University of Calgary

PRISM Repository **https://prism.ucalgary.ca**

The Vault Open Theses and Dissertations

2012-12-12

Information Theoretic Security over Physical-Layer Channels

Ahmadi, Hadi

Ahmadi, H. (2012). Information Theoretic Security over Physical-Layer Channels (Doctoral thesis, University of Calgary, Calgary, Canada). Retrieved from https://prism.ucalgary.ca. doi:10.11575/PRISM/26527 http://hdl.handle.net/11023/341

Downloaded from PRISM Repository, University of Calgary

UNIVERSITY OF CALGARY

Information Theoretic Security over Physical-Layer Channels

by

Hadi Ahmadi

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER SCIENCE

CALGARY, ALBERTA

DECEMBER, 2012

© Hadi Ahmadi 2012

Abstract

Wyner [96] proved that unconditionally secure communication over noisy channels is possible if the wiretapping channel is noisier than the main channel. The work has developed the following belief: Physical-channel characteristics are great resources to build security functionalities in the information-theoretic framework. We follow this belief and investigate the three problems of *secret key establishment*, *manipulation detection*, and *distance bounding verification* over physical-layer channels.

We investigate secret key establishment (SKE) between Alice and Bob when they are connected through a pair of noisy wiretap channels with leakage to Eve. Our results show the possibility of SKE even in cases where the main channels are noisier than Eve's channels. We then notice two implicit assumptions of this work: (i) local randomness is freely available, and (ii) the wiretap channels are independent. We remove Assumption (i) by considering no local randomness for the parties. The results appreciate the role of noise as a single resource for randomness derivation and key generation in this setting. Regarding the second assumption, we consider the general two-way wiretap channel, where simultaneous data transmission can help achieve higher key rates. We show under what condition our security requirements can be strengthened without sacrificing the SK capacity.

We consider manipulation detection against physical-layer adversaries noticing their limitations. We define leakage-resilient algebraic manipulation detection (LR-AMD) codes and prove optimal LR-AMD code constructions in general and special leakage scenarios. We show two applications of these codes: (i) robust nonperfect secret sharing and (ii) manipulation detection over wiretap channels. We then discuss how these codes can be composed with other primitives to guarantee bitwise manipulation detection and SKE against active adversaries over binary wiretap channels.

Distance bounding verification (DBV) allows a verifier to check an upper bound on a claimed distance from a prover. We study DBV over physical channels with security against distance fraud (DFA), mafia fraud (MFA) and terrorist fraud (TFA) attacks. We show efficient DFA- and MFA-secure protocols only using physical channel properties. We further prove that TFA-security becomes feasible if the parties' communication is limited by the bounded retrieval model (BRM).

Acknowledgements

First and foremost, I convey my special thanks to my supervisor, Dr. Rei Safavi-Naini, who provided me with an extra-ordinary support and valuable guidance throughout this work. I am the most grateful to Rei due to her influence on my philosophy of research which turned my thesis into a successful piece of work.

I would be remiss if I did not acknowledge my wife, Nastaran Pedrood, who was there for me in all moments of happiness and sadness over these years. I would not be able to accomplish this work without her encouragement and support. I am also thankful to my family back home who have always been giving me hope and inspiration towards finishing my PhD research.

I would also like to thank my supervisory committee members, Dr. Zongpeng Li, Dr. Payman Mohassel, Dr. Philipp Woelfel for their technical advises and comments on my work. My sincere thanks also go to Dr. Wolfgang Tittel 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.

Finally, I would like to acknowledge the financial support I received as teaching and research assistantships as well as scholarships via the University of Calgary and the Alberta Innovates Technology Futures.

Dedicated to my wife and my dad.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Abbreviations

Abbreviation	Definition
2.	
2BSWC	a pair of independent BSWCs
2BSWC^{-r}	2BSWC without initial randomness
2DMWC	a pair of independent DMWCs
2DMWC^{-r}	2DMWC without initial randomness
A.	
AEP	Asymptotic Equipartition Property
AMD	Algebraic Manipulation Detection
AoA	Angle of Arrival
B.	
BEWC	Binary Erasure Wiretap Channel
BLR-AMD	Block Leakage Resilient AMD
BPSK	Binary Phase Shift Key
BRM	Bounded retrieval Model
BSC	Binary Symmetric Channel
BSWC	Binary Symmetric Wiretap Channel
D.	
DB	Distance Bounding
DBV	Distance Bounding Verification
DFA	Distance Fraud Attack
DHKE	Diffie-Hellman Key Exchange
DLP	Discrete Logarithm Problem
DMWC	Discrete Memoryless Wiretap Channel
DM	Discrete Memoryless
DMC	Discrete Memoryless Channel
DMMS	Discrete Memoryless Multiple Source
DMS	Discrete Memoryless Source
DMWC	Discrete Memoryless Wiretap Channel
E.	
EWC	Erasure Wiretap Channel
G.	
GPS	Global Positioning System
GWC	Gaussian Wiretap Channel

L.

LPFC	Limited Public Forward Channel
LR-AMD	Leakage Resilient AMD

M.

MAC	Message Authentication Code
MAD	Mutual Authentication with Distance bounding
MFA	Mafia Fraud Attack
MW	Maurer and Wolf

P.

PBC	Public Backward Channel
pd-2DMWC	physically-degraded 2DMWC
PDC	Public Discussion Channel
PFC	Public Forward Channel
PLAN	Pass Loss and Additive Noise

R.

RFID	Radio Frequency IDentification
RSS	Received Signal Strength
RV	Random Variable

S.

sd-2DMWC	stochastically-degraded 2DMWC
SK	Secret Key
SKE	Secret Key Establishment
SMT	Secure Message Transmission
SR	Somewhere Random
SSS	Secret Sharing Scheme
SWC	Symmetric Wiretap Channel

T.

TFA	Terrorist Fraud Attack
ToF	Time of Flight
TWBWC	Two-Way Binary Symmetric Wiretap Channel
TWDMWC	Two-Way Discrete Memoryless Wiretap Channel

"An expert is one who knows more and more about less and less until he knows absolutely everything about nothing."

– Nicholas Murray Butler

Chapter 1

Introduction

Traditional cryptography considers security as an objective to be achieved over higher layers of the network stack, where the communication is modeled by a graph with communicating devices as nodes that are connected through error-free links. According to this paradigm, a channel between a sender and a receiver is defined as a path connecting them over the graph. The channel is not necessarily reliable nor secure as its content can be observed and arbitrarily changed by untrusted middle-node adversaries over the path. Providing security functionalities in this communication model has thus become a real challenge in the cryptography community.

Practical approaches to security in the above scenario have been given for the *computational setting* that assumes the adversary has limited computational power and can only handle problems that are solvable in polynomial time. However, almost all these approaches rely on complexity assumptions which are yet open to be proven. Furthermore, none of these solutions resist computationally unbounded adversaries and this renders them vulnerable to future threats, especially, the emerging quantum computers. For instance, Diffie and Hellman [32] considered the problem of key exchange between Alice and Bob when they are connected by a two-way error-free channel whose content is public to Eve as a passive adversary with limited computational power. They provided an elegant solution to the above problem, namely the Diffie-Hellman Key Exchange (DHKE) protocol, whose (computational) security relies on the difficulty of solving the discrete logarithm problem (DLP) [25]. Although DLP is still believed to be a hard problem, it has not been proven to be infeasible, implying that the security of DHKE (and many other similar approaches in the computational setting) is not guaranteed. There are

polynomial-time solutions to DLP that assume little prior knowledge [66]. More significantly, the most worrisome future threat to DLP-based cryptosystems comes from quantum computers. Shor [79] showed that if such machines are built, the DLP (and the factorization of composite numbers) can be solved in polynomial time.

To address this concern, the research community attempted to approach security based on information theory rather than complexity theory. Unfortunately, the solutions appeared drastically less practical as they required access to long keys shared between the devices. Shannon [77] initiated the study of *information-theoretically secure* communication, where Alice wants to transmit a message securely to Bob, using a public (but authentic) channel that reveals all its content to the eavesdropper, Eve. Shannon proved that to provide perfect secrecy in this model, Alice and Bob must share a secret key with entropy at least equal to the message entropy and thus for a full entropy message, the key length must be at least equal to the message length. This result is particularly disappointing because, in the information theoretic setting and without making extra assumptions (such as prior correlated information), it is impossible to establish secure shared keys by communication over (reliable) public channels [59].

As an alternative to approaching security over public channels, there is a second paradigm that seeks for security solutions in the physical-layer of the network stack, where natural characteristics of the environment are viewed as great resources to build security functionalities. Indeed the physical-layer environment bears properties that make information-theoretic security not only possible, but also practical. In this thesis, we follow this paradigm and investigate new solutions to information-theoretic security using physical-layer resources of the network. In the next chapters, we particularly study three security-related problems, namely *secret key establishment*, *manipulation detection*, and *distance bounding verbification* and show how physical channel properties can be used to design secure protocols for these tasks.

1.1 Secret Key Establishment

Wyner [96], and subsequently Csiszár and Körner [26], pioneered the study of secure communication from Alice to Bob over a noisy channel with a wiretapper, Eve. They showed that Alice can communicate securely to Bob without using any shared key if the wiretapping channel is noisier than the main channel. The authors also derived the *secrecy capacity*, which represents the highest achievable secure transmission rate in bits per channel use on average. The result can be used for secret key establishment (SKE) as Alice can generate a random key and send it securely to Bob. Similarly, the *SK capacity* is defined as the highest achievable key rate. When the wiretapping channel is less noisy, no key bits can be generated in the above setting. To resolve this, the followup work assumed additional resources such as public discussion [59], secure feedback [2], or modulo-additive feedback [53] channels, along with the noisy wiretap channel. In many communication scenarios however, assuming access to such resources is not realistic. This creates a gap between the theoretical study of SKE and its use in practice.

In Chapter 3, we investigate the SKE problem in more natural settings where parties are connected to each other only through noisy wiretap channels. We first consider SKE over a pair of noisy wiretap channels in opposite directions. This is a realistic model that matches, e.g., a wireless environment where two nodes communicate in both directions and their communication is wiretapped by their neighbors. We prove lower and upper bounds on the SK capacity and derive the capacity for special cases. Finding the capacity in general remains an open problem. The above work holds two main assumptions: (i) likewise the previous work [26, 96], local randomness is freely available to the communicants, and (ii) the two wiretap channels are independent without influence on each other. We revisit the problem by removing the first assumption, i.e., considering no randomness of any kind (independent or correlated) for the parties. The results

appreciate the role of channel noise as a single resource for both purposes of randomness derivation and key generation at the same time. More specifically, we show that the setup allows for SKE even in cases when the wiretapper's channels are less noisy than the main channels. Although this work is dedicated to the SKE problem, it initiates a new research direction: possibility and construction of cryptographic primitives when the only resource for randomness is the channel noise. We next remove the second assumption and extend the study of SKE to the two-way wiretap channel setting, where simultaneous data transmission in the two directions affect the observations over the channel. Our results show that the communicants can use this property to achieve higher key rates over the two-way channels.

In the final part of this chapter, we notice that the security notion used in our work follows the weak SK capacity definition given in [3, 26, 59, 96] that requires negligible key leakage in rate, as opposed to the strong SK capacity where the total key leakage must be negligible. Maurer and Wolf [60] proved that the weak and the strong SK capacities in the setups of [3,26,59,96] are equal. However, the proof cannot be immediately applied to all SKE setups thereafter. We modify Maurer-and-Wolf's proof and show that the weak and the strong SK capacities equal in any setup that allows reliable data transmission from Alice to Bob or vice versa. We furthermore extend this study to the problem of secure message transmission (SMT) and show the equality of weak and strong secrecy capacities for any setup that allows the sender to have access to a random source.

1.2 Manipulation Detection

Chapter 3 explores security against an unbounded adversary who only "observes" messages over the channel. In this chapter, we consider an adversary who can also tamper with the communication. For this adversary, manipulation detection is required in order

to enable the receiver to verify whether the transmitted message has stayed untouched. Classical solutions to this, referred to as message authentication codes (MACs), propose appending to the message a relatively short authentication tag which is calculated based on the message and a shared key between the devices. Followup research proposed mechanisms that rely on correlated information [61]. Unfortunately, this is the closest one can get to keyless message authentication, i.e., when the adversary can arbitrarily change messages over the channel, it is impossible to achieve authentication without keys or correlated information. This also raises the question whether our SKE results become prevailed by the above impossibility result when active adversaries are present.

In Chapter 4, we notice that adversaries targeting physical channels may not necessarily be able to fully control the communication and change messages arbitrarily. In other words, the set of tampering functions an adversary can choose from to change a communicated message is usually limited. This limitation in tampering with the channel may allow us to design coding schemes to protect against such adversaries while not requiring shared keys. We model tampering over physical-layer channels by an abstract communication channel with leakage that can be algebraic manipulable by the adversary, i.e., the adversary can decide on an adversarial noise variable that is added to the transmitted data over the channel. We formalize this study and define leakage-resilient algebraic manipulation detection (LR-AMD) codes to detect manipulation over this channel model. We develop the study of LR-AMD codes as an independently interesting primitive that can be used in other cryptographic applications, in addition to manipulation detection over physical channel.

Depending on whether manipulation detection is guaranteed for a randomly or an adversarially chosen message, we define LR-AMD codes with weak and strong security notions, respectively. We prove lower bounds on the minimum additional bits (code redundancy) required by weak and strong LR-AMD codes. We also derive general trans-

formations from AMD to LR-AMD coding which prove that currently existing optimal (in redundancy) weak/strong AMD codes can be used as optimal weak/strong LR-AMD codes. While in strong LR-AMD codes the redundancy can become vanishingly small compared to the message length, for weak LR-AMD codes it will be proportional to the message length. We consider a particular type of leakage, called *block leakage*, and design a block-leakage-resilient (BLR)-AMD code construction that requires negligible redundancy. We show two applications of LR-AMD and BLR-AMD codes in cryptography: First, adding robustness to linear *nonperfect* secret sharing schemes and second, detection of algebraic manipulation over wiretap channels. Additionally, we show how our BLR-AMD code construction can be composed with other primitives to provide unlimited bitwise manipulation detection, in addition to privacy, in message transmission or key agreement over binary symmetric and binary erasure wiretap channels.

We also study online-adversarial channel, where the adversary has a linear/constant delay in receiving codeword bits before using them to decide on her manipulation of a codeword bit. For linear-delay adversaries algebraic manipulation detection can be achieved by strong systematic AMD codes. For constant delay adversaries, we show that unary coding achieves arbitrary small failure probability, at the price of requiring much redundancy. The work raises a number of open problems and directions to future work.

1.3 Distance Bounding Verification

Distance bounding verification (DBV) is a variant of the distance bounding problem where the proving party claims an upper bound on its distance to the verifying party and the verifier checks whether this claim is true. Current approaches to this problem [16, 18, 19, 44, 74, 94] use signal's time of flight as a resource to estimate the prover's distance by calculating the time of a rapid challenge-response phase between the verifier

and the prover, thus requiring the verifier to have an accurate clock. Accurate time measurement in these protocols introduces implementation challenges [72], especially in hostile environments where estimating the prover's processing time is a big challenge.

In Chapter 5, we formalize the study of secure DBV using physical channel properties as an alternative to time measurement. We consider a signal propagation environment that attenuates the signal as a function of distance, and then corrupts it by an additive noise. We consider three well-studied attack scenarios against DBV: (1) *distance fraud attack* (DFA) where a malicious prover claims a distance that is lower than its actual distance, (2) *mafia fraud attack* (MFA) where an intruder positions itself between the verifier and an honest prover to claim that the prover is closer, and (3) *terrorist fraud attack* (TFA) where a malicious prover colludes with an intruder to convince the verifier that the prover is closer.

We show that it is possible to construct efficient protocols with security against DFA and MFA, even if the adversary has unlimited computational power; on the other hand, it is impossible to design TFA-secure protocols without time measurement, even if the adversary is computationally bounded. We further show that by limiting the adversary's communication capability to the bounded retrieval model (BRM), it is possible to construct protocols that are secure against all three attacks. We use numerical analysis to elaborate on the parameter conditions and the communication cost required by our DBV protocols for providing security. The work opens a new direction to the study of secure distance bounding protocols.

1.4 Thesis Organization

We begin in Chapter 2 by introducing the notations, preliminary definitions, and basic concepts which we use throughout this work. Chapter 3 involves the study of secret key

establishment including our SKE protocols and bounds on the SK capacity with proofs in Appendix A. We next study the problem of manipulation detection and LR-AMD codes in Chapter 4 and provide in Appendix B the detailed proof of our results in the chapter. The problem of distance bounding verification is included in Chapter 5, where we introduce secure DBV protocols whose proof of security is given in Appendix C. We provide this work with a conclusion and remark directions to future work in Chapter 6.

Chapter 2

Preliminaries and Definitions

This chapter provides the reader with the basic concepts and definitions that will be required in the next chapters. We describe the most common notations used throughout this work, discuss about communication resources and its terminology, and give information-theoretic-security definitions, primitives and existing results, which are related to our study.

2.1 Notations

We use calligraphic $\mathcal{X}$ letters to show sets/groups of elements and their sizes, and use uppercase X and lowercase x letters to denote random variables and their realizations over sets, respectively. Consider $\mathcal{X}^n$, the set of all sequences of length n whose elements are in $\mathcal{X}$. A member $x^n \in \mathcal{X}^n$ is called an n-sequence, x_i denotes its i-th element, and x_i^j denotes the subsequence of i-th to j-th elements. When it is clear from the context, we remove the superscript from an n-sequence notation x^n (or if random X^n) and replace the letter by bold $\mathbf{x}$ (or if random $\mathbf{X}$).

We use P_X and P_{XY} and $P_{X|Y}$, respectively, to denote the marginal distribution of $X \in \mathcal{X}$ as well as the joint and conditional distributions of $(X, Y) \in \mathcal{X} \times \mathcal{Y}$. $\Pr_X(\mathcal{E})$ shows the probability of event $\mathcal{E}$ over the distribution P_X of X, and for random variable $Y = f(X)$, its expected value over the distribution of X is shown by $\mathbb{E}_x Y = \sum_{x \in \mathcal{X}} P_X(x) f(x)$. We use $X \leftrightarrow Y \leftrightarrow Z$ to show a Markov chain between $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$ in the given order: the Markovity means that for any $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, we have $P_{X|YZ}(x|y, z) = P_{X|Y}(x|y)$, which by itself implies $P_{Z|XY}(z|x, y) = P_{Z|Y}(z|y)$.

For $n \in \mathbb{N}$ and $x \in \mathbb{R}$, we let $[n] = \{1, 2, \ldots, n\}$ and $[x]_+ = \max\{0, x\}$. For two variables $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, we use $x||y$ to show their concatenation. The notation $|\mathcal{X}|$ indicates the size of the set $\mathcal{X}$; some times (mainly in Chapter 4), we use the Fraktur letter $\mathfrak{X}$ to replace this notation in showing the size of $\mathcal{X}$. The function $d_H(x, y)$ denotes the Hamming distance of two bit strings $x, y \in \{0, 1\}^n$. All logarithms are base 2, unless mentioned otherwise. For a probability value $0 \leq p \leq 1$, we use $h(p) = -p \log p - (1 - p) \log(1 - p)$ to denote the binary entropy function.

2.2 Communication Resources: Sources and channels

2.2.1 Sources and channels: basic concepts

A *source* is a communication resource that outputs random variables according to a distribution over an alphabet. A *channel* refers to a part of the communication system which transports random variables from an input to an output based on a probability distribution, when each input/output variable is defined over a certain alphabet. In this work, we are particularly interested in *discrete-time sources and channels* whose input/output variables (over time) are sequences of elements [36]; in this setting, a channel/source use is defined as follows.

Definition 1 (resource use)**.** *A source use refers to the act of receiving one variable from the source output alphabet. A channel use refers to sending one variable as the channel input and receiving the resulting variable from the channel output.*

We define two other main concepts related to communication resources, namely the alphabet type and the memory. Depending on the input/output alphabets, communication resources are divided into discrete and continuous, defined as follows.

Definition 2 (discrete vs. continuous resource)**.** *A resource (source or channel) is called*

discrete if its its (input/ouput) alphabets are sets of discrete elements; otherwise, it is called continuous.

Regarding memory, a resource can be divided into memoryless and stateful.

Definition 3 (memoryless vs. stateful resource)**.** *A source is memoryless (otherwise stateful) if the probability distribution of its output at any time is independent of the output at other times. A channel is memoryless (otherwise stateful) if the probability distribution of its output depends only on the input at that time and is conditionally independent of other channel inputs or outputs.*

2.2.2 Discrete memoryless sources and channels: terminology

Our work mainly focuses on *discrete memoryless (DM)* resources, i.e., sources and channels that are both discrete and memoryless: such a resource can be specified by its input/ouput alphabet as well as a probability distribution. Definitions 4-8 show our DM source and channel terminology.

Definition 4 (DMS)**.** *A discrete memoryless source (DMS)* $(\mathcal{S}, P_S)$ *is a source that in each use returns a random variable* $S \in \mathcal{S}$ *according to the probability distribution* P_S*.*

Definition 5 (DMMS)**.** *A discrete memoryless multiple source (DMMS)* $(\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_E, P_{S_A,S_B,S_E})$ *for three parties Alice, Bob, and Eve, is a correlated three-output source that in each use returns to the above parties three random variables* $S_A \in \mathcal{S}_A$*,* $S_B \in \mathcal{S}_B$*, and* $S_E \in \mathcal{S}_E$*, respectively, according to the probability distribution* P_{S_A,S_B,S_E}*.*

Definition 6 (DMWC)**.** *A (one-way) discrete memoryless wiretap channel (DMWC)* $(\mathcal{X}_A, \mathcal{Y}_B, \mathcal{Y}_E, P_{Y_B,Y_E|X_A})$*, from Alice to Bob and Eve, is a channel that in each use, takes an input* $X_A \in \mathcal{X}_A$ *from Alice and returns to Bob and Eve random variables* $Y_B \in \mathcal{Y}_B$*, and* $Y_E \in \mathcal{Y}_E$*, respectively, according to the probability distribution* $P_{Y_B,Y_E|X_A}$*.*

Given a DMWC and a known input distribution, we define its *inverse* as a virtual channel in the opposite direction, described below.

Definition 7. *Given a distribution P_X, for a DMWC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$, we define its* inverse *as $(\mathcal{Y}, \mathcal{X}, \mathcal{Z}, P_{XZ|Y})$ such that $P_{XZ|Y}$ is calculated as*

$$P_{XZ|Y} = \frac{P_X.P_{YZ|X}}{P_Y}, \qquad \text{where} \quad P_Y = \sum_{x,z} P_X.P_{YZ|X}.$$

Definition 8 (TWDMWC)**.** *A two-way discrete memoryless wiretap channel (TWDMWC) $(\mathcal{X}_A, \mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_B, \mathcal{Y}_E, P_{Y_A,Y_B,Y_E|X_A,X_B})$ is a channel that in each use, takes inputs $X_A \in \mathcal{X}_A$ from Alice and $X_B \in \mathcal{X}_B$ from Bob, and returns to the parties random variables $Y_A \in \mathcal{Y}_A$, $Y_B \in \mathcal{Y}_B$, and $Y_E \in \mathcal{Y}_E$, respectively, according to the probability distribution $P_{Y_A,Y_B,Y_E|X_A,X_B}$.*

Remark 1. *The above resource types can all be seen as special cases of the last one, i.e., a TWDMWC by specifying which inputs and/or outputs are present, noting that a source can be defined as a channel with no input.*

The above definitions cover describe DM resources considered in SKE scenarios in the literature, cf. [2, 3, 26, 28, 48, 59, 69, 86, 96] as well as continuous memoryless resources by using probability density function instead of probability distribution. An example of such a continuous-alphabet resource is the *Gaussian wiretap channel (GWC)* [56].

Definition 9 (GWC)**.** *A (real-input) Gaussian wiretap channel (GWC), from Alice to Bob and Eve, is a continuous memoryless channel that in each use, takes an input $X_A \in \mathbb{R}$ from Alice and returns to Bob and Eve random variables $Y_B \in \mathbb{R}$ and $Y_E \in \mathbb{R}$, respectively, such that*

$$Y_B = X_A + N_B, \qquad \text{and} \qquad Y_E = X_A + N_E,$$

where N_B and N_E are independent, real Gaussian noise variables with zero mean and standard deviations σ_B and σ_E.

2.3 Information-theoretic security: definitions and primitives

2.3.1 Random variables and information measures

Shannon [76] introduced an information measure to quantify the amount of uncertainty associated with a random variable. Known as Shannon entropy (or briefly entropy), this measure returns the expected value of information contained in the random variable in terms of bits. Below, we give a definition of Shannon entropy, followed by conditional entropy and mutual information as two related measures.

Definition 10 ((Shannon) entropy)**.** *For a random variable $X \in \mathcal{X}$ with distribution P_X, its (Shannon) entropy is denoted by $H(X)$ and is obtained as $H(X) = -\mathbb{E}_x \log P_X(x)$. Given $Y \in \mathcal{Y}$ such that (X, Y) has joint distribution P_{XY}, their conditional entropy of X given Y given by $H(X|Y) = -\mathbb{E}_{x,y} \log P_{X|Y}(x|y)$.*

Definition 11 ((Shannon) mutual information)**.** *For random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ with joint distribution P_{XY}, their mutual information is denoted by $I(X;Y)$ and is obtained as $I(X;Y) = -\mathbb{E}_{x,y} \log \frac{P_X(x)P_Y(y)}{P_{XY}(x,y)}$.*

Lemma 1 shows the relation between the above measures.

Lemma 1. [23] *The following relationships hold between Shannon information measures.*

$$H(X|Y) = H(XY) - H(Y),$$
$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(XY).$$

The following lemma, known as Fano's inequality, relates the conditional entropy to the probability of error between two variables.

Lemma 2 (Fano's inequality)**.** [23] *For random variables $X, X' \in \mathcal{X}$ with $p_e = \Pr(X \neq X')$, it holds that $H(X|X') \leq h(p_e) + p_e \log |\mathcal{X} - 1| < 1 + p_e \log |\mathcal{X}|$.*

We use three further measures to capture the uncertainty in a random variable, namely statistical distance, Rényi entropy and min-entropy. The statistical distance between two random variables is a difference metric that shows how similar the two variables are distributed.

Definition 12 (Statistical distance)**.** *For two random variables $X, X' \in \mathcal{X}$ with distributions P_X and $P_{X'}$, their statistical distance is denoted by $|X - X'|_s$ and is obtained as $|X - X'|_s = \frac{1}{2}\sum_{x\in\mathcal{X}} |P_X(x) - P_{X'}(x)|$.*

Rényi entropy generalizes the notion of Shannon entropy in quantifying uncertainty with different orders. Here by Rényi entropy of random variable, we mean the its collision entropy (that is Rényi entropy of order 2) which is defined as follows.

Definition 13 (Rényi-entropy)**.** *For a random variable $X \in \mathcal{X}$ with distribution P_X, its Rényi -entropy is denoted by $H_2(X)$ and is obtained as $H_2(X) = -\log \sum_x \big(P_X(x)\big)^2$.*

The min-entropy measure (also known as Rényi entropy of order ∞) returns the minimum (instead of the expected) information contained in the variable in bits.

Definition 14 (Min-entropy)**.** [34] *For a random variable $X \in \mathcal{X}$ with distribution P_X, its min-entropy is denoted by $H_\infty(X)$ and is obtained as $H_\infty(X) = -\log \max_x P_X(x)$. Given $Y \in \mathcal{Y}$ such that (X, Y) has joint distribution P_{XY}, the conditional min-entropy of X given Y is given by $\tilde{H}_\infty(X|Y) = -\log(\mathbb{E}_y \max_x P_{X|Y}(x|y))$.*

In the following, we defined three classes of sources based on the min-entropy of their output. For simplicity, we use the concepts of a source and its (output) random variable interchangeably. The first definition introduces weak sources as a class of sources (or random variables) with min-entropy greater than a certain value.

Definition 15 (Weak source)**.** *A random variable X over the set $\mathcal{X}$ of size $\mathfrak{X}$ is called a* β-weak source *if it holds $H_\infty(X) \geq \beta \log \mathfrak{X}$. The source is called* β-weak conditioned on the random variable Z *if it holds $\tilde{H}_\infty(X|Z) \geq \beta \log \mathfrak{X}$.*

The following definitions give two subclasses of weak sources with additional restrictive properties, named *block sources* and *somewhere-random sources*.

Definition 16 (Block source)**.** *A random variable* $X = (X_1, \ldots, X_n)$ *with elements* $X_i \in \mathcal{X}_i$ *of size* $\mathfrak{X}_i$ *is called a* β-block source *if for all* $1 \leq i \leq n$ *and* $x_j \in \mathcal{X}_j$, $1 \leq j < i$, *it holds* $H_\infty(X_i|(X_j = x_j)_{j<i}) \geq \beta \log \mathfrak{X}_i$.

Definition 17 (Somewhere-random source)**.** *A random variable* $X = (X_1, \ldots, X_n)$ *with elements* $X_i \in \mathcal{X}_i$ *of size* $\mathfrak{X}_i$ *is called a* β-somewhere random *(or shortly* κ*-SR) source if for some* $1 \leq i \leq n$, *it holds* $H_\infty(X_i) \geq \beta \log \mathfrak{X}_i$. *The source is called* β-SR conditioned on the random variable Z *if for some* $1 \leq i \leq n$, *it holds* $\tilde{H}_\infty(X_i|Z) \geq \beta \log \mathfrak{X}_i$.

2.3.2 Randomness extraction and privacy amplification

Many cryptographic primitives/protocols are based on randomized algorithms that require sources of perfect (uniform) randomness. Nevertheless, perfect randomness is not always immediately accessible, and in many communication scenarios, only imperfect (non-uniform) randomness is provided to start with. This non-uniformity can also be caused in a scenario where the source output is partially leaked to an adversary and hence does not remain a uniform random variable. A well-studied problem is whether and how one can make uniform randomness from sources of imperfect randomness. The problem is called *randomness extraction*. We note that *privacy amplification* is also an extension of this to cases where there is leakage to the adversary and hence the objective is to extract a random variable that remains uniform even given the adversary's view. The solution to this problem depends on what is known about the source (output) distribution.

When the source distribution is known, Shannon's source coding theorem [76] shows that one can obtain (arbitrarily close to) uniformly distributed randomness by using the source sufficiently many times independently, and then applying a deterministic source

coding rule to the source output. The coding rule is based on the concept of typicality (defined below) for a sequence that requires its occurrence probability to be close to a certain typical probability.

Definition 18 (Typical sequence)**.** [23, Chapter 3] *For $\epsilon > 0$, integer $n > 0$, and probability distribution P_X over the set $\mathcal{X}$, the sequence x^n is called ϵ-typical with respect to P_X if*

$$|nH(X) + \log P(x^n)| \leq n\epsilon, \qquad \textit{where} \qquad P(x^n) = \prod_{i=1}^{n} P_X(x_i).$$

Lemma 3 also known as asymptotic equipartition property (AEP) shows that, using sufficiently many independent copies of the source output, the resulting sequence is a typical sequence according the source distribution with high probability.

Lemma 3 (AEP)**.** [23, Chapter 3] *Let X^n be identical, independently distributed (i.i.d.) according to the distribution P_X over $\mathcal{X}$. For any $\epsilon > 0$, for sufficiently large $n > 0$, the sequence X^n is an ϵ-typical sequence with respect to P_X with probability at least $1 - \epsilon$.*

This property suggests (informally) that although the source output may be a biased random variable, independently repeated use of this source gives a sequence of i.i.d. variables that is either not typical (with arbitrarily small probability) or it occurs with almost the same probability among all typical sequences. Shannon's deterministic source coding (or data compression) [23] simply repeats the source to obtain X^n and labels it either i (or its binary representation) if it is the i-th ϵ-typical sequence or $\perp$ if it is not ϵ-typical. The result is formalized as follows.

Theorem 1 (Source coding theorem)**.** [23, Chapter 3] *Let X^n be identical, independently distributed (i.i.d.) according to the distribution P_X over $\mathcal{X}$. For any $\epsilon > 0$, for sufficiently large $n > 0$, there are deterministic encoding/decoding functions $Enc_s : \mathcal{X}^n \to \{0,1\}^k \cup \{\perp\}$ and $Dec_s : \{0,1\}^k \to \mathcal{X}^n$, where $k \leq nH(X) + \epsilon$, such that $Dec_s(Enc_s(x^n))$ returns x^n if $Enc_s(x^n) \neq \perp$ or returns $\perp$ otherwise, and we have $\Pr_X(Enc(X^n) = \perp) \leq \epsilon$.*

Source coding converts the source output into a new uniform variable that can be later inverted to the original source output. In other words, although source coding gives uniform randomness as output, it is proposed for invertible compression of data which is an over functionality from the randomness extraction viewpoint. There are other communication primitives, however, that look only at extracting uniform randomness (without invertibility). For instance, a communication primitive called *equipartition* is introduced to derive uniform randomness from a channel output, i.e., a randomness that is independent of the channel input.

Definition 19 (Equipartition)**.** *An* (Γ, ϵ)-equipartition *of* $\mathcal{C} \subseteq \mathcal{Y}^n$ *w.r.t.* $c \in \mathcal{X}^n$ *for the DMC* $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ *is a function* $\psi : \mathcal{C} \to [\Gamma] \cup \{\perp\}$ *such that when* X^n *is input to the channel and* Y^n *is the output, it holds that* $\Pr(\psi(Y^n) = j | X^n = c)$ *is the same for all* $1 \leq j \leq \Gamma$ *and* $\Pr(\psi(Y^n) = \perp | X^n = c) \leq \epsilon$.

Lemma 4 shows that there exists an equipartition for a DMC $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ that can derive randomness rates up to $H(Y|X)$ bits per channel use. This implies the noisier the channel, the higher the achievable rate of randomness that is independent from the channel input.

Lemma 4. [92, Lemma 3.2] *For any* P_X*, typical* $c \in \mathcal{X}^n$ *w.r.t.* P_X*,* $\mathcal{C} \subseteq \mathcal{Y}^n$*, large enough* n*, and* $R_e < H(Y|X)$*, there exists a* (Γ, ϵ)*-equipartition* $\psi(.)$ *over the DMC* $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ *with* $\Gamma = \lfloor 2^{nR_e} \rfloor$*,* $\epsilon = 2^{n(R_e - H(Y|X))} \to 0$*. Furthermore, for each* $j \in \Gamma$ *it holds that* $\psi^{-1}(j)$ *has size at most* $2^{n\epsilon}|\mathcal{C}|/\Gamma$.

Theorem 1 and Lemma 4 show the possibility of randomness extraction using deterministic functions; however, they both rely on two main assumptions: (1) the resource distribution is known, and (2) the resource can be used unlimitedly many times. Allowing extractors that use some extra uniform randomness as seed, both assumptions can

be removed. For instance, if only Rényi entropy of a source (instead of the distribution information) is known, we can use universal hashing to derive uniform randomness.

Definition 20. [20] *A family $\mathcal{G}$ of hash functions $g : \mathcal{X} \to \mathcal{Y}$ is called universal if, for any x_1 and x_2 in $\mathcal{X}$, the equality $g(x_1) = g(x_2)$ happens with probability $1/|\mathcal{X}|$ when $h(.)$ is chosen uniformly at random from $\mathcal{G}$.*

Lemma 5. [14] *Let $X \in \mathcal{X}$ be a random variable with the Rényi entropy $H_2(X) \geq \kappa_0$ and $G(.)$ be randomly selected from a universal family $\mathcal{G} : \mathcal{X} \to \{0,1\}^\kappa$ of hash functions. Then $S = G(X)$ satisfies $H(S|G) \geq \kappa - \frac{2^{\kappa-\kappa_0}}{\ln 2}$.*

A disadvantage of using universal hashing is that it requires extra randomness to select a hash function from the family and this randomness is not small. An alternative to this is using seeded extractors that need much smaller extra randomness as seed. This primitive however requires a bound on the min-entropy of the input source, rather than its Rényi entropy.

Definition 21 (Seeded extractor)**.** [65] *For positive integer κ and positive ϵ, a function $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^r$ is called a (κ, ϵ)-extractor if, for any random variable $X \in \{0,1\}^n$ with $H_\infty(X) \geq \kappa$, it holds $|Ext(X, U^d) - U^r|_s \leq \epsilon$, where U^l is an independent uniform distribution over $\{0,1\}^l$. The function is called a (κ, ϵ)-strong-extractor if $|[U^d, Ext(X, U^d)] - U^{d+r}|_s \leq \epsilon$.*

Lemma 6. [88] *For any choice of $n > 0$, $0 < k \leq n$, and $\epsilon > 0$, there exists an explicit (k, ϵ)-strong-extractor, $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^r$, such that*

$$r = k - 2\log(\frac{1}{\epsilon}) - O(1),$$
$$d = O(\log(k)\left(\log(\frac{n}{\epsilon})\right)^2).$$

When only deterministic extraction is allowed, we can still remove "either" of the assumptions. Given (at least) two independent outputs of the source, we can remove

the first assumption and covert the two outputs to a uniform random variable. This is achieved via two-source extractors.

