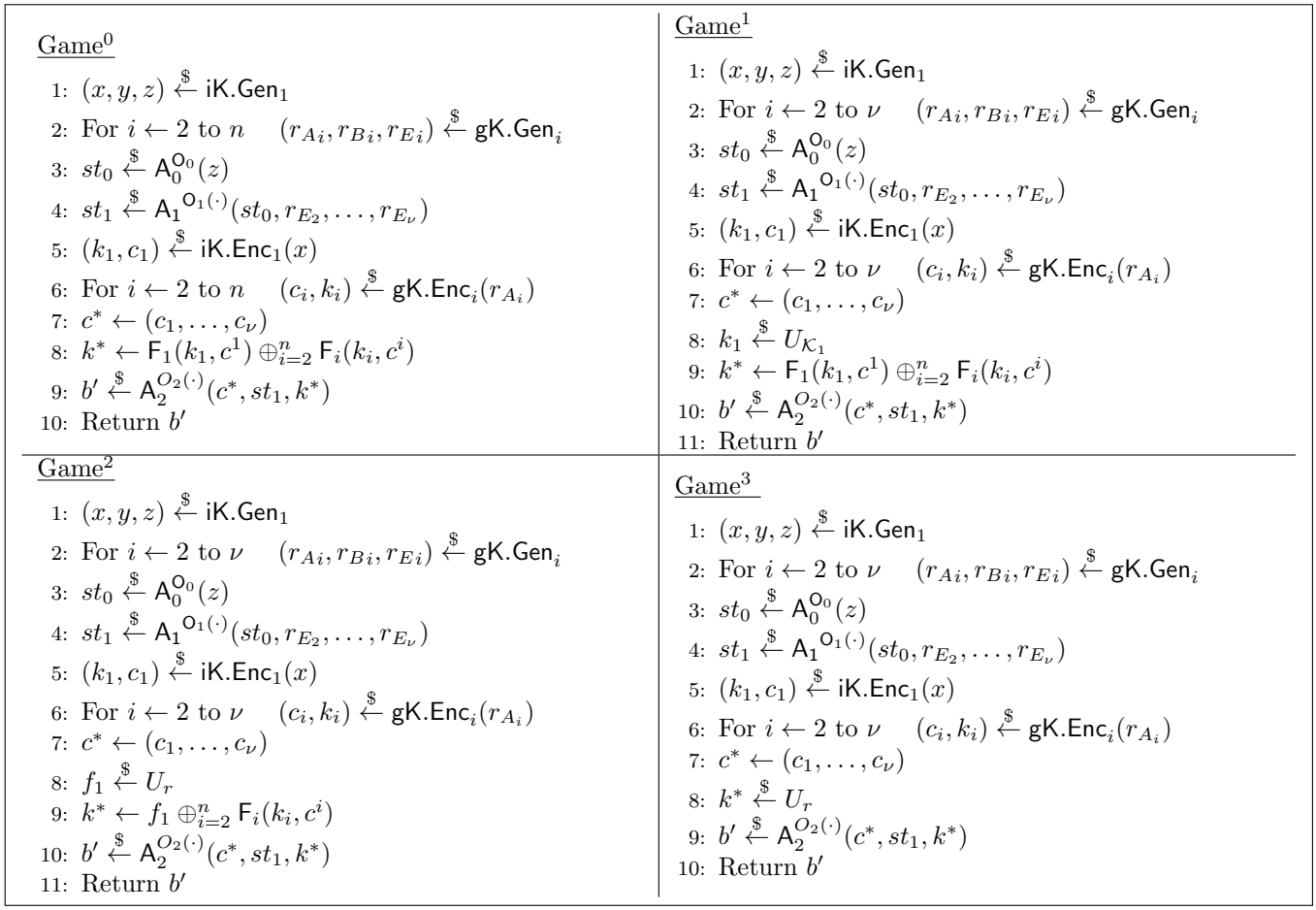

Figure C.7: Four close games to prove the security of the PRF-then-XOR combiner

Claim C.5. $\Pr[\mathrm{gKIND}_{\mathsf{A}}^{q_c\text{-}cca\text{-}1} = 1] = \Pr[\mathrm{Game}_{\mathsf{A}}^3 = 1]$.