Definition 22 (Two-source extractor)**.** [22] *For positive integers κ_1, κ_2 and positive ϵ, a function $TExt : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^r$ is called a $(\kappa_1, \kappa_2, \epsilon)$-two-source-extractor if, for any two independent random variables $X_1 \in \{0,1\}^{n_1}$ with $H_\infty(X_1) \geq \kappa_1$ and $X_2 \in \{0,1\}^{n_2}$ with $H_\infty(X_2) \geq \kappa_2$, it holds $|TExt(X_1, X_2) - U^r|_s \leq \epsilon$.*

Lemma 7 shows a recent result on the construction of two-source extractors.

Lemma 7. [33] *For any choice of parameters $n > 0$, $0 < \kappa_1 \leq n$, $0 < \kappa_2 \leq n$, and $\epsilon > 0$ that satisfy $\kappa_1 + \kappa_2 \geq n + \Omega(\text{polylog}(n/\epsilon))$, there exists an efficient $(\kappa_1, \kappa_2, \epsilon)$-two-source-extractor, $TExt : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^r$, with*

$$r = \max(\kappa_1, \kappa_2) + \kappa_1 + \kappa_2 - n - 4\log(1/\epsilon).$$

On the other hand, when the source distribution is known, the following theorem shows the existence of deterministic extractors that do not require repeated use of the source.

Lemma 8 (Deterministic extractor)**.** [27] *For any $\epsilon > 0$ and any κ-source $X \in \mathcal{X}$, there exists a deterministic extractor $Ext : \mathcal{X} \to \{0,1\}^l$ with $l \geq \kappa - \epsilon$ such that $|Ext(X) - U_l|_s \leq \epsilon$, where $U_l \in \{0,1\}^l$ is uniform.*

2.3.3 Information reconciliation and error-correcting codes

Consider a communication scenario where two parties Alice and Bob are provided with correlated (but not identical) random variables X and Y. Information reconciliation is the task of generating an identical shared variable S from these correlated variables. When there is a noiseless channel say from Alice to Bob, information reconciliation can be attained by sending error-correction information G over this noiseless channel, so that

Y and G can be used to recover X. A universal family of hash functions can be used for this purpose.

Lemma 9. [60] *Let X^n and Y^n be random sequences of length n drawn i.i.d. according to the joint probability distribution $P_{X,Y}$ over $\mathcal{X} \times \mathcal{Y}$. For any $\epsilon > 0$, for sufficiently large $n > 0$, $L = (1+\epsilon)nH(X|Y)$, and any universal family $\mathcal{H}$ of functions from $\mathcal{X}^n$ to $\{0,1\}^L$, there exists a function $h \in \mathcal{H}$ such that X^n can be decoded from Y^n and $h(X^n)$ with error probability at most ϵ.*

Lemma 9 shows that information reconciliation is doable when (1) the joint distribution P_{XY} is known, and (2) independent repetition of these variables X and Y is allowed. These assumptions can be relaxed for particular classes of correlation using a primitive called *secure sketch* [34]. The study of this primitive is out of the scope of this work.

When the communication channel is noisy, the task of information reconciliation is achieved using error correcting codes. Error-correction coding is a technique to enable reliable data transmission over unreliable (noisy) communication channels. Block code is a primitive used for reliable communication over noisy channels (DMCs).

Definition 23. *An (n, M, ϵ)-*block code *for the DMC $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ is a pair of encoding and decoding functions $Enc : [M] \to \mathcal{X}^n$ and $Dec : \mathcal{Y}^n \to [M]$ such that for any $i \in [M]$ when $x^n = Enc(i)$ is input to the channel and Y^n is the output, it holds that $\Pr(Dec(Y^n) = i) \geq 1 - \epsilon$.*

Channel coding theorem shows the existence of block codes, for a DMC $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$, that achieve reliable communication rates up to $I(X;Y)$.

Theorem 2 (Channel coding theorem)**.** *For any P_X, $R_c < I(X;Y)$, and large enough n, there exists an (n, M, ϵ)-block code for the DMC $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ with ϵ-typical codewords $c_i \in \mathcal{X}^n$ w.r.t. P_X such that $M = \lfloor 2^{nR_c} \rfloor$ and $\epsilon = 2^{n(R_c - I(X;Y))} \to 0$.*

Proof. See e.g. [23, 41].

2.3.4 Message authentication

A message authentication code (MAC) is a shared key cryptographic primitive that protects a message against arbitrary tampering of an adversary. The code is defined by a function $\mathsf{Mac} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ takes a shared key $\mathsf{sk} \in \mathcal{K}$ as well as a message $m \in \mathcal{M}$ and returns an authentication tag $t = \mathsf{Mac}(\mathsf{sk}; m)$. A message and tag pair (m', t') are then verified if $t' = \mathsf{Mac}(\mathsf{sk}; m')$ holds. We limit ourselves to one-time MACs, defined as follows.

Definition 24 (MAC). *A function* $\mathsf{Mac} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ *is called an* ϵ*-secure one-time message authentication code (MAC) if for any message* $m \in \mathcal{M}$ *and any adversary* $\mathcal{A}dv : \mathcal{T} \to \mathcal{M} \times \mathcal{T}$*, it holds that* $\Pr[t' = \mathsf{Mac}(\mathsf{SK}; m') | (m', t') = \mathcal{A}dv(\mathsf{Mac}(\mathsf{SK}; m))] \leq \epsilon$*, with the probability taken over the uniform key* $\mathsf{SK} \in \mathcal{K}$*.*

Chapter 3

Secret Key Establishment over Physical-Layer Channels

In a seminal paper [96], Wyner proposed a new model for secure communication in the information-theoretic setting, called *the wiretap channel*, where Eve receives a noisier version of what Bob receives from Alice. This approach is interesting as it takes advantage of noise in the physical-layer channels and does not require Alice and Bob to have prior shared keys. The model was generalized by Csiszár and Körner [26] to discrete memoryless wiretap channel (DMWC) in which a message sent by Alice is received in noisy forms by both Bob and Eve. The results in [26, 96] show that wiretap codes for perfectly secure communication exist if and only if Bob's channel is less noisy [51] than Eve's channel. The optimality of a wiretap code is measured in terms of the secrecy rate which is the average number of message bits it transmits securely per channel use. The secrecy capacity of a wiretap channel is the highest achievable secrecy rate.

In real life, all communication channels are inherently noisy and reliable communication is attained by using layers of channel coding to remove noise from the communication. One can look at the above two approaches to secure communication as implementing security at two different layers of a multilayer network architecture. Reliable communication is always implemented at the physical layer of the network stack, making it possible to assume error-free channels for higher layers. Traditional cryptography considers security in the upper layers of the network; hence, it assumes existence of error-free channels. The noisy channel paradigm, on the other hand, considers message reliability and security as two properties that can be achieved simultaneously at the physical layer.

Related work

Maurer [59] considered the wiretap channel model for the purpose of secret key establishment (SKE), where Alice and Bob want to establish a shared key that is secure against Eve. Following the definition of secrecy capacity, he defined the secret-key (SK) capacity of a wiretap channel as the highest rate of secure and reliable key that Alice and Bob can establish by communicating over the channel. For the one-way wiretap channel setup [26, 96], the SK capacity equals the secrecy capacity as highest key rate is achieved by Alice sending a random key securely and reliably to Bob. Maurer [59] thus revisited the SKE problem assuming a public discussion channel in addition to correlated randomness (e.g., obtained from a wiretap channel). The public discussion channel is an error-free channel that can be used unlimitedly by Alice and Bob to communicate in both directions; however, its content is completely available to Eve. Maurer proved that SK capacity in the new setup is strictly higher than that of a single wiretap channel; more interestingly, Alice and Bob are able establish keys in some cases where the secrecy capacity of the wiretap channel is zero. Similar results were independently derived by Ahlswede and Csiszár [3]. In the above, the public channel is assumed to be freely available to Alice and Bob in the sense that the communication over this channel is not counted in calculating the SK rate.

The followup work on SKE has studied the problem if various communication settings. Csiszár and Narayan [28] studied SKE using correlated sources and a limited-rate one-way public channel from Alice to Bob. Ahlswede and Cai [2] showed that the secrecy capacity in Wyner's setup can be increased by adding an unlimited secure (and reliable) *output feedback channel*. Noisy feedback over modulo-additive wiretap channels [53] is another extension of the SKE problem. SKE using correlated sources and a (one-way) wiretap channel was considered in [48] and [69] independently.

Our work

Assuming the existence of the above resources lets achieve higher secret-key rates. In many communication scenarios, however, access to such resources may not be realistic and it may not be necessarily the best strategy (for maximizing the secret-key rate) to realize them from existing resources. In this chapter, we investigate SKE in a very basic setting where Alice and Bob can send messages to each other over noisy channels that are eavesdropped. This is the scenario that models for instance two devices that are communicating in a wireless environment and their communication is intercepted by other devices in the neighborhood.

SKE in a DM setup. We start by describing the SKE problem in a general *discrete memoryless (DM) setup* in Section 3.1. We define a DM *setup* as specific communication scenario with a set of discrete-alphabet and memoryless resources (See Section 2.2.2) that can be used as many times as required by the communicants. The performance of a SKE protocol over a setup is measured in terms of rate, that is the number of key bits divided by the *cost* imposed to the resources by the protocol. The cost for a resource is generally a function of how many times the resource is used. We define the SK capacity as the highest achievable key rate based on certain security conditions. We also explain a number of important results on SKE in various setting.

SKE using 2DMWC and TWDMWC. In Section 3.4, we study SKE over a pair of discrete memoryless wiretap channels (DMWCs) in two directions. We refer to this setup as 2DMWC. We show lower and upper bounds on the SK capacity in the 2DMWC setup and derive the capacity for special cases. We notice however two restrictive assumptions in this study:

(i) Local randomness is freely available to the parties (similar to the previous work).

(ii) The two DMWCs in the two directions are independent.

The first assumption is not realistic in many SKE scenarios, e.g., when communicating devices with limited/even no access to random sources are available. In practice, generating randomness with high entropy needs specialized hardware and/or software as well as access to complex processes that could be hard to obtain specially when devices with low computational resources are considered. A natural question is then whether the need for a separate random source can be eliminated. In Section 3.5, we revisit SKE over 2DMWC removing the first assumption; in other words, considering no randomness of any kind (independent or correlated) for the parties. The results appreciate the role of channel noise as a single resource for both purposes of randomness derivation and key generation at the same time. We show that the setup allows secure SKE even in cases when the wiretapper's channels are less noisy than the main channels.

The second assumption does not match for example wireless scenarios where simultaneous signal transmission by parties in the two directions can cause superpositions of the signals and hence affect observations over the channel. In Section 3.6, we remove the second assumption by studying the two-way discrete memoryless wiretap channel (TWDMWC) setup, which is a more general communication model. The communicants can use this property as an advantage to achieve higher secret-key rates by benefiting from simultaneous transmission to confuse the wiretapper.

From weak to strong capacity. The above study of SKE over noisy channel considers a weak notion of SK capacity that requires negligible information leakage about the key to the adversary. Maurer and Wolf [60] suggest an alternative definition to the weak SK capacity, called strong SK capacity, where the secrecy requires absolutely negligible information leakage about the key. The authors prove the equality of weak and strong SK capacities for the early setups in [3, 26, 59, 96]. Whether this equality holds for any DM setup is not answered in the literature. We show that weak and strong SK capacities are equal for any DM setup that allows reliable transmission in at least one direction. We

extend this study to secure message transmission and show that weak and strong *secrecy capacities* are equal if the setup allows the sender to use randomness. We provide trivial counterexamples that show these sufficient conditions are not always necessary for the equality of the capacities.

Remark 2. *For consistency of our results, we assume full-duplex model of communication in both 2DMWC and TWDMWC setups. In this model,* each channel use *lets both Alice and Bob send one symbol over their DMWC, and in* each communication round*, the parties send a message of the same length over their DMWC. This communication model is used to simplify the presentation of our results and to better compare the SK capacity behavior over different setups. We note that the SKE results over 2DMWC can be easily adapted to half-duplex communication model, where in each communication round, either Alice or Bob sends a message (cf. Section 5).*

3.1 Secret Key Establishment in a Discrete Memoryless Setup

To establish a secret key over a DM setup $\mathfrak{S}$, Alice and Bob follow a SKE protocol Π that is publicly known to all parties. The SKE protocol Π may generally proceed in multiple rounds, say t, provided that the communication resources allow interaction between Alice and Bob. In each communication round $1 \leq r \leq t$, Alice and Bob (either or both) send input sequences and/or receive output sequences of symbols through the setup, based on the ability of their communication resources. We denote the input and output sequences in round r by $\mathbf{X}_A^{:r}$, $\mathbf{X}_B^{:r}$, $\mathbf{Y}_A^{:r}$, and $\mathbf{Y}_B^{:r}$, respectively. Eve may also receive a sequence of symbols, denoted by $\mathbf{Y}_E^{:r}$, over the setup. Note that the output sequences by the setup can be generated by sources or channels in the setup. An input sequence of a party in round r is calculated as a function of their *view* of the protocol at the end of round $r-1$, which includes the so-far received output sequences (from sources and/or channels). We

denote by $\mathbb{V}_A^{:r}$, $\mathbb{V}_B^{:r}$, and $\mathbb{V}_E^{:r}$, the views of Alice, Bob, and Eve at the end of round r, respectively, which can be written as

$$\mathbb{V}_A^{:r} = ||_{i=1}^{r} \left(\mathbf{X}_A^{:i} || \mathbf{Y}_A^{:i}\right), \quad \mathbb{V}_B^{:r} = ||_{i=1}^{r} \left(\mathbf{X}_B^{:i} || \mathbf{Y}_A^{:i}\right), \quad \mathbb{V}_E^{:r} = ||_{i=1}^{r} \mathbf{Y}_E^{:i}. \tag{3.1}$$

When the communication rounds are complete, Alice and Bob use their final views $View_A = \mathbb{V}_A^{:t}$ and $View_B = \mathbb{V}_B^{:t}$ to calculate $S_A \in \mathcal{S}$ and $S_B \in \mathcal{S}$, respectively, as estimates of a shared secret key S over the predefined alphabet $\mathcal{S}$. Eve also uses her $View_E = \mathbb{V}_E^{:t}$ to obtain information about S.

Figure 3.1 shows how the parties' views in round $t-1$ and t are related to the keys, calculated by Alice and Bob. For instance, Alice calculates $X_A^{:t}$ based on her view $\mathbb{V}_A^{:t-1}$ as $X_A^{:t} = f(\mathbb{V}_A^{:t-1})$, where f is a deterministic function. This means that, given $\mathbb{V}_A^{:t-1}$, $X_A^{:t}$ is independent of $\mathbb{V}_B^{:t-1}$ which implies the Markov chain $\mathbb{V}_B^{:t-1} \leftrightarrow \mathbb{V}_A^{:t-1} \leftrightarrow X_A^{:t}$. In a similar way, one can derive Markov chains between other sets of variables in a general SKE protocol.

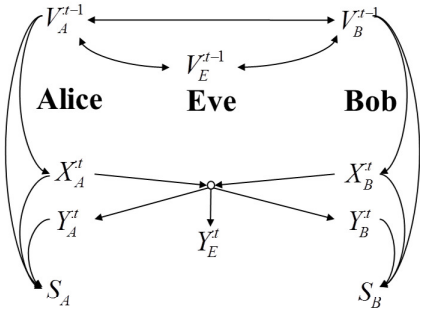


Figure 3.1: The relationship between variables in a general SKE

We measure the communication efficiency of the protocol Π in terms of *its cost* over $\mathfrak{S}$, which is defined as the sum of costs it imposes to the resources. In general, we define the cost for a resource as follows.

Definition 25 (resource cost)**.** *The cost function of a resource $\mathfrak{R}$, denoted by $Cost_{\mathfrak{R}} : \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$, is a non-decreasing function, satisfying $Cost_{\mathfrak{R}}(0) = 0$, that returns a cost*

value given the number of resource uses. The resource $\mathfrak{R}$ is called free if the function $Cost_{\mathfrak{R}}$ is zero for all inputs.

Remark 3. *Our work only considers resources $\mathfrak{R}$ whose cost function is linear and hence can be specified by a* per-use cost *value $c_{\mathfrak{R}}$, i.e., the cost of using the resource n times is simply calculated as $Cost_{\mathfrak{R}}(n) = nc_{\mathfrak{R}}$. With this assumption, we define cost of a protocol as follows.*

Definition 26 (cost of a protocol)**.** *Let the setup $\mathfrak{S}$ provide the resources $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_m$ with per-use costs $c_{\mathfrak{R}1}, c_{\mathfrak{R}2}, \ldots, c_{\mathfrak{R}m}$, respectively. For a protocol Π that uses the resources for $n_1, n_2, \ldots, n_m$ number of times, respectively, its cost is calculated as*

$$Cost_{\Pi}^{\mathfrak{S}} = \sum_{i=1}^{m} n_i c_{\mathfrak{R}i}. \tag{3.2}$$

The security of SKE requires the resulting secret key S to be *random*, *reliable*, and *secret*. The following provides a formal definition of a secure protocol for a given setup.

Definition 27 (Weak SK capacity)**.** *For $R_{sk} \geq 0$ and $\delta \geq 0$, a SKE protocol Π over a setup $\mathfrak{S}$ is* (R_{sk}, δ)-weakly-secure *if there exists a random variable $S \in \mathcal{S}$ such that the following holds*

$$\textit{Reliability:} \qquad \Pr(S_A = S_B = S) \geq 1 - \delta, \tag{3.3a}$$

$$\textit{Weak secrecy:} \qquad I(S; View_E) \leq \delta, \tag{3.3b}$$

$$\textit{Randomness:} \qquad H(S) \geq Cost_{\Pi}^{\mathfrak{S}}(R_{sk} - \delta). \tag{3.3c}$$

The weak secret key (SK) capacity, $C_{wsk}^{\mathfrak{S}}$, is the largest R_{sk} such that, for any arbitrarily small $\delta > 0$, there exists an (R_{sk}, δ)-weakly-secure SKE protocol.

Remark 4. *The above definition of SK capacity matches those in [3, 26, 59, 96]. Maurer and Wolf [60] notice two weaknesses of this definition. The first is the key randomness: (3.3c) does not require the key to be even close to uniform. The second weakness is the*

secrecy: (3.3b) requires negligible "rate" of information leakage about the key. Uniformity is partially addressed in Definition 28.

Definition 28 (Uniform SK capacity)**.** *The SKE protocol* Π *in Definition 27 is called* (R_s, δ)*-uniformly-secure if in addition to (3.3a)-(3.3c) it holds that*

$$\textit{Uniformity:} \qquad H(S_A) \geq \log |\mathcal{S}| - \delta Cost_{\Pi}^{\mathfrak{S}}. \tag{3.4}$$

The uniform SK capacity, $C_{usk}^{\mathfrak{S}}$*, is the largest* R_s *such that, for any arbitrarily small* $\delta > 0$*, there exists an* (R_s, δ)*-uniformly-secure SKE protocol.*

We define *strongly-secure protocols* that satisfy stronger uniformity and secrecy conditions: (i) the key is perfectly uniform and (ii) the secrecy condition is on total key information leakage, rather than rate.

Definition 29 (Strong SK capacity)**.** *A SKE protocol* Π*, as in Definition 27, is called* (R_s, δ)*-strongly-secure the following holds*

$$\textit{Reliability:} \quad \Pr(S_A = S_B) \geq 1 - \delta, \tag{3.5a}$$

$$\textit{Strong secrecy:} \quad I(S_A; View_E) \leq \delta, \tag{3.5b}$$

$$\textit{Strong uniformity:} \quad H(S_A) = \log |\mathcal{S}| \geq (R_s - \delta) Cost_{\Pi}^{\mathfrak{S}}. \tag{3.5c}$$

The strong SK capacity, $C_{ssk}^{\mathfrak{S}}$*, is the largest* R_s *such that, for any arbitrarily small* $\delta > 0$*, there exists an* (R_s, δ)*-strongly-secure SKE protocol.*

In the sequel, we first consider only weak SK capacity and later give a general relation between weak and strong SK capacities for any DM setup. Throughout if not explicitly mentioned, by SK capacity, wean mean the weak SK capacity.

3.2 SKE over Existing Setups

The first results on SKE are due to Wyner [96] as well as Csiszár and Körner [26] who considered secure communication over a noisy wiretap channels. The setup consists of a (one-

way) discrete memoryless wiretap channel (DMWC), denoted by $(\mathcal{X}_A, \mathcal{Y}_A, \mathcal{Y}_E, P_{Y_B Y_E|X_A})$, from Alice to Bob and Eve, and a (single) discrete memoryless source (DMS) of randomness with uniform distribution for Alice. The channel's per-use cost equals 1, but the source is free (zero cost) and can be used unlimitedly many times. This implies that the total cost of a protocol over the setup equals to the number of channel uses. We refer to this setup by DMWC. The results in [26, 96] show that the SK capacity of this setup equals:

$$C_{wsk}^{DMWC} = \max_{W_A, X_A} \left[I(W_A; Y_B) - I(W_A; Y_E) \right], \tag{3.6}$$

where W_A is a random variable from an arbitrary set such that $W_A \leftrightarrow X_A \leftrightarrow (Y_B, Y_E)$ forms a Markov chain. Leung-Yan-Cheong and Hellman [56] proved similar results for when the DMWC is replaced by a Gaussian wiretap channel (GWC) such that the maximum signal transmission power is E_0 and the noise powers of Bob's and Eve's channels are Σ_B and Σ_E, respectively. The SK capacity expression for this setup can be simplified as

$$C_{wsk}^{GWC+DMS} = C_B - C_E, \quad \text{where} \quad C_B = \tfrac{1}{2}\log(1 + \tfrac{E_0}{\Sigma_B}) \quad \text{and} \quad C_E = \tfrac{1}{2}\log(1 + \tfrac{E_0}{\Sigma_E}) \tag{3.7}$$

Maurer [59], and independently Ahlswede and Csiszár, [3] studied the advantage of using a public discussion channel (PDC) for SKE. The PDC is a free two-way (wiretap) channel between Alice ad Bob whose content is noiselessly available to all parties (including Eve). The work considers using free public discussion together with free independent randomness (DMS) and correlated randomness generated for the parties by a discrete memoryless multiple source (DMMS), denoted by $(\mathcal{S}_A, \mathcal{S}_B, \mathcal{S}_E, P_{S_A, S_B, S_E})$. The DMMS has a per-use cost of 1, implying the cost of a protocol is given by the number of source uses. We refer to this setup as DMMS+PDC. The tight characterization of the SK capacity over this setup is unknown in general; however, when the PDC can only be used in either forward or backward direction (we use PFC and PBC to denote these restricted

cases of PDC, respectively), the SK capacity equals [3]

$$C_{wsk}^{DMMS+PFC} = \max_{V_{1A},V_{2A}} \left[I(V_{1A}; S_B|V_{2A}) - I(V_{1A}; S_E|V_{2A}) \right], \tag{3.8}$$

$$C_{wsk}^{DMMS+PBC} = \max_{V_{1B},V_{2B}} \left[I(V_{1B}; S_A|V_{2B}) - I(V_{1B}; S_E|V_{2B}) \right], \tag{3.9}$$

where (V_{1A}, V_{2A}) and (V_{1B}, V_{2B}) are independent pairs of random variables from arbitrary sets, satisfying the Markov chains $V_{2A} \leftrightarrow V_{1A} \leftrightarrow S_A \leftrightarrow (S_B, S_E)$ and $V_{2B} \leftrightarrow V_{1B} \leftrightarrow S_B \leftrightarrow (S_A, S_E)$. In the case of PDC, which can be used in both directions, the SK capacity is bounded as [3, 59]

$$\max\left(C_{wsk}^{DMMS+PFC}, C_{wsk}^{DMMS+PBC}\right) \leq C_{wsk}^{DMMS+PDC} \leq I(S_A; S_B|S_E), \tag{3.10}$$

and it is shown that the lower bound is not tight. Similar results have been derived for when the DMMS is replaced by the DMWC $(\mathcal{X}_A, \mathcal{Y}_A, \mathcal{Y}_E, P_{Y_B Y_E|X_A})$ from Alice to Bob and Eve, where the SK capacity is bounded as

$$\max\left(C_{wsk}^{DMWC+PFC}, C_{wsk}^{DMWC+PBC}\right) \leq C_{wsk}^{DMWC-PDC} \leq \max_{X_A} I(X_A; Y_B|Y_E), \tag{3.11}$$

$$\text{where} \quad C_{wsk}^{DMWC+PFC} = \max_{W_A,X_A} \left[I(W_A; Y_B) - I(W_A; Y_E) \right], \quad \text{and}$$

$$C_{wsk}^{DMWC+PBC} = \max_{W_B,X_B} \left[I(W_B; X_A) - I(W_B; Y_E) \right].$$

where the lower bound maximization is conditioned on the Markov chains $W_A \leftrightarrow X_A \leftrightarrow (Y_B, Y_E)$ and $W_B \leftrightarrow Y_B \leftrightarrow (X_A, Y_E)$. Csiszár and Narayan [28] considered a more restricted version of DMMS+PFC where the public forward channel is *limited* in rate (hence LFPC in brief); in precise, the number of source uses and public channel uses should be equal and furthermore, in each channel use, at most R bits of information can be transmitted. This restriction is made because in real-life communication channels are limited in the amount of information they can transmit reliably (per channel-use) and this imposes a cost on the resource. In this case, the SK capacity is obtained by modifying (3.8) as below.

$$C_{wsk}^{DMMS+LPFC} = \max_{V_{1A},V_{2A}} \left[I(V_{1A};S_B|V_{2A}) - I(V_{1A};S_E|V_{2A}) \text{ s.t. } I(V_{1A};S_A|S_B) \leq R \right]. \quad (3.12)$$

Khisti et al. [48] as well as Prabhakaran et al. [69] studied a variant of SKE when the parties are provided with a DMMS and a DMWC from Alice to Bob and Eve. It was again assumed that parties have free access to independent uniform randomness. The motivation is that in many communication scenarios, (noiseless) public channels are realized by error correction over noisy channels (possibly with leakage). It is thus interesting to determine when noiseless channel realization is or is not optimal. Assuming per-use costs of 1 for each of the resources, one obtains the cost of using the DMMS+DMWC setup by adding the total number of channel and source uses. The results of [48,69] show the following lower bounds on the SK capacity in this setup.

$$C_{wsk}^{DMMS+DMWC} \geq \max_{\mu,V_A,W_{2A},W_{1A},X_A} \left[\frac{\mu R^{DMMS} + [R^{DMWC}]_+}{1+\mu} \text{ s.t. } I(W_{1A};Y_B) > \mu I(V_A;S_A|S_B) \right] \quad (3.13)$$

where

$$R^{DMMS} = I(V_A;S_B) - I(V_A;S_E), \quad \text{and} \quad R^{DMWC} = I(W_{1A};Y_B|W_{2A}) - I(W_{1A};Y_E|W_{2A}). \quad (3.14)$$

The key rates R^{DMMS} and R^{DMWC} denote the number of key bits achieved (on average) from each source and channel use, respectively, and μ denotes the ratio between the number of source uses to channel uses. When the DMMS does not have an ouput for Eve (i.e., $\mathcal{S}_E = \emptyset$), the following upper bound on the SK capacity has been derived [48]

$$C_{sk}^{DMMS+DMWC} \leq \max_{\mu,V_A,X_A} \left[\mu \frac{I(V_A;S_B) + I(X_A;Y_B|Y_E)}{1+\mu} \text{ s.t. } I(X;Y) > \mu I(V_A;S_A|S_B) \right]. \quad (3.15)$$

3.3 Basic primitives for SKE

In this chapter, we prove our lower bounds on the SK capacity in different setups by showing the existence of SKE protocols with certain key rates. Random coding arguments and the concept of typicality are primary tools for such proof. In Chapter 2, we defined typical sequences as those whose occurrence probability is close to a typical probability based on a given distribution. In the following, we slightly extend this to *bipartite typical sequences* which are concatenation of two subsequences and their occupance probability is close to a typical probability based on two given distributions. We define bipartite typical and bipartite jointly-typical sequences as follows.

Definition 30. *A sequence* $x^N = (u^n||t^d)$ *is an* (ϵ, n)-bipartite typical sequence *with respect to the probability distribution pair* (P_U, P_T)*, iff*

$$\begin{aligned} &|-\frac{1}{N}\log P(x^N) - \frac{nH(U)+dH(T)}{N}| < \epsilon, \ \textit{where} \\ &P(x^N) = \prod_{i=1}^{N} P(x_i) = \prod_{i=1}^{n} P_U(u_i) \times \prod_{i=1}^{d} P_T(t_i). \end{aligned} \tag{3.16}$$

Definition 31. *A pair of sequences* $(x^N, y^N) = ((u^n||t^d), (u'^n||t'^d))$ *is an* (ϵ, n)-bipartite jointly typical pair of sequences *with respect to the probability distribution pair* $(P_{U,U'}(u,u'), P_{T,T'}(t,t'))$*, iff* x^N *and* y^N *are* (ϵ, n)*-bipartite typical sequences with respect to the marginal probability distribution pairs* $(P_U(u), P_T(t))$ *and* $(P_{U'}(u'), P'_T(t'))$*, respectively, and*

$$\begin{aligned} &|-\frac{1}{N}\log P(x^N, y^N) - \frac{nH(U,U')+dH(T,T')}{N}| < \epsilon, \quad \textit{where} \\ &P(x^N, y^N) = \prod_{i=1}^{N} P(x_i, y_i) = \prod_{i=1}^{n} P_{U,U'}(u_i, u'_i) \times \prod_{i=1}^{d} P_{T,T'}(t_i, t'_i). \end{aligned} \tag{3.17}$$

The set $A_\epsilon^{(N,n)}$ *is the set of all* (ϵ, n)*-bipartite jointly typical pairs of sequences* $(x^N, y^N) = ((u^n||t^d), (u'^n||t'^d))$ *with respect to the probability distribution pair* $(P_{U,U'}(u,u'), P_{T,T'}(t,t'))$.

The following lemma extends the result of Lemma 3 for bipartite joint-typicality.

Lemma 10 (Joint AEP for bipartite sequences)**.** *Let* $(X^N, Y^N) = ((U^n||T^d), (U'^n||T'^d))$ *be a pair of bipartite random sequences of length* N*, (each part) drawn i.i.d. according to the distribution pair* $(P_{U,U'}(u,u'),\ P_{T,T'}(t,t'))$*. Then, for large enough* n *and* d*, we have*

1. $\Pr((X^N, Y^N) \in A_\epsilon^{(N,n)}) \to 1$
2. $(1-\epsilon)2^{nH(U,U')+dH(T,T')-N\epsilon} \leq |A_\epsilon^{(N,n)}| \leq 2^{nH(U,U')+dH(T,T')+N\epsilon}$
3. *If* $\tilde{X}^N$ *and* $\tilde{Y}^N$ *are independent with the same marginal distributions as* $P(x^N, y^N)$*, i.e.,* $(\tilde{X}^N, \tilde{Y}^N)$ *is generated according to the distribution* $P(x^N)P(y^N)$*, then*

$$\Pr((\tilde{X}^N, \tilde{Y}^N) \in A_\epsilon^{(N,n)}) \leq 2^{-nI(U;U')-dI(T;T')+3N\epsilon}. \tag{3.18}$$

$$\Pr((\tilde{X}^N, \tilde{Y}^N) \in A_\epsilon^{(N,n)}) \geq (1-\epsilon)2^{-nI(U;U')-dI(T;T')-3N\epsilon}. \tag{3.19}$$

Proof. Appendix A.1.1. □

In the following, we introduce *secure block code* and *secure equipartition* as two fundamental primitives that we use in our SKE protocol constructions. We define a *secure block code* for a DMWC as the composition of a block code (see Definition 23) and a *key derivation function*. A secure block code can be used by two parties, connected through a DMWC, to establish a secret key.

Definition 32. *An* (n, M, K, ϵ)-secure block code*, with* $K \leq M$*, for the DMWC* $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ *consists of an* (n, M, ϵ)*-block code Enc/Dec for the DMC* $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$*, and a key derivation function* $\phi_{sk} : [M] \to [K]$*, such that for uniformly chosen* $B \in [M]$ *and* $S = \phi_s(B)$*, it holds that* $I(S; Z^n) \leq \epsilon \log(K)$*.*

Although the above definition of a secure block code as a primitive is new to the literature, the work on secure message transmission or key agreement over one-way DMWCs [26, 96] implicitly studies the existence of such a primitive. For instance, one

can send a message $S \in [K]$ using a secure block code (defined as above), by randomly choosing a codeword in $\phi_s^{-1}(S)$ and sending it over the channel. The receiver decodes the codeword and applies ϕ_s to obtain the secure message. The results in [26, 96] let us conclude the following lemma. For completeness we give a proof of the lemma in Appendix A.1.2.

Lemma 11. *Let (W_1, W_2, X, Y, Z) be such that $W_2 \leftrightarrow W_1 \leftrightarrow X \leftrightarrow (Y, Z)$ is a Markov chain. Also let $R_c < I(W_1; Y)$, $R_{sc} \leq I(W_1; Y|W_2) - I(W_1; Z|W_2)$. When $R_c, R_{sc} \neq 0$, for large enough n, there exists an (n, M, K, ϵ)-secure block code for the DMWC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ with ϵ-typical codewords $c_i \in \mathcal{X}^n$ such that $M = \lfloor 2^{nR_c} \rfloor$, $K = \lfloor 2^{nR_{sc}} \rfloor$, and $\epsilon = (2R_c + 1)/R_{sc} 2^{n(R_c - I(W_1;Y))} \to 0$.*

Proof. See Appendix A.1.2. □

Lemma 11 indicates that, for the above DMWC, there exists a secure block code that achieves key rates up to $I(W_1; Y|W_2) - I(W_1; Z|W_2)$. In the following, we extend this result by showing that there are sufficiently many secure block codes such that any $X^n \in \mathcal{X}^n$ as input to the channel belongs to at least one of them, with high probability.

Lemma 12. *Let (W_1, W_2, X, Y, Z), R_c, and R_{sc} be as in Lemma 11, and $R' > H(X) - R_c$. For large enough n, there exist N (not necessarily disjoint) (n, M, K, ϵ)-secure block codes for the DMWC $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ with ϵ-typical codewords, such that $M = \lfloor 2^{nR_c} \rfloor$, $K = \lfloor 2^{nR_{sc}} \rfloor$, $N = \lfloor 2^{nR'} \rfloor$, and $\epsilon = (2R_c + 1)/R_{sc} 2^{n(R_c - I(W_1;Y))} \to 0$; furthermore, the probability that a randomly selected ϵ-typical sequence $X^n \in \mathcal{X}^n$ belongs to at least one of the secure-block codes is at least $1 - e^{-\gamma}$, where $\gamma = 2^{n(R' + R_c - H(X) - \epsilon)} \to \infty$.*

Proof. See Appendix A.1.3. □

A secure equipartition is an extension of equipartition (see Definition 19) for randomness extraction over a DMWC that ensures the derived randomness is not only indepen-

dent of the input but also independent of Eve's received sequence. In other words, Eve is uncertain about the extracted random variable.

Definition 33. *An* (Γ, ϵ)-secure equipartition *of* $\mathcal{C} \subseteq \mathcal{Y}^n$ *w.r.t.* $c \in \mathcal{X}^n$ *over the DMWC* $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ *is a function* $\psi : \mathcal{C} \to [\Gamma] \cup \{\perp\}$ *such that when* X^n *is input to the channel and* Y^n *and* Z^n *are the outputs, it holds that* $\Pr(\psi(Y^n) = j | X^n = c)$ *is the same for all* $1 \leq j \leq \Gamma$, $\Pr(\psi(Y^n) = \perp | X^n = c) \leq \epsilon$, *and furthermore,*

$$I(\psi(Y^n); Z^n | X^n = c) \geq (1 - \epsilon) \log(\Gamma). \tag{3.20}$$

The following lemma shows the existence of a secure equipartition over the DMWC that achieves randomness rates up to $H(Y|XZ)$ bits per channel use.