This is straightforward from the definition of $\mathrm{gKIND}^{q_c\text{-}cca\text{-}1}$.

Proof of the second part of Theorem C.6. From Claims 2 to 6 we have

$$|\Pr[\mathrm{gKIND}_{\mathsf{A}}^{q_c\text{-}cca\text{-}0} = 1] - \Pr[\mathrm{gKIND}_{\mathsf{A}}^{q_c\text{-}cca\text{-}1} = 1]| \leq Adv_{\mathsf{K}_1,\mathsf{B}}^{kind\text{-}q_c\text{-}cca} + Adv_{\mathsf{F}_1,\mathsf{C}}^{PRF},$$

which proves (C.28). ■

Remark C.1. *From (C.28), we see that the security of the iKEM is reduced to the security of the PRF which a computationally secure primitive. Thus the resulting gKEM will not retain the information theoretic security of the iKEM.*

Constructing a combiner that retain information theoretic security of an ingredient iKEM is an interesting

open question.

C.5 Related works

KEM framework. KEM/DEM paradigm is widely used as a PKE for encrypting arbitrary length messages. This approach was first formalized by Cramer and Shoup [31, 127], and the relation between different security notions of KEM, DEM and the resulting hybrid encryption scheme is given in [69]. Generic constructions for KEM from standard public-key encryption schemes are proposed by Dent [38]. Identity-based KEMs were introduced by Bentahar et al. [16] and a generic construction was given. Other IB-KEMs were proposed in [27, 53, 63]. CPA secure KEMs using post-quantom assumptions are given in [41] (LWE based) and [101] (lattice based) and a post-quantum latice-based CCA secure KEM is proposed recently in [21].

Information theoretic key agreement in source model was first studied by Maurer [89, 92], and Ahlswede and Csiszár [2] , and extended to general IID distributions by Maurer and Wolf [93]. Implementation of key agreement protocols and engineering techniques for correlation generation between devices in wireless setting, have been extensively studied (see the review paper [147] and the references therein). The extension of the secret-key agreement to more than two parties was studied by Csiszár and Narayan [35]. Variants of this problem have been studied in the "fuzzy Extractors" context [44], where the goal is to turn noisy information (like two noisy readings of bio-metric information) into keys usable for cryptographic application. The two main steps in information theoretic key agreement are *reconciliation* where the goal is to arrive at a common random string by legitimate parties, and *privacy amplification* where the goal is to extract a secret key from the shared string. Both these steps have been widely studied [13, 96, 108]. The feasibility of a two party information theoretic key agreement protocol under active adversaries (who can perform the (wo)man-in-the- middle attack), was first shown by Renner and Wolf [106]. A practical protocol was then proposed by Dodis et al. [46] for the setting where correlated variables are "close" according to some distance metric. An interactive protocol based on [46] was proposed for the more general setting with less entropy loss by Kanukurthi and Reyzin [79].

Combining cryptographic primitives. Shannon studied the security implications of multiple encryption for the first time. He suggested to use "weighted sum" or "product ciphers" to combine two different secrecy systems resulting in a more secure system [115] . Combining encryption systems for the purpose of security amplification was further explored in symmetric-key settings under the "cascade cipher" name [51, 91]. Combining cryptographic primitives promise two benefits: (i) stronger security guarantees as noted in [7] and [3] and also papers on cascade ciphers, and (ii) ensuring security as long as at least one of the components remains secure. This approach is used in [42, 148], and [70], where Chosen ciphertext security

of multiple encryption is considered. Harnik et al. [64] defined the term "robust combiner" to formalize such combinations for different cryptographic premitives. A combiner for KEMs is studied in the recent work by Giacon et al. [55] which proposed various KEM combiner constructions.

C.6 Concluding remarks

We initiated the study of information theoretic KEM, that we called iKEM, by proposing a generalization of KEM to gKEM to provide a unifying framework for the study of iKEMs and traditional computational KEMs. iKEMs require initial correlated inputs for the parties. We constructed an iKEM when this initial correlation is modelled by a family of probability distributions and evaluated its security when Eve has a bounded number of encapsulation, or decapsulation queries. We also defined and constructed combiners for combining the two types of KEMs. iKEMs significantly increase the set of available gKEMs with post-quantum security, and the combiners improve robustness of KEMs in practice. iKEMs have the unique security property of being secure against offline attacks that is particularly important in long-term security.

There are numerous interesting open questions that arise from our work, including constructing iKEMs for other initial settings such the one considered in fuzzy extractors, and designing combiners that retain information theoretic security of an ingredient iKEM.

Appendix A

Proof of Lemma C.2. The proof has two parts:

(a) Suppose a given gKEM in $\sigma(n)$- indistinguishable, then (C.9) holds. Because if it doesn't, for the view $\mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}$, there exist a set $\mathcal{W} \subset \mathcal{R}_E \times \mathcal{K} \times \mathcal{C}$ for which

$$(\Pr\left([]\right)(R_E, , C^*, K^* | \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) \in \mathcal{W}] - \Pr\left([]\right)(R_E, C^*, U_{\mathcal{K}} | \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) \in \mathcal{W}]) > \sigma(n).$$

We use $\mathcal{W}$ and define an adversary algorithm A^* with $\text{gKIND}_{\mathsf{iK},\mathsf{A}}^{q_e\text{-}ena\text{-}b}(n) > \sigma(n)$ that contradicts the assumption.

(b) Suppose (C.9) holds then the corresponding gKEM is $\sigma(n)$-indistinguishable. To prove this let $\mathsf{F}_{\mathsf{A}} : \mathcal{R}_E \times \mathcal{K} \times \mathcal{C} \to \{0,1\}$ be an arbitrary function that takes A's inputs (r_E,c^*, k^* and $\mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}$) and output

0 or 1. Then we have

$$
\begin{aligned}
&Adv^{gkind\text{-}atk}_{\mathsf{iK},\mathsf{A}}(n) \\
&\leq \max_{\mathsf{F_A}} |\Pr\left([]\, \mathsf{F_A}(R_E, C^*, K^*, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) = 1\right] - \Pr\left([]\, \mathsf{F_A}(R_E, C^*, U_{\mathcal{K}}, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) = 1\right].
\end{aligned}
$$

Let $\mathcal{W} \subset \mathcal{R}_E \times \mathcal{K} \times \mathcal{C}$ be the set for which $(\Pr\left([]\, (R_E, C^*, K^* | \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) \in \mathcal{W}\right] - \Pr\left([]\, (R_E, C^*, U_{\mathcal{K}} | \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) \in \mathcal{W}\right])$ is maximized, then define $\mathsf{F_A}(\cdot)$ to be 1 only if its input is in $\mathcal{W}$. From the definition of the *statistical distance* (Definition C.1), it is easy to see that

$$
\begin{aligned}
&\leq \max_{\mathsf{F_A}} |\Pr\left([]\, \mathsf{F_A}(R_E, C^*, K^*, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) = 1\right] - \Pr\left([]\, \mathsf{F_A}(R_E, C^*, U_{\mathcal{K}}, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}) = 1\right] \\
&= \mathbf{SD}\big((R_E, C^*, K^*, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}); (R_E, C^*, U_{\mathcal{K}}, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena})\big),
\end{aligned}
$$

and we have

$$
Adv^{gkind\text{-}atk}_{\mathsf{iK},\mathsf{A}}(n) \leq \mathbf{SD}\big((R_E, C^*, K^*, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena}); (R_E, C^*, U_{\mathcal{K}}, \mathbf{v}_{\mathsf{A}}^{q_e\text{-}ena})\big) \leq \sigma(n) \ \blacksquare
$$