Lemma 13. *For any* P_X, *typical* $c \in \mathcal{X}^n$, $\mathcal{C} \subseteq \mathcal{Y}^n$ *of size less than* $2^{nH(Y)}$, $R_{se} < H(Y|XZ)$, *and large enough* n, *there exists a* (Γ, ϵ)*-secure equipartition for the DMWC* $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{YZ|X})$ *such that* $\Gamma = \lfloor 2^{nR_{se}} \rfloor$ *and*

$$\epsilon = \frac{3I(Y; X, Z)h(\epsilon')}{H(Y|XZ) - \epsilon'} \to 0, \quad \textit{where} \quad \epsilon' = 2^{n(R_{se} - H(Y|XZ))}.$$

Proof. See Appendix A.1.4. □

3.4 SKE in the 2DMWC Setup

The 2DMWC setup [1] consists of a pair of discrete and memoryless wiretap channels in the two directions between Alice and Bob. There is a forward DMWC $(\mathcal{X}_A, \mathcal{Y}_A, \mathcal{Y}_{fE}, P_{Y_B Y_{fE}|X_A})$ from Alice to Bob and Eve, and a backward DMWC and $(\mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_{bE}, P_{Y_A Y_{bE}|X_A})$ from Bob to Alice and Eve. The DMWCs are independent, i.e., a channel's input does not affect the other channel's outputs. See Figure 3.2. We assume that the parties are provided with free access to local (independent) randomness. We also assume full-duplex

[1] The results of this section have been published in proceedings of the International Symposium on Information Theory and its Applications (ISITA), 2010 [6, 7].

communication model when in each 2DMWC use with cost of 1, both parties can send one symbol over their channels.

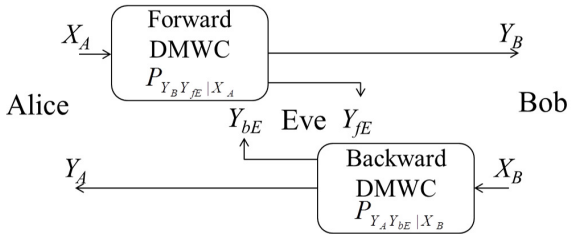


Figure 3.2: The 2DMWC setup.

Although the 2DMWC setup has not been consider for SKE before, solutions to SKE over 2DMWC can rely on existing results in Section 3.2.

(i) One approach to establish a shared key over a 2DMWC is key transport: Either Alice or Bob chooses a random secret key and sends it in a secure and reliable way over forward or backward DMWC, respectively. This implies a lower bound on the SK capacity of a 2DMWC that equals the maximum of the SK capacities of forward and backward DMWCs.

(ii) Another approach is to use the 2DMWC to realize a DMMS and a (limited rate) public channel, whose SK capacity is given by (3.12): The DMMS can be realized by either party (Alice or Bob) sending an independent identically distributed (i.i.d.) random sequence over their channel, where the other party and Eve receive correlated noisy versions. The public channel in forward/backward direction is realized by using a capacity-achieving error correction code over the forward/backward DMWC. The rate limit for a DMWC (used as a public channel) equals its capacity for reliable transmission, i.e., $R = \max_X I(X;Y)$. Depending on which channel is used to create the DMMS and which channel is used to create the public channel,

four possible cases of DMMS and public channel are realized. The lower bound attained by this approach is the maximum of the four SK rates achieved by these four realizations.

The above approaches to SKE over 2DMWC result in positive SK rates in many scenarios; however, they do not always lead to the best achievable rate. Note that channel noise is a potential resource for secrecy and removing it via error-correction coding may sometimes decrease the key rate. Higher SK rates can be achieved by taking into consideration channel noise in both DMWCs. Using the 2DMWC, one can realize the DMMS+DMWC setup by leaving one DMWC as is and creating a DMMS by having an i.i.d. sequence transmitted the other DMWC. This lower bound on the SK capacity can be obtained by directly applying the expression of (3.13). For the sake of completeness, we prove the lower bound by proposing a two-round channel coding construction, and proving that it achieves the rate.

3.4.1 SK capacity: lower bound

Let the RVs (X_A, Y_B, Y_{fE}) and (X_B, Y_A, Y_{bE}) be consistent with the channel distributions $P_{Y_B,Y_{fE}|X_A}$ and $P_{Y_A,Y_{bE}|X_B}$, respectively. Let V_A, V_B, (W_{1A}, W_{2A}), and (W_{1B}, W_{2B}) be independent random variables from arbitrary sets, that satisfy the following Markov chains:

$$V_A \leftrightarrow Y_A \leftrightarrow (X_B, Y_{bE}) \quad \text{and} \quad W_{2A} \leftrightarrow W_{1A} \leftrightarrow X_A \leftrightarrow (Y_B, Y_{fE}), \tag{3.21a}$$

$$V_B \leftrightarrow Y_B \leftrightarrow (X_A, Y_{fE}) \quad \text{and} \quad W_{2B} \leftrightarrow W_{1B} \leftrightarrow X_B \leftrightarrow (Y_A, Y_{bE}). \tag{3.21b}$$

Theorem 3. *Taking the above variables and letting*

$$R_{scf^{-1}} = I(V_B; X_A) - I(V_B; Y_{fE}), \tag{3.22a}$$

$$R_{scf} = I(W_{1A}; Y_B|W_{2A}) - I(W_{1A}; Y_{fE}|W_{2A}), \tag{3.22b}$$

$$R_{scb^{-1}} = I(V_A; X_B) - I(V_A; Y_{bE}), \tag{3.22c}$$

$$R_{scb} = I(W_{1B}; Y_A|W_{2B}) - I(W_{1B}; Y_{bE}|W_{2B}), \tag{3.22d}$$

the secret-key capacity is lower bounded as

$$C_{wsk}^{2DMWC} \geq Lbnd_{sk}^{2DMWC} \triangleq \max_{\mu \geq 0, X_A, X_B, V_A, V_B, W_{2A}, W_{2B}, W_{1A}, W_{1B}} \{Lbnd_1 + Lbnd_2\}, \tag{3.23}$$

where

$$Lbnd_1 = \frac{\mu R_{scf^{-1}} + [R_{scb}]_+}{1+\mu} \text{ s. t. } I(W_{1B}; Y_A) > \mu I(V_B; Y_B|X_A), \tag{3.24}$$

$$Lbnd_2 = \frac{\mu R_{scb^{-1}} + [R_{scf}]_+}{1+\mu} \text{ s. t. } I(W_{1A}; Y_B) > \mu I(V_A; Y_A|X_B). \tag{3.25}$$

Proof. Appendix A.2. □

Notes about the lower bound. The SKE protocol proceeds in two independent and parallel instances: instance 1 that is initiated by Alice in round 1 and finished by Bob in round 2 and instance 2 where the communication is in the opposite direction. While the detailed protocol description is given is Appendix A.2, we give a brief explanation of instance 1. Alice sends a random sequence $\mathbf{X}_A$ over the forward channel, where Bob and Eve receive $\mathbf{Y}_B$ and $\mathbf{Y}_{fE}$, respectively. Bob obtains $\mathbf{V}$ by inputting $\mathbf{Y}_B$ to the DMC $(\mathcal{Y}_A, \mathcal{V}, P_{V|Y_B})$, and then finds (I_B, J_B) such that $\mathbf{V} = Enc'_{J_B}(I_B)$, i.e., the I_A-th codeword in the J_A-th secure block code over the inverse forward DMWC. In the second round, Bob sends back to Alice the code index J_B together with some fresh randomness U_B in a secure way via a secure block codeword $\mathbf{X_B} = Enc(J_B, U_B)$; Alice and Eve receive $\mathbf{Y}_A$ and $\mathbf{Y}_{bE}$, respectively. Alice first decodes $(J_B, U_B) = Dec(\mathbf{Y}_A)$ and then uses the knowledge of J_B

to decode $I_B = Dec'_{J_B}(\mathbf{X}_A)$. Now that both parties have shared (I_B, J_B, U_B), they apply the key derivation function in their secure block codes to derive secret keys.

The lower bound expression (3.23) is obtained by maximizing the sum of two key rates $Lbnd_1$ and $Lbnd_2$ which are achieved by instances 1 and 2 of the SKE protocol. On the following, we explain how expression (3.24) for $Lbnd_1$ is obtained ($Lbnd_2$ in (3.25) can be discussed similarly). The key rate $Lbnd_1$ is a weighted average of the two quantities $R_{scf^{-1}}$ and R_{scb}, which indicate the secure transmission rates over the inverse forward and the backward DMWCs, achieved in the first and the second communication rounds, respectively. The parameter μ shows the ratio between the number of DMWC channel uses in the first and the second round. The condition $I(W_{1B}; Y_A) > \mu I(V_B; Y_B|X_A)$ implies that the backward channel should have enough reliability capacity so that Bob can send error-correcting information to remove Alice's uncertainty about what he has received through the forward channel.

3.4.2 SK capacity: upper bound

While the lower bound in Theorem 3 is achieved by a two round protocol, a general key establishment protocol may consist of many rounds. Each communication round can contribute to the shared key between the two parties at the cost of channel uses of that round. Theorem 4 gives an upper bound on the key rate achievable by any protocol with any number of communication rounds.

Theorem 4. *The SK capacity of the 2DMWC is upper bounded as*

$$C_{wsk}^{2DMWC} \leq Ubnd_{sk}^{2DMWC} \triangleq \max_{X_A, X_B} [I(X_A; Y_B|Y_{fE}) + I(X_B; Y_A|Y_{bE})] \tag{3.26}$$

Proof. The expression (3.26) falls as a special case of the upper bound (3.65) on the SK capacity for the TWDMWC setup, which is proved in Appendix A.12. □

Notes about the upper bound. The expression (3.26) is the only known upper bound on the SK capacity in the 2DMWC setup. The upper bound however is not a tight. To see this, consider the case where the forward DMWC has zero secrecy capacity and the backward channel from Bob to Alice is fully noisy, i.e., it cannot transmit even a single bit of information reliably to Alice. In this case, the SK capacity clearly equals to that of the one-way forward DMWC [26], which equals zero. However, the upper bound (3.26) results in $\max_{X_A}[I(X_A;Y_B|Y_{fE})]$ (since $I(X_B;Y_A|Y_{bE})=0$ for all distributions X_B) which can remain positive in many cases.

The upper bound (3.26) equals the sum of two terms, $\max_{X_A} I(X_A;Y_B|Y_{fE})$ and $\max_{X_B} I(X_B;Y_A|Y_{bE})$, each of which is calculated independently using the forward and the backward channel probability distributions, respectively. Rephrasing the upper bound as

$$Ubnd_{sk}^{2DMWC} = \max_{\mu\geq 0, X_A, X_B} \left[\frac{\mu I(X_A;Y_B|Y_{fE}) + I(X_B;Y_A|Y_{bE})}{1+\mu}\right],$$

shows that the gap between our lower and upper bounds come from the conditions on μ in the lower bound. One may argue that the upper bound expression can be improved by deriving conditions on the channel use ratio μ in a general SKE protocol. Improving the upper bound remains an interesting open question.

While the two bounds are not tight in general, they coincide in certain cases. In what follows, we give our results on physically degraded channels which is as special case where the lower and upper bound coincide and the SK capacity is known.

Remark 5. *As noted earlier in Remark 2, the above lower and upper bounds are given for SK capacity in full-duplex communication model, rather than a half-duplex. In the former, a channel use with the cost of* 1 *involves both Alice and Bob to send one symbol over their DMWCs, whereas in the latter, each channel use allows only either of the two parties to send a symbol. It is easy to show that for a half duplex communication model*

the bounds are obtained by replacing (3.23) and 3.26 by

$$C_{wsk}^{2DMWC} \geq \max_{\mu \geq 0, X_A, X_B, V_A, V_B, W_{2A}, W_{2B}, W_{1A}, W_{1B}} \{Lbnd_1 \ , \ Lbnd_2\}, \quad and$$
$$C_{wsk}^{2DMWC} \leq \max_{X_A, X_B} \left[I(X_A; Y_B | Y_{fE}) \ , \ I(X_B; Y_A | Y_{bE}) \right].$$

3.4.3 Physically degraded 2DMWC

A physically degraded DMWC is a special case of a DMWC where the adversary always receives a degraded version of what the receiver observes through the channel. Wyner's "wiretap channel" [96] which has founded this line of research is a physically degraded DMWC. Physically degraded channels can be formally shown by a Markov chain relation between the input/ouput variables of the channel.

Definition 34 (pd-2DMWC)**.** *The DMWC* $(\mathcal{X}_A, \mathcal{Y}_A, \mathcal{Y}_E, P_{Y_B, Y_E|X_A})$ *is called* physically degraded in obverse (resp. reverse) order *if* $X_A \leftrightarrow Y_B \leftrightarrow Y_E$ *(resp.* $X_A \leftrightarrow Y_E \leftrightarrow Y_B$*) forms a Markov chain. A* pd-2DMWC *is a 2DMWC whose DMWCs are physically degraded (either in obverse or reverse order).*

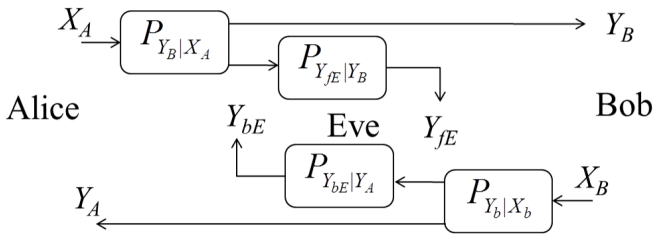


Figure 3.3: 2DMWC with physically degraded channels (pd-2DMWC).

The following proposition shows the SK capacity in the case of pd-2DMWC. A 2DMWC is called physically degraded (pd-2DMWC) if both its DMWCs are physically degraded. See Figure 3.3.

Proposition 1. *For the pd-2DMWC with channels* $(\mathcal{X}_A, \mathcal{Y}_A, \mathcal{Y}_{fE}, P_{Y_B,Y_{fE}|X_A})$ *and* $(\mathcal{X}_A, \mathcal{Y}_A, \mathcal{Y}_{bE}, P_{Y_B,Y_{bE}|X_A})$*, the SK capacity equals*

$$C_{wsk}^{pd-2DMWC} = \max_{X_A,X_B} \left[I(X_A; Y_B|Y_{fE}) + I(X_B; Y_A|Y_{bE}) \right].$$

and this capacity can be achieved by a one-round SKE protocol.

Proof. Appendix A.3. □

3.4.4 Stochastically degraded 2DMWC

For pd-2DMWCs, the lower and the upper bounds coincide and the capacity is achieved by a one-round SKE protocol. This implies that interaction over a pd-2DMWC cannot increase the SKE rate. However, this is not generally true for a 2DMWC that has *stochastically degraded*, instead of physically degraded, wiretap channels. In communication setups that do not offer interactive communication [26, 28, 48, 69], physically and stochastically degraded wiretap channels are equivalent in terms of the secret-key capacity. For the 2DMWC setup in which interactive communication is permitted, the upper bound in (3.26) does not necessarily coincide with the lower bound in (3.23).

In the following, we consider a special class of 2DMWC where each DMWC is *stochastically degraded with independent channels*. We refer to this setup as *sd-2DMWC*. Two important classes of stochastically degraded channels with independent components are binary symmetric wiretap channels and Gaussian wiretap channels. Although the results of this section are given for discrete channels, they can be easily extended to continuous memoryless channels.

Definition 35 (sd-2DMWC)**.** *The DMWC* $(\mathcal{X}_A, \mathcal{Y}_A, \mathcal{Y}_E, P_{Y_B,Y_E|X_A})$*, is* stochastically degraded *in obverse (resp. reverse) order if there exist two RVs* $\tilde{Y}_B$ *and* $\tilde{Y}_E$ *such that* $X_A \leftrightarrow \tilde{Y}_B \leftrightarrow \tilde{Y}_E$ *(resp.* $X_A \leftrightarrow \tilde{Y}_E \leftrightarrow \tilde{Y}_B$*) forms a Markov chain and for all* $x \in \mathcal{X}_A$*,*

$y \in \mathcal{Y}_A$, *and* $y' \in \mathcal{Y}_E$*:*

$$P_{X_A,Y_B}(x,y) = P_{X_A,\tilde{Y}_B}(x,y), \qquad P_{X_A,Y_E}(x,y') = P_{X,\tilde{Y}_E}(x,y').$$

It consists of independent channels *if* $P_{Y_B,Y_E|X_A} = P_{Y_B|X_A}.P_{Y_E|X_A}$*. A* sd-2DMWC *is a 2DMWC whose DMWCs are stochastically degraded (either in obverse or reverse order), and each consists of independent channels.*

For this setup, the lower bound expression can be simplified to contain fewer axillary variables; this makes much easier the maximization problem in calculating the lower bound. The expressions (3.28) and (3.29) do not contain the RVs W_{1A}, W_{2A}, W_{1B} and W_{2B} (3.24) and (3.25).

Proposition 2. *The SK capacity in the sd-2DMWC setup is lower bounded as*

$$C_{wsk}^{sd-2DMWC} \geq \max_{\mu \geq 0, X_A, X_B, V_A, V_B} \{Lbnd_1' + Lbnd_2'\}, \tag{3.27}$$

where the random variables follow the Markov chains (3.21), and

$$Lbnd_1' = \frac{\mu I(V_B; X_A|Y_{fE}) + [I(X_B;Y_B) - I(X_B;Y_{bB})]_+}{1+\mu} \text{ s.t. } I(X_B;Y_A) > \mu I(V_B;Y_B|X_A), \tag{3.28}$$

$$Lbnd_2' = \frac{\mu I(V_A; X_B|Y_{bE}) + [I(X_A;Y_A) - I(X_A;Y_{fB})]_+}{1+\mu} \text{ s.t. } I(X_A;Y_B) > \mu I(V_A;Y_A|X_B). \tag{3.29}$$

Proof. Appendix A.4. □

The following theorem gives a tight characterization of the SK capacity under the condition that one of the parties can only send only i.i.d variables. This capacity is achieved by a two-round protocol. An example of such a scenario is when a base station wants to establish keys with several users in different locations. The offline computation power of the base station is high but its realtime computation power is limited. So, the base station sends i.i.d. variables in realtime and stores the received variables from all other nodes in all communication rounds. Next, it calculates the common keys with each

user from the stored information in the offline mode. Our study of the above scenario provides a solution to this problem.

Theorem 5. *When one of the legitimate parties can only send i.i.d. variables, the lower bound in (3.27) is tight and the SK capacity is achieved by a two-round protocol.*

Proof. Appendix A.5. □

Remark 6. *In the above study of secret key establishment via interactive communication, we have made two restrictive assumptions: (i) uniform local randomness is freely available to the parties (similar to [26, 96] and the followup work) and (ii) the two DMWCs work independently of each other. In the next two sections, we revisit the above work by removing either of the two assumptions.*

3.4.5 Comparing the bounds for binary channels

We consider a special case of 2DMWC, as illustrated in Fig. 3.4, where each DMWC consists of two binary symmetric channels (BSCs), one from the sender to the legitimate receiver (referred to as the main channel) with bit error probability p_m, and one from the sender to Eve (referred to as eavesdropping channel) with bit error probability p_e. We refer to this setting as 2BSWC. The binary noise variables in the main forward, main backward, eavesdropping forward, and eavesdropping backward channels are all independent and are respectively denoted by $N_{m,f}$, $N_{e,f}$, $N_{m,b}$ and $N_{e,b}$, i.e.,

$$Y_B = X_A + N_{m,f}, \qquad Y_{fE} = X_A + N_{e,f}, \tag{3.30}$$

$$Y_A = X_B + N_{m,b}, \qquad Y_{bE} = X_B + N_{e,b}. \tag{3.31}$$

Recall that the 2BSWC setup falls into the class of stochastically degraded 2DMWC with independent channels (sd-2DMWC), defined in Section 3.4.4. We apply the results

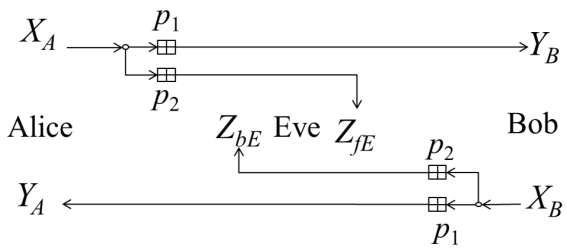


Figure 3.4: 2DMWC with independent BSCs (2BSWC).

of Proposition 2 and Theorem 4 to this case and obtain lower and upper bounds on the SK capacity.

Remark 7. *Throughout, for probability values $0 \leq x, y \leq 1$, we denote the error probability in the cascade of two BSCs with error probabilities x and y by $x \star y = x + y - 2xy$. The following lemma indicates the the cascade of any two BSCs is noisier than both.*

Lemma 14. *For any real values $0 \leq x, y \leq 1$, we have*

$$|x \star y - 0.5| \leq \min\{|x - 0.5|, |y - 0.5|\}, \quad \textit{and} \tag{3.32}$$

$$h(x \star y) \geq \max\{h(x), h(y)\}. \tag{3.33}$$

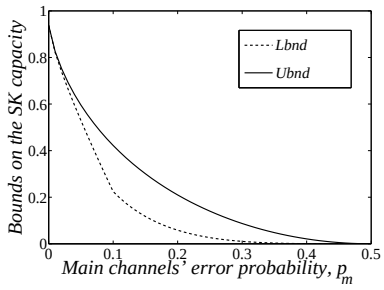
Proof. See Appendix A.13. □

Lemma 15. *The SK capacity for 2BSWC is bounded from below and above as*

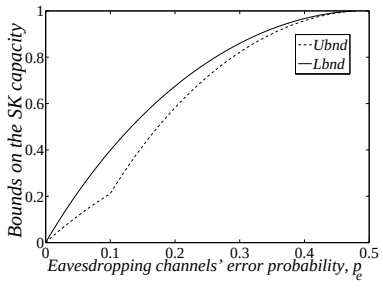
$$2\Big((1 - h(p_m))[h(p_m \star p_e) - h(p_m)] + h(p_m)[h(p_e) - h(p_m)]_+\Big) \leq C_{wsk}^{2BSWC} \leq 2[h(p_m \star p_e) - h(p_m)] \tag{3.34}$$

Proof. See Appendix A.6. □

In Fig. 3.5, we graph the behavior of the two bounds with respect to p_m and p_e, i.e., the main and the eavesdropping channels' error probabilities. Fig. 3.5(a) compares the rates for various values of p_m when $p_e = 0.1$. The lower and the upper bounds only coincide at the highest rate and the lowest rate. These correspond to the cases where



(a) $0 \leq p_m \leq 0.5$ and $p_e = 0.1$



(b) $p_m = 0.1$ and $0 \leq p_e \leq 0.5$

Figure 3.5: The changes in the bound values with respect to the error probabilities.

the main channels are noiseless or fully noisy, respectively. Fig. 3.5(b) compares the rates for various values of p_e when $p_m = 0.1$. Again the bounds only coincide when Eve's channels are noiseless or fully noisy. The former implies impossibility of SKE and the latter depicts a pure common randomness generation scenario, i.e., a special case of SKE when no information is leaked to the adversary; hence, the SK rate equals the main channel reliability capacity.

3.5 SKE in the 2DMWC Setup without local randomness

In this section [2] , we revisit SKE in the 2DMWC setup when Alice and Bob have neither independent nor correlated randomness initially, i.e., they can only use fixed hardwired constant strings, such as identification strings that are publicly known, and there is no other resource for randomness except channel noise. We refer to this setup by 2DMWC^{-r} and its SK capacity by $C_{wsk}^{2DMWC^{-r}}$. We start by discussing special cases of interest where SKE is impossible, and then argue the possibility of SKE via a simple construction for binary symmetric channels that achieves some rates of secret key. We derive general lower-bound and upper-bound expressions for the SK capacity of 2DMWC without ran-

[2]The results of this section have been published in the proceedings of Advances in Cryptology–EUROCRYPT 2011 [10] and the proceedings of Foundations and Practice of Security (FPS) 2011 [9].

domness, and discuss their relationship for the case of binary symmetric channels.

3.5.1 Impossibility cases

It is clear that a SKE protocol is expected to result in a key that is random; therefore, with no local randomness and only using public channels, the task is impossible. This observation is true even in the computational setting, e.g., the Diffie-Hellman key exchange protocol [32] where Eve has limited (polynomially bounded) computational power. This is true because all parameters in the system are deterministic, and Eve can execute the same algorithms as Alice and Bob to derive the final key. This shows once more that using error correcting codes to remove noise can limit cryptographers in designing secure systems.

Although the existence of channel noise is a necessary condition for SKE without local randomness, it is not sufficient. For instance, SKE over a one-way DMWC [26, 96] becomes impossible when no randomness is available for the parties. Irrespective of the protocol, Alice will never have a single bit of randomness in her view and, without randomness, she cannot have a secret key. This gives that without local randomness the SK capacity of a one-way DMWC equals zero. This result holds true even if parties are additionally connected by a public discussion channel (PDC) [3, 59]. Although Alice can receive random data through the public channel, her view of the protocol is completely known to Eve. Eve can simply follow Alice's deterministic steps of calculating the key, and this render's the key insecure. So the SK capacity remains zero.

The above cases can be viewed as special cases of 2DMWC. Recall that in the previous section, we could achieve positive SK rates by realizing a one-way DMWC with/without public discussion from a 2DMWC and running known SKE protocols on them. By removing the assumption of local randomness the achievable key rate collapses to zero.

3.5.2 A simple SKE construction for binary symmetric channels

Consider the 2BSWC setup of Figure 3.4, which includes four independent binary symmetric channels (BSCs): main channels with bit error probability p_m and eavesdropping channels with bit error probability p_e. Assume that Alice has an all-zero sequence of length m, $\mathbf{a} = \underline{0}^m$. We describe a two-round construction that uses the following primitives to establish a secret key between Alice and Bob.

Randomness extraction (see Section 2.3.2). This step allows the parties to derive uniform randomness from the channel output with non-uniform (biased) distribution. We use the von Neumann extractor [93] that takes a Bernoulli sequence $\mathbf{Y} = (Y_1Y_2, Y_3Y_4, \ldots, Y_{q-1}Y_q)$ of even length q and returns a uniformly distributed output as follows. It first divides the input sequence into $q/2$ pairs of bits and uses the following mapping on each pair

$$00 \to \Lambda, \qquad 01 \to 0, \qquad 10 \to 1, \qquad 11 \to \Lambda,$$

where Λ indicates no output. The output sequence is the concatenation of the mapped bits. This extractor is computationally efficient and the output bits are independently and uniformly distributed. Although the von Neumann extractor does not return a fixed-length output, we can convert it to a fixed-length extractor $Ext : \{0,1\}^q \to \{0,1\}^l \cup \{\perp\}$ that derives an l-bit uniform string from an q-bit Bernoulli sequence. The Ext function runs the von Neumann extractor on the q-bit sequence $\mathbf{Y}$. If the output length is less l, it returns $\perp$; otherwise, it returns the first l bits of the output. The probability that for an q-bit Bernoulli sequence (with $P(Y_i) = p$), Ext returns $\perp$ equals

$$\Pr(\mathcal{E}rr_{ext}) = \sum_{i=0}^{l-1} \binom{\frac{q}{2}}{i} (2p(1-p))^i \, (1-2p(1-p))^{\frac{q}{2}-i}. \tag{3.35}$$

Error-correction coding (see Section 2.3.3). Error-correcting codes are used to provide reliable transmission over the noisy channels, so that Alice and Bob can come up with shared randomness. For this purpose, we assume we have a capacity achieving binary

block code Enc_b/Dec_b that can correct up to $t = \lfloor (n-k)/2 \rfloor$ bit errors over the BSC, where k and n indicate the message length and the code length, respectively. When used over a BSC with error probability p, the decoding error probability of such a code equals the probability that the number of errors is greater than t, i.e.,

$$\Pr(\mathcal{E}rr_{enc}) \geq \Pr(n_{err} > t) = \sum_{i=t+1}^{n} \binom{n}{i} p^i \ (1-p)^{n-i}. \tag{3.36}$$

Privacy amplification (see Section 2.3.2). This step lets Alice and Bob convert their shared randomness to a secure key. Here, we use use a universal family of computationally efficient hash functions, described as follows [95]

$$\mathcal{H} = \{h_c : GF(2^k) \to \{0,1\}^\kappa, \quad c \in GF(2^k)\},$$

where $h_c(x)$ returns the first κ bits of $c.x$, and the multiplication is over the polynomial representation of $GF(2^k)$.

Protocol description. Using the above primitives, the SKE protocol proceeds as follows. Alice sends her constant sequence $\mathbf{X}_A = \mathbf{a} = (\underline{0})^q$ over the forward DMWC. Bob and Eve receive the q-sequences $\mathbf{Y}_A$ and $\mathbf{Y}_{fE}$ (q is even). Bob views this as an q-bit Bernoulli sequence, $\mathbf{Y}_A = (Y_{A,1}, \ldots, Y_{A,q})$, with $P(Y_{A,i} = 1) = p_m$ and finds $\mathbf{U} = Ext(\mathbf{Y}_A)$. If $\mathbf{U} = \perp$, the error $\mathcal{E}rr_{ext}$ occurs; otherwise, Bob splits the l-bit $\mathbf{U}$ into two independent and uniform k-bit sequences $\mathbf{U}_1$ and $\mathbf{U}_2$, where $k = l/2$. He calculates the n-bit codewords $\mathbf{X}_{1B} = Enc_b(\mathbf{U}_1)$ and $\mathbf{X}_{2B} = Enc_b(\mathbf{U}_2)$ and sends them over the backward DMWC; Alice and Eve receive $(\mathbf{Y}_{1A}, \mathbf{Y}_{2A})$ and $(\mathbf{Y}_{1bE}, \mathbf{Y}_{2bE})$, respectively. Alice calculates the k-sequences $\hat{\mathbf{U}}_1 = Dec(\mathbf{Y}_{1A})$ and $\hat{\mathbf{U}}_2 = Dec(\mathbf{Y}_{2A})$. The error event $\mathcal{E}rr_{enc1}$ (resp. $\mathcal{E}rr_{enc2}$) occurs when $\hat{\mathbf{U}}_1 \neq \mathbf{U}_1$ (resp. $\hat{\mathbf{U}}_2 \neq \mathbf{U}_2$). Next, Alice and Bob use universal hashing for privacy amplification, i.e., to derive keys that are secure against Eve. The secret key is $S = h_C(\mathbf{U}_1)$ where $C = \mathbf{U}_2$. Bob calculates $S_B = S$ and Alice calculates $S_A = h_{\hat{C}}(\hat{\mathbf{U}}_1)$ where $\hat{C} = \hat{\mathbf{U}}_2$.

Randomness, reliability, and secrecy. The above protocol provides Alice and Bob with κ uniformly random bits of key. The rate of key establishment is calculated as the number of the key bits divided by the number of channel uses, i.e., $R_{sk} = \frac{\kappa}{q+2n}$. Regarding reliability (3.3a), we observe that $S_A = S_B = S$ holds if none of the errors $\mathcal{E}rr_{ext}$, $\mathcal{E}rr_{enc1}$, and $\mathcal{E}rr_{enc2}$ occurs. This gives

$$\Pr(S_A = S_B = S) \geq 1 - \Pr(\mathcal{E}rr_{ext}) - \Pr(\mathcal{E}rr_{enc1}) - \Pr(\mathcal{E}rr_{enc2}), \tag{3.37}$$

where $\Pr(\mathcal{E}rr_{ext})$, $\Pr(\mathcal{E}rr_{enc1}) = \Pr(\mathcal{E}rr_{enc2})$ are obtained from (3.35) and (3.36) for $p = p_m$, respectively. For an arbitrarily small $\delta > 0$, we can, for instance, choose the parameters q, l, n, and $k = l/2$ such that each of the above error probabilities is at most $\delta/3$ and so (3.3a) is satisfied. The secrecy property (3.3b) is proved as follows. We first obtain the entropy term $H(\mathbf{U}_1|\mathbf{Y}_{1bE})$ as

$$H(\mathbf{U}_1|\mathbf{Y}_{1bE}) = H(\mathbf{U}_1) - H(\mathbf{Y}_{1bE}) + H(\mathbf{Y}_{1bE}|\mathbf{U}_1) \geq k - n(1 - h(p_e)). \tag{3.38}$$

Since the channels are memoryless, asymptotic equipartition property (AEP) (see, e.g., [23, Chapter 3]) gives the equality of the Rényi entropy $H_2(\mathbf{U}_1|\mathbf{Y}_{1bE} = \mathbf{y})$ with Shannon entropy as in (3.38). Using Lemma 5 with $X = (\mathbf{U}_1|\mathbf{Y}_{1bE} = \mathbf{y})$ and $\kappa_0 = k - n(1 - h(p_e))$ proves the following:

$$\begin{aligned} H(S|\mathbf{Y}_{1bE}, \mathbf{Y}_{2bE}, \mathbf{Y}_{fE}) &\overset{(a)}{=} H(S|\mathbf{Y}_{1bE}, \mathbf{Y}_{2bE}) \geq H(S|\mathbf{Y}_{1bE}, \mathbf{U}_2) \\ &= H(S|\mathbf{Y}_{1bE}, C) \overset{(b)}{\geq} \kappa - \frac{2^{\kappa-\kappa_0}}{\ln 2} \\ \Rightarrow I(S; \mathbf{Y}_{1bE}, \mathbf{Y}_{2bE}, \mathbf{Y}_{fE}) &\leq H(S)\delta, \end{aligned} \tag{3.39}$$

where $\delta = \frac{2^{\kappa-\kappa_0}}{\kappa \ln 2}$. Equality (a) holds since the randomness in $\mathbf{Y}_{fE}$ comes only from Eve's BSC noise that is independent of all the variables including $(S, \mathbf{Y}_{1bE}, \mathbf{Y}_{2bE})$, and inequality (b) follows from Lemma 5. For an arbitrarily small $\delta > 0$, we can choose the parameters k ,n and κ such that (3.39) holds.

δ	n	k	l	q	R_{sk}
10^{-2}	458	330	660	5430	0.0158
10^{-3}	508	358	716	5590	0.0151
10^{-4}	560	388	776	5730	0.0146

Table 3.1: SKE construction parameters with respect to δ for $\kappa = 100$.

Table 3.1 shows the construction parameters for SKE over binary symmetric channels with $p_m = 0.1$ and $p_e = 0.2$ when the secret key length is $\kappa = 100$ and the security parameter δ has different values. According to this table, the achievable SK rate by this construction is about $R_{sk} = 0.015$. Considering the full-duplex communication model, Alice and Bob can follow another run of the above with Bob as the initiator without affecting the cost over the setup. This will double the secret key rate by this construction to around 0.03 bit per 2DMWC use.

The aim of giving this construction is to show the feasibility of efficient SKE with no initial randomness. The construction is simple and computationally efficient; however, it is not optimal in term of secret key rate. In the next section, we derive a lower bound on the SK capacity that is achieved more optimal multi-round SKE protocol.