Proof of Lemma 3. The proof is identical to the proof of Lemma C.2 except that the probability distribution is conditioned on $\mathbf{qr}_{\mathsf{A}}^{q_c\text{-}cca}$, the vector of adversary's queries. ■

Copyright Permissions

SPRINGER NATURE LICENSE
TERMS AND CONDITIONS

May 11, 2020

This Agreement between University of calgary -- setareh Sharifian ("You") and Springer Nature ("Springer Nature") consists of your license details and the terms and conditions provided by Springer Nature and Copyright Clearance Center.

License Number	4826080789615
License date	May 11, 2020
Licensed Content Publisher	Springer Nature
Licensed Content Publication	Springer eBook
Licensed Content Title	Hash-then-Encode: A Modular Semantically Secure Wiretap Code
Licensed Content Author	Setareh Sharifian, Fuchun Lin, Reihaneh Safavi-Naini
Licensed Content Date	Jan 1, 2018
Type of Use	Thesis/Dissertation
Requestor type	academic/university or research institute
Format	print and electronic
Portion	full article/chapter

Will you be translating?	no
Circulation/distribution	1 - 29
Author of this Springer Nature content	yes
Title	Contributions to Information Theoretically Secure Communication
Institution name	University of Calgary
Expected presentation date	May 2020
Requestor Location	University of calgary 5136 vanstone cres NW Calgary, AB T3k0w6 Canada Attn: University of calgary
Total	0.00 USD

Terms and Conditions

Springer Nature Customer Service Centre GmbH
Terms and Conditions

This agreement sets out the terms and conditions of the licence (the **Licence**) between you and **Springer Nature Customer Service Centre GmbH** (the **Licensor**). By clicking 'accept' and completing the transaction for the material (**Licensed Material**), you also confirm your acceptance of these terms and conditions.

1. Grant of License

1. 1. The Licensor grants you a personal, non-exclusive, non-transferable, world-wide licence to reproduce the Licensed Material for the purpose specified in your order only. Licences are granted for the specific use requested in the order and for no other use, subject to the conditions below.

1. 2. The Licensor warrants that it has, to the best of its knowledge, the rights to license reuse of the Licensed Material. However, you should ensure that the material you are requesting is original to the Licensor and does not carry the copyright of another entity (as credited in the published version).

1. 3. If the credit line on any part of the material you have requested indicates that it was reprinted or adapted with permission from another source, then you should also seek permission from that source to reuse the material.

2. Scope of Licence

2. 1. You may only use the Licensed Content in the manner and to the extent permitted by these Ts&Cs and any applicable laws.

2. 2. A separate licence may be required for any additional use of the Licensed Material, e.g. where a licence has been purchased for print only use, separate permission must be obtained for electronic re-use. Similarly, a licence is only valid in the language selected and does not apply for editions in other languages unless additional translation rights have been granted separately in the licence. Any content owned by third parties are expressly excluded from the licence.

2. 3. Similarly, rights for additional components such as custom editions and derivatives require additional permission and may be subject to an additional fee. Please apply to Journalpermissions@springernature.com/bookpermissions@springernature.com for these rights.

2. 4. Where permission has been granted **free of charge** for material in print, permission may also be granted for any electronic version of that work, provided that the material is incidental to your work as a whole and that the electronic version is essentially equivalent to, or substitutes for, the print version.

2. 5. An alternative scope of licence may apply to signatories of the STM Permissions Guidelines, as amended from time to time.

3. Duration of Licence

3. 1. A licence for is valid from the date of purchase ('Licence Date') at the end of the relevant period in the below table:

Scope of Licence	Duration of Licence
Post on a website	12 months
Presentations	12 months
Books and journals	Lifetime of the edition in the language purchased

4. Acknowledgement

4. 1. The Licensor's permission must be acknowledged next to the Licenced Material in print. In electronic form, this acknowledgement must be visible at the same time as the figures/tables/illustrations or abstract, and must be hyperlinked to the journal/book's homepage. Our required acknowledgement format is in the Appendix below.

5. Restrictions on use

5. 1. Use of the Licensed Material may be permitted for incidental promotional use and minor editing privileges e.g. minor adaptations of single figures, changes of format, colour and/or style where the adaptation is credited as set out in Appendix 1 below. Any other changes including but not limited to, cropping, adapting, omitting material that affect the meaning, intention or moral rights of the author are strictly prohibited.

5. 2. You must not use any Licensed Material as part of any design or trademark.

5. 3. Licensed Material may be used in Open Access Publications (OAP) before publication by Springer Nature, but any Licensed Material must be removed from OAP sites prior to final publication.

6. Ownership of Rights

6. 1. Licensed Material remains the property of either Licensor or the relevant third party and any rights not explicitly granted herein are expressly reserved.

7. Warranty

IN NO EVENT SHALL LICENSOR BE LIABLE TO YOU OR ANY OTHER PARTY OR ANY OTHER PERSON OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, HOWEVER CAUSED, ARISING OUT OF OR IN CONNECTION WITH THE DOWNLOADING, VIEWING OR USE OF THE MATERIALS REGARDLESS OF THE FORM OF ACTION, WHETHER FOR BREACH OF CONTRACT, BREACH OF WARRANTY, TORT, NEGLIGENCE, INFRINGEMENT

OR OTHERWISE (INCLUDING, WITHOUT LIMITATION, DAMAGES BASED ON LOSS OF PROFITS, DATA, FILES, USE, BUSINESS OPPORTUNITY OR CLAIMS OF THIRD PARTIES), AND
WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY PROVIDED HEREIN.

8. Limitations

8. 1. ***BOOKS ONLY:***Where '**reuse in a dissertation/thesis**' has been selected the following terms apply: Print rights of the final author's accepted manuscript (for clarity, NOT the published version) for up to 100 copies, electronic rights for use only on a personal website or institutional repository as defined by the Sherpa guideline (www.sherpa.ac.uk/romeo/).

9. Termination and Cancellation

9. 1. Licences will expire after the period shown in Clause 3 (above).

9. 2. Licensee reserves the right to terminate the Licence in the event that payment is not received in full or if there has been a breach of this agreement by you.

Appendix 1 — Acknowledgements:

For Journal Content:
Reprinted by permission from [**the Licensor**]: [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT**] (year of publication)

For **Advance Online Publication papers:**
Reprinted by permission from [**the Licensor**]: [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT**] (year of publication), advance online publication, day month year (doi: 10.1038/sj.[JOURNAL ACRONYM].)

For Adaptations/Translations:
Adapted/Translated by permission from [**the Licensor**]: [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT**] (year of publication)

Note: For any republication from the British Journal of Cancer, the following

credit line style applies:

Reprinted/adapted/translated by permission from [**the Licensor**]: on behalf of Cancer Research UK: : [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT]** (year of publication)

For **Advance Online Publication** papers:
Reprinted by permission from The [**the Licensor**]: on behalf of Cancer Research UK: [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT**] (year of publication), advance online publication, day month year (doi: 10.1038/sj. [JOURNAL ACRONYM])

For Book content:
Reprinted/adapted by permission from [**the Licensor**]: [**Book Publisher** (e.g. Palgrave Macmillan, Springer etc) [**Book Title**] by [**Book author**(s)] [**COPYRIGHT**] (year of publication)

Other Conditions:

Version 1.2

Questions? customercare@copyright.com or +1-855-239-3415 (toll free in the US) or +1-978-646-2777.