3.5.3 SK capacity: lower bound

Let the RVs (X_A, Y_B, Y_{fE}) and (X_B, Y_A, Y_{bE}) be consistent with the channel distributions $P_{Y_B,Y_{fE}|X_A}$ and $P_{Y_A,Y_{bE}|X_B}$, respectively. Also let V_A, V_B, (W_{1A}, W_{2A}), and (W_{1B}, W_{2B}) be independent random variables from arbitrary sets, that satisfy Markov chains

$$V_A \leftrightarrow Y_A \leftrightarrow (X_B, Y_{bE}) \quad \text{and} \quad W_{2A} \leftrightarrow W_{1A} \leftrightarrow X_A \leftrightarrow (Y_B, Y_{fE}), \tag{3.40a}$$

$$V_B \leftrightarrow Y_B \leftrightarrow (X_A, Y_{fE}) \quad \text{and} \quad W_{2B} \leftrightarrow W_{1B} \leftrightarrow X_B \leftrightarrow (Y_A, Y_{bE}). \tag{3.40b}$$

Theorem 6. *Taking the above variables and letting*

$$R_{scf^{-1}} = I(V_B; X_A) - I(V_B; Y_{fE}), \tag{3.41a}$$

$$R_{scf} = I(W_{1A}; Y_B|W_{2A}) - I(W_{1A}; Y_{fE}|W_{2A}), \tag{3.41b}$$

$$R_{scb^{-1}} = I(V_A; X_B) - I(V_A; Y_{bE}), \tag{3.41c}$$

$$R_{scb} = I(W_{1B}; Y_A|W_{2B}) - I(W_{1B}; Y_{bE}|W_{2B}), \tag{3.41d}$$

the SK capacity of the 2DMWC^{-r} is lower bounded as

$$C_{wsk}^{2DMwC^{-r}} \geq \max_{\mu\geq 0, X_A, X_B, V_A, V_B, W_{2A}, W_{2B}, W_{1A}, W_{1B}} \{Lbnd_A^{-r} + Lbnd_B^{-r}\}, \tag{3.42}$$

where

$$Lbnd_A^{-r} = \frac{1}{1+\mu}\left(\mu R_{scf^{-1}} + \gamma_1 [R_{scb}]_+\right), \tag{3.43}$$

$$Lbnd_B^{-r} = \frac{1}{1+\mu}\left(\mu R_{scb^{-1}} + \gamma_2 [R_{scf}]_+\right), \tag{3.44}$$

for

$$\gamma_1 = \min\{1, \frac{I(V_A; Y_A|X_B, Y_{bE}) + \mu(I(V_A; Y_A|X_B) - H(X_A))}{I(W_{1A}; Y_B)}\}, \tag{3.45}$$

$$\gamma_2 = \min\{1, \frac{I(V_B; Y_B|X_A, Y_{fE}) + \mu(I(V_B; Y_B|X_A) - H(X_B))}{I(W_{1B}; Y_A)}\}, \tag{3.46}$$

such that

$$I(V_A; Y_A|X_B, Y_{bE}) > \mu H(X_A), \qquad I(W_{1A}; Y_B) > \mu I(V_A; Y_A|X_B), \tag{3.47}$$

$$I(V_B; Y_B|X_A, Y_{fE}) > \mu H(X_B), \qquad I(W_{1B}; Y_A) > \mu I(V_B; Y_B|X_A). \tag{3.48}$$

Proof. See Appendix A.7. □

Notes about the lower bound. The lower bound (3.42) is achieved by the so-called *main protocol*, which is briefly described as follows (the full description of this protocol is given in Appendix A.7). The main protocol consists of an initialization round followed by multiple iteration of a two-round *basic protocol*. The initialization round provides the

initial randomness for the first iteration of the basic protocol. The basic protocol then uses the randomness given by the previous iteration (or the initialization round) and generates new randomness for the next iteration, together with a new piece of secret key. The construction of the basic protocol is a very similar to the two-round SKE protocol of Theorem 3 for 2DMWC (with randomness), except that the protocol is also outputs new randomness. Note that the main protocol would achieve secret key rates, even if the basic protocol is used only once. Yet as the number of iterations increases, the SK rate of the main protocol approaches the lower bound, which is in fact the SK rate of the basic protocol, i.e., the cost of initialization becomes negligible. In the full-duplex channel model, the basic protocol proceeds as two parallel instances of a two-round sub-protocol: The first (resp. second) instance is initiated by Alice (resp. Bob) and achieves the key rate $Lbnd_A^{-r}$ (resp. $Lbnd_B^{-r}$), for fixed values μ, X_A, and X_B that are chosen to maximize (3.42). Each of the key rates, $Lbnd_A^{-r}$ and $Lbnd_B^{-r}$, is the sum of two terms, each corresponding to the key rate achievable in one round of the basic protocol (see (3.43)-(3.44)). The real value μ is the ratio between the number of channel uses in the first and the second rounds, e.g., $\mu = 0$ implies no channel use in the first round, implying a one-round basic protocol. The real values γ_1 and γ_2 are to relate the amount of achievable key rate as a function of the randomness obtained from channel noise.

As mentioned above, each round of the basic protocol generates some key rates. The keys rate achieved by the second round depends on the DMWCs (i.e., R_{scf} and R_{scb}), and the key rate achieved in the first round depends on the "inverse" DMWCs (see Definition 7) (i.e., $R_{scf^{-1}}$ and $R_{scb^{-1}}$). When the DMWCs are in favor of Alice and Bob (i.e., when R_{scf} and R_{scb} are positive), $Lbnd_A^{-r}$ and $Lbnd_B^{-r}$ will be positive by simply choosing $\mu = 0$; this implies a positive SK capacity. When the channels are in favor of Eve, the lower bound may remain positive (for some values of $\mu > 0$) if one of the inverse DMWCs is in favor of Alice and Bob. The study of the lower bound for BSCs in Section 3.5.6 shows

clearly the existence positive SK rates in the latter case (see Figure 3.6).

3.5.4 SK capacity: upper bound

Theorem 7. *The SK capacity of 2DMWC^{-r} is upper bounded as*

$$C_{wsk}^{2DMWC^{-r}} \leq \max_{X_A, X_B} \{Ubnd_A^{-r} + Ubnd_B^{-r}\}, \tag{3.49}$$

where

$$Ubnd_A^{-r} = \min\{H(Y_A|X_B, Y_{bE}), I(X_A; Y_B|Y_{fE})\}, \quad \textit{and} \tag{3.50}$$

$$Ubnd_B^{-r} = \min\{H(Y_B|X_A, Y_{fE}), I(X_B; Y_A|Y_{bE})\}. \tag{3.51}$$

Proof. See Appendix A.8. □

Notes about the upper bound. We note that the impossibility results of Section 3.5.1 are also implied by the above upper bound. In the case of one way communication, e.g., when the backward channel returns constant values at its ouputs, both terms $I(X_B; Y_A|Y_{bE})$ and $H(Y_A|X_B, Y_{bE})$ equal zero, implying a zero upper bound on SK rates. The same argument can be used to prove impossibility when the backward channel is noiseless and public or it is noisy but returns identical outputs to Alice and Eve.

3.5.5 2DMWC^{-r} with no leakage

Theorem 8 shows that the two bounds coincide when the two DMWCs do not leak information. This is not a new result, but rather shows that our derived bounds for this special case match the common randomness capacity of a pair of independent DMCs, given in [92].

Theorem 8. *When the DMWCs do not leak information to Eve, the bounds coincide and the SK capacity equals*

$$C_{wsk}^{2DMWC^{-r}} = \max_{X_A, X_B} \{\min\{H(Y_A|X_B), I(X_A; Y_B)\} + \min\{H(Y_B|X_A), I(X_B; Y_A)\}\}. \tag{3.52}$$

Proof. See Appendix A.9. □

3.5.6 Comparing lower and upper bounds for binary channels

Consider the 2DMWC^{-r} setup when each DMWC consists of independent BSCs with error probabilities p_m and p_e, i.e., the special case discussed in Section 3.5.2 (see Figure 3.4). We refer to this case as 2BSWC^{-r}. Lemma shows the lower and upper bounds of the SK capacity in this special case. (Recall from Section 3.4.5 that $\star$ denotes the error probability in the cascade of two BSCs.)

Lemma 16. *The SK capacity for 2BSWC^{-r} is lower bounded by*

$$C_{wsk}^{BSWC^{-r}} \geq 2\max_{\mu\in\{0,\mu_1^*,\mu_2^*\}}\{Lbnd^{-r}\},\ \textit{such that} \tag{3.53}$$

$$Lbnd^{-r} = \frac{(\mu(h(p_m\star p_e)-h(p_m))+\gamma(h(p_e)-h(p_m))_+)}{1+\mu}, \tag{3.54}$$

$$\gamma = \min\{1, \tfrac{h(p_m)}{1-h(p_m)} - \mu\}, \tag{3.55}$$

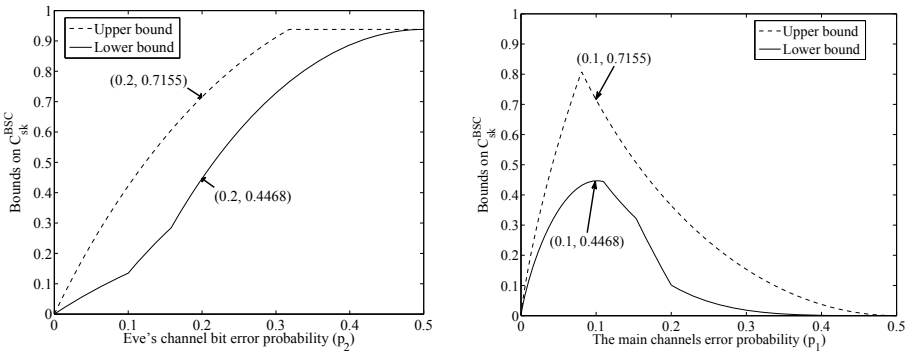
$$\mu_1^* = \tfrac{h(p_m)}{1-h(p_m)} - 1 \qquad \textit{and} \qquad \mu_2^* = \min\{h(p_m), \tfrac{1-h(p_m)}{h(p_m)}\}, \tag{3.56}$$

and is upper bounded by

$$C_{wsk}^{BSWC^{-r}} \leq 2\min\{h(p_m), h(p_m\star p_e) - h(p_m)\}. \tag{3.57}$$

Proof. See Appendix A.10. □

In Figure 3.6, we graph the lower and the upper bounds, in (3.53) and (3.57), for different values of the main channels error probability p_m and Eve's channels error probability p_e. Figure 3.6(a) illustrates the changes in the two bounds with respect to $0 \leq p_e \leq 0.5$ when $p_m = 0.1$ is fixed. According to this graph, the two bounds coincide when $p_e = 0$ or when $p_e = 0.5$. When $p_e = 0$ all information sent over the 2DMWC is seen by Eve and SKE is impossible; so, both bounds equal zero. When $p_e = .5$, the setup does not leak any information to Eve and using Theorem 8, the two bounds are expected to coincide.



(a) The bounds w.r.t p_e for $p_m = 0.1$ (b) The bounds w.r.t. p_m for $p_e = 0.2$

Figure 3.6: Lower and upper bounds on the SK capacity with respect to p_m and p_e

Figure 3.6(b) graphs the changes of the two bounds when $0 \leq p_m \leq 0.5$ and $p_e = 0.2$ is fixed. This graph shows that when the main channels are noiseless ($p_m = 0$) or completely noisy ($p_m = 0.5$), the two bounds coincide at zero and so SKE is impossible. This is expected because in the former case, no randomness exists in the system for Alice and Bob and in the latter, there is no chance of reliable communication. The graphs also show the possibility of SKE even when both DMWCs are in favor of Eve. This can be observed in Figure 3.6(a) for values of $0 < p_e < (p_m = 0.1)$ and in Figure 3.6(b) for values of $(p_e = 0.2) < p_m < 0.5$.

In Section 3.5.2, we have provided an example of a simple and efficient SKE construction. For the values $p_m = 0.1$ and $p_e = 0.2$, the construction achieves the SK rate 3%. As depicted in Figure 3.6, the lower and the upper bounds on the SK capacity for these values of p_m and p_e are about 45% and 72%, respectively. This reveals how the example construction of Section 3.5.2 works far from optimal achievable rates. As noted earlier, one can improve the performance of the protocol by using more suitable primitives.

3.6 SKE in the TWDMWC Setup

A two-way DMWC (TWDMC) [3] , shown in Figure 3.7, is a generalization of 2DMWC to the case where data transmission in forward and backward directions are not necessarily treated independently. The channel is specified by $(\mathcal{X}_A, \mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_A, \mathcal{Y}_E, P_{Y_A,Y_B,Y_E|X_A,X_B})$, which consists of input alphabets, output alphabets, and the channel probability distribution. This specification implies the 2DMWC setup of Section 3.4 as a special case when $P_{Y_A,Y_B,Y_E|X_A,X_B} = P_{Y_B,Y_{fE}|X_A}.P_{Y_A,Y_{bE}|X_B}$, by letting $Y_E \in \mathcal{Y}_E$ be written as $(Y_{fE}, Y_{bE}) \in \mathcal{Y}_{fE} \times \mathcal{Y}_{bE}$. We again assume that each party has free access to an independent source of randomness.

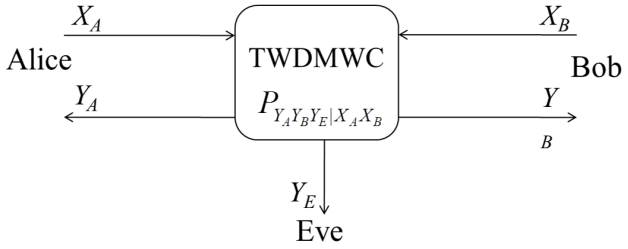


Figure 3.7: The Two-Way Discrete Memoryless Wiretap Channel (TWDMWC) setup.

3.6.1 Trivial SK capacity lower bound for TWDMWC

Tekin and Yener [85, 86] considered secure message transmission (SMT) over Gaussian and binary two-way wiretap channels. The authors proved the following set of achievable

[3]The results of this section have been published in proceedings of International Conference on Information Theoretic Security (ICITS), 2011 [8].

pairs as an inner bound on the secrecy capacity region. Letting $P = P_{X_A,X_B,Y_A,Y_B,Y_E}$,

$$\begin{aligned}\mathcal{R}_s(P) = \{ \ & (R_{s,AB}, R_{s,BA}) : R_{s,AB} \le [I(X_A;Y_B|X_B) - I(X_A;Y_E)]_+, \\ & R_{s,BA} \le [I(X_B;Y_A|X_A) - I(X_B;Y_E)]_+, \\ & R_{s,AB} + R_{s,BA} \le [I(X_A;Y_B|X_B) + I(X_B;Y_A|X_A) - I(X_A,X_B;Y_E)]_+ \ \}, \\ \mathcal{G}_{s,I} = & \bigcup_{P_{X_A,X_B} = P_{X_A}.P_{X_B}} \mathcal{R}_s(P). \end{aligned} \tag{3.58}$$

The bound on $R_{s,AB}$ (if maximized w.r.t. P_{X_A,X_B}) shows the secrecy capacity of the channel $X_A \to (Y_A, Y_E)$ when X_B is known to Bob; similar is the bound on R_{BA}. We show a trivial lower bound on the SK capacity for TWDMWC using the inner bound (3.58). Note that when free randomness is allowed to the parties, any achievable pair of secrecy rates (R_{AB}, R_{BA}) implies an achievable SK rate $R_{AB} + R_{BA}$: Alice can send her share of the key securely at rate R_{AB} and Bob can send his share security at rate R_{BA}. This suggests the following lower bound on the SK capacity, C_{wsk}^{TWDMWC}:

$$\max_{P_{X_A,X_B} = P_{X_A}.P_{X_B}} \Big[[I(X_A;Y_B|X_B) - I(X_A;Y_E)]_+ + [I(X_B;Y_A|X_A) - I(X_B;Y_E)]_+ \Big]. \tag{3.59}$$

One may ask whether the above trivial lower bounds can be improved or more generally, whether the secrecy capacity region gives the SK capacity by maximizing $R_{AB} + R_{BA}$ over all choices of achievable pairs. We give a negative answer to this question using the following simple example. Consider the TWDMC shown in Figure 3.8 which is a modified version of Shannon's modulo-two additive two-way channel example [78, Figure 4], where there exists a binary symmetric channel (BSC) with bit error probability $\frac{1}{2}$, right after the XOR operand. In this example, the channel outputs are independent of the inputs; hence, little chance of reliable message transmission. This implies that no pair of rates except $(R_{AB} = 0, R_{BA} = 0)$ is achievable; in this case, the inner bound (3.58) is tight and represents the capacity region.

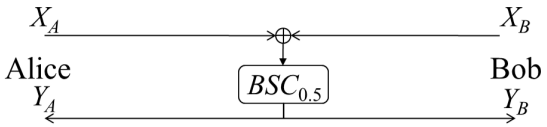


Figure 3.8: Fully-noisy TWDMC example.

Using (3.59), which is obtained from (3.58), we derive a "zero" lower bound on the SK capacity. However, this lower bound is not tight since Alice and Bob can share one random bit ($Y_A = Y_B$) each time they use the channel. The key observation is that the secret key is a function of channel noise and the parties' inputs, and it does not need to be selected a priori by the parties. This concludes that the secrecy capacity region of a TWDMWC does not necessarily give a tight lower bound on the SK capacity in general.

Remark 8. *Although (3.58) has been later improved in [40, 46, 67], we emphasize that none of the inner bounds can possibly lead to a tight bound for the SK capacity since even knowing the tight secrecy capacity region is not enough to determine the SK capacity.*

3.6.2 Tighter SK capacity lower bound for TWDMWC

We provide a new lower on the SK capacity in the TWDMWC setup that is tighter than the trivial lower bound given in the above section. Let the RVs X_A, Y_A, X_B, Y_B, and Y_E correspond to the channel probability distribution $P_{Y_A,Y_B,Y_E|X_A,X_B}$ and let V_A, W_{1A}, W_{2A}, V_B, W_{1B}, and W_{2B} be random variables from arbitrary sets $\mathcal{V}_A$, $\mathcal{W}_{1A}$, $\mathcal{W}_{2A}$, $\mathcal{V}_B$, $\mathcal{W}_{1B}$, and $\mathcal{W}_{2B}$, respectively, such that the following Markov chains hold,

$$V_A \leftrightarrow (X_A, Y_A) \leftrightarrow (X_B, Y_B) \leftrightarrow V_B, \tag{3.60a}$$

$$W_{2A} \leftrightarrow W_{1A} \leftrightarrow X_A \leftrightarrow (X_B, Y_A, Y_B, Y_E), \tag{3.60b}$$

$$W_{2B} \leftrightarrow W_{1B} \leftrightarrow X_B \leftrightarrow (X_A, Y_A, Y_B, Y_E). \tag{3.60c}$$

Theorem 9. *Taking the above variables and letting*

$$R_{stwc^{-1}} = I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A) - I(V_A, V_B; Y_E), \tag{3.61a}$$

$$R_{stwc} = I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B}) - I(W_{1A}, W_{1B}; Y_E|W_{2A}, W_{2B}), \tag{3.61b}$$

the SK capacity in the TWDMWC setup is lower bounded as

$$C_{wsk}^{TWDMWC} \geq \max_{\mu \geq 0, X_A, X_B, V_A, V_B, W_{2A}, W_{2B}, W_{1A}, W_{1B}} \Big[\frac{\mu R_{stwc^{-1}} + [R_{stwc}]_+}{1+\mu}, \tag{3.62}$$

$$s.t. \qquad P_{X_A, X_B} = P_{X_A}.P_{X_B}$$

$$I(W_{1A}; X_B, Y_B) > \mu I(V_A; X_A, Y_A|X_B, Y_B), \tag{3.63}$$

$$I(W_{1B}; X_A, Y_A) > \mu I(V_B; X_B, Y_B|X_A, Y_A) \Big]. \tag{3.64}$$

Proof. See Appendix A.11. □

Notes about the lower bound. The above lower bound is achieved using a two-round SKE protocol that is described and analyzed in Appendix A.11. We give a brief description of this protocol in the following. In round 1, Alice and Bob send i.i.d. n_1-sequences $\mathbf{X}_A^{:1}$ and $\mathbf{X}_B^{:1}$ according to the distributions X_A and X_B, and receive the n_1-sequences $\mathbf{Y}_A^{:1}$ and $\mathbf{Y}_B^{:1}$, respectively, while Eve receives $\mathbf{Y}_E^{:1}$. Alice searches in $\mathcal{V}_{A,\epsilon}^{n_1}$ to find a sequence $\mathbf{V}_A$ that is jointly typical to $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ w.r.t. $P_{(X_A,Y_A),V_A}$. Similarly, Bob searches for a sequence $\mathbf{V}_B$ that is jointly typical to $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ w.r.t. $P_{(X_B,Y_B),V_B}$. Now, $(\mathbf{V}_A, \mathbf{V}_B)$ represents the common randomness that needs to be made reliable in the second round. In round 2, Alice computes $T_A = \mathfrak{t}_A(\mathbf{V}_A)$, which can help Bob decode his $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ to $\mathbf{V}_A$. Bob also computes $T_B = \mathfrak{t}_B(\mathbf{V}_B)$. Alice and Bob encode T_A and T_B to n_2-sequences $\mathbf{X}_A^{:2} = Enc(T_A)$ and $\mathbf{X}_B^{:2} = Enc(T_B)$ and send them over the channel. The parties and Eve receive $\mathbf{Y}_A^{:2}$, $\mathbf{Y}_B^{:2}$, and $\mathbf{Y}_E^{:2}$, respectively. Alice first decodes $(\mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})$ to $\hat{T}_B \approx T_B$, and uses this for decoding $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ to $\hat{\mathbf{V}}_B \approx \mathbf{V}_B$. The decoding function relies on jointly-typical decoding for long sequences (cf. [23, Chapter 8]). Similarly Bob finds $\hat{T}_A \approx T_A$ and then $\hat{\mathbf{V}}_A \approx \mathbf{V}_A$. Now, the parties have a reliable common randomness, but it is not perfectly secure against Eve. To derive a secret key, the parties compute $\phi(\mathbf{V}_A, \mathbf{V}_B)$.

The key rate quantities R_{stwc} and $R_{stwc^{-1}}$ indicate the secure transmission rates of the two-way channel and its inverse that are taken advantage of within the second and the first communication rounds, respectively. The conditions (3.63) and (3.64) implt that the amount of uncertainty about the transmitted information in the first round can not be more than the capability of the channel for reliable transmission in the second round.

3.6.3 SK capacity upper bound for TWDMWC

Let Q be a random variable from an arbitrary set $\mathcal{Q}$ such that

$$Q \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B, Y_E)$$

forms a Markov chain.

Theorem 10. *The SK capacity in the TWDMWC setup is upper bounded by*

$$C_{wsk}^{TWDMWC} \leq \max_{Q, X_A, X_B} \Big[I(X_A; Y_B|X_B, Y_E) + I(X_B; Y_A|X_A, Y_E) + I(Y_A; Y_B|X_A, X_B, Y_E) + I(X_A; X_B|Y_E, Q) - I(X_A; X_B|Q) \Big]. \quad (3.65)$$

Proof. See Appendix A.12. □

Notes about the upper bound. The expression (3.65) gives the upper bound (3.26) on the SK capacity for the 2DMWC as a special case when $Y_E \in \mathcal{Y}_E$ equals $(Y_{fE}, Y_{bE}) \in \mathcal{Y}_{fE} \times \mathcal{Y}_{bE}$ and the channel distribution satisfies $P_{Y_A,Y_B,Y_E|X_A,X_B} = P_{Y_B,Y_{fE}|X_A}.P_{Y_A,Y_{bE}|X_B}$, and hence the Markov chain

$$(Y_B, Y_{bE}) \leftrightarrow X_B \leftrightarrow X_A \leftrightarrow (Y_A, Y_{fE})$$

holds. First, this Markov chain results in $I(X_A; X_B|Y_E, Q) \leq I(X_A; X_B|Q)$ which implies that the last two terms can be removed from the upper bound expression (3.65). The

other three terms in that expression can be further simplified as follows.

$$\begin{aligned} & I(X_A; Y_B|X_B, Y_{fE}, Y_{bE}) + I(X_B; Y_A|X_A, Y_{fE}, Y_{bE}) + I(Y_A; Y_B|X_A, X_B, Y_{fE}, Y_{bE}) \\ & \quad \overset{(a)}{\leq} I(X_A; Y_B|Y_{fE}) + I(X_B; Y_A|Y_{bE}) + I(Y_A; Y_B|X_A, X_B, Y_{fE}, Y_{bE}) \\ & \quad \overset{(b)}{=} I(X_A; Y_B|Y_{fE}) + I(X_B; Y_A|Y_{bE}) \end{aligned} \tag{3.66}$$

Inequality (a) is due to $(Y_{bE}, X_B) \leftrightarrow X_A \leftrightarrow Y_B$ and $(Y_{fE}, X_A) \leftrightarrow X_B \leftrightarrow Y_A$, and equality (b) is due to $Y_B \leftrightarrow (X_A, X_B) \leftrightarrow Y_A$. This proves the upper bound in Theorem 4.

It is easy to show that when the TWDMWC consists of independent DMWCs (i.e., 2DMWC) with physically degraded channels, then the lower and the upper bounds coincide and the SK capacity is achieved by a one-round protocol. This result as expected matches Proposition 1 for the pd-2DMWC setup.

3.6.4 Comparing trivial and new bounds for binary channels

Consider the Two-Way Binary Symmetric Wiretap Channel (TWBSWC) setup as in Figure 3.9, where the inputs and the outputs are binary variables. In this model, the two input bits X_A and X_B to the channel are XORed (added modulo two). Alice and Bob receive noisy versions of the XOR bit through independent BSCs, with noises N_{rA} and N_{rB}, respectively, where $\Pr(N_{rA} = 1) = p_{r_a}$ and $\Pr(N_{rB} = 1) = p_{r_b}$; Eve also receives a noisy version through an eavesdropping channel with noise N_E, where $\Pr(N_E = 1) = p_e$. One can relate the channel output bits to the input bits as

$$Y_A = X_A + X_B + N_{rA}, \quad Y_B = X_A + X_B + N_{rB}, \quad \text{and} \quad Y_E = X_A + X_B + N_E, \tag{3.67}$$

where '+' indicates modulo-two addition.

In this section, we compare our trivial and new lower bounds in Sections 3.6.1 and 3.6.2, applied to the case of TWBSWC. We use Theorem 9 to obtain a lower bound, $Lbnd_N$, on the SK capacity in the above model.

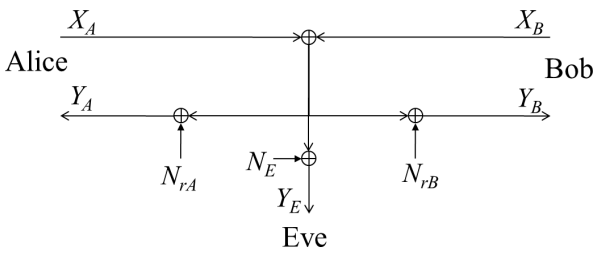


Figure 3.9: Two-way binary symmetric wiretap channel(TWBSWC).

Lemma 17. *The SK capacity in the TWBSWC setup is lower bounded as*

$$C_{wsk}^{TWBSWC} \geq Lbnd_N^{tw} \stackrel{\triangle}{=} \max_{0\leq p_1,p_2\leq 1} \left[\mu Lbnd_1^{tw} + (1-\mu)[Lbnd_2^{tw}]_+\right], \quad \textit{where} \tag{3.68}$$

$$Lbnd_1^{tw} = 1 + h(p_1 \star p_2 \star p_{r_a} \star p_{r_b} \star p_e) - h(p_1 \star p_{r_a}) - h(p_2 \star p_{r_b}), \tag{3.69}$$

$$Lbnd_2^{tw} = 1 + h(p_1 \star p_2 \star p_e) - h(p_1 \star p_{r_a}) - h(p_2 \star p_{r_b}), \tag{3.70}$$

$$\mu = \min\{\frac{1-h(p_1 \star p_{r_a})}{1-h(p_1 \star p_{r_a})+h(p_2 \star p_{r_b})}, \frac{1-h(p_2 \star p_{r_b})}{1-h(p_2 \star p_{r_b})+h(p_1 \star p_{r_a})}\}; \tag{3.71}$$

furthermore,

$$Lbnd_N^{tw} \geq \max_{0\leq p_1,p_2\leq 1} [Lbnd_2^{tw}]_+. \tag{3.72}$$

Proof. See Appendix A.14. □

Remark 9. *Lemma 17 provides a lower bound on the SK capacity that dominates the trivial lower bound, achieved from the previous work. This is shown in the sequel. Nevertheless, the lower bound (3.68) is not the highest rate one can obtain from the results of Theorem 9; in other words, one may use the result of Theorem 9 to derive a tighter lower bound in the TWBSWC model. This is left as future work.*

Secure message transmission in the above TWBSWC model has been considered in [40,85]. We choose to study the results in [40], which provide a strictly larger achievable

rate region for secure message transmission:

$$\begin{aligned}\mathcal{G}_{s,I} \;=\; & \text{convex hull of}\{(R_{s,AB}, R_{s,BA}), \;\; \text{s.t.} \;\; \exists 0 \le p_1, p_2 \le 1 : \;\; R_{s,AB} \le 1 - h(p_2 \star p_{r_b}), \\ & R_{s,BA} \le 1 - h(p_1 \star p_{r_a}), \\ & R_{s,AB} + R_{s,BA} \le [1 + h(p_1 \star p_2 \star p_e) - h(p_1 \star p_{r_a}) - h(p_2 \star p_{r_b})]_+\}. \end{aligned} \tag{3.73}$$

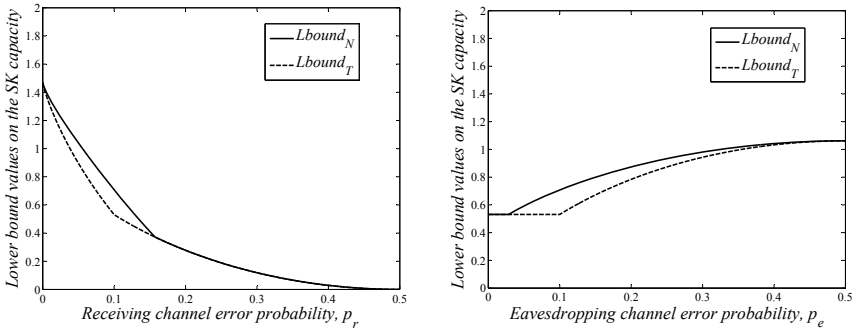
This implies the following lower bound on the SK capacity.

$$\begin{aligned} Lbnd_T^{tw} &= \max_{(R_{s,AB}, R_{s,BA}) \in \mathcal{G}_{s,I}} [R_{s,AB} + R_{s,BA}] \\ &= \max_{0 \le p_1, p_2 \le 1} [1 + h(p_1 \star p_2 \star p_e) - h(p_1 \star p_{r_b}) - h(p_2 \star p_{r_a})]_+ \\ &= \max_{0 \le p_1, p_2 \le 1} [Lbnd_2^{tw}]_+, \end{aligned} \tag{3.74}$$

where the last equality follows from (3.70). Comparing (3.72) and (3.74) leads to the following corollary.

Corollary 1. *The new lower bound (3.68) on the SK capacity in the TWBSWC setup is always greater than or equal to the trivial lower bound (3.74), i.e.,*

$$Lbnd_N^{tw} \ge Lbnd_T^{tw}. \tag{3.75}$$



(a) $0 \le p_r \le 0.5$ and $p_e = 0.1$ (b) $0 \le p_e \le 0.5$ and $p_r = 0.1$

Figure 3.10: Comparison of the lower bound values with respect to the error probabilities.

To better understand the gap between the trivial lower bound $Lbnd_T^{tw}$ and the newly proved lower bound $Lbnd_N^{tw}$, we evaluate these two quantities with respect to different

choices of channel error probabilities in Figure 3.10, where the two bounds are indicated by dashed and solid lines, respectively. For simplicity, we assume that the receiving channel noise for Alice and Bob is the same, i.e., $p_{r_a} = p_{r_b} = p_r$. Figure 3.10(a) compares the two lower bound values with respect to p_r when $p_e = 0.1$. Observe the non-zero gap between $Lbnd_N^{tw}$ and $Lbnd_T^{tw}$ for receiving channel noise $p_r < 0.15$. This confirms that our new lower bound strictly dominates the trivial bounds from the previous results on secure message transmission. Figure 3.10(b) compares the bound values as functions of p_e when $p_r = 0.1$. It shows the gap between the two bounds expect for much small or much large values of the eavesdropping channel error probability p_e.

3.7 From Weak to Strong Capacity: Equality Conditions

Maurer and Wolf [60] suggested an alternative definition to the weak SK capacity, called strong SK capacity, where the secrecy requires absolutely negligible leakage of information to the adversary. See Definitions 27 and 29 to recall the two variants of the SK capacity. The authors furthermore provided an interesting proof for the equality of weak and strong SK capacities for the early two setups in [3, 26, 59, 96]. Followup work (including ours in the above) however studied new settings of SKE by considering the weak SK capacity and without discussing whether the results also hold for the strong definition. In this section, we investigate general conditions for any DM setup that allow us to derive the equality of weak and strong SK capacities. We also extend this study to secure message transmission (SMT) and investigate the equality of weak and strong *secrecy capacities*. For SKE, we show that weak and strong SK capacities are equal for any setup that allows reliable transmission in any direction. For SMT, the secrecy capacities are equal when the setup allows the sender to use randomness. We furthermore provide trivial counterexamples that show these sufficient conditions are not always necessary for the

equality of the capacities. Whether the conditions can be removed or relaxed by tight (necessary and sufficient) conditions remains an interesting question for future. [4]

3.7.1 Equality of weak and strong SK capacities

We revisit Maurer-and-Wolf's (MW) proof for the equality of weak and strong SK capacities and study whether it can be applied to any DM setup. The work gives two different equality proofs for the two setups of (1) correlated randomness and public discussion channel (DMMS+PDC) [3, 59], and (2) one-way discrete memoryless wiretap channel (DMWC) [26, 96]. We focus on the second proof method because it is more generic and does not rely on PDC as a free noiseless channel resource. The MW approach proceeds in two phases.

Phase 1: Equality of weak and uniform SK capacities. This phase shows that the weak and the uniform (see Definitions 27 and 28) SK capacities are equal. This is done by constructing, for arbitrarily small $\delta > 0$, an (R_s, δ)-uniformly-secure SKE protocol Π_u by using an (R_s, δ')-weakly-secure protocol Π_w (for suitably small δ'). The protocol Π_u is obtained roughly by repeating the protocol Π_w independently many times to get sequences of i.i.d. secret keys, and accept these sequences only if they are ϵ-typical with respect to the output distribution of Π_w, for suitably small $\epsilon > 0$ (determined from δ).

The proof in this phase does not depend on any communication resources (sources/channels) in addition to those required repeatedly for executing the weakly-secure protocol Π_w. This concludes that the result can be extended to any DM setup.

Lemma 18. [60, Lemma 5] *For any discrete memoryless setup $\mathfrak{S}$, the weak and uniform SK capacities are equal, i.e., $C_{wsk}^{\mathfrak{S}} = C_{usk}^{\mathfrak{S}}$.*

Phase 2: Equality of uniform and strong SK capacities. The second phase shows

[4] The results of this section have been published in proceedings of Foundations and Practice of Security (FPS) 2012 [11].

how to construct, for arbitrarily small $\delta > 0$, an (R_s, δ)-strongly secure SKE protocol Π_s using an (R_s, δ')-uniformly-secure one Π_u (for suitably small δ') without sacrificing the key rate. The construction consists of four steps: (i) *independent repetition* of the uniformly-secure protocol, (ii) *information reconciliation* with universal hashing, (iii) *privacy amplification* using a seeded-extractor, and (iv) *uniformization*. For information reconciliation, Alice uses the wiretap channel to send error-correction bits. For privacy amplification, she uses her (free) independent source to generate uniformly random bits and sends them to Bob over the wiretap channel, so they both agree on the random seed used in the extractor. By repeating the uniformly-secure protocol sufficiently many times, in step (i), the number of channel uses in steps (ii) and (iii) becomes negligible and the key rate tends toward that of the uniformly-secure protocol.

The MW approach is indeed generic enough so that a slight modification of the proof (esp. the key rate analysis) makes it applicable to most of the current setups, for instance 2DMWC as well as the DMMS+DMWC setup [48, 69]. Yet, the proof is based on two main assumptions that make it not adaptable to "all" setups.

(i) There is a channel with positive (reliability) capacity in at least one direction.

(ii) There is a free local source of randomness available to at least one party.

Assumption (i) is hidden in the proof as when a one-way DMWC has positive weak SK capacity, it is definitely capable of reliable transmission. The statement however does not necessarily hold in all communication scenarios since there are instances of the TWDMWC setup (see Figure 3.8) that despite positive SK capacity, do not allow for even a single bit of reliable transmission. This implies that reliable transmission is not generally an implicit capability of all setups with positive SK capacity and hence is required to be checked separately in each case. Similarly, Assumption (ii) does not hold in scenarios where local randomness is not free. We note that the freeness of local

randomness is not the main issue. The MW approach requires generation of uniform randomness of length negligible to the key length; hence, using a local random source with a constant cost does not affect the key rate analysis and so the equality result. However, the existence of local randomness is crucially required by the MW approach. The 2DMWC^{-r} setup in Section 3.5 is an example where no local randomness is not provided as a resource.

We ask whether the proof can be modified so that any of the above assumption are not necessary for the equality proof. We give a positive answer to this by providing a modified proof that does not require Assumption (ii) to hold. Our modification targets specifically step (iii), privacy amplification, where we use a (deterministic) two-source extractor in place of the seeded extractor. For completeness, we describe the modified construction below. We denote the keys returned by the uniformly-secure protocol Π_u by $S_{uA} \in \mathcal{S}_u$ for Alice and $S_{uB} \in \mathcal{S}_u$ for Bob. We also use $\mathbb{V}_{uE}$ to denote Eve's view of this protocol. Let $K = \log|\mathcal{S}_u|$, N be a sufficiently integer, and L and r be integers such that $L \leq \delta_1 NK$ and $r \geq 2NK(1-\delta_4)$, for sufficiently small δ_1, δ_4 as mentioned in Appendix A.15.

Step (i): Independent repetition. Alice and Bob repeat Π_u over the setup $\mathfrak{S}$ independently $2N$ times. This results in the pairs of independent sequences (S_{uA1}^N, S_{uA2}^N) for Alice, (S_{uB1}^N, S_{uB2}^N) for Bob, and the view $(\mathbb{V}_{uE1}^N, \mathbb{V}_{uE2}^N)$ for Eve.

* This step requires resources for $2N$ repetition of Π_u that costs $2NCost_{\Pi_u}^{\mathfrak{S}}$.