SPRINGER NATURE LICENSE
TERMS AND CONDITIONS

May 11, 2020

This Agreement between University of calgary -- setareh Sharifian ("You") and Springer Nature ("Springer Nature") consists of your license details and the terms and conditions provided by Springer Nature and Copyright Clearance Center.

License Number	4826080983057
License date	May 11, 2020
Licensed Content Publisher	Springer Nature
Licensed Content Publication	Springer eBook
Licensed Content Title	A Virtual Wiretap Channel for Secure Message Transmission
Licensed Content Author	Setareh Sharifian, Reihaneh Safavi-Naini, Fuchun Lin
Licensed Content Date	Jan 1, 2017
Type of Use	Thesis/Dissertation
Requestor type	academic/university or research institute
Format	print and electronic
Portion	full article/chapter

Will you be translating?	no
Circulation/distribution	1 - 29
Author of this Springer Nature content	yes
Title	Contributions to Information Theoretically Secure Communication
Institution name	University of Calgary
Expected presentation date	May 2020
Requestor Location	University of calgary 5136 vanstone cres NW Calgary, AB T3k0w6 Canada Attn: University of calgary
Total	0.00 USD

Terms and Conditions

Springer Nature Customer Service Centre GmbH
Terms and Conditions

This agreement sets out the terms and conditions of the licence (the **Licence**) between you and **Springer Nature Customer Service Centre GmbH** (the **Licensor**). By clicking 'accept' and completing the transaction for the material (**Licensed Material**), you also confirm your acceptance of these terms and conditions.

1. Grant of License

1. 1. The Licensor grants you a personal, non-exclusive, non-transferable, world-wide licence to reproduce the Licensed Material for the purpose specified in your order only. Licences are granted for the specific use requested in the order and for no other use, subject to the conditions below.

1. 2. The Licensor warrants that it has, to the best of its knowledge, the rights to license reuse of the Licensed Material. However, you should ensure that the material you are requesting is original to the Licensor and does not carry the copyright of another entity (as credited in the published version).

1. 3. If the credit line on any part of the material you have requested indicates that it was reprinted or adapted with permission from another source, then you should also seek permission from that source to reuse the material.

2. Scope of Licence

2. 1. You may only use the Licensed Content in the manner and to the extent permitted by these Ts&Cs and any applicable laws.

2. 2. A separate licence may be required for any additional use of the Licensed Material, e.g. where a licence has been purchased for print only use, separate permission must be obtained for electronic re-use. Similarly, a licence is only valid in the language selected and does not apply for editions in other languages unless additional translation rights have been granted separately in the licence. Any content owned by third parties are expressly excluded from the licence.

2. 3. Similarly, rights for additional components such as custom editions and derivatives require additional permission and may be subject to an additional fee. Please apply to Journalpermissions@springernature.com/bookpermissions@springernature.com for these rights.

2. 4. Where permission has been granted **free of charge** for material in print, permission may also be granted for any electronic version of that work, provided that the material is incidental to your work as a whole and that the electronic version is essentially equivalent to, or substitutes for, the print version.

2. 5. An alternative scope of licence may apply to signatories of the STM Permissions Guidelines, as amended from time to time.

3. Duration of Licence

3. 1. A licence for is valid from the date of purchase ('Licence Date') at the end of the relevant period in the below table:

Scope of Licence	Duration of Licence
Post on a website	12 months
Presentations	12 months
Books and journals	Lifetime of the edition in the language purchased

4. Acknowledgement

4. 1. The Licensor's permission must be acknowledged next to the Licenced Material in print. In electronic form, this acknowledgement must be visible at the same time as the figures/tables/illustrations or abstract, and must be hyperlinked to the journal/book's homepage. Our required acknowledgement format is in the Appendix below.

5. Restrictions on use

5. 1. Use of the Licensed Material may be permitted for incidental promotional use and minor editing privileges e.g. minor adaptations of single figures, changes of format, colour and/or style where the adaptation is credited as set out in Appendix 1 below. Any other changes including but not limited to, cropping, adapting, omitting material that affect the meaning, intention or moral rights of the author are strictly prohibited.