Step (ii): Information reconciliation. Either party finds suitable functions h_1 and h_2 from a universal family of hash functions $\mathcal{H} : \mathcal{S}_u^N \to \{0,1\}^L$, applies h_1 and h_2 to their pair of sequences and sends the outputs reliably (not securely) to the other party. This additional information lets the parties come up with equal pairs of sequences with high probability. For instance, Alice can find functions h_1 and h_2 in $\mathcal{H}$ such that the knowledge of $(h_1(S_{uA1}^N), h_2(S_{uA2}^N))$ together with (S_{uB1}^N, S_{uB2}^N) can be used to obtain (S_{uA1}^N, S_{uA2}^N) with

high probability. We denote by (S'^N_{uA1}, S'^N_{uA2}) and (S'^N_{uB1}, S'^N_{uB2}) the sequences owned by Alice and Bob at the end of this step, respectively. We also use $(\mathbb{V}_{rE1}, \mathbb{V}_{rE2})$ to denote Eve's view of the information reconciliation step for the two key sequences, respectively.

* This step requires resources for transmission of $2L$ bits reliably in either direction.

Step (iii): Privacy amplification. Let $Bin : \mathcal{S}_u^N \to \{0,1\}^n$, where $n = \lceil NK \rceil$, be an injective binary mapping function. Alice calculates the n-bit strings $\tilde{S}_{A1} = Bin(S'^N_{uA1})$ and $\tilde{S}_{A2} = Bin(S'^N_{uA2})$, and Bob calculates $\tilde{S}_{B1} = Bin(S'^N_{uB1})$ and $\tilde{S}_{B2} = Bin(S'^N_{uB2})$. Alice and Bob apply the two-source extractor $TExt : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^r$ of Lemma 7 on their n-bit strings to extract strongly-secure keys over the set $\mathcal{S} = \{0,1\}^r$. Alice calculates $\tilde{S}_A = TExt(\tilde{S}_{A1}, \tilde{S}_{A2})$ and Bob calculates $S_B = TExt(\tilde{S}_{B1}, \tilde{S}_{B1})$. Eve's overall view of this protocol is denoted by $View_E = (\mathbb{V}^N_{uE1}, \mathbb{V}^N_{uE2}, \mathbb{V}_{rE1}, \mathbb{V}_{rE2})$.

Step (iv): Uniformitarian.. Alice obtains S_A by sending $\tilde{S}_A$ over a probabilistic channel, with uniform distribution $P_{S_A|\tilde{S}_A}$, that minimizes the error probability $\Pr(S_A \neq \tilde{S}_A)$ over all such distributions.

Appendix A.15 shows that Π_s is a $(C^{\mathfrak{S}}_{usk}, \delta)$-strongly-secure protocol for arbitrarily small $\delta > 0$. The requirement for the proof is that the reliability capacity $C^{\mathfrak{S}}_m$ be positive, since the construction requires to send $2L$ information bits reliably in one direction.

Lemma 19. *Let the maximum reliability capacity $C^{\mathfrak{S}}_m$ be positive. For any $\delta > 0$, the protocol Π_s, constructed as above, is a $(C^{\mathfrak{S}}_{usk}, \delta)$ strongly-secure SKE protocol for the setup $\mathfrak{S}$, implying $C^{\mathfrak{S}}_{ssk} = C^{\mathfrak{S}}_{usk}$.*

Proof. See Appendix A.15. □

Remark 10. *Another approach to privacy amplification (step (iii)) without requiring randomness is to applying a deterministic (one-source) extractor. Assuming that the output distribution of the uniformly-secure SKE protocol is known, one can use deterministic extractors whose existence has been proved (see Lemma 8). The use of two-source extractors*

in the above is preferred as they are constructive and do not assume any knowledge about the distribution of S_{uA}, S_{uB}, and $\mathbb{V}_{uE}$ except those implied by the protocol definition.

Combining Lemmas 18 and 19 concludes the following.

Corollary 2. *The weak and the strong SK capacities are equal for any discrete memoryless setup $\mathfrak{S}$ that allows reliable transmission in at least one direction, i.e., $C_m^{\mathfrak{S}} > 0$.*

3.7.2 Equality of weak and strong secrecy capacities

We follow a similar approach to the above to give a construction of a strongly-secure secure message transmission (SMT) protocol using a weakly-secure SMT protocol. In SMT, either Alice or Bob wants to send a message reliably to the other party, such that the message remains private to Eve. We use *forward (or backward) direction* to mention the direction of message transmission from Alice to Bob (or vice versa). We first give the deifications of an SMT protocol and the secrecy capacity in a setup.

Definition 36 (Secrecy capacity)**.** *For real constants $R_s \geq 0$ and $\delta > 0$, a SMT protocol, Π, using a discrete memoryless setup, $\mathfrak{S}$, is called is called (R_s, δ)-weakly, respectively, -strongly secure if*

$$\textit{reliability:} \quad \Pr(M = \hat{M}) \geq 1 - \delta, \tag{3.76a}$$

$$\textit{randomness:} \quad \frac{K}{Cost_{\Pi}^{\mathfrak{S}}} \geq R - \delta, \tag{3.76b}$$

and

$$\textit{weak secrecy:} \quad H(M|View_E) \geq K(1 - \delta), \tag{3.77}$$

respectively,

$$\textit{strong secrecy:} \quad H(M|View_E) \geq K - \delta, \tag{3.78}$$

where $View_E$ is Eve's view of the communication. The weak/strong forward/backward secrecy capacity of the setup $\mathfrak{S}$, respectively denoted by $C^{\mathfrak{S}}_{wfs}$, $C^{\mathfrak{S}}_{wbs}$, $C^{\mathfrak{S}}_{sfs}$, and $C^{\mathfrak{S}}_{sbs}$, is the largest $R_s \geq 0$ such that, for any arbitrarily small $\delta > 0$, there exists an (R, δ)-weakly/strongly forward/backward SMT protocol.

Definition 36 trivially implies that strong secrecy in message transmission implies weak secrecy, i.e., $C^{\mathfrak{S}}_{sfs} \leq C^{\mathfrak{S}}_{wfs}$ and $C^{\mathfrak{S}}_{sbs} \leq C^{\mathfrak{S}}_{wbs}$. In the sequel, we acquire conditions that allow us to write the above inequalities in the opposite direction. We discuss this for the forward (Alice-to-Bob) direction of SMT (the backward direction can be shown similarly). Let $C^{\mathfrak{S}}_{wfs}$ be the weak forward secrecy capacity of setup $\mathfrak{S}$. We give a four-step construction that for any $\delta > 0$, gives a $(C^{\mathfrak{S}}_{wfs}, \delta)$-strongly-secure forward SMT protocol Π_s by using a $(C^{\mathfrak{S}}_{wfs}, \delta')$-weakly-secure forward SMT protocol Π_w for sufficiently small δ'.

Similarly to Section 3.7.1, let K and N be sufficiently large integers and $L \leq \delta_1 NK$ and $r \geq 2NK(1-\delta_4)$ be integers as chosen in Appendix A.15. Let Π_w be capable of sending K bits of information from Alice to Bob, $M \in \{0,1\}^r$ be the message to be sent by Π_s, and the function $Inv : \{0,1\}^\rho \times \{0,1\}^r \to \{0,1\}^n \times \{0,1\}^n$, where $n = NK$ and $\rho = 2n - r$, be the inverter for the two-source extractor $TExt : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^r$ of Lemma 7.

Step (i): Message expanding. Alice expands the message M to $(S_{A1}, S_{A2}) = Inv(Rnd, M)$, where $Rnd \in \{0,1\}^\rho$ is uniformly random.

* This step requires resources for ρ uniform bits, where $\rho = 2NK - r \leq 2NK\delta_4$.

Step (ii): Split and sent. Alice splits S_{A1} and S_{A2} into N independent K-bit pieces, $(S_{A1,i})_{i=1}^2$ and $(S_{A2,i})_{i=1}^N$, and sends each piece independently using the weakly-secure protocol Π_w. Bob obtains message estimates $S_{B1} = (S_{B1,i})_{i=1}^N$ and $S_{B2} = (S_{B2,i})_{i=1}^N$. Eve's view of this is $(\mathbb{V}_{E1}, \mathbb{V}_{E2}) = (\mathbb{V}_{E1,i}, \mathbb{V}_{E2,i})_{i=1}^N$.

* This step requires resources for $2N$ repetition of Π_w that costs $2NCost^{\mathfrak{S}}_{\Pi_w}$.

Step (iii): Information reconciliation. Alice finds error-correction functions h_1 and h_2 from a universal family of hash functions $\mathcal{H} : \{0,1\}^n \to \{0,1\}^L$. She calculates $h(S_{A1})$ and $h(S_{A2})$, and sends them reliably to Bob. Bob uses these to decode (S_{B1}, S_{B2}) into $(\hat{S}_{A1}, \hat{S}_{A2})$. Eve's view of this is $(\mathbb{V}_{rE1}, \mathbb{V}_{rE2})$.

* This step requires reliable transmission of $2L$ bits, which costs at most $2LCost^{\mathfrak{S}}_{\Pi_w}$.

Step (iv): Message extraction. Bob calculates $\hat{M} = TExt(\hat{S}_{A1}, \hat{S}_{A2})$.

Proving that the above construction is strongly-secure requires the setup to allow local randomness for Alice to use in step (ii), message expansion. The proof is very similar to that of Lemma 19 in Appendix A.15 for SKE, hence omitted. The ultimate result of is the following.

Corollary 3. *For any discrete memoryless setup $\mathfrak{S}$, the weak and the strong (forward or backward) secrecy capacities are equal if the setup allows the sender to use randomness.*

3.7.3 Equality conditions: sufficiency vs. necessity

Maurer and Wolf [60] proved the equality of weak and strong SK capacities for the setups in [3,26,59,96]. Their approach can also be applied to a general discrete memoryless setup as long as the following two conditions hold: (1) randomness is accessible, and (2) reliable transmission is possible. We have modified this approach and proved the above equality only requiring condition (2). We have also provided a proof for the equality of the weak and the strong secrecy capacities in SMT, where we require condition (1). This suggests a duality between SMT and SKE. In both cases, we have not shown whether these derived conditions are necessary. In the following, we argue against their necessity.

We argue that the condition of Corollary 2 is not always necessary. A trivial counterexample is a multiple-source $(\mathcal{X}_A, \mathcal{X}_B, \mathcal{X}_E)$ with per-use cost of 1 and distribution P_{X_A,X_B,X_E} that generates $X_A = X_B$ for Alice and Bob as well as X_E for Eve such that

Table 3.2: The requirements for proving the equality of capacities.

Requirement	**MW approach** (SK capacity)	**Our approach** (SK capacity)	**Our approach** (Secrecy capacity)
Randomness access	required	-	required
Reliable transmission	required	required	-

$H(X_A|X_E) = c$ for some constant $c > 0$. The setup has zero reliability capacity as there is no communication channel. However, Alice and Bob can establish a strongly-secure key of rate c by generating many source outputs and applying a two-extractor. It is easy to show that both weak and strong SK capacities equal c. Similarly, the condition of Theorem 3 is not always necessary. Consider a scenario where Alice is connected to Bob through a one-way noisy channel that does not leak to Eve. Alice can send a message to Bob using deterministic coding and without requiring randomness. Both weak and strong secrecy capacities in this case equal the channel (reliability) capacity. It is interesting to know whether there are non-trivial setups for which these conditions are not required, and to derive necessary and sufficient conditions for the equality of weak and strong secrecy/SK capacities.

3.8 Conclusion

The work on key establishment over physical noisy channels is inspired by real-life communication between peers, e.g., in wireless environments where the communication between the parties, Alice and Bob, can be intercepted by neighbors, Eve, in the communication range. We modeled the communication environment by a discrete memoryless setup and defined the secret-key (SK) capacity to indicate the highest key rate that can be achieved using resources in the setup. We first considered 2DMWC which consists of a pair of independent noisy wiretap channels between Alice and Bob in the two directions. We

proved lower and upper bounds on the SK capacity in this setup. The lower bound is achieved by a two-round SKE protocol that uses a two-level coding construction. We showed that the lower and upper bounds coincide in the following two cases: (1) When the DMWCs are physically degraded, where the SK capacity is achieved by a one-round SKE protocol, and (2) when the channels are stochastically degraded with independent channels and under the condition that one of the parties sends only i.i.d. variables, where the capacity is achieved by a two round protocol. However, our derived bounds are not tight in general. This can be clearly observed from the analysis of the SK capacity over binary channels. *Improving the bounds to provide tighter estimations of the SK capacity in general is a subject of future work.*

The above study relies on two restrictive assumptions about the communication environment: (1) local randomness is freely available to the parties (similar to all above referenced work) and (2) the two DMWCs are independent and have no influence on each other. We removed the first assumption by considering SKE over a pair of noisy channels when there is no initial randomness available to the parties. Although without randomness SKE is impossible over many of the currently proposed setups, we showed that the task can be fulfilled in cases where parties can interact over the 2DMWC setup. We obtained lower and upper bounds on the SK capacity that coincide when the channels leak zero information to Eve. We applied the bounds to the case of binary channels to show the gap between the two bounds that remains to be bridged. *This work also suggests asking the possibility of other cryptographic primitives when channel noise is the only source of randomness.*

We removed the second assumption above, by considering SKE using two-way wiretap channels that allow transmission in the forward and the backward directions put influence on each other. We discussed how current results on secure message transmission (SMT) over two-way wiretap channels can be used to obtain a "trivial" lower bound on the

SK capacity. We then showed that this trivial bound can be improved by a two-round protocol that can achieve higher SK rates. We applied the results to the case of two-way binary channels to show the improvements of the new lower bound. We also derived an upper bound on the SK capacity and discussed cases where the lower and the upper bounds coincide. *It has not been shown whether any of the bounds are tight in general, or more specifically, whether one can improve the lower bound by allowing more rounds of interaction.*

All the above results involve the weak notion of SK capacity which requires the information leakage to Eve to be negligible only in "rate". A stronger security requirement is to have negligible total information leakage. The final section of this chapter showed that weak and strong SK capacities are equal for any discrete memoryless setup that allows reliable transmission in at least one direction. We investigated a similar strengthening of the secrecy capacity for the SMT problem and showed that the weak and the strong secrecy capacities are equal for any discrete memoryless setup that allows the sender to use randomness. Trivial counterexamples show that these sufficient conditions are not always necessary for the equality of the capacities. *Whether the conditions can be completely removed or shall be replaced by tight (necessary and sufficient) conditions remains an interesting question for future.*

Chapter 4

Manipulation Detection over Physical-Layer Channels

Message authentication using cryptographic primitives has been a well studied subject in information security: The sender wants to deliver a message to the receiver in the presence of an adversary who can manipulate the communication. The goal of manipulation detection is to enable the receiver to detect adversarial manipulations with high probability. The problem, also known as *manipulation detection*, was first addressed by Gilbert et al. [42] who constructed "codes which detect deception". Simmons [80–82] later gave a formal treatment of the problem with followup work on developing bounds and constructions for such codes. Information theoretic approaches to manipulation detection propose appending to the message a relatively short authentication tag, calculated based on the message and a shared secret key between the legitimate parties. In the computational setting, message authentication can also be attained via public key cryptography using signature schemes.

The classical message authentication problem is defined over a higher layer of the network where communicating nodes, Alice and Bob, are connected to each other through links to other nodes, say Eve. This translation of the problem naturally allows Eve to have complete read and write access to the communication and to arbitrarily modify messages in real-time, as in the strong Dolev-Yao attacker model [35]. Keyless detection of such a powerful adversarial manipulation with the message is impossible. In lower layers of the network (e.g., a wireless environment) where Alice and Bob are connected by a physical-layer channel, a less powerful adversary with limited read and write access

is present [57, 68, 84] and hence, the seemingly impossible task of keyless manipulation detection may become possible. We ask the following question.

Q1. *Is is possible to detect adversarial manipulation with a physical-layer channel without having access to a shared key or correlated randomness?*

Our work

In this chapter [1] , we study the problem of manipulation detection in an abstract communication model that partially leaks its content to an adversary as well as leaves it open to "algebraic" manipulation, i.e., the adversary can decide on an adversarial noise sequence to be added to the transmitted sequence. We use the algebraic manipulation setting as a model to capture the adversary's write access over a physical-layer channel. This is a well-studied model and covers a wide class of adversarial channel models considered in information and communication theory, c.f. [43, 54, 55]. We note that this problem is different from the classical message authentication also because we seek protection only against the substitution attack that means changing a transmitted message, and not impersonation where the adversary generates and sends a message. It is easy to observe that keyless protection against the impersonation attack is impossible.

The above problem can be seen as an extension of the work in [24] on leakage-free *algebraic manipulation detection (AMD)* to cases where there is information leakage to the adversary. We therefore follow the same terminology as in [24] develop our results as a followup on that work. We refer to codes that detect algebraic manipulation in our communication model as *leakage-resilient (LR)-AMD* codes. The study of LR-AMD codes is of independent interest as we show application of these codes to other areas of cryptography such as robust nonperfect secret sharing, besides manipulation detection over (physical-layer) wiretap channels.

[1] The results of this chapter have been submitted to Advances in Cryptology EUROCRYPT 2013 [4].

Formalization of LR-AMD codes. We start by giving formal definition of weak and strong LR-AMD codes, respectively, depending on whether manipulation detection is provided for a randomly or an adversarially chosen message. The leakage bound in LR-AMD codes is specified in terms leakage rate parameter $0 \leq \alpha \leq 1$ which roughly indicates the fraction of message/randomness that can be leaked. We measure the *optimality* of an LR-AMD code construction by its *effective tag length* as well as its *asymptotic rate*: The former is the extra storage required for storing a coded message and the latter is the asymptotic information rate (message length divided by the code length). These measures allow us to study optimality of code families in concrete and asymptotic ways.

LR-AMD codes: bounds and constructions. We prove lower bounds on the effective tag lengths of weak and strong LR-AMD codes. The new lower bounds reveal how leakage affects the redundancy/asymptotic rate of codes for a required security level. It is interesting to see that while strong LR-AMD code families with asymptotic rate of 1 may exist, it is impossible to have weak LR-AMD code families with asymptotic rate higher than $1/(1+\alpha)$. We also derive general transformations from AMD to LR-AMD coding which prove that currently existing optimal (in asymptotic rate/effective tag length) weak/strong AMD codes can be used as optimal weak/strong LR-AMD codes. While in strong LR-AMD codes the redundancy can become vanishingly small compared to the message length, for weak LR-AMD codes it will be proportional to the message length. We also consider a particular type of leakage, called *block leakage*, and design a block-leakage-resilient (BLR)-AMD code construction that requires negligible redundancy.

LR-AMD codes: applications. We show two applications of LR-AMD and BLR-AMD codes in cryptography: First, adding robustness to linear *nonperfect* secret sharing schemes and second, detection of algebraic manipulation over wiretap channels. We show how strong systematic LR-AMD codes can be used to add robustness to linear nonperfect secret sharing schemes that leak less than half of the secret to the adversary. We

furthermore consider a particular class of nonperfect schemes, called *somewhere perfect*, and show that schemes of this class with any leakage rate can be made robust using BLR-AMD codes.

For the second application, we study erasure (resp. symmetric) type of wiretap channels consisting of a noiseless, but additively tamperable channel main channel as well as a u-ary erasure (resp. symmetric) wiretapping channel that erases (resp. corrupt) codeword symbols with some probability p. We prove that strong LR-AMD codes detect algebraic manipulation over erasure wiretap channels with $p > 0.5$. More interestingly, we show that using our deterministic BLR-AMD construction allows for smaller error probabilities, as low as $p > u^{-1}$. Adaption of this result to symmetric wiretap channels concludes detection guarantees for error probability $u^{-1} - u^{-2} < p \leq 1 - u^{-1}$. We next show how our BLR-AMD code construction can be composed with other primitives to provide unlimited bitwise manipulation detection, in addition to privacy, in message transmission or key agreement over binary symmetric and binary erasure channels.

AMD for online adversarial channels. We consider another type of communication with leakage, where the codeword is transmitted as a sequence of blocks and the adversary's view evolves with the number of transmitted codeword blocks; in other words, although she eventually observes the whole codeword, the adversary can only use her current view at a time to generate a particular noise element. Note that this scenario cannot be generally modeled by our formulation of LR-AMD codes since here, the adversary's view varies over time. For online adversaries, we introduce a *delay* as a function of the codeword length. The delay parameter captures the computation time required by the adversary to process the view information and to calculate the next bit of the adversarial noise. We consider *linear-delay* and *constant-delay* adversaries whose delay is a linear (γl for $0 \leq \gamma \leq 1$) and constant $0 \leq \Gamma \leq l$ function of the codeword length (l). We show that strong AMD codes can be used to protect against any ($\gamma > 0$)-linear-delay adversary,

but not all Γ-constant-delay adversaries. Further studying constant-delay adversaries, we propose unary codes which achieve arbitrarily small decoding error probability for the 1-constant-delay (the strongest positive delay) adversary. Unfortunately, the rate of this code approaches zero by increasing the code length. Investigating the possibility of protection against constant-delay adversaries remains open.

4.1 Algebraically Manipulable Detection with Leakage

A leakage-resilient algebraic manipulation detection (LR-AMD) code is specified by a pair of encoding/decoding functions $Enc : \mathcal{M} \to \mathcal{X}$ and $Dec : \mathcal{X} \to \mathcal{M} \cup \{\perp\}$, where $\mathcal{M}$ is the message space, $\mathcal{X}$ is and additive group consisting of the codeword elements, and $\perp$ represents the manipulation detection symbol. Fig. 4.1 shows Alice using this code to send Bob a message reliably over an algebraically manipulable channel with partial leakage. To send a message $M \in \mathcal{M}$, Alice calculates the codeword $X = Enc(M)$ and sends it over the channel that leaks some information Z to Eve. Eve uses this view to choose $\Delta = \mathcal{A}dv(Z) \in \mathcal{X}$, for some computationally unbounded adversarial function $\mathcal{A}dv : \mathcal{X} \to \mathcal{Z}$, and replaces X with $X' = X + \Delta$. Upon receiving X', Bob retrieves the message as $\hat{M} = Dec(X')$. We say the *decoding fails* whenever $\hat{M} \notin \{M, \perp\}$.

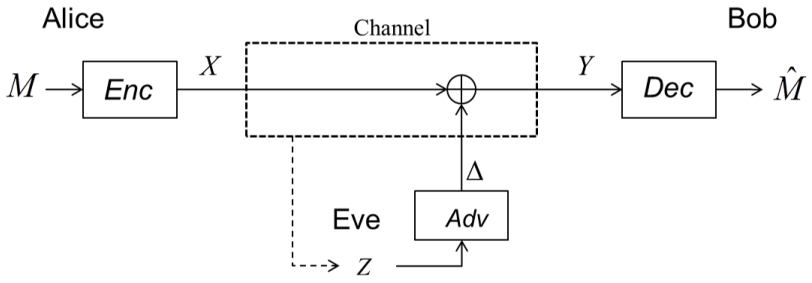


Figure 4.1: Algebraic manipulable channel with leakage.

An LR-AMD code must satisfy *correctness* and *security*. The former requires that

$\hat{M} = M$ always holds for $\Delta = 0$, and the latter requires small decoding failure probability (for $\Delta \neq 0$). For the purpose of code construction, we mainly consider *systematic* LR-AMD codes whose codeword is obtained by simply appending to the message a tag applying a tag generation function. A systematic LR-AMD code is specified by its tag generation function $\mathbf{Tag} : \mathcal{M} \to \mathcal{T}$ such that $\mathcal{M}$ and $\mathcal{T}$ are additive groups. The correctness property of a systematic LR-AMD code follows immediately from its construction and hence the only requirement for such codes is security.

Depending on whether or not randomness is allowed in the tag generation function, two types of LR-AMD codes can be defined. A *weak LR-AMD code* provides security guarantee for a randomly chosen message and this lets the code construction be deterministic. In a *strong LR-AMD code* however, the security property must hold for an adversarillay chosen message and hence the code must be randomized. The leakage bound in LR-AMD codes is specified in terms of a leakage rate parameter $0 \leq \alpha \leq 1$, measure by min-entropy (see Definitions 15 and 16 in Section 2.3 for weak and block sources), which roughly indicates the fraction of message/randomness that can be leaked. In this work, we only consider "deterministic" weak LR-AMD codes, defined as follows.

Definition 37 (Weak LR-AMD code)**.** *Let $Enc : \mathcal{M} \to \mathcal{X}$ and $Dec : \mathcal{X} \to \mathcal{M} \cup \{\perp\}$ be the deterministic encoding and decoding functions of a block code, and $\mathfrak{M}$ and $\mathfrak{X}$ be the sizes of $\mathcal{M}$ and $\mathcal{X}$, respectively. For $0 \leq \alpha < 1$ and $0 \leq \epsilon \leq 1$, the above code is called a $(\mathfrak{M}, \mathfrak{X}, \alpha, \epsilon)$-weak LR-AMD code if $\forall m : \ Dec(Enc(m)) = m$, and for any random variables $M \in \mathcal{M}$ and $Z \in \mathcal{Z}$ such that M is $(1-\alpha)$-weak conditioned on Z, and any computationally unbounded adversary $\mathcal{A}dv : \mathcal{Z} \to \mathcal{X}$ it holds:*

$$\Pr_{M,\mathcal{A}dv}\Big(Dec(Enc(M) + \mathcal{A}dv(Z)) \notin \{m, \perp\}\Big) \leq \epsilon. \tag{4.1}$$

The code is systematic if $Enc(M) = (M, \mathbf{Tag}(M))$ for some function $\mathbf{Tag} : \mathcal{M} \to \mathcal{T}$, where $\mathcal{M}$ and $\mathcal{T}$ are additive groups.

A strong LR-AMD code, however, must provide small failure probability for all messages, even one chosen by the adversary, in the message space. Satisfying this property requires the encoding function to be randomized; because otherwise, the adversary can choose $\delta = x_2 - x_1$ for two codewords $x_1 = Enc(m_1)$ and $x_2 = Enc(m_2)$; hence, there is a message m_1 for which the security does not hold since the decoding returns m_2.

Definition 38 (Strong LR-AMD Code)**.** *Let $Enc : \mathcal{R} \times \mathcal{M} \to \mathcal{X}$ be the randomized encoding function and $Dec : \mathcal{X} \to \mathcal{M} \cup \{\perp\}$ be the (deterministic) decoding function of a block code, and let $\mathfrak{M}$, $\mathfrak{R}$, and $\mathfrak{X}$ be the sizes of $\mathcal{M}$, $\mathcal{R}$, and $\mathcal{X}$, respectively. For $0 \leq \alpha < 1$ and $0 < \epsilon \leq 1$, the above code is called a $(\mathfrak{M}, \mathfrak{X}, \mathfrak{R}, \alpha, \epsilon)$-strong LR-AMD code if $\forall m :\ Dec(Enc(m)) = m$, and for any random variables $R \in \mathcal{R}$ and $Z \in \mathcal{Z}$ such that R is $(1-\alpha)$-weak conditioned on Z, and any computationally unbounded adversary $\mathcal{A}dv : \mathcal{Z} \to \mathcal{X}$, it holds*

$$\forall m : \quad \Pr_{R,\mathcal{A}dv}\Big(Dec(Enc(R;m) + \mathcal{A}dv(Z)) \notin \{m, \perp\}\Big) \leq \epsilon. \tag{4.2}$$

The code is systematic if $Enc(R;M) = (M, \mathbf{Tag}(R;M))$ for some function $\mathbf{Tag} : \mathcal{R} \times \mathcal{M} \to \mathcal{R} \times \mathcal{G}$, where $\mathcal{M}$, $\mathcal{R}$, and $\mathcal{G}$ are additive groups.

Remark 11. *Definitions 37 and 38 restrict leakage in terms of leftover min-entropy (weak sources). The work on leakage resilient cryptography (cf. [39]) however often uses a more natural definition by assuming the data (message/key/randomness) has uniform distribution and the adversary can apply any function with limited length on the data. Note that our definitions are give in a more general way so that they follow the previous work and also cover cases where the data is not a priori uniform.*

The weak and the strong AMD code definitions in [24] are special cases of Definitions 37 and 38, when there is no leakage to the adversary, $\alpha = 0$; for brevity, we remove the parameter α and refer to these codes as $(\mathfrak{M}, \mathfrak{X}, \epsilon)$-weak AMD code and $(\mathfrak{M}, \mathfrak{X}, \mathfrak{R}, \epsilon)$-strong

AMD code, respectively. It is of both theoretical and practical significance to design a construction that provides us with a set of of LR-AMD codes with flexible parameters, rather than a single code.

Definition 39 (LR-AMD code family)**.** *A class $\mathcal{F}$ of LR-AMD codes is called a* (weak/strong) LR-AMD code family *if for any integers $\kappa, \nu \in \mathbb{N}$, it contains a (weak/strong) LR-AMD code with message size $\mathfrak{M} \geq 2^{\nu}$ and failure probability $\epsilon \leq 2^{-\kappa}$.*

We use *effective tag length* [24] to measure the optimality of an LR-AMD code family.

Definition 40 (Effective tag length)**.** *For integers $\kappa, \nu \in \mathbb{N}$ and leakage rate $0 \leq \alpha \leq 1$, the effective tag length $\varpi^*_{\mathcal{F}}$ of a (weak/strong) LR-AMD code family $\mathcal{F}$ is defined as $\varpi^*_{\mathcal{F}}(\kappa, \nu, \alpha) = \min_{\mathcal{F}^*} \log \mathfrak{X} - \nu$ where $\mathcal{F}^*$ denotes all codes in the family with $\mathfrak{M} \geq 2^{\nu}$ and $\epsilon \leq 2^{-\kappa}$. For $\alpha = 0$, the effective tag length is denoted by $\varpi^*_{\mathcal{F}}(\kappa, \nu) = \varpi^*_{\mathcal{F}}(\kappa, \nu, 0)$.*

We also use *asymptotic code rate* as an alternative that shows the asymptotic behavior of LR-AMD code families.

Definition 41 (Asymptotic rate)**.** *For leakage rate $0 \leq \alpha \leq 1$, the asymptotic rate of a (weak/strong) LR-AMD code family $\mathcal{F}$ is defined as $Rate_{\mathcal{F}}(\alpha) = \lim_{\kappa \to \infty} \max_{\nu} \max_{\mathcal{F}^*} \frac{\nu}{\log \mathfrak{X}}$ where $\mathcal{F}^*$ indicates all codes in the family with $\mathfrak{M} \geq 2^{\nu}$ and $\epsilon \leq 2^{-\kappa}$.*

Comparing the two definitions suggests the following.

Corollary 4. *For leakage rate $0 \leq \alpha \leq 1$, the asymptotic rate $Rate_{\mathcal{F}}$ of a (weak/strong) LR-AMD code family $\mathcal{F}$ can be obtained as*

$$Rate_{\mathcal{F}}(\alpha) = \lim_{\kappa \to \infty} \max_{\nu} \frac{\nu}{\nu + \varpi^*_{\mathcal{F}}(\kappa, \nu, \alpha)}.$$

4.1.1 Lower bounds on the effective tag length

Theorem 11 shows lower bounds on the effective tag length of weak and strong LR-AMD code families. For $\alpha = 0$, the bounds reduce to those derived in [24] for AMD codes (without leakage).

Theorem 11. *Any weak, resp. strong, LR-AMD code family $\mathcal{F}$ has an effective tag length lower bounded as*

$$\varpi^*_{\mathcal{F}}(\kappa,\nu,\alpha) \geq \max\{\frac{\kappa}{1-\alpha} - 2\ ,\ \kappa + \alpha\nu - 2\},\ \textit{resp.}\ \varpi^*_{\mathcal{F}}(\kappa,\nu,\alpha) \geq \frac{2\kappa}{1-\alpha} - 2. \quad (4.3)$$

Proof. See Appendix B.1. □

Notice the difference between the effect of leakage rate $\alpha \neq 0$ on the effective tag length of weak and strong LR-AMD codes. For strong code families, the effective tag length does not depend on ν; hence, it can be made negligible to the message length by letting ν be sufficiently large. This suggests the possibility of strong LR-AMD codes with the asymptotic rate of 1. For weak code families however, when $\nu \gg \kappa/(1-\alpha)$, the effective tag length increases proportionally to ν. This upper bounds the asymptotic rate of weak LR-AMD code families by $1/(1+\alpha)$.

4.1.2 Weak and strong AMD code constructions

Cramer et al. [24] proposed the following randomized construction of strong AMD codes.

Lemma 20. [24] *Let $\mathbb{F}$ be a field of size q and characteristic p, and d be any integer such that $d+2$ is not divisible by p. The tag generation function $f_s : \mathbb{F} \times \mathbb{F}^d \to \mathbb{F} \times \mathbb{F}$, given by $f_s(r;m) = (r\ ,\ r^{d+2} + \sum_{i=1}^{d} m_i r^i)$ gives a family of systematic $(q^d, q^{d+2}, q, \frac{d+1}{q})$-strong AMD codes with effective tag length $\varpi^*_s(\kappa,\nu) \leq 2\kappa + 2\log(\nu/\kappa + 3) + 2$ when $p = 2$.*

The above construction is nearly optimal as its effective tag length is close to the lower bound (4.3) when $\alpha = 0$. Furthermore, the construction can be used as (deterministic) weak AMD code, by replacing the randomness R with message symbols. This property holds for any systematic AMD code construction in general, since the strong security condition (4.2) implies the weak security condition (4.1) when randomness is replaced by uniform message.

Corollary 5. *Any systematic* $(\mathfrak{M}, \mathfrak{X}, \mathfrak{R}, \epsilon)$*-strong AMD code is converted to a* $(\mathfrak{M}\mathfrak{R}, \mathfrak{X}, \epsilon)$*-weak AMD code by replacing the randomness by a message piece. This implies the tag generation function* $f_{w1}(m) = f_s(m_{d+1}; m_1^d)$*, for* f_s *as in Lemma 20, gives a family of systematic* $(q^{d+1}, q^{d+2}, \frac{d+1}{q})$*-weak AMD codes with effective tag length* $\varpi^*_{w1}(\kappa, \nu) \leq \kappa + \log(\nu/\kappa + 2) + 1$.

Despite the above corollary, there are direct constructions of weak AMD codes with better parameters. See the following construction for instance.

Theorem 12. *Let* $\mathbb{F}$ *be a field of size* q *and characteristic* p*,* $d \in \mathbb{N}$*, and* $t \in \{2, 3\}$ *be such that* $t \neq p$*. The tag generation function* $f_{w2} : \mathbb{F}^d \to \mathbb{F}$*, given by* $f_{w2}(m) = \sum_{i=1}^{d} (m_i)^t$ *gives a family of systematic* $(q^d, q^{d+1}, \frac{2}{q})$*-weak AMD codes with the effective tag length* $\varpi^*_{w2}(\kappa, \nu) \leq \kappa + 1$.

Proof. See Appendix B.2. □

The computational cost of the above construction is linear (multiplications) in d compared to the quadratic cost in the construction of Corollary 5. It furthermore shows much smaller effective tag length.

4.1.3 From AMD codes to LR-AMD codes

We show that an optimal AMD code construction gives an optimal family of LR-AMD codes too.

Theorem 13. *Any* $(\mathfrak{M}, \mathfrak{X}, \mathfrak{R}, \epsilon)$*-strong AMD code is a* $(\mathfrak{M}, \mathfrak{X}, \mathfrak{R}, \alpha, \mathfrak{R}^\alpha \epsilon)$*-strong LR-AMD code, for* $0 \leq \alpha \leq 1$*. This implies that for a family* $\mathcal{F}$ *of strong AMD codes* $\varpi^*_{\mathcal{F}}(\kappa, \nu, \alpha) \leq \min_{\mathcal{F}'} \varpi^*_{\mathcal{F}}(\kappa + \alpha \log \mathfrak{R}, \nu)$*, where* $\mathcal{F}'$ *includes all codes in* $\mathcal{F}$ *with* $\mathfrak{R}^\alpha \epsilon \leq 2^{-\kappa}$ *and* $\mathfrak{M} \geq 2^\nu$.

Proof. See Appendix B.3. □

Theorem 13 shows that any family of strong AMD codes with $\mathfrak{R} = o(2^{\kappa/\alpha})$ gives a family of LR-AMD codes for leakage rate α with failure probability $o(1)$ which can be made arbitrarily small for sufficiently large κ; hence, the asymptotic rate of 1. Applying this to the construction of Lemma 20 shows a family of $(q^d, q^{d+2}, q, \alpha, \frac{d+1}{q^{1-\alpha}})$-strong LR-AMD codes whose failure probability becomes arbitrarily small by choosing q sufficiently large. The effective tag length of this family is upper bounded as $\varpi_s^*(\kappa, \nu, \alpha) \leq 2/(1-\alpha)(\kappa + \log(u/k+3)) + 2$ for when $p = 2$. A similar proof to that of Theorem 13 can be used to derive a similar result for weak AMD codes.

Corollary 6. *Any $(\mathfrak{M}, \mathfrak{X}, \epsilon)$-weak AMD code is a $(\mathfrak{M}, \mathfrak{X}, \alpha, \mathfrak{M}^{\alpha}\epsilon)$-weak LR-AMD code.*

Applying this to the construction of Theorem 12 gives a family of $(q^d, q^{d+1}, \frac{t}{q^{1-\alpha d}})$-weak LR-AMD codes. The effective tag length of this LR-AMD code family is upper bounded by $\varpi_{w2}^*(\kappa, \nu, \alpha) \leq \kappa + \alpha\nu + 2\alpha\kappa/\nu + 3$ which is close to the lower bound (4.3). The asymptotic rate of this code family remains however less than $1/(1+\alpha)$, as expected from Theorem 11. In the following we consider a restricted type of leakage, called *block leakage*, and show how to design weak block-leakage-resilient AMD codes with asymptotic rate 1.

4.1.4 AMD codes for block leakage

In the block leakage scenario, we assume that the message is a block source and furthermore the codeword can be split into arbitrarily many (equal-sized) blocks and the leakage is through any arbitrary function that does not depend on (at least) two codeword block. We first define the block-leakage function

Definition 42. *Let $\mathcal{F}^l$ and $\mathcal{L}$ be arbitrary sets that indicate input and output (leakage) alphabets, respectively. A function $f : \mathcal{F}^l \to \mathcal{L}$ is called a t-block-leakage function if there exists a function $f' : \mathcal{F}^t \to \mathcal{L}$ and fixed indices $I = (i_1, i_2, \ldots, i_t) \subseteq \{1, 2, \ldots, n\}$ such*

that

$$\forall x \in \mathcal{F}^l \ : f(r,x) = f'(r', x_I).$$

A block leakage resilient (BLR)-AMD code is defined as follows.

Definition 43. *Let $Enc : \mathcal{U}^d \to \mathcal{F}^l$ and $Dec : \mathcal{F}^l \to \mathcal{U}^d \cup \{\perp\}$ denote a weak AMD code. For $0 \leq \alpha < 1$ and $0 < \epsilon \leq 1$, the code is called a $(\mathfrak{U}^d, \mathfrak{F}^l, \alpha, \epsilon)$-weak BLR-AMD code, where $\mathfrak{U} = |\mathcal{U}|$ and $\mathfrak{F} = |\mathcal{F}|$, if $\forall m : \ Dec(Enc(m)) = m$, and for any computationally unbounded adversary $\mathcal{A}dv$, $(l-2)$-block-leakage function $f : \mathcal{F}^l \to \mathcal{L}$, $(1-\alpha)$-block-source message M, and leakage information $Z = f(Enc(M))$, the security property (4.1) holds.*

Theorem 14 introduces a deterministic BLR-AMD code construction that is nearly optimal as it achieves the asymptotic rate of 1, when d (hence κ) tends towards infinity.

Theorem 14. *Let d be a positive integer, $\mathbb{F}$ be a field of size q with primitive element τ, and G be any $d \times d$ non-singular matrix over the commutative ring $\mathbb{Z}_{q-1} = \{0, 1, 2, \ldots, q-2\}$ such that*

- *each column of G consists of distinct entries, i.e., $\forall j, i, i' \neq i : \ g_{i,j} \neq g_{i',j}$;*
- *entries of G are upper-bounded by ψd for constant ψ, i.e., $\forall i, j : \ g_{i,j} \leq \psi d$.*

The tag generation function $f_{dlr} : \mathbb{F}^d \to \mathbb{F}$, given by $f_{dlr}(m) = \sum_{i=1}^{d} \tau^{\sum_j g_{i,j} m_j}$ gives a systematic $(q^d, q^{d+1}, \alpha, \frac{\psi d+1}{q^{1-\alpha}})$-weak BLR-AMD code, for $0 \leq \alpha \leq 1$.

Proof. See Appendix B.4. □

Remark 12. *There are different ways to construct the matrix G in Theorem 14, e.g., using non-singular circulant matrices [29]. In Appendix B.11, we give a simple method to construct G with $\psi = 3$ when $q - 1$ is prime, which suggests for instance a family of $(2^{ud}, 2^{u(d+1)}, \alpha, \frac{3d+1}{2^{u(1-\alpha)}})$-weak BLR-AMD codes over binary fields $\mathbb{F} = GF(2^u)$, where $2^u - 1$ is a Mersenne prime.*

4.2 LR-AMD codes for robust nonperfect secret sharing

Secret sharing is the task of distributing a secret as shares among n players such that only qualified subsets of those players can recover the secret. We may assume that the players are indexed by numbers 1 through n and define a secret sharing scheme (SSS) by two functions, **Share** and **Rec**. The share function **Share** maps the secret $S \in \mathcal{S}$ to the share vector $Sh = (Sh[1], Sh[2], \ldots, Sh[n]) \in \mathcal{SH}$, where $\mathcal{SH} = \mathcal{SH}[1] \times \mathcal{SH}[2] \times \cdots \times \mathcal{SH}[n]$. The reconstruction function **Rec** maps the collected shares $Sh' = (Sh'[1], \ldots, Sh'[n])$ with $Sh'[i] \in \mathcal{SH}[i] \cup \{\Lambda\}$ to $\hat{S} \in \mathcal{S} \cup \{\perp\}$, where Λ and $\perp$ indicate share absence and reconstruction error detection, respectively. For every subset $\mathcal{B} \subseteq \{1, 2, \ldots, n\}$ of players, we denote the collective share of $\mathcal{B}$ by $Sh^{\mathcal{B}}$ such that $Sh^{\mathcal{B}}[i]$ equals $Sh[i]$ for $i \in \mathcal{B}$ and Λ elsewhere. An SSS is called linear if it has a linear reconstruction function, i.e., for any two share vectors $Sh, Sh' \in \mathcal{SH} \cup \{\Lambda\}$, with $S = \mathbf{Rec}(Sh)$ and $S' = \mathbf{Rec}(Sh')$, the reconstructed of their element-wise addition $\mathbf{Rec}(Sh + Sh')$ returns either $S + S'$ if $\perp \notin \{S, S'\}$ or $\perp$ otherwise, noting that $sh[i] + \Lambda = \Lambda$.

In a perfect SSS, every subset $\mathcal{B}$ is tagged either qualified or unqualified: For qualified $\mathcal{B}$, the correctness property of SSS requires the reconstruction of $Sh^{\mathcal{B}}$ gives S. For unqualified $\mathcal{B}$, the privacy property requires zero information leakage about S. A nonperfect SSS in contrast may reveal partial secret information to some intermediate subset $\mathcal{B}$ of players that are yet not qualified. The motivation for this security relaxation is gaining efficiency in terms of the size of the distributed shares [52]. A well-known example of this is ramp SSS, where leakage about the secret grows linearly with respect to the size of the intermediate subset of players. Different information measures such as probability difference [15] and Shannon entropy [52] have been used to formalize leakage in a nonperfect SSS. We give another formalization by using min-entropy measure for the definition of nonperfect secret sharing.

Definition 44. *A nonperfect SSS, denoted by* $\mathbf{Share} : \mathcal{S} \to \mathcal{SH}$ *and* $\mathbf{Rec} : \mathcal{SH} \cup \{\Lambda\} \to \mathcal{S} \cup \{\perp\}$ *is called* β-perfect *(for* $0 \leq \beta \leq 1$*) if for the random secret* S *and any unqualified or intermediate subset* $\mathcal{B}$ *of players, we have the following: Let* $Sh = \mathbf{Share}(S)$*, then* $\tilde{H}_\infty(S|Sh^{\mathcal{B}}) \geq \beta H_\infty(S)$.

Robustness of an SSS requires that an intermediate/unqualified subset of players cannot cheat to deceive honest players to recover a different secret value $\hat{S} \neq S$.

Definition 45. *A perfect/non-perfect SSS, defined by* $\mathbf{Share} : \mathcal{S} \to \mathcal{SH}$ *and* $\mathbf{Rec} : \mathcal{SH} \cup \{\Lambda\} \to \mathcal{S} \cup \{\perp\}$*, is* ϵ*-robust for secret distribution* P_S *if for any unbounded adversary* $\mathcal{A}dv$ *who corrupts an unqualified or intermediate subset* $\mathcal{B}$ *of players and secret* $S \in \mathcal{S}$ *with distribution* P_S*, we have the following. Let* $Sh = \mathbf{Share}(S)$ *and* Sh' *be such that*

$$\forall 1 \leq i \leq n : \quad Sh'[i] = \begin{cases} \mathcal{A}dv(i, Sh^{\mathcal{B}}), & \text{if } i \in \mathcal{B} \\ Sh[i] \text{ or } \Lambda, & \text{else} \end{cases}.$$

Then $\Pr(\mathbf{Rec}(Sh') \notin \{S, \perp\}) \leq \epsilon$*, where the probability is taken over the SSS randomness and the secret distribution. The schemes is called* ϵ*-strongly-robust when* P_S *is a constant distribution.*

Remark 13. *The above definition is a generalization of [24, Definition 4] to non-perfect SSS. The security notion is in general weaker as the adversary's success probability is taken over the secret distribution too. We adopt this definition since it bounds the true success probability of an intermediate/unqualified subset in cheating when the secret is unavoidably random.*

4.2.1 Strong LR-AMD code with nonperfect SSS

In [24], a construction of strongly-robust linear perfect SSS is given by composing a strong AMD code and a linear perfect SSS. This construction cannot be directly used for

nonperfect SSS as leakage in these schemes may render the AMD code insecure. Taking advantage of systematic AMD codes, we can have strongly-robust nonperfect SSS by modifying the construction of [24] as follows. The secret S is given to a systematic strong (LR-)AMD code with uniform randomness R, the codeword $(S, R, f_s(R;S))$ is returned, and each of the components is separately shared by nonperfect SSS. This approach causes the nonperfect SSS to distribute its leakage over $(S, R, f_s(R;S))$. Considering this for the construction of Lemma 20 gives us the following (the proof is simple and hence omitted).

Corollary 7. *Let $f_s(.;.)$ be the strong (LR-)AMD code of Lemma 20 with uniform randomness $R \in \mathbb{F}_q$, and $(\mathbf{Share}, \mathbf{Rec})$ denote a linear β-perfect SSS with secret being from $\mathbb{F}_q$. The SSS $(\mathbf{Share}^*, \mathbf{Rec}^*)$ with secret from $\mathbb{F}_q^d$, given by*

$$\mathbf{Share}^*(S) = \left(\left(\mathbf{Share}(S_i)\right)_{i=1}^{d}, \mathbf{Share}(R), \mathbf{Share}(f_s(R;S)) \right), \quad \textit{and}$$

$$\mathbf{Rec}^*\left(\left(Sh_i\right)_{i=1}^{d+2}\right) = \begin{cases} \perp, & \textit{if } \exists i : \mathbf{Rec}(Sh_i) = \perp \vee \ \mathbf{Rec}(Sh_{d+2}) \neq f_s\left(\mathbf{Rec}(Sh_{d+1}); (\mathbf{Rec}(Sh_i))_{i=1}^{d}\right) \\ \left(\mathbf{Rec}(Sh_i)\right)_{i=1}^{d}, & \textit{else} \end{cases}$$

is ϵ-strongly-robust, where $\epsilon = \frac{d+1}{q^{2\beta-1}}$.

The robustness parameter ϵ in the above equals the failure probability of the strong LR-AMD code for leakage rate $2\beta-1$. Informally speaking, this leakage rate is obtained as follows. A β-perfect SSS leaks $(1-\beta)\log q$ bits from each of R and $f_s(R;S)$. The leftover uncertainty of the randomness is thus only guaranteed to be above $\beta \log q - (1-\beta)\log q = (2\beta-1)\log q$. Providing robustness for β-perfect SSS with $\beta \leq 0.5$ is an interesting open question of this section.

4.2.2 BLR-AMD code and somewhere-perfect SSS

We consider a special class of nonperfect secret sharing schemes, called *somewhere-perfect* SSS, and show that schemes of this class can be made robust using BLR-AMD codes. A somewhere-perfect SSS distributes the secret $S = (S_1, S_2, \ldots, S_l)$ as shares $Sh =$

$(Sh_1, Sh_2, \ldots, Sh_n)$ such that for any unqualified or intermediate subset $\mathcal{B}$ of players, their collective information $Sh^{\mathcal{B}}$ comes from a block-leakage function.

Definition 46. *A non-perfect SSS, with functions* $\mathbf{Share} : \mathcal{S} \to \mathcal{SH}$ *and* $\mathbf{Rec} : \mathcal{SH} \cup \{\Lambda\} \to \mathcal{S} \cup \{\perp\}$*, where* $\mathcal{S} = \mathcal{F}^n$ *and* $\mathfrak{F} = |\mathcal{F}|$*, is called* somewhere-perfect *if for the secret* $S = (S_1, S_2, \ldots, S_n)$*, shares* $Sh = \mathbf{Share}(S)$*, and any unqualified or intermediate subset* $\mathcal{B}$ *of players, we have* $Sh^{\mathcal{B}} = f(S)$ *for some* $(n-1)$*-block leakage function* f*.*

Theorem 15 shows how to make a linear somewhere-perfect SSS robust using a BLR-AMD code.

Theorem 15. *Let* $(\mathbf{Share}, \mathbf{Rec})$ *denote a linear somewhere-perfect SSS with secret in* $\mathcal{F}^n$*, and Enc/Dec be a* $(\mathfrak{U}^d, \mathfrak{F}^l, \alpha, \epsilon)$*-weak BLR-AMD code with* $d = w.n$*, for integer* $w \geq 2$*. Then the SSS* $(\mathbf{Share}^*, \mathbf{Rec}^*)$*, given by* $\mathbf{Share}^*(S) = \big(\mathbf{Share}(X_1^n), \mathbf{Share}(X_{n+1}^{2n}) \ldots, \mathbf{Share}(X_{(t-1)n+1}^{d})\big)$ *and*

$$\mathbf{Rec}^*\left(\left(Sh_i\right)_{i=1}^{t}\right) = \begin{cases} \perp, & \text{if } \exists i : \mathbf{Rec}(Sh_i) = \perp \\ Dec(\left(\mathbf{Rec}(Sh_i)\right)_{i=1}^{t}), & \text{else} \end{cases},$$

is ϵ*-robust for* $(1-\alpha)$*-block-source secrets over* $\mathcal{U}^d$*.*

Proof. See Appendix B.5. □

Applying Theorem 14 to the above shows for $\alpha < 1$, any somewhere-perfect SSS (e.g., Shamir's polynomial-based ramp SSS) with $(1-\alpha)$-block-source secrets over $\mathbb{F}_q^{d+1}$ can be made ϵ-robust, where $\epsilon = \frac{\psi d+1}{q^{1-\alpha}}$ can be arbitrarily small by choosing q sufficiently large.

4.3 LR-AMD codes over wiretap channels

We consider the wiretap communication scenario as in Fig. 4.1, when leakage is through a probabilistic noisy channel: The wiretap channel consists of a *noiseless but additively*

tamperable main channel from Alice to Bob and a *wiretapping noisy channel* from Alice to Eve. For this channel, Wyner proved keyless private communication is possible with a slight noise over the wiretapping channel. Keyless manipulation detection is however trivially impossible if the adversary's manipulation access to the main channel is not restricted. We consider a scenario where the adversary's manipulation is of algebraic (additive) type, i.e., the adversary can only choose a tampering symbol to be added to a transmitted codeword. We consider symmetric and erasure u-ary wiretap channels, defined as follows.

Definition 47 (Erasure wiretap channel)**.** *A (u, p)-erasure wiretap channel (EWC) transmits the codeword as a sequence of symbol elements in $\mathbb{F}$ of size u such that its wiretapping component, denoted by $EC_{u,p}$, either transmits a symbol correctly with probability $1-p$ or erases it completely (converts it to erasure symbol Λ) with probability p.*

Definition 48 (Symmetric wiretap channel)**.** *A (u, p)-symmetric wiretap channel (SWC) transmits the codeword as a sequence of symbol elements in (additive) group $\mathbb{F}$ of size u such that its wiretapping component, denoted by $SC_{u,p}$, either transmits a symbol correctly with probability $1-p$ or adds to it any of the non-zero group elements with probability $p/(u-1)$.*

When $u = 2$, we denote the above (binary) wiretap channels as p-BEWC and p-BSWC. The wiretap channel is a special case of channel with leakage, so one may use LR-AMD codes to detect algebraic manipulation over the wiretap channel. Consider a systematic $(\mathfrak{M}, \mathfrak{MR}\mathfrak{G}, \mathfrak{R}, \alpha, \epsilon)$-strong LR-AMD code, denoted by $\mathbf{Tag}(.;.)$, over a (u, p)-EWC. For message m and uniform randomness R, let (m, R, G) be the codeword. The erasure channel erases p fraction of symbols in the codeword on average, i.e., it leaks to the adversary $1-p$ fraction of R and $1-p$ fraction of G. Letting Z denote the adversary's view, the leftover min-entropy in R is approximately $p \log \mathfrak{R} - (1-p) \log \mathfrak{G}$ which needs

to be greater than $(1-\alpha)\log\mathfrak{R}$ for the code to promise ϵ-security guarantee. Applying this to the construction of Lemma 20 implies the following.

Corollary 8. *For $0.5 < p \leq 1$, the (LR-)AMD code construction of Lemma 20 detects algebraic manipulation over the (u,p)-EWC with detection failure probability at most $\frac{d+1}{2^{(2p-1)q}}$.*

When $p \leq 0.5$, no security guarantees can be made by the code construction. It is thus interesting to investigate the possibility of algebraic manipulation detection over (u,p)-EWCs with $p \leq 0.5$. We focus on uniform message distribution and show that the BLR-AMD code construction of Theorem 14 detects algebraic manipulation over EWCs with $p > u^{-1}$, with arbitrarily small failure probability by choosing the code length sufficiently large.

Theorem 16. *Let $u \in \mathbb{N}$ and p be such that $u^{-1} < p \leq 1$. The BLR-AMD code construction of Theorem 14, with q such that $\log q$ is divisible by $\log u$, detects algebraic manipulation over the (u,p)-EWC with detection failure probability at most $\frac{\psi d+1}{q} + \exp\left(-\frac{(d+1)}{8q^{1-\zeta}}\right)$ for uniform message distribution, where $\zeta = \log_u(up) > 0$. This probability can be made arbitrarily small, e.g., by choosing $d = q^{1-\zeta/2}$ and q sufficiently large.*

Proof. See Appendix B.6. □

The same result holds for any (u,p')-SWC with $p' = (1-u^{-1})p$ since for the codeword $X \in \mathbb{F}_u^l$, the adversary's view $Z' = SC_{u,p'}(X)$ can be simulated from the erasure channel output $Z = EC_{u,p}(X)$ by letting $Z'_i = r$ for uniformly random $r \in \mathbb{F}_u$ when $Z_i = \Lambda$ or $Z'_i = Z_i$ otherwise. This together with Theorem 16 lets us conclude the following.

Corollary 9. *Let $u \in \mathbb{N}$ and p be such that $u^{-1} - u^{-2} < p \leq 1 - u^{-1}$. The BLR-AMD code construction of Theorem 14 detects algebraic manipulation over the (u,p)-SWC with failure probability at most $\frac{\psi d+1}{q} + \exp\left(-\frac{(d+1)}{8q^{1-\zeta}}\right)$ for uniform message, where $\zeta = \log_u(up) > 0$.*

The existence and construction of wiretap AMD codes remains open for when the condition on p and u in Theorem 16 (or Corollary 9) is not satisfied. This includes binary wiretap channels p-BEWC with $p < 0.5$ and p-BSWC with $p < 0.25$.

4.3.1 Composability of the BLR-AMD construction

As discussed above, our BLR-AMD construction detects algebraic manipulation over a certain range of erasure/symmetric wiretap channels. When the adversary uses all (not just algebraic) manipulation functions, no security guarantee is provided. We show however that over binary wiretap channels, detection of unrestricted bitwise manipulation can be promised by combining coding and modulation techniques. A binary wiretap channel transmits data as a sequence of separate bits and hence the adversary's manipulation is bit-by-bit using the set of four possible bitwise manipulation functions, namely additive functions (keep and flip) and overwrite functions (set-to-0 and set-to-1). To protect a message from all bitwise manipulation functions, we (i) encode the message using our BLR-AMD construction, (ii) apply *Manchester coding* on the BLR-AMD codeword, and (iii) transmit the resulting codeword via *on-off keying*. The Manchester code is a simple binary error-detecting code that appends to each bit its complement. On-off keying is a pre-modulation step that transmits the bit "one" as the presence a carrier wave signal and the bit "zero" as the absence of the signal. This prevents the adversary from applying the set-to-0 function deterministically (see Appendix B.12). Proposition 3 formalizes our results on bitwise manipulation detection over p-BEWCs with $p > 0.5$ and p-BEWCs with $0.25 < p \leq 0.5$.

Proposition 3. *Let Enc_{mn}/Dec_{mn} be the Manchester encoding/decoding functions, and f_{dlr} denote the BLR-AMD code of Theorem 14, where $q = 2^v$ and $\mathbb{F} = GF(2^v)$. The code*

given by Enc_b/Dec_b such that $Enc_b(m) = (m, f_{dlr}(m))$ and

$$Dec_b(c) = \begin{cases} \hat{m}, & \text{if } Dec_{mn}(c) = (\hat{m}, \hat{t}) \neq \perp, \text{ and } \hat{t} = f_{dlr}(\hat{m}) \\ \perp, & \text{else} \end{cases}, \tag{4.4}$$

has code rate $\frac{d}{2(d+1)}$ and detects bitwise manipulation for uniform message over a p-BEWC (or p/2-BSWC) with $p > 0.5$ with failure probability at most $\frac{\psi d+1}{2^v} + \exp\left(-\frac{(d+1)p^v}{8}\right)$, if the codeword is transmitted via on-off keying.

Proof. See Appendix B.7. □

The above shows the possibility of manipulation detection over symmetric/erasure binary channels. We further show that composing the above construction with wiretap codes results in both privacy and manipulation detection in message transmission (or key agreement). Wiretap coding has been studied first by Wyner [96] to achieve privacy in message transmission. There have been since a lot of research on designing efficient and optimal (in rate) wiretap codes (cf. [13, 58]). The following provides a definition of wiretap codes, specifically for our binary wiretap channels.

Definition 49. *A pair of encoding and decoding functions $Enc_w : \{0,1\}^t \to \{0,1\}^k$ and $Dec_w : \{0,1\}^k \to \{0,1\}^t$ is called (t, k, ϵ)-wiretap code over the p-BEWC (resp. p-BSWC) if $\forall m \in \{0,1\}^t : \ Dec_w(Enc_w(m)) = m$ and for uniform $M \in \{0,1\}^t$ it holds $I(M; Z)/t \leq \epsilon$, where $Z = BEC_p(Enc_w(M))$ (resp. $Z = BSC_p(Enc_w(M))$).*

Proposition 4. *Let Enc_w/Dec_w be a (t, k, ϵ)-wiretap code over the p-BEWC (resp. p/2-BSWC), for $p > 0.5$, such that for uniform $M \in \{0,1\}^t$ $X = Enc_w(M)$ is uniform. Also let Enc_b/Dec_b be the code construction of Proposition 3 with $v \leq t\epsilon$. The code given by Enc_{wb} and Dec_{wb} such that $Enc_{wb}(m) = Enc_b(Enc_w(m))$ and*

$$Dec_{wb}(c) = \begin{cases} Dec_w(Dec_b(c)), & Dec_b(c) \neq \perp \\ \perp, & else \end{cases}. \tag{4.5}$$

has code rate $\frac{td}{2k(d+1)}$*, satisfies* $I(M;Z)/t \leq 2\epsilon$ *for* $Z = BEC_p(X)$ *(resp.* $Z = BSC_p(X)$*), and detects bitwise manipulation of* M *over the* p*-BEWC (or* $p/2$*-BSWC) with failure probability at most* $\frac{\psi d+1}{2^v} + \exp\left(-\frac{(d+1)p^v}{8}\right)$*, if the codeword is transmitted via on-off keying.*

Proof. See Appendix B.8. □

Known results give (t, k, ϵ)-wiretap code constructions over p-BEWC (resp. p-BSWC) with arbitrarily small $\epsilon > 0$ and of rate arbitrarily close to $1 - p$ (resp. $h(p) = -p\log(p) - (1-p)\log(1-p)$). This proves that by choosing the code length sufficiently large, the above code construction achieves rates arbitrarily close to $(1-p)/2$ (resp. $h(p)/2$) and provides both privacy and manipulation detection with arbitrarily small failure probabilities.

4.4 AMD for online adversarial channels

The online adversarial scenario models a communication system with leakage where the codeword is transmitted as a sequence of bits $\mathbf{X} \in \{0,1\}^n$ and the adversary's (algebraic) manipulation strategy Δ_i for a current bit X_i depends on the so-far received (and processed) codeword bits, i.e., X_j for $j \leq i$. This channel model has been first studied by Langberg et al. [55] for the purpose of reliable transmission when the adversary corrupts up to a p-fraction of symbols. For online adversaries, we introduce a *delay* as a function of the codeword length. The delay parameter captures latency in processing the received data for constructing an adversarial noise block. In the following, we study two types of online adversaries with delay: constant-delay and linear-delay adversaries.

Definition 50. *For* $\Gamma \in \mathbb{Z}_{\geq 0}$*, a* Γ*-constant-delay (online) adversary* $\mathcal{A}dv_{\mathbf{cdo},\Gamma}$ *is an adversary whose algebraic manipulation is written as* $\forall 1 \leq i \leq n:\ \Delta_i = \mathcal{A}dv_{\mathbf{cdo},\Gamma}(X_1^{i-\Gamma})$*, where* n *is the transmission (codeword) length.*

Definition 51. *For real $0 \leq \gamma \leq 1$, a γ-linear-delay (online) adversary $\mathcal{A}dv_{\mathbf{ldo},\gamma}$ is an adversary whose algebraic manipulation is written as $\forall 1 \leq i \leq n:\ \Delta_i = \mathcal{A}dv_{\mathbf{ldo},\gamma}(X_1^{i-\gamma n})$, where n is the transmission (codeword) length.*

Generally, the online adversarial channel is not captured by the leakage scenario given in Section 4.1.3, since the view of an online adversary changes over time as the codeword blocks pass by. However, it is not hard to observe that protection against (non-zero) linear-delay adversaries can be attained by using a strong systematic AMD code that is chosen appropriately such that the adversary does observe the tag (including the randomness) before manipulating with the last codeword block.

Proposition 5. *Let $f_s(.;.)$ denote the strong systematic AMD code construction of Lemma 20 over a binary field $\mathbb{F} = GF(2^v)$.*

- *Choosing $d \geq \lceil \frac{2}{\gamma} - 2 \rceil$ and arbitrary v, the code detects algebraic manipulation of any message $m \in \mathbb{F}^d$ over the γ-linear-delay adversarial channel with failure probability at most $\frac{d+1}{2^v}$.*
- *Choosing $v \leq \lfloor \frac{\Gamma}{2} \rfloor$ and arbitrary d, the code detects algebraic manipulation of any message $m \in \mathbb{F}^d$ over the Γ-constant-delay adversarial channel with failure probability at most $\frac{d+1}{2^v}$.*

Proof. See Appendix B.9. □

Theorem 5 also shows that protection against any (non-zero) linear-delay adversary and with arbitrarily small failure probability can be attained by using the construction of Lemma 20 with sufficiently large code length. This suggest a family of AMD codes over linear-delay adversarial channels. The result for constat-delay adversaries however implies that the code failure probability cannot exceed $(d+1)/2^{\Gamma/2}$ which implies the maximum security parameter for which an AMD code exists is $\kappa = \lfloor \Gamma/2 - \log(d+1) \rfloor$;

thus, the above construction does not suggest a family of AMD codes for constant-delay adversarial channels.

Further investigating the constant-delay adversarial channel, we show that by using unary codes, we can achieve arbitrarily small failure probability against the 1-constant-delay (i.e., the strongest positive delay) adversary, however, at the price of adding large redundancy to the code (i.e., sacrificing the code rate). In the following, we define a variation of unary codes with fixed encoding length of n.

Definition 52 (Unary code)**.** *The n-unary code is a deterministic coding scheme, with $n+1$ codewords, that is defined by an encoding function $Enc_u : \{0,1,\ldots,n\} \to \{0,1\}^n$, and decoding function $Dec_u : \{0,1\}^n \to \{0,1,\ldots,n\}$, such that*

$$Enc_u(m) = \underline{1}^m || \underline{0}^{n-m} \quad \textit{and} \quad Dec_u(\mathbf{x}) = w_H(\mathbf{x}),$$

where $w_H(\mathbf{x})$ represents the Hamming weight of $\mathbf{x}$.

Theorem 17. *The n-unary code detects algebraic manipulation of uniform message $M \in \{0,1,\ldots,n\}$ over the 1-constant-delay adversarial channel with failure probability at most $\frac{2}{n+1}$.*

Proof. See Appendix B.10. □

Although the unary code construction introduces an AMD code family over the constant-delay adversarial channel, its rate is obtained as $\log(n+1)/n$ which tends to 0 asymptotically. This leaves open the existence/construction of AMD code families with positive asymptotic rates in the constant-delay adversarial scenario.

4.5 Conclusion

We investigated the problem of keyless manipulation detection when the adversary's read/write access to the channel is naturally restricted, i.e., the adversary's tampering

with the communication is by injecting an adversarial noise to the channel and, furthermore, her read (view) access to the communication may be imperfect. This models realistic cases of adversarial scenarios in the physical-layer of the network, esp. wireless environments. We began by considering an abstract model of an algebraic manipulable channel with leakage and developing the study of LR-AMD codes for manipulation detection over this communication channel. Our work is also considered as an extension of the current work on "algebraic manipulation detection" [24] to scenarios where there is arbitrary but bounded leakage about the codeword to the adversary.

We derived lower bounds on the effective tag length of (weak and strong) LR-AMD code families and proved optimal LR-AMD constructions. The results show strong LR-AMD code constructions can achieve arbitrarily small failure provability with negligible redundancy (asymptotic rate of 1), however, weak LR-AMD code constructions cannot exceed rate more than $1/(1+\alpha)$ where α is the leakage rate: When α is close to 1, the highest achievable asymptotic rate is 1/2. We then introduced a *block-leakage-resilient (BLR)-AMD* code construction with the asymptotic rate of 1 that detects algebraic manipulation when leakage is through any adversarially chosen function that does not depend on at least two codeword blocks.

We showed two important applications of these codes to robust secret sharing and to manipulation detection over wiretap channels. We showed how to add robustness to linear β-perfect SSS with $\beta > 0.5$ by using strong systematic LR-AMD codes; furthermore, how to add robustness to linear *somewhere perfect* SSS using BLR-AMD codes. We studied algebraic manipulation over (u, p)-erasure and -symmetric wiretap channels and showed when $p > .5$ a strong systematic AMD code can achieve this purpose. We also showed our deterministic BLR-AMD construction detects algebraic manipulation over the above erasure and symmetric channels when $p > u^{-1}$ and $u^{-1} - u^{-2} < p \leq 1 - u^{-1}$, respectively. Composing this construction with a few other primitives, we can provide unlimited bitwise

manipulation detection, in addition to privacy, in message transmission or key agreement over binary symmetric and binary erasure channels. *Providing robustness for β-perfect SSS with $\beta \leq 0.5$ and manipulation detection over (u, p)-EWC (and $(u, p/2)$-SWC) with $p < u^{-1}$ are open problems that we have not provided an answer for.*

We also studied another class of communication with leakage called online-adversarial channel, where the adversary has a linear/constant delay in receiving codeword bits and using them to decide on her manipulation strategy. For linear-delay adversaries algebraic manipulation detection can be achieved by strong systematic AMD codes. For constant delay adversaries, we showed unary coding construction as an AMD code family achieves arbitrary small failure probability; however, its asymptotic rate is zero. *Existence and construction of AMD code families over the constant-delay adversarial channel is an open question, which we leave for future research.*

This chapter raises a number directions to future work. Investigating manipulation detection in other realistic adversarial/leakage scenarios is an interesting question. We also encourage studying the application of LR-AMD codes to other areas of cryptography.

Chapter 5

Distance Bounding Verification over Physical-Layer Channels

A distance bounding (DB) protocol is an interactive protocol with two parties, a *verifier* and a (possibly untrusted) *prover*, that enables the verifier to find an upper bound on its distance to the prover. The DB problem was first introduced by Brands and Chaum [16] and has since been studied in different settings [18, 19, 44, 74, 94]. DB protocols have found numerous applications in security: they are used as building blocks for secure localization [83], location-based access control [71], and wormhole detection [47]. Protocols for distance bounding combine cryptographic tools with methods of estimating distance such as received signal strength (RSS), its angle of arrival (AoA), and its time of flight (ToF). The currently-proposed protocols for "secure" distance bounding, however, are based on ToF as other signal properties are more susceptible to adversarial scenarios including the well-studied *distance fraud* (DFA), *mafia fraud* (MFA), and *terrorist fraud* (TFA) attacks [30].

Despite the variety of the settings, all ToF-based techniques use a common approach which is based on a *rapid exchange of challenge-response messages* between the verifier and the prover. For each challenge-response, the verifier measures the round-trip time, subtracts the processing time of the prover, and divides this by the signal traveling speed to have an estimate of its distance to the prover. Accurate time measurements in these protocols introduce implementation challenges [72]. Firstly, the verifier needs access to a high-precision clock to be able to measure the round-trip time with sufficient accuracy, since a small error leads to a large inaccuracy in distance estimates. Secondly,

the verifier either needs a good estimate of the prover's processing time, or must assume it is negligible compared to the signal's time of flight. In hostile environments, one cannot make a good estimate of the adversary's processing time and this may result in large errors in distance estimation. This all supports that the design and implementation of accurate ToF-based DB protocols is still a challenge. This concern lets us raise the following question:

- Are there particular cases of the DB problem that can be solved without using time measurement?

Our work

In this chapter [1] , we address the above question and study secure *distance bounding verification* in circumstances where the verifier does not have access to an accurate clock and so cannot use ToF-based solutions. Distance bounding verification (DBV) is a variant of distance bounding that is defined in a setting where the prover supposedly knows its location (or distance) a priori and the DBV protocol is initiated by the prover sending a location claim to the verifier. We assume that the prover and the verifier communicate over a wireless environment that attenuates the transmitted signal and adds noise to it. In our setting, signal attenuation is a deterministic variable that reduces as a function of distance and noise is modeled by an additive Gaussian random variable with zero mean and certain variance.

We study three main types of attacks against DBV [30] which have also been considered for the distance bounding problem [17, 18]. Distance fraud attack (DFA) refers to a scenario where a dishonest prover claims a closer distance to the verifier. In mafia fraud attack (MFA), the prover is honest and claims its real distance, bit there is a man-in-the-middle intruder that tampers with the communication to convince the verifier that the

[1] The results of this chapter have been submitted to Advances in Cryptology EUROCRYPT 2013 [5].

prover is closer. In terrorist fraud attack (TFA), the dishonest prover helps an intruder convince the verifier about an incorrect (closer) distance claim.

DFA and MFA security. We show that it is possible to construct efficient protocols with security against DFA and MFA, even if the adversary has unlimited computational power. We give a basic DFA-secure protocol by simply using the above challenge-response phase, where the challenge is transmitted over the PLAN environment via the binary phase shift keying (BPSK) modulation. Our DFA-secure DBV protocol can be changed to a DFA/MFA-secure protocol by simply using a message authentication code (MAC) to protect the messages from the prover to the verifier, particularly the prover's response to the challenge message. This is not surprising because in distance bounding verification, the prover knows its distance (or location) in a priori and when the prover is honest (as in MFA), it can authenticate its legitimate claim by a MAC so that the intruder cannot substitute this with another claim. We note that MFA-security in "distance bounding" is much more challenging only because the prover is unaware of its distance/location. We explain this further in Section 5.5.

TFA security. Unlike security against DFA and MFA, it is impossible to design TFA-secure protocols without time measurement, even if the adversary is computationally bounded. The reason is an appropriately located intruder can relay all protocol messages (including any signal-related information) back and forth between the other the prover and the verifier, without the verifier noticing. We adopt a restriction on the adversary's communication capability that will allow for TFA-secure DBV protocols without time measurement. We consider a variation of the *bounded retrieval model* (BRM) [31, 38], described as follows. There is a high throughput uniform source, called the *BRM oracle*, that generates and transmits a uniform binary string with a high speed such that all parties (including the verifier) can only retrieve a *constant fraction* of the string. The verifier can adjust the transmission power of the oracle, however has no control on its content.

We assume that the honest parties can only sample individual bits from the transmitted signal. Depending on the adversary's retrieval capability however, we study two cases: a *sampling adversary* who can only sample individual bits, and a *general adversary* who can apply any limited length function to her observation. We propose a *BRM-DBV protocol* and derive conditions under which the protocol achieves DFA/MFA/TFA-security in the BRM against general and sampling adversaries. The TFA-security in this protocol is attained by incorporating the BRM oracle as well as an *averaging sampler* [12, 89] to the basic DFA-secure protocol.

Numerical analysis. The DBV protocols designed in this work use computationally-efficient functions. The communication complexity of the protocols and the conditions for security, however, depend on input parameters. We use numerical analysis to elaborate on the performance of our designed protocols with respect to input parameters. The analysis shows that TFA-security against general adversaries is achievable only for certain set of input parameters. For the rest of the settings however, security is guaranteed for all input parameters.

Related work

Brands and Chaum [16] proposed the first time-based DB protocol with security against DFA and MFA. Their protocol assumes a private key for the prover and consists of three phases: commitment, rapid bit-exchange, and signature-verification. The rapid bit-exchange phase allows the verifier to put an upper bound on the prover's distance; the other two phases are to provide DB security guarantees against the two adversarial scenarios. The protocol is not secure against TFA. The follow-up work has since considered different formalizations of the problem in various settings and attack scenarios [18, 21, 37, 49, 72, 91]. Distance-bounding for RFID has also been extensively studied in recent years. Such protocols provide a method of proximity based authentication.

Bussard and Bagga [18] proposed the first TFA-secure DB protocol. The protocol uses public key cryptography and zero-knowledge proofs and so is computationally inefficient. More recent work (cf. [50, 63, 64, 73, 74]) improves security and efficiency of this result.

The effect of noise in the environment of time-based distance bounding protocols has been considered by [44, 63, 83]. Noisy environment can interfere with the operation of the protocols and the aim of all these works is to provide protection against this noise. For example authors in [83] considered the MAD protocol [91], which is an extension of Brands and Chaum's protocol with mutual authentication, and propose methods of protecting the rapid bit-exchange phase against noise in the environment. In our work the environment noise is a "blessing" in the sense that it allows protection against the eavesdropper at the blocked distance. Using appropriate coding methods allows the verifier to control reception of a challenge such that a legitimate receiver can have (almost) perfect reception while the intruder at the blocked distance remains uncertain.

5.1 Preliminaries

The basic component of our DBV protocols is a challenge-response phase over the noisy environment that lets the verifier accept only if the prover's response is close enough to the transmitted challenge. The DFA-security of this approach follows from the fact that receivers at far distances cannot guess a bit string that is close enough to the challenge with high probability. To formalize this notion of security, we define a class of sources, named *almost-secure sources*, as a generalization of weak sources (see Definition 15), that require an upper-bound on the probability of any element being close (in Hamming distance) to the source output.

Definition 53 (Almost-secure source)**.** *A random variable* $X \in \{0,1\}^n$ *is called* (β, δ)*-almost-secure if* $\max_x \Pr(d_H(X, x) \leq \beta n) \leq 2^{-\delta n}$*. The source is called* (β, δ)*-almost-*

secure conditioned on the random variable $Y \in \mathcal{Y}$ *if* $E_y \max_x \Pr(d_H(X,x) \leq \beta n | Y = y) \leq 2^{-\delta n}$.

Lemma 21 shows how leakage can affect the almost-security property of a source. The proof of this lemma follows from the chain rule for min-entropy (cf. [34]).

Lemma 21. *Let the random variable* $X \in \{0,1\}^n$ *be* (μ, δ)*-almost-secure conditioned on* $Y \in \mathcal{Y}$ *and let* A *be any random variable in* $\mathcal{A}$ *of (support) size* $\mathfrak{A}$*. Then* X *is* $(\mu, \delta - \log(\mathfrak{A})/n)$*-almost-secure conditioned on* (Y, A).

To protect DBV against mafia fraud, we use (information-theoretic) message authentication codes (MACs). A MAC is a shared key cryptographic primitive that protects a message against arbitrary tampering of an adversary. The code is defined by a function $\mathsf{Mac} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ takes a shared key $\mathsf{sk} \in \mathcal{K}$ as well as a message $m \in \mathcal{M}$ and returns an authentication tag $t = \mathsf{Mac}(\mathsf{sk}; m)$. A message and tag pair (m', t') are then verified if $t' = \mathsf{Mac}(\mathsf{sk}; m')$ holds. We limit ourselves to one-time MACs, defined as follows.

Definition 54 (MAC). *A function* $\mathsf{Mac} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ *is called an* ϵ*-secure one-time message authentication code (MAC) if for any message* $m \in M$ *and any adversary* $\mathcal{A}dv : \mathcal{T} \to \mathcal{M} \times \mathcal{T}$*, it holds that* $\Pr[t' = \mathsf{Mac}(\mathsf{SK}; m') | (m', t') = \mathcal{A}dv(\mathsf{Mac}(\mathsf{SK}; m))] \leq \epsilon$*, with the probability taken over the uniform key* $\mathsf{SK} \in \mathcal{K}$.

Another primitive used in this work is a *sampler*, which is an efficiently-computable function that receives some randomness as input and lets the BRM-DBV protocol retrieve part of BRM oracle output in the BRM setting. It is shown that sampling a random subset of bits from a source nearly preserves its min-entropy rate. However, choosing a completely random set of positions is expensive in the seed length. Vadhan [89] has proposed using *averaging samplers* [12] that achieve the task of sampling in a randomness-efficient way.

Definition 55 (Averaging sampler)**.** [89] *A function* $Samp : \{0,1\}^r \to [n]^k$ *is a* (μ, θ, γ) *averaging sampler if for every function* $f : [n] \to [0,1]$ *with average value* $\frac{1}{n}\sum_i f(i) \geq \mu$*, it holds that* $\Pr\left(\frac{1}{k}\sum_{j=1}^{k} f(i_j) < \mu - \theta\right) < \gamma$*, where* $(i_1, i_2, \ldots, i_k) = Samp(U_r)$ *and* U_r *is uniform over* $\{0,1\}^r$*. The sampler has distinct samples if for every* $x \in \{0,1\}^r$*, the samples produced by* $Samp(x)$ *are all distinct.*

Vadhan [89] shows an explicit efficient construction for averaging sampling with distinct samples (as defined above), by modifying an existing sampler based on random walks on expander graphs. It has been proven [89] that averaging sampler also preserves the min-entropy rate of the source. Nevertheless, we cannot apply this result as we will need another property: We require the sampling output to remain almost-secure (as in Definition 53) in the adversary's view. This property is required in proving the TFA-security of our BRM-DBV protocol. We show in Lemma 22 that averaging samplers keep the almost-security property of a source.

Lemma 22. *Let the random variable* $X \in \{0,1\}^n$ *be* (μ, δ)*-almost-secure conditioned on* Y*. Suppose* $Samp : \{0,1\}^r \to [n]^k$ *is a* (μ, θ, γ)*-averaging sampler with distinct samples. Then for uniformly distributed* $U_r \in \{0,1\}^r$*, the random variable* $M = X_{Samp(U_r)}$ *is* $(\mu - \theta, \delta')$*-almost-secure conditioned on* (U_r, Y)*, where* $\delta' = \log(\gamma + 2^{-\delta n})/k$*.*

Proof. See Appendix C.1. □

5.2 Distance Bounding Verification: Problem Definition

A distance bounding verification (DBV) protocol is a two-party protocol between a *verifier* $\mathbb{V}$ and a (possibly untrusted) *prover* $\mathbb{P}$ that enables the verifier to verify an upper-bound on distance claim by the prover. The protocol is initiated by $\mathbb{V}$ receiving a distance claim $d_{\mathbf{c}}$ supposedly sent by $\mathbb{P}$ whose real distance is $d_{\mathbf{r}}$. The protocol may have multiple rounds. In each round, one of the parties constructs a message using its current view

of the protocol, including its secret state and the messages received so far. At the end of the protocol the verifier outputs a Boolean value $\mathbb{V}_{out} \in \{\texttt{Acc}, \texttt{Rej}\}$ indicating $\mathbb{V}$ has accepted or rejected the claim, respectively.

Let d_0 be the maximum distance the DBV protocol is designed for and let $\psi > 1$ be a real-valued parameter called the *distance bounding (DB) ratio*. A distance claim $d_{\mathbf{c}} \leq d_0$ together with ψ partitions the area around $\mathbb{V}$ into three distance regions: (i) $d_{\mathbf{r}} \leq d_{\mathbf{c}}$, (ii) $d_{\mathbf{c}} < d_{\mathbf{r}} < \psi d_{\mathbf{c}}$, and (iii) $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$. See Figure 5.1. Region (i) that is the closest to $\mathbb{V}$ corresponds to the *honest setting*, denoted by $\texttt{Hon}[\mathbb{V} \leftrightarrow \mathbb{P}]$, where $\mathbb{V}$ is expected to output `Acc`. Region (iii) which is the farthest from $\mathbb{V}$ corresponds to an *adversarial setting* `Att` , where $\mathbb{V}$ should output `Rej`. There is finally a region (ii) between the other two regions where the protocol output cannot be guaranteed. This uncertain region can be controlled by appropriate choice of ψ.

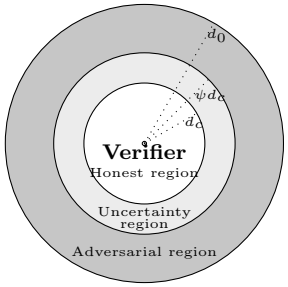


Figure 5.1: The distance bounding verification regions specified by $d_{\mathbf{c}}$ and ψ.

The performance of a DBV protocol is measured in terms of *completeness* and *soundness* using the two false rejection and false acceptance error rates, respectively.

Definition 56 (DBV protocol). *Let* `Att` *denote ad adversarial scenario against DBV. A DBV protocol* Π *is called a* $(\psi, \epsilon_{\texttt{FA}}, \epsilon_{\texttt{FR}})$-`Att` *-secure, when it satisfies*

$$\textit{Completeness}: \quad \Pr(\mathbb{V}_{out}(\texttt{Hon}[\mathbb{V} \leftrightarrow \mathbb{P}]) = \texttt{Acc}) \geq 1 - \epsilon_{\texttt{FR}}, \tag{5.1}$$

$$\textit{Soundness}: \quad \Pr(\mathbb{V}_{out}(\texttt{Att}) = \texttt{Rej}) \geq 1 - \epsilon_{\texttt{FA}}, \tag{5.2}$$

where $\mathbb{V}_{out}(\mathtt{x})$ *indicates the verifier's output in scenario* $\mathtt{x}$ *and the probability is taken over the randomness of the protocol, the adversary, and the environment.*

5.2.1 Adversarial scenarios

We assume that the DBV protocol, its parameters and implementation, are publicly known. The adversary can listen to and tamper with the communicated messages: that is replacing a transmitted message with one of its choice. Let $\psi > 1$ be the DB ratio given as part of the DBV protocol specification. In this work, we consider three adversarial scenarios (introduced in [30]) that are commonly considered for distance bounding protocols [17, 18]. We note that an adversarial scenario always refers to a case where $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$ holds.

Distance fraud attack (DFA). There are two entities: an honest verifier $\mathbb{V}$ and a dishonest prover $\mathbb{P}$ at distance $d_{\mathbf{r}}$ to the verifier. $\mathbb{P}$ claims distance $d_{\mathbf{c}}$, where $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$ and its goal is to convince $\mathbb{V}$ of its claim. The attack scenario is denoted by $\mathtt{DFA}[\mathbb{V} \leftrightarrow \mathbb{P}]$.

Mafia fraud attack (MFA). The mafia fraud, denoted by $\mathtt{MFA}[\mathbb{V} \leftrightarrow \mathbb{I} \leftrightarrow \mathbb{P}]$, consists of three parties: an honest verifier $\mathbb{V}$, an honest prover $\mathbb{P}$ at the distance $d_{\mathbf{r}}$, and an intruder $\mathbb{I}$ who launches a man-in-the-middle attack. No restriction is put on the location of $\mathbb{I}$. The attack begins with $\mathbb{P}$ sending an honest distance claim and $\mathbb{I}$ modifying it to a claim $d_{\mathbf{c}}$, where $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$. The rest of the attack is about $\mathbb{I}$ trying to convince $\mathbb{V}$ about this claim. Protection against MFA requires $\mathbb{P}$ and $\mathbb{V}$ to share secret key information by which $\mathbb{V}$ can distinguish $\mathbb{P}$ from $\mathbb{I}$.

Terrorist Fraud Attack (TFA). The terrorist fraud, denoted by $\mathtt{TFA}[\mathbb{V} \leftrightarrow \mathbb{I} \leftrightarrow \mathbb{P}]$, also includes three parties: an honest verifier $\mathbb{V}$, a malicious prover $\mathbb{P}$ at the distance $d_{\mathbf{r}}$, a colluding intruder $\mathbb{I}$ that can be at any location. Similar to MFA-security, TFA-security also relies on secret key information shared between $\mathbb{V}$ and $\mathbb{P}$. The prover's goal is to help $\mathbb{I}$ convince $\mathbb{V}$ of the distance claim $d_{\mathbf{c}}$ where $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$, nevertheless without revealing

crucial secret key information that would increase $\mathbb{I}$'s success chance in impersonating the prover without its permission. An *impersonation attack*, denoted by $\texttt{Imp}[\mathbb{V} \leftrightarrow \mathcal{A}dv]$, refers to a scenario where an adversary $\mathcal{A}dv$ initiates the conversation with $\mathbb{V}$ by sending a distance claim $d_{\mathbf{c}}$, while the prover at some distance $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$ is unaware of this conversation.

Different definitions for TFA have been proposed to capture the above requirement (cf. [37]). However, all these definitions are dedicated to time-based distance bounding solutions and furthermore, they assume multiple-time distance bounding where $\mathbb{I}$ may use the leaked information in one session to gain advantage in other sessions. This formalization thus cannot be immediately applied to our setting of one-time distance bounding verification without time measurement.

We provide a slightly different formalization of TFA, described as follows. In our setting, $\mathbb{P}$ can leak any secret key information W to $\mathbb{I}$ as long as $\mathbb{I}$ is not encouraged to launch an impersonation attack instead of following the TFA. Clearly if W is leaked after $\mathbb{V}$ receives the TFA distance claim, a session has already been started and $\mathbb{I}$ cannot replace it by impersonation. When leakage occurs before $\mathbb{V}$ receives a claim, the intruder may succeed in launching an impersonation attack sooner than the TFA begins. Our formalization thus puts a restriction on $\mathbb{I}$'s view by the time the distance claim is received by $\mathbb{V}$.

Definition 57. *Let* $\textit{TFA}[\mathbb{V} \leftrightarrow \mathbb{I} \leftrightarrow \mathbb{P}]$ *be an attack scenario that provides* $\mathbb{I}$ *with view* V *before* $\mathbb{V}$ *receives the distance claim. This attack scenario is a valid TFA if for any impersonator* $\mathcal{A}dv$ *that takes* V *as input, there exists a simulator* $\mathbb{S}$ *such that*

$$\Pr(\mathbb{V}_{out}(\textit{Imp}[\mathbb{V}, \mathbb{S}(\perp)]) = \texttt{Acc}) = \Pr(\mathbb{V}_{out}(\textit{Imp}[\mathbb{V}, \mathcal{A}dv(V)]) = \texttt{Acc}).$$

Remark 14. *Applying Definition 57 to one-time DBV protocols shows that* $\mathbb{P}$ *is allowed to reveal its key completely after being sure that* $\mathbb{V}$ *has received the claim and thus the*

$\mathbb{I}$ *cannot launch an impersonation. Moreover,* $\mathbb{P}$ *may even reveal some parts of its key to* $\mathbb{I}$ *before the protocol starts, provided that the leakage does not cause advantage in impersonation.*

5.2.2 Physical-layer model: PLAN

We consider an environment where wireless signal transmission is affected by *Path Loss and Additive Noise* (PLAN). We assume long-distance path loss ($d \gg 1m$) without fading, in which signal amplitude at a distance d from the transmitter is obtained by dividing the signal strength by $\sqrt{\xi d^{\alpha}}$, where $\xi \geq 1$ is a constant representing the *system loss* and $\alpha > 0$ is the *path loss exponent* whose value varies between 2 (free-space) and 4 (flat-earth) [70, Chapter 4]. The additive noise is a Gaussian signal with zero mean and variance Σ. Thus in our model, a signal transmitted with the initial power E will be received at a distance d with power $\frac{E}{\xi d^{\alpha}}$. We specify a PLAN communication environment by $\texttt{PLAN}^{\xi,\alpha,\Sigma}$where the three superscript parameters denote the system loss, the path loss exponent, and the noise power, respectively.

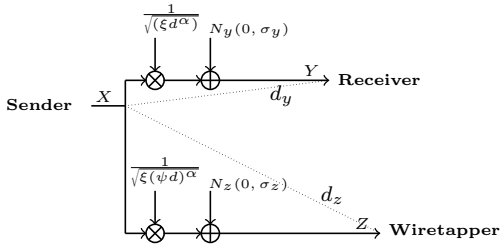


Figure 5.2: The $\texttt{PLAN}^{\xi,\alpha,\Sigma}$model

Remark 15. *We* assume *that the noise signals at two "different" receiving positions in* $\texttt{PLAN}^{\xi,\alpha,\Sigma}$ *are independent random variables. This common assumption is supported by the fact that in general signals reach their destinations through multiple independent routes. In our case this is a reasonable assumption as long as the two receivers are sufficiently*

apart [87, 90].

Figure 5.2 models the transmission of a signal X over $\texttt{PLAN}^{\xi,\alpha,\Sigma}$, where two receivers at distances d and ψd, for $\psi > 1$, receive signals $Y = (\xi d^{\alpha})^{-0.5} X + N_y$ and $Z = (\xi(\psi d)^{\alpha})^{-0.5} X + N_z$, where N_y and N_z are independent Gaussian random variables with zero mean and variance Σ. Assuming independence of noise variables the above two positions, the communication channel from the transmitter to the two receivers can be modeled as a Gaussian wiretap channel [56] (see Definition 9) with signal-to-noise ratios $SNR_y = \frac{E}{\xi d^{\alpha}\Sigma}$ at the legitimate receiver and $SNR_z = \frac{E}{\xi(\psi d)^{\alpha}\Sigma} = SNR_y/\psi^{\alpha}$ at the wiretapper, where E is the signal transmission power at the sender.

5.3 Distance Bounding Verification over PLAN

5.3.1 Challenge-Response with BPSK: DFA-secure DBV

We describe a basic DFA-secure DBV protocol which is simply a challenge-response protocol which relies on Binary Phase Shift Key (BPSK) modulation for signal transmission.

BPSK modulation and binary wiretap channel

For the purpose of signal transmission over the PLAN environment, we use Binary Phase Shift Key (BPSK) modulation with adjustable power, such that the modulator power is adjusted for an intended transmission distance d. Let E_{max} denote the maximum allowed power at the transmitter, and d_0 be the maximum distance that may be claimed to $\mathbb{V}$. We define the modulator $Mod_E : \{0,1\} \to \mathbb{R}$ and demodulator $Demod : \mathbb{R} \to \{0,1\}$ functions as

$$Mod_E(s) = \begin{cases} -\sqrt{E}, & \text{if } s = 0 \\ \sqrt{E}, & \text{if } s = 1 \end{cases}, \quad \text{and} \quad Demod(x) = \begin{cases} 0, & \text{if } x < 0 \\ 1, & \text{else} \end{cases}, \tag{5.3}$$

with power $E = \left(\frac{d}{d_0}\right)^{\alpha} E_0$ such that $E_0 \leq E_{max}$ is the transmission power for the highest distance bound d_0. We also use $Mod_E/Demod$ functions for sequences where we mean applying them on each symbol of the sequence, one by one.

The benefit of using $Mod_E/Demod$ over $\texttt{PLAN}^{\xi,\alpha,\Sigma}$is that it gives fixed signal-to-noise ratios SNR_0 and SNR_0/ψ^{α} for all pairs of intended/blocked distances $(d, \psi d)$, where $SNR_0 = \frac{E_0}{\Sigma \xi d_0^{\alpha}}$ is a constant determined by the system parameters. The above implies that all such pairs of channels can be mapped to a single binary symmetric wiretap channel (BSWC) as shown in Lemma 23.

Lemma 23. *Using $Mod_E/Demod$ over $\texttt{PLAN}^{\xi,\alpha,\Sigma}$converts any pair of channels from the verifier $\mathbb{V}$ to distances d and ψd into a BSWC with main and wiretapping bit error probabilities*

$$p_{\mathbf{i}} = \frac{1}{2}\text{erfc}(\sqrt{SNR_0}) \quad \textit{and} \quad p_{\mathbf{b}} = \frac{1}{2}\text{erfc}(\sqrt{\frac{SNR_0}{\psi^{\alpha}}}), \tag{5.4}$$

where $SNR_0 = \frac{E_0}{\Sigma \xi d_0^{\alpha}}$ and $\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt$ is the complementary error function [1].

Proof. See Appendix C.2. □

Challenge-response protocol

The challenge-response protocol takes advantage of noise in the $\texttt{PLAN}^{\xi,\alpha,\Sigma}$environment to distinguish whether a claim belongs to an honest scenario or a distance fraud scenario. For positive integer k and real $E_0 \leq E_{max}$ and $0 \leq \beta \leq 1$, the (E_0, k, β)-challenge-response protocol, Π_1, is described as follows.

Challenge:. On receiving a distance claim $d_{\mathbf{c}}$, $\mathbb{V}$ chooses a random k-bit challenge M, and broadcasts $X = Mod_E(M)$, where $E = (d_{\mathbf{c}}/d_0)^{\alpha} E_0$; $\mathbb{P}$ receives Y.

Response: $\mathbb{P}$ demodulates and sends back $\hat{M} = Demod(Y)$ to $\mathbb{V}$ "reliably".

Verify: $\mathbb{V}$ accepts if $d_H(\hat{M}, M) \leq \beta k$.

Remark 16. *Notice the difference between communication from the prover to the verifier and that in the opposite direction. The prover communicates to the verifier by using appropriate coding techniques and signal power to provide reliable reception; thus, we assume this communication is error-free. The verifier, however, transmits the challenge string with certain power to cause distinguishably different signal-to-noise ratios between acceptable distances $d_{\mathbf{r}} \leq d_{\mathbf{c}}$ and fraud distances $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$.*

A (E_0, k, β)-challenge-response protocol is a $(\psi, \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}})$-DFA-secure DBV protocol if for any claim $d_{\mathbf{c}} \leq d_0$, no more than βk challenge bits are corrupted at distances $\leq d_{\mathbf{c}}$, and more than βk challenge bits are corrupted at distance $\geq \psi d_{\mathbf{c}}$, except with probabilities $\epsilon_{\mathtt{FR}}$ and $\epsilon_{\mathtt{FA}}$, respectively.

Proposition 6. *Given $\mathtt{PLAN}^{\xi,\alpha,\Sigma}$ and DBV parameters $\psi > 1$ and $0 < \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}} \leq 1$, choose $E_0 \leq E_{max}$ and $p_{\mathbf{i}} \leq \beta \leq p_{\mathbf{b}}$, where $p_{\mathbf{i}}$ and $p_{\mathbf{b}}$ are determined from (5.4). The (E_0, k, β)-challenge-response protocol, Π_1, with challenge length*

$$k \geq \lceil \max\{ \frac{(p_{\mathbf{i}} + \beta)\ln(1/\epsilon_{\mathtt{FR}})}{(\beta - p_{\mathbf{i}})^2} \ , \ \frac{(2p_{\mathbf{b}})\ln(1/\epsilon_{\mathtt{FA}})}{(p_{\mathbf{b}} - \beta)^2} \} \rceil, \tag{5.5}$$

is a $(\psi, \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}})$-DFA-secure DBV protocol over $\mathtt{PLAN}^{\xi,\alpha,\Sigma}$.

Proof. See Appendix C.3. □

5.3.2 Adding MFA-security to DBV

The Distance bounding verification problem assumes that the prover $\mathbb{P}$ knows its distance (or location) in a priori and the protocol is initiated by the verifier $\mathbb{V}$ receiving a distance claim from $\mathbb{P}$. In mafia fraud attack, $\mathbb{P}$ is honest and hence sends a legitimate claim, say $d_{\mathbf{r}}$. This suggests that MFA-security can be simply achieved by protecting $\mathbb{P}$'s messages from being manipulated, by using a message authentication code (MAC). Figure 5.3 shows a DFA/MFA-secure DBV protocol, Π_2, which is obtained by incorporating an ϵ-secure one-time MAC (with $\epsilon \leq \epsilon_{\mathtt{FA}}$) to $\mathbb{P}$'s response in the protocol Π_1 of Section 5.3.1.

We denote the MAC function by $\mathsf{Mac} : \mathcal{K}_a \times (\{0,1\}^n \times \mathcal{D}) \to \mathcal{T}$ and assume $\mathbb{V}$ and $\mathbb{P}$ share a secret key $\mathsf{SK}_a \in \mathcal{K}_a$. The communication, shown in brackets, from $\mathbb{P}$ to $\mathbb{V}$ is assumed to error-free (see Remark 16).

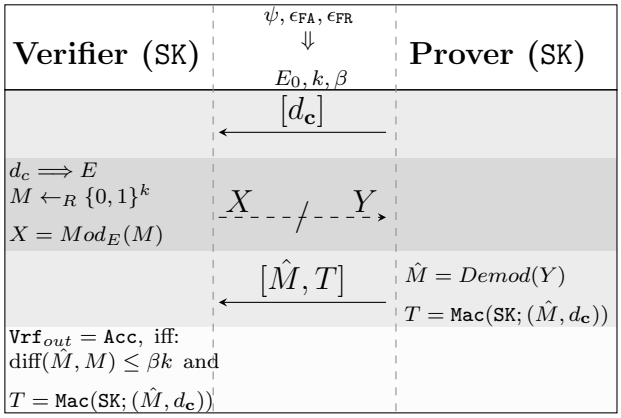


Figure 5.3: DFA/MFA-secure DBV protocol Π_2

Corollary 10. *Let parameters (E_0, k, β) be chosen as in Proposition 6 and* Mac *be an ϵ-secure one-time MAC with $\epsilon \leq \epsilon_{\mathtt{FA}}$. The DBV protocol Π_2 is $(\psi, \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}})$-DFA/MFA-secure over $\mathit{PLAN}^{\xi,\alpha,\Sigma}$.*

5.3.3 TFA-security and the bounded retrieval model

The DBV protocols Π_1 and Π_2 cannot resist TFA: The prover $\mathbb{P}$ can succeed in giving an acceptable response if an intruder stays within the claimed distance $d_{\mathbf{c}}$, demodulate the challenge signal, and pass it (reliably) to $\mathbb{P}$ with a distance $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$. More generally, without assuming any restriction on the communication capability of the $\mathbb{P}$ and $\mathbb{I}$, it is impossible to design a TFA-secure DBV protocol that does not rely on time measurement on the verifier's side. This can be seen by noting that the channel between $\mathbb{P}$ and $\mathbb{I}$ can be made error-free (by using error correcting codes) and instantaneous (without time measurement). The appropriately located intruder can relay all protocol messages (and other related signal information) back and forth between the other $\mathbb{P}$ and $\mathbb{V}$, without $\mathbb{V}$

noticing. Such an attack scenario does not require $\mathbb{I}$ to know any secret key information owned by $\mathbb{P}$ and is thus a valid terrorist fraud as in Definition 57.

Protecting against terrorist fraud in DBV may be possible if restrictive assumptions are made about the adversary's communication power. In the following, we describe a variant of the bounded retrieval model (BRM) that restricts the communication capability of the parties in the system. BRM is a variation of bounded storage model first proposed in [62]. In both cases there is a random source that generates strings with high min-entropy. Bounded storage model puts a bound on the amount of parties' storage. In BRM however [31, 38], there is no limit on the parties storage, rather the adversary's retrieval rate of the stored strings is limited.

We assume there is an oracle that generates a binary uniform string and transmits this string using BPSK. We assume that $\mathbb{V}$ can select the transmission power, but has no control over the string content. The signal transmission over the PLAN environment results in different (attenuated and noisy) observations at different points. The transmission speed is so high that the parties (including $\mathbb{V}$) can only retrieve a constant fraction $0 < \lambda < 1$ of what they observe. We always assume the honest parties retrieve λn individual bits from their n-bit observation by sampling. We however consider two types of adversaries: a *sampling adversary* who can only retrieve individual bits at specific indices, and a *general adversary* who can apply any λn-bit function to her observation. While the latter adversary is more powerful, the sampling adversary is reasonably interesting as one may argue that the applying any function other than sampling would require retrieving more bits from observation and hence would violate the BRM condition.

BRM oracle. The λ-BRM oracle, denoted by $\texttt{Orcl}_\lambda$, takes as input the transmission power $E \in \mathbb{R}_{>0}$, generates a uniformly random n-bit string O and transmits $X_O = Mod_E(O)$. The retrieval rate λ implies that each party can retrieve at most λn bits from the string.

Averaging sampler. We use "averaging sampler" *Samp*, defined in Definition 55. This primitive allows $\mathbb{V}$ and $\mathbb{P}$ can agree on which λn positions to pick from the BRM oracle output, by inputting a shared uniformly random key $\mathsf{SK}_e \in \mathcal{K}_e = \{0,1\}^r$.

The BRM-DBV Protocol. We describe the BRM-DBV protocol Π_3 that is secure against all three fraud attacks in the BRM. We assume that $\mathbb{V}$ and $\mathbb{P}$ share a key SK_e that is used for sampling the BRM oracle output. The reason for TFA-security is that the challenge in the BRM-DBV protocol is hidden in the BRM oracle output and retrieving it needs SK_e. Without a fair knowledge of this key, the intruder can only retrieve a random part of the oracle output and this cannot much help the (malicious) prover find an acceptable response. The protocol proceeds in three rounds as shown in Figure 5.4. As before, the communication from $\mathbb{P}$ to $\mathbb{V}$ is assumed to be error-free.

1. $\mathbb{P}$ sends a distance claim $[d_{\mathbf{c}}]$ reliably to $\mathbb{V}$.
2. $\mathbb{V}$ invokes the λ-BRM oracle $\mathtt{Orcl}_\lambda(E)$ with $n = k/\lambda$ and $E = \left(\frac{d_{\mathbf{c}}}{d_0}\right)^\alpha E_0$; the signal $X_O \in \mathbb{R}^n$ is transmitted and $\mathbb{P}$ receives Y_O.
3. $\mathbb{P}$ uses *Samp* to retrieve $Y_M = Y_{O,Samp(\mathsf{SK}_e)}$, obtains $\hat{M} = Mod_E(Y_M)$, and sends back $[\hat{M}]$.

* **Verify:** $\mathbb{V}$ obtains $M = X_{O,Samp(\mathsf{SK}_e)}$ and accepts iff $d_H(\hat{M}, M) \leq \beta k$.

Theorem 18. *Given* $0 < \lambda < \log(e)/2$, $\mathtt{PLAN}^{\xi,\alpha,\Sigma}$, *and DBV parameters* $\psi > 1$ *and* $0 < \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}} \leq 1$, *if there exists* $E_0 \leq E_{max}$ *such that* $p_{\mathbf{i}} < p_{\mathbf{b}} - \sqrt{2\ln(2)p_{\mathbf{b}}\lambda}$, *where* $p_{\mathbf{i}}$ *and* $p_{\mathbf{b}}$ *are determined from Lemma 23, then the following holds.*

Choose β, θ, μ, k, n *such that* $p_{\mathbf{i}} < \beta$, $\mu = \beta + \theta$, $\mu < p_{\mathbf{b}} - \sqrt{2\ln(2)p_{\mathbf{b}}\lambda}$, *and*

$$k \geq \lceil \max\{ \frac{(p_{\mathbf{i}} + \beta)\ln(1/\epsilon_{\mathtt{FR}})}{(\beta - p_{\mathbf{i}})^2} \ , \ \frac{2p_{\mathbf{b}}\lambda \ln(1/(\epsilon_{\mathtt{FA}} - \gamma))}{(p_{\mathbf{b}} - \mu)^2 - 2\ln(2)p_{\mathbf{b}}\lambda} \} \rceil, \quad \textit{and} \quad n = \lceil k/\lambda \rceil. \tag{5.6}$$

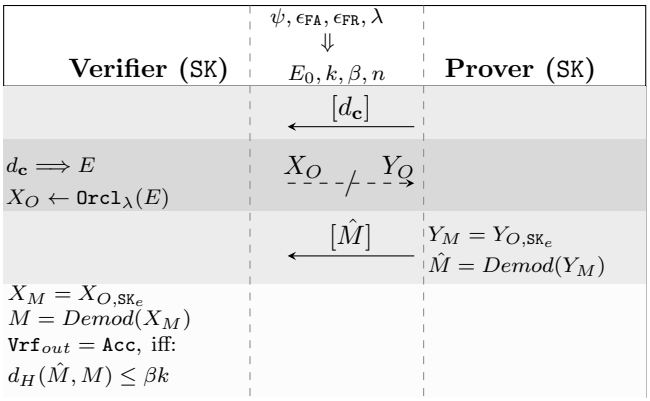


Figure 5.4: TFA-secure BRM-DBV protocol Π_3

The BRM-DBV protocol Π_3 *is* $(\psi, \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}})$*-DFA/MFA/TFA-secure over* $\mathtt{PLAN}^{\xi,\alpha,\Sigma}$ *in the* λ*-BRM with general intruder.*

Proof. See Appendix C.4. □

The above result shows the possibility of TFA-secure distance bounding verification in the BRM. The construction however will work when certain conditions are satisfied. Firstly, the retrieval rate λ must be less than $\log(e)/2 \approx 0.72$; otherwise, the inequality $p_{\mathbf{i}} < p_{\mathbf{b}} - \sqrt{2\ln(2)p_{\mathbf{b}}\lambda}$ cannot hold as the right hand side becomes non-positive. Secondly, the relationship among parameters is complex and so simply keeping $\lambda < \log(e)/2$ is not sufficient as there may be a set of system parameters that make it impossible to find a transmission power $E_0 \leq E_{max}$ so that the above inequality holds. The numerical analysis of Section 5.4.1 makes this more clear. In the following, we show that our BRM-DBV protocol in the BRM is TFA-secure at any retrieval rate $0 < \lambda < 1$, assuming $\mathbb{I}$ behaves like a sampling adversary.

Theorem 19. *Given* $0 < \lambda < 1$, $\mathtt{PLAN}^{\xi,\alpha,\Sigma}$*, and DBV parameters* $\psi > 1$ *and* $0 < \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}} \leq 1$*, if there exists* $E_0 \leq E_{max}$ *such that* $p_{\mathbf{i}} < (1-\lambda)p_{\mathbf{b}}$*, where* $p_{\mathbf{i}}$ *and* $p_{\mathbf{b}}$ *are determined from Lemma 23, the the following holds.*

Choose β, θ, μ, k, n *such that* $p_{\mathbf{i}} < \beta$, $\mu = \beta + \theta$, $\mu < (1-\lambda)p_{\mathbf{b}}$, *and*

$$k \geq \lceil \max\{ \frac{(p_{\mathbf{i}} + \beta)\ln(1/\epsilon_{\mathtt{FR}})}{(\beta - p_{\mathbf{i}})^2} \ , \ \frac{2(1-\lambda)p_{\mathbf{b}}\ln(1/(\epsilon_{\mathtt{FA}} - \gamma))}{((1-\lambda)p_{\mathbf{b}} - \mu)^2} \} \rceil, \quad \textit{and} \quad n = \lceil k/\lambda \rceil. \quad (5.7)$$

The BRM-DBV protocol Π_3 *is* $(\psi, \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}})$*-DFA/MFA/TFA-secure over* $\mathtt{PLAN}^{\xi,\alpha,\Sigma}$ *in the* λ*-BRM with sampling intruder.*

Proof. See Appendix C.5. □

From (5.4), any arbitrarily small $\frac{p_{\mathbf{i}}}{p_{\mathbf{b}}}$ is achieved by choosing E_0 and hence SNR_0 sufficiently large enough. We however should note that when E_{max} is not very large, some values of $\frac{p_{\mathbf{i}}}{p_{\mathbf{b}}}$ may not be achievable with $E_0 \leq E_{max}$. We explain this more in Section 5.4.2.

5.4 Numerical Analysis

The DBV protocols porposed in this work are computationally efficient as they use light-computation functions such as Hamming distance calculation, message authentication codes, samplers. The protocols however have communication costs that depend on the system parameters. In particular, the communication cost is tightly related to the challenge length which depends on the protocol parameters $(\psi, \epsilon_{\mathtt{FA}}, \epsilon_{\mathtt{FR}})$. Moreover, the BRM-DBV protocol may not provide TFA-security against a general intruder for all input parameters, and it is interesting to know under what input conditions TFA-security is guaranteed.

In the following, we analyze the performance of our designed protocols with respect to protocol parameters. Throughout, we suppose we are required to design DBV protocols for a distance range of $d_0 = 100$km over the $\mathtt{PLAN}^{\xi,\alpha,\Sigma}$ environment with the following parameters: no system loss $\xi = 1$, outdoor path loss exponent $\alpha = 3$, and noise power $\Sigma = 1\text{pW} \approx -90\text{dBm}$. Let the maximum allowed power at the transmitter be $E_{max} = 30\text{kW} \approx 75\text{dBm}$ which is reasonable for small radio stations.

5.4.1 DBV protocols Π_1 and Π_2

Given $\texttt{PLAN}^{\xi,\alpha,\Sigma}$and DBV parameters $\psi > 1$ and $0 < \epsilon_{\texttt{FA}}, \epsilon_{\texttt{FR}} \leq 1$, we shall obtain the challenge-response parameters (E_0^*, k^*, β^*) that give a $(\psi, \epsilon_{\texttt{FA}}, \epsilon_{\texttt{FR}})$-DFA-secure DBV protocol, while minimizing the challenge length required. We analyze the behavior of the minimal challenge length k^* with respect to the DBV protocol parameters $(\psi, \epsilon_{\texttt{FA}}, \epsilon_{\texttt{FR}})$; for simplicity, we assume equal error probabilities $\epsilon_{\texttt{FA}} = \epsilon_{\texttt{FR}} = \epsilon$. Following Proposition 6, the optimal challenge-response parameters are determined by minimizing (5.5) as

$$k^* = \lceil \ln(1/\epsilon) \min_{E_0 \leq E_{max}} \min_{p_{\mathbf{i}} < \beta < p_{\mathbf{b}}} \max\{\frac{(p_{\mathbf{i}} + \beta)}{(\beta - p_{\mathbf{i}})^2} \ , \ \frac{(2p_{\mathbf{b}})}{(p_{\mathbf{b}} - \beta)^2}\}\rceil, \tag{5.8}$$

and letting E_0^* and β^* be choices that result in k^*. Figure 5.5 graphs the changes in k^* (in bits) and E_0^* (in dBm) as functions of $1 < \psi \leq 1.5$ for $\epsilon \in \{10^{-3}, 10^{-4}, 10^{-5}\}$. The upper graph shows reasonable challenge length increases by decreasing the DB ratio ψ; however, it remains in a reasonable range, e.g., changing ψ from 1.1 to 1.01 causes k^* to increase from 231 bits to 2629 bits. The lower graph shows that optimal power E_0^* increases when ψ increases; however, its value does not depend on ϵ as also appears from (5.8). We also note that the optimal choice of E_0 is typically far less than the maximum allowed power $E_{max} = 75$dBm. The reason is that increasing E_0, increases the signal-to-noise ratio at both receivers and does not necessarily minimize the term (5.8).

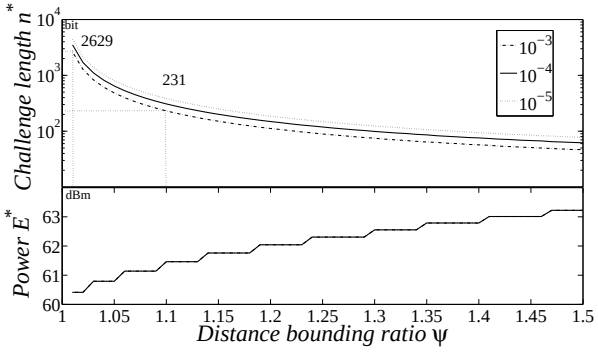


Figure 5.5: Protocol Π_1: changes in challenge length n^* and power E_0^* w.r.t. ψ and ϵ.

5.4.2 DBV protocol Π_3 against sampling and general intruders

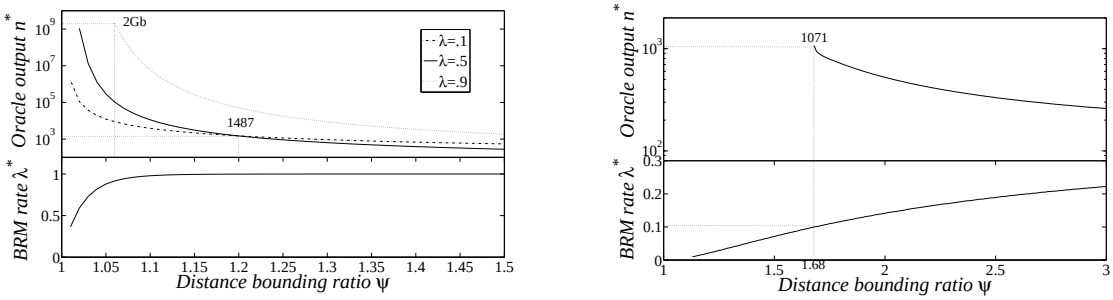
We follow a similar approach to the previous section to find the minimum n that is required by this protocol in the BRM. We start by requiring TFA-security against sampling intruder and then discuss about the general intruder case.

Sampling intruder. According to Theorem 18, the minimum n is obtained as (by considering θ and γ to be negligible)

$$n^* = \lceil \frac{1}{\lambda} \ln(1/\epsilon) \min_{E_0 \leq E_{max}} \quad \min_{p_{\mathbf{i}} < \beta < (1-\lambda)p_{\mathbf{b}}} \max\{\frac{(p_{\mathbf{i}} + \beta)}{(\beta - p_{\mathbf{i}})^2} \ , \ \frac{2(1-\lambda)p_{\mathbf{b}}}{((1-\lambda)p_{\mathbf{b}} - \beta)^2}\}\rceil, \qquad (5.9)$$

The above expression for n^* is very similar to (5.8) for k^*, except that $p_{\mathbf{b}}$ is replaced by $(1-\lambda)p_{\mathbf{b}}$ and a $1/\lambda$ coefficient is included in the expression. This reveals that the communication complexity of Π_3 can be much higher than Π_1 (and also Π_2). For small λ, we get $(1-\lambda)p_{\mathbf{b}} \approx p_{\mathbf{b}}$ and increase in the communication complexity is caused by $1/\lambda$ factor in (5.9). For larger λ, the minimization in (5.9) results in much higher value than that of (5.8). Figure 5.6(a) includes two graphs. The lower graph shows the maximum BRM rate λ^* (for which TFA-security against sampling intruder is guaranteed) as a function of the DB ratio ψ. When ψ is too small, the TFA-security cannot not hold for all λ's only because the transmission powers is bounded by E_{max}. Of course, by letting E_{max} be sufficiently large the protocol Π_3 will work for all ψ's and λ's. The upper graph illustrates the behavior of n^* with respect to ψ for $\lambda \in \{0.1, 0.5, 0.9\}$. Both increment of λ and decrement of ψ cause drastic increase in the length n^*, such that for $\psi = 1.06$ and $\lambda = 0.9$, the BRM oracle should send around 2 Gigabits of random data.

General intruder. For general intruder the results are more restrictive, mainly because Theorem 18 provides security guarantees only if the set of input parameters satisfy $p_{\mathbf{i}} < p_{\mathbf{b}} - \sqrt{2\ln(2)p_{\mathbf{b}}\lambda}$, and these cases are quite limited as shown in Figure 5.6(b). The lower graph indicates that the BRM rate λ should be too small for TFA-security against



(a) Sampling intruder scenario.

(b) General intruder scenario.

Figure 5.6: Protocol Π_3: Changes in oracle length n^* and BRM rate λ^* w.r.t. ψ.

general intruder, e.g., for $\psi = 1.68$ the rate λ cannot be more than 0.1. The upper graph then draws n^* as a function of ψ when $\lambda = 0.1$: the numbers suggest that when security guarantee can be provided, the oracle output length can be reasonably small, e.g., $n^* = 1071$ for $\psi = 1.68$.

5.5 Conclusion

We studied the problem of distance bounding verification (DBV) through which the prover claims an upper bound on its distance the verifier. The existing approaches to this problem with security concerns propose using time of flight for estimating the distance between the verifier to the prover. We proposed an alternative solution that uses physical properties of the signal propagation environment for this purpose. We showed possibility and impossibility results for protocols achieving different levels of security, using this approach. We showed that it is possible to construct efficient DFA/MFA-secure DBV protocols only relying on physical channel properties; however, TFA-security without time measurement is impossible. We next considered the bounded retrieval model (BRM) and introduced a TFA-secure protocol in this model. We analyzed the performance and the security of our protocols via numerical analysis. There are numerous open questions

and future research directions that follow from this work. We give these questions while discussing our assumptions and results in the following.

Practicality of the results. This work provides a practical approach to distance bounding verification with DFA/MFA-security in real-life communication environments. The growing area of location-based services for mobile devices [75] is a good example that matches our DBV setting. Most of location-based services provide their costumers with rewards and benefits when they check in at certain locations and this creates incentive for malicious users to cheat on their location [45]. Such an attack scenario can be addressed by our DFA-secure DBV protocol and without requiring specialized time-measurement hardware, noting that mobile devices are often sophisticated with Global Positioning System (GPS) tools.

The study of distance bounding verification in the bounded retrieval model (BRM), on the other hand, is a theoretically interesting area that provides an example of the adversary's restriction that makes possible TFA-secure DBV without time measurement. A similar work to this is the study of BRM in position based cryptography [21]. *Proposing more realistic models for designing secure distance bounding without time measurement is an interesting open question.*

The environment setting. We assume a widely-accepted, yet simple model for wireless communication that includes signal attenuation and additive Gaussian noise. *With a slight revision of our primitive parameters, similar solutions can be used for more complex communication models, such as Reighley fading channels.* We also assume all communicating devices have the same reception gain and so, a farther receiver obtains a more attenuated signal. This assumption can be relaxed by considering a more powerful receiver for the adversary, whose reception gain is a constant times that of the honest party. Secure DBV in this relaxed case can be achieved at the price of requiring a higher DB ratio ψ.

Channel noise versus time of flight. This work inquires the physical properties of a natural propagation environment as an alternative to time measurement for the purpose of distance bounding verification. Despite the promising results, our study acknowledges time of flight as a more powerful resource that potentially allows for higher levels of security, e.g., against terrorist fraud attacks without additional assumptions. *An interesting open question is if one can combine physical channel properties with time measurement to achieve better performance, for instance to reduce the required clock accuracy of time-based protocols without sacrificing security.*

From DBV to DB protocols. *It is quite important to know whether our DBV protocols can be used to build secure DB protocols that do not require the prover to know its distance*, i.e., expect the protocol to output a verified distance bound. We do not treat this problem formally, but here are a few words on this topic. Assuming that the protocol should estimate a distance bound from a limited number of distances, say d_1 to d_l for some small l, distance bounding can be obtained by repeating a DBV protocol (with carefully chosen parameters) for all these values in place of the distance claim and outputing the smallest i such that the claim d_i is verified via DBV. This approach provides distance bounding with security against distance fraud, but not mafia fraud since a relay man-in-the middle attack becomes irresistible. We believe that this approach achieves MFA- and TFA-security in the bounded retrieval model.

One-time versus multiple-time DBV. Our study involves one-time distance bounding verification in the information-theoretic setting (against computationally unbounded adversaries). The protocols though can be converted to work for multiple-time DBV, by each time creating fresh randomness for the challenge and fresh keys for the secret-key primitives, namely the MAC and the sampler. This latter can be also achieved by using multiple-time MACs and samplers to reduce the required key size. We also note that the DBV protocols can be easily modified for usage in the computational setting and

for polynomially many times, by using computationally-secure MAC (and sampler) with more efficiency in the key size.

Chapter 6

Conclusion and Future Work

Providing security functionalities over physical-layer channels is a growing area in information security and cryptography. In this thesis, we considered three security-related problems, namely *secret key establishment*, *manipulation detection*, and *distance bounding verbification* and investigated solutions to these problems that benefit from physical-layer properties as resources. In the following, we summarize our results of studying these problems and point out open questions and future work directions. This work also encourages revisiting other security primitives and protocols when physical-layer properties can be used to improve the effeciency/performace of the current results.

6.1 Secret Key Establishment

We formalized the problem of secret key establishment (SKE) in a communication scenario (referred to as a *setup*) that consists of discrete memoryless sources and channels available to Alice and Bob as legitimate users and Eve as an eavesdropper. We defined the SK capacity as the highest key rate that can be achieved using resources in the setup.

2DMWC. We first considered 2DMWC which consists of a pair of discrete memoryless wiretap channels (DMWCs) between Alice and Bob in the two directions. We proved lower and upper bounds on the SK capacity in this setup, showed their coincidence in special cases, and analyzed these results using numerical analysis for binary channels.

2DMWC without randomness. We noticed two implicit assumptions in the above work: (i) local randomness is freely available to the parties and (ii) the independence of the two DMWCs. We removed assumption (i) by considering SKE using 2DMWC when

there is no initial randomness available to the parties. We showed that channel noise can be used as a single resource for both extracting the required randomness and establishing the secret key. We obtained lower and upper bounds on the SK capacity and applied the two bounds to the case of binary channels to show the gap between them.

TWDMWC. We removed assumption (ii) by considering SKE using two-way discrete memoryless wiretap channel (TWDMWC), which receives two inputs from Alice and Bob and returns three outputs to the parties (including Eve). We showed a "trivial" lower bound on the SK capacity of TWDMWC that follows immediately from previous work We next showed an improvement of the trivial lower bound and analyzed this improvement over binary channel. We also derived an upper bound on the capacity and discussed cases where the bounds coincide.

Weak vs. strong capacity. We noticed that the above work uses the weak SK capacity definitions that needs negligible rate of key leakage to Eve, whereas the strong SK capacity requires negligible total key leakage. Maurer and Wolf [60] showed the equality of the weak and the strong SK capacities for one-way DMWC with/without public discussion [3, 26, 59, 96]. We modified their proof to make it applicable to any discrete memoryless setup and showed the equality of the two SK capacities for any discrete memoryless setup that allows for reliable transmission. Extending this proof to the secure message transmission problem showes that the weak and the strong secrecy capacities are equal for any discrete memoryless setup that allows the sender to provide randomness. Trivial counterexamples show that these sufficient conditions are not always necessary for the equality of the capacities.

Open questions and challenges. The work creates a number of open questions/challenges that remain to be answered.

- Improving our lower and upper bounds on the SK capacity in the 2DMWC

and TWDMWC setups is a subject of future work. This would imply tighter estimations of the SK capacity for these setups.

- Except for when initial randomness does not exist, the SKE protocols proposed by this work are two-round protocols. It is interesting to know whether one can achieve higher key rates by using more rounds of interaction.

- Exploring the role of randomness in other cryptographic tasks and the existence of cryptographic primitives when channel noise is the only source of randomness is an interesting problem to work on.

- The equality results for the weak and the strong capacities are conditional. Whether the conditions can be completely removed or shall be replaced by tight (necessary and sufficient) conditions remains open.

- The main assumption of this work (and the related work in the literature) is that sources and channels follow certain probability distributions (states) that are known by the protocol. In hostile environments however, it may be hard to have a good estimate of the wiretapper's source/channel states. It is practically important to relax the assumptions used by the above work and allow for some inaccuracies in source/channel state estimation.

6.2 Manipulation Detection

We formalized the problem of keyless manipulation detection over physical-layer channels by introducing an abstract communication model including an algebraic manipulable channel with leakage. We defined LR-AMD codes to achieve the above goal in this

communication model. Depending on the security requirement we defined two types of such codes, namely weak and strong LR-AMD codes.

LR-AMD codes: bounds and constructions. We derived lower bounds on the minimum coding redundancy of weak and strong LR-AMD codes and proved optimal LR-AMD constructions. The results show that strong LR-AMD codes can achieve negligible redundancy, but weak LR-AMD code constructions cannot. We defined and proposed *block-leakage-resilient (BLR)-AMD* code constructions as weak AMD codes that require negligible redundancy to detect algebraic manipulation in certain leakage scenarios.

LR-AMD codes: applications. We studied two applications of LR-AMD and BLR-AMD codes. We first considered robust secret sharing schemes (SSSs) and showed

(i) composing a strong systematic LR-AMD code with a linear nonperfect SSS that leaks less than half of the secret makes it robust, and

(ii) composing a BLR-AMD code with a linear somewhere-perfect SSS makes it robust.

We also studied manipulation detection over u-ary erasure- and symmetric-wiretap channels and showed

(i) There are strong systematic LR-AMD codes which detect algebraic manipulation over wiretap channels that erase (or corrupt) more than half of the communication, on average, for the adversary.

(ii) There are BLR-AMD codes which detect algebraic manipulation over wiretap channels that erase (resp. corrupt) more than u^{-1} (resp. $1 - u^{-1}$) fraction of the communication for the adversary.

Composing these constructions with other primitives, we can provide unlimited bitwise manipulation detection, in addition to privacy, in message transmission or key agree-

ment over binary symmetric and binary erasure channels. We also studied the online-adversarial channel, where the adversary has a linear/constant delay in receiving codeword bits and using them to decide on her manipulation strategy. For linear-delay adversaries algebraic manipulation detection can be achieved by strong systematic AMD codes. For constant delay adversaries, we showed unary coding construction as an AMD code family achieves arbitrary small failure probability; however, its asymptotic rate is zero.

Open questions and challenges. This work raises many questions and directions to future work.

- Providing robustness for nonperfect SSSs that leak more than half of the secret to the cheating adversary is a question we do not have an answer for.

- Further investigation of keyless manipulation detection in different settings of leakage is a problem with both theoretical and practical significance. This includes the questions which have remained open from this work, e.g., algebraic manipulation detection over wiretap channels that erase (resp. corrupt) "less" than u^{-1} (resp. $u^{-1} - u^{-2}$) fraction of the communication for the adversary.

- Existence and construction of AMD code families over the constant-delay adversarial channel is another open question of this work.

- LR-AMD codes are quite useful primitives which may find applications to other areas of cryptography. Finding such connections would be a nice piece of work.

6.3 Distance Bounding Verification

We considered distance bounding verification (DBV) protocols that are initiated by the prover claiming (an upper bound on) its distance and are continued by the verifier checking the correctness of this claim. The problem matches for instance verifying the customer's distance in location-based mobile services [45]. Unlike the current time-based approaches to this problem, we investigated solving the problem using physical-layer properties instead of time measurement. We adopted a widely-accepted model of wireless communication that includes signal attenuation and additive Gaussian noise. We considered three attack scenarios called distance fraud attack (DFA), mafia fraud attack (MFA), and terrorist fraud attack (TFA) against DBV.

DFA and MFA security. We began by introducing a DFA-secure DBV protocol that is based on a challenge-response phase whose content is transmitted over the wireless environment, via binary phase shift keying. We derived the challenge-repones specification which guarantees security for given environment and security parameters. The DFA-secure protocol can be changed to a DFA/MFA-secure protocol by simply using a message authentication code to protect the messages from the prover to the verifier, particularly the prover's response to the challenge message.

TFA security. We showed it is impossible to design TFA-secure protocols without time measurement, even if the adversary is computationally bounded; however, by limiting the adversary's communication capability to the bounded retrieval model (BRM), it is possible to construct protocols that are secure against all three attacks. The BRM assumes a high-throughput random string that parties (including the verifier) can only retrieve a *constant fraction* of. Depending on the adversary's retrieval capability, we considered security against *the sampling adversary* and *the general adversary*. We proposed a *BRM-DBV protocol* and derived conditions under which the protocol achieves

DFA/MFA/TFA-security in the BRM against general and sampling adversaries.

Numerical analysis. We used numerical analysis to elaborate on the performance of our designed protocols with respect to input parameters. The analysis shows that TFA-security against the general adversary is achievable only under certain conditions, but DFA-, MFA-, and TFA-security against the sampling adversary can be provided for all input parameters.

Open questions and challenges. The work opens a new direction to the study of secure distance bounding verification protocols. The open questions of this work are listed below.

- It is practically important to investigate where our DBV protocols can be implemented in real-life wireless environments with more complex limitations.
- Proposing more realistic models (than BRM) for designing secure distance bounding without time measurement is of both theoretical and practical interest.
- Another interesting question is whether one can combine physical-layer properties with time measurement to achieve better performance, for instance to reduce the required clock accuracy of time-based protocols without sacrificing security.
- It is also important to find the connection of DBV protocols to DB protocols that do not require the prover to know its distance, i.e., expect the protocol to output a verified distance bound. In Section 5.5, we pointed out a few thoughts regarding the topic. The formal treatment of this problem however remains an interesting question for future work.

Bibliography

[1] M. Abramowitz and I. Stegun. *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*, volume 55. Dover publications, 1965.

[2] R. Ahlswede and N. Cai. Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder. *General Theory of Information Transfer and Combinatorics*, pages 258–275, 2006.

[3] R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography. i. secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.

[4] H. Ahmadi and R. Safavi-Naini. Leakage-resilient detection of algebraic manipulation. In *Advances in Cryptology–EUROCRYPT 2013*. in submission.

[5] H. Ahmadi and R. Safavi-Naini. Secure distance bounding verification without time measurement. In *Advances in Cryptology–EUROCRYPT 2013*. in submission.

[6] H. Ahmadi and R. Safavi-Naini. New results on key establishment over a pair of independent broadcast channels. In *International Symposium on Information Theory and its Applications (ISITA)*, pages 191 –196, 2010.

[7] H. Ahmadi and R. Safavi-Naini. Secret key establishment over a pair of independent broadcast channels. In *International Symposium on Information Theory and its Applications (ISITA)*, pages 185 –190, 2010.

[8] H. Ahmadi and R. Safavi-Naini. Common randomness and secret key capacities of two-way channels. In *International Conference on Information Theoretic Security (ICITS)*, pages 76–93, 2011.

[9] H. Ahmadi and R. Safavi-Naini. Secret key establishment over noisy channels. In *Foundations and Practice of Security*, pages 132–147, 2011.

[10] H. Ahmadi and R. Safavi-Naini. Secret keys from channel noise. In *Advances in Cryptology–EUROCRYPT 2011*, pages 266–283, 2011.

[11] H. Ahmadi and R. Safavi-Naini. Message transmission and key establishment: Conditions for equality of weak and strong capacities. In *Foundations and Practice of Security*. Springer, 2012.

[12] M. Bellare and J. Rompel. Randomness-efficient oblivious sampling. In *35th Annual Symposium on Foundations of Computer Science*, pages 276 –287, 1994.

[13] M. Bellare, S. Tessaro, and A. Vardy. Semantic security for the wiretap channel. *Advances in Cryptology–CRYPTO 2012*, pages 294–311, 2012.

[14] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[15] G. Blakley and C. Meadows. Security of ramp schemes. In *Advances in Cryptology*, pages 242–268, 1985.

[16] S. Brands and D. Chaum. Distance-bounding protocols. In *Advances in Cryptology EUROCRYPT 93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. 1994.

[17] L. Bussard. *Trust Establishmenrt Protocols for Communications Devices*. PhD thesis, Eurecom-ENST, September 2004.

[18] L. Bussard and W. Bagga. Distance-bounding proof of knowledge to avoid real-time attacks. In *Security and Privacy in the Age of Ubiquitous Computing*, volume 181

of *IFIP Advances in Information and Communication Technology*, pages 223–238. 2005.

[19] S. Capkun and J.-P. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221 – 232, 2006.

[20] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of computer and system sciences*, 18(2):143–154, 1979.

[21] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position based cryptography. In *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 391–407. 2009.

[22] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.

[23] T. M. Cover and J. A. Thomas. *Elements of information theory, Edition 2*. Wiley-IEEE, 2006.

[24] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. *Advances in Cryptology–EUROCRYPT 2008*, pages 471–488, 2008.

[25] R. Crandall and C. Pomerance. *Prime numbers: a computational perspective*, volume 182. Springer, 2005.

[26] I. Csiszár and J. Köorner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[27] I. Csiszar and J. Körner. *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[28] I. Csiszár and P. Narayan. Common randomness and secret key generation with a helper. *IEEE Transactions on Information Theory*, 46(2):344–366, 2000.

[29] P. J. Davis. *Circulant matrices*. Chelsea Publishing Company, 1994.

[30] Y. Desmedt. Major security problems with the "unforgeable" (Feige)-Fiat-Shamir proofs of identity and how to overcome them. In *SecuriCom '88*, pages 15–17, 1998.

[31] G. Di Crescenzo, R. Lipton, and S. Walfish. Perfectly secure password protocols in the bounded retrieval model. In *Theory of Cryptography*, volume 3876 of *Lecture Notes in Computer Science*, pages 225–244. 2006.

[32] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[33] Y. Dodis, A. Elbaz, R. Oliveira, and R. Raz. Improved randomness extraction from two independent sources. *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 334–344, 2004.

[34] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances in cryptology-Eurocrypt 2004*, pages 523–540, 2004.

[35] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[36] R. Dorf. *The electrical engineering handbook*. CRC Press, 1997.

[37] U. Durholz, M. Fischlin, M. Kasper, and C. Onete. A formal approach to distance-bounding rfid protocols. In *Information Security*, volume 7001 of *Lecture Notes in Computer Science*, pages 47–62. 2011.

[38] S. Dziembowski. Intrusion-resilience via the bounded-storage model. In *Theory of Cryptography*, volume 3876 of *Lecture Notes in Computer Science*, pages 207–224. 2006.

[39] S. Dziembowski and K. Pietrzak. Leakage-resilient cryptography. In *49th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 293–302, 2008.

[40] A. El Gamal, O. O. Koyluoglu, M. Youssef, and H. El Gamal. The two way wiretap channel: Theory and practice. *arXiv preprint arXiv:1006.0778*, 2010.

[41] R. Gallager. *Information theory and reliable communication*. Wiley, 1968.

[42] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane. Codes which detect deception. *Bell System Technical Journal*, 53(3):405–424, 1974.

[43] V. Guruswami and A. Smith. Codes for computationally simple channels: Explicit constructions with optimal rate. In *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 723–732, 2010.

[44] G. Hancke and M. Kuhn. An rfid distance bounding protocol. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm '05*, pages 67 – 73, 2005.

[45] W. He, X. Liu, and M. Ren. Location cheating: A security challenge to location-based social network services. In *31st International Conference on Distributed Computing Systems (ICDCS)*, pages 740 –749, 2011.

[46] X. He and A. Yener. On the role of feedback in two-way secure communication. In *Asilomar Conference on Signals, Systems and Computers*, pages 1093–1097, 2008.

[47] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1-2):21–38, 2005.

[48] A. Khisti, S. Diggavi, and G. Wornell. Secret-key generation with correlated sources and noisy channels. In *IEEE International Symposium on Information Theory (ISIT)*, pages 1005–1009, 2008.

[49] C. Kim and G. Avoine. Rfid distance bounding protocol with mixed challenges to prevent relay attacks. In *Cryptology and Network Security*, volume 5888 of *Lecture Notes in Computer Science*, pages 119–133. 2009.

[50] C. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira. The swiss-knife RFID distance bounding protocol. In *Information Security and Cryptology - ICISC 2008*, volume 5461 of *Lecture Notes in Computer Science*, pages 98–115. 2009.

[51] J. Körner and K. Marton. Comparison of two noisy channels. *Topics in information theory*, (16), 1977.

[52] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii. Nonperfect secret sharing schemes and matroids. In *Advances in Cryptology - EUROCRYPT'93*, pages 126–141, 1994.

[53] L. Lai, H. El Gamal, and H. Poor. The wiretap channel with feedback: Encryption over the channel. *IEEE Transactions on Information Theory*, 54(11):5059–5067, 2008.

[54] M. Langberg. Oblivious communication channels and their capacity. *IEEE Transactions on Information Theory*, 54(1):424–429, 2008.

[55] M. Langberg, S. Jaggi, and B. K. Dey. Binary causal-adversary channels. In *IEEE International Symposium on Information Theory (ISIT)*, pages 2723–2727, 2009.

[56] S. Leung-Yan-Cheong and M. Hellman. The gaussian wire-tap channel. *IEEE Transactions on Information Theory*, 24(4):451 – 456, 1978.

[57] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential dsss: Jamming-resistant wireless broadcast communication. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9, 2010.

[58] H. Mahdavifar and A. Vardy. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Transactions on Information Theory*, 57(10):6428–6443, 2011.

[59] U. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[60] U. Maurer and S. Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in CryptologyEUROCRYPT 2000*, pages 351–368, 2000.

[61] U. Maurer and S. Wolf. Secret key agreement over unauthenticated public channels. i. definitions and a completeness result. *IEEE Transactions on Information Theory*, 49(4):822–831, 2003.

[62] U. M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5:53–66, 1992.

[63] J. Munilla and A. Peinado. Distance bounding protocols for rfid enhanced by using void-challenges and analysis in noisy channels. *Wireless Communications and Mobile Computing*, 8(9):1227–1232, 2008.

[64] V. Nikov and M. Vauclair. Yet another secure distance-bounding protocol. In *International Conference on Security and Cryptography*, SECRYPT' 08, pages 218–221, 2008.

[65] N. Nisan and D. Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, 1996.

[66] A. Odlyzko. Discrete logarithms: The past and the future. *Designs, Codes and Cryptography*, 19(2):129–145, 2000.

[67] A. J. Pierrot and M. R. Bloch. Strongly secure communications over the two-way wiretap channel. *IEEE Transactions on Information Forensics and Security*, 6(3):595–605, 2011.

[68] C. Pöpper, N. Tippenhauer, B. Danev, and S. Capkun. Investigation of signal and message manipulations on the wireless channel. *Computer Security–ESORICS 2011*, pages 40–59, 2011.

[69] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran. Secrecy via sources and channelsa secret key-secret message rate tradeoff region. In *IEEE International Symposium on Information Theory (ISIT)*, pages 1010–1014, 2008.

[70] T. S. Rappaport. *Wireless communications principles and practices, Second Edition.* Prentice-Hall, 2002.

[71] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 410–419, 2009.

[72] K. B. Rasmussen and S. Čapkun. Realization of rf distance bounding. In *Proceedings of the 19th USENIX Security Symposium*, 2010.

[73] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji. Detecting relay attacks with timing-based protocols. In *Proceedings of the 2nd ACM Symposium on Information*

Computer and Communications Security, ASIACCS '07, pages 204–213, 2007.

[74] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of the 2nd ACM Workshop on Wireless Security*, WiSe '03, pages 1–10, 2003.

[75] J. H. Schiller and A. Voisard. *Location-based services*. Morgan Kaufmann, 2004.

[76] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, 1948.

[77] C. E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[78] C. E. Shannon. Two-way communication channels. In *Proc. 4th Berkeley Symp. Math. Stat. Prob*, volume 1, pages 611–644, 1961.

[79] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[80] G. J. Simmons. A game theory model of digital message authentication. In *11th Annual Conference on Numerical Mathematics and Computing, Conaressus Numerantiumn*, pages 413–424, 1981.

[81] G. J. Simmons. Message authentication: a game on hypergraphs. *Congressus Numerantium*, 45:161–192, 1984.

[82] G. J. Simmons. Authentication theory/coding theory. In *Advances in cryptology CRYPTO 84*, pages 411–431, 1985.

[83] D. Singelee and B. Preneel. Location verification using secure distance bounding protocols. In *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, pages 840–847, 2005.

[84] M. Strasser, S. Capkun, C. Popper, and M. Cagalj. Jamming-resistant key establishment using uncoordinated frequency hopping. In *IEEE Symposium on Security and Privacy (SP)*, pages 64–78, 2008.

[85] E. Tekin and A. Yener. Achievable rates for two-way wire-tap channels. In *IEEE International Symposium on Information Theory (ISIT)*, pages 941–945, 2007.

[86] E. Tekin and A. Yener. The general gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, 2008.

[87] E. Telatar. Capacity of multi-antenna gaussian channels. *European Transactions on Telecommunications*, 10(6):585–595, 1999.

[88] S. Vadhan. Extracting all the randomness from a weakly random source. Technical report, Electronic Colloquium on Computational Complexity, 1998.

[89] S. P. Vadhan. On constructing locally computable extractors and cryptosystems in the bounded storage model. *Journal of Cryptology*, 17:43–77, 2004.

[90] S. V. Vaseghi. *Advanced digital signal processing and noise reduction, Third Edition.* John Wiley & Sons, 2006.

[91] S. Čapkun, L. Buttyán, and J.-P. Hubaux. Sector: secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks*, SASN '03, pages 21–32, 2003.

[92] S. Venkatesan and V. Anantharam. The common randomness capacity of a pair of independent discrete memoryless channels. *IEEE Transactions on Information Theory*, 44(1):215–224, 1998.

[93] J. Von Neumann. Various techniques used in connection with random digits. *Applied Math Series*, 12(36-38):1, 1951.

[94] B. Waters and E. Felten. Secure, private proofs of location. Technical Report TR-667-03, Princeton Computer Science, 2003.

[95] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22(3):265–279, 1981.

[96] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54:pp. 1355–1367, 1975.

Appendix A

Proof Results on Secret Key Establishment

A.1 Preliminaries

A.1.1 Proof of Lemma 10: Joint-AEP for bipartite sequences

Part 1) To prove $\Pr((X^N, Y^N) \in A_\epsilon^{(N,n)}) \to 1$

We shall show that with high probability X^N and Y^N are (ϵ, n)-bipartite typical and (X^N, Y^N) is (ϵ, n)-bipartite jointly typical as in Definitions 30 and 31, respectively. For large enough n and d, by the weak law of large numbers, we have

$$-\tfrac{1}{n}\log P_U(U^n) \to -E[\log P_U(U)] = H(U) \text{ in probability}$$

$$\Rightarrow \exists n_1 :\ \forall n > n_1, \Pr(|-\tfrac{1}{n}\log P_U(U^n) - H(U)| > \epsilon) < \tfrac{\epsilon}{6},$$

Similarly, we can conclude the following for the other parts of the sequences.

$$\exists d_1 :\ \forall d > d_1, \Pr(|-\tfrac{1}{d}\log P_T(T^d) - H(T)| > \epsilon) < \tfrac{\epsilon}{6},$$

$$\exists n_2 :\ \forall n > n_2, \Pr(|-\tfrac{1}{n}\log P_{U'}(U'^n) - H(U')| > \epsilon) < \tfrac{\epsilon}{6},$$

$$\exists d_2 :\ \forall d > d_2, \Pr(|-\tfrac{1}{d}\log P_{T'}(T'^d) - H(T')| > \epsilon) < \tfrac{\epsilon}{6}.$$

Since these sequences are i.i.d., we have

$$\log P(X^N) = \log P_U(U^n) + \log P_T(T^d),$$

$$\log P(Y^N) = \log P_{U'}(U'^n) + \log P_{T'}(T'^d),$$

which finally results in

$$\forall n > n_1, \forall d > d_1, \Pr(|-\tfrac{1}{N}\log P(X^N) - \tfrac{nH(U)+dH(T)}{N}| > \epsilon) < \tfrac{\epsilon}{3}, \tag{A.1}$$

$$\forall n > n_2, \forall d > d_2, \Pr(|-\tfrac{1}{N}\log P(Y^N) - \tfrac{nH(U')+dH(T')}{N}| > \epsilon) < \tfrac{\epsilon}{3}. \tag{A.2}$$

The same approach results in the following relations for the joint distribution,

$$\exists n_3 : \ \forall n > n_3, \Pr(|-\tfrac{1}{d}\log P_{T,T'}(T^d, T'^d) - H(T,T')| > \epsilon) < \tfrac{\epsilon}{6},$$

$$\exists d_3 : \ \forall d > d_3, \Pr(|-\tfrac{1}{n}\log P_{U,U'}(U^n, U'^n) - H(U,U')| > \epsilon) < \tfrac{\epsilon}{6},$$

$$\Rightarrow \forall n > n_3, \forall d > d_3, \Pr(|-\tfrac{1}{N}\log P(X^N, Y^N) - \tfrac{nH(U,U')+dH(T,T')}{N}| > \epsilon) < \tfrac{\epsilon}{3}. \quad \text{(A.3)}$$

By choosing $n > \max\{n_1, n_2, n_3\}$ and $d > \max\{d_1, d_2, d_3\}$, (A.1), (A.2), and (A.3) are satisfied. The probability union bound (over these three equations) states that $(X^N, Y^N) \notin A_\epsilon^{(N,n)}$ holds with probability less than ϵ, i.e., $\Pr((X^N, Y^N) \in A_\epsilon^{(N,n)}) \geq 1-\epsilon$. This proves the first part of the theorem.

Part 2) To prove $(1-\epsilon)2^{nH(U,U')+dH(T,T')-N\epsilon} \leq |A_\epsilon^{(N,n)}| \leq 2^{nH(U,U')+dH(T,T')+N\epsilon}$

$$1 = \sum P(x^N, y^N) \geq \sum_{A_\epsilon^{(N,n)}} P(x^N, y^N) \overset{(a)}{\geq} |A_\epsilon^{(N,n)}| 2^{-(nH(U,U')+dH(T,T')+N\epsilon)}$$
$$\Rightarrow |A_\epsilon^{(N,n)}| \leq 2^{nH(U,U')+dH(T,T')+N\epsilon},$$

and

$$1-\epsilon \leq \sum_