5. 2. You must not use any Licensed Material as part of any design or trademark.

5. 3. Licensed Material may be used in Open Access Publications (OAP) before publication by Springer Nature, but any Licensed Material must be removed from OAP sites prior to final publication.

6. Ownership of Rights

6. 1. Licensed Material remains the property of either Licensor or the relevant third party and any rights not explicitly granted herein are expressly reserved.

7. Warranty

IN NO EVENT SHALL LICENSOR BE LIABLE TO YOU OR ANY OTHER PARTY OR ANY OTHER PERSON OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, HOWEVER CAUSED, ARISING OUT OF OR IN CONNECTION WITH THE DOWNLOADING, VIEWING OR USE OF THE MATERIALS REGARDLESS OF THE FORM OF ACTION, WHETHER FOR BREACH OF CONTRACT, BREACH OF WARRANTY, TORT, NEGLIGENCE, INFRINGEMENT

OR OTHERWISE (INCLUDING, WITHOUT LIMITATION, DAMAGES BASED ON LOSS OF PROFITS, DATA, FILES, USE, BUSINESS OPPORTUNITY OR CLAIMS OF THIRD PARTIES), AND
WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY PROVIDED HEREIN.

8. Limitations

8. 1. ***BOOKS ONLY:***Where '**reuse in a dissertation/thesis**' has been selected the following terms apply: Print rights of the final author's accepted manuscript (for clarity, NOT the published version) for up to 100 copies, electronic rights for use only on a personal website or institutional repository as defined by the Sherpa guideline (www.sherpa.ac.uk/romeo/).

9. Termination and Cancellation

9. 1. Licences will expire after the period shown in Clause 3 (above).

9. 2. Licensee reserves the right to terminate the Licence in the event that payment is not received in full or if there has been a breach of this agreement by you.

Appendix 1 — Acknowledgements:

For Journal Content:
Reprinted by permission from [**the Licensor**]: [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT**] (year of publication)

For **Advance Online Publication papers:**
Reprinted by permission from [**the Licensor**]: [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT**] (year of publication), advance online publication, day month year (doi: 10.1038/sj.[JOURNAL ACRONYM].)

For Adaptations/Translations:
Adapted/Translated by permission from [**the Licensor**]: [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT**] (year of publication)

Note: For any republication from the British Journal of Cancer, the following

credit line style applies:

Reprinted/adapted/translated by permission from [**the Licensor**]: on behalf of Cancer Research UK: : [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT]** (year of publication)

For **Advance Online Publication** papers:
Reprinted by permission from The [**the Licensor**]: on behalf of Cancer Research UK: [**Journal Publisher** (e.g. Nature/Springer/Palgrave)] [**JOURNAL NAME**] [**REFERENCE CITATION** (Article name, Author(s) Name), [**COPYRIGHT**] (year of publication), advance online publication, day month year (doi: 10.1038/sj. [JOURNAL ACRONYM])

For Book content:
Reprinted/adapted by permission from [**the Licensor**]: [**Book Publisher** (e.g. Palgrave Macmillan, Springer etc) [**Book Title**] by [**Book author**(s)] [**COPYRIGHT**] (year of publication)

Other Conditions:

Version 1.2

Questions? customercare@copyright.com or +1-855-239-3415 (toll free in the US) or +1-978-646-2777.

A Modular Semantically Secure Wiretap Code with Shared Key for Weakly Symmetric Channels

Conference Proceedings: 2019 IEEE Information Theory Workshop (ITW)

Author: Setareh Sharifian

Publisher: IEEE

Date: Aug. 2019

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Secret key agreement using a virtual wiretap channel

Conference Proceedings:
IEEE INFOCOM 2017 - IEEE Conference on Computer Communications

Author: Setareh Sharifian

Publisher: IEEE

Date: May 2017

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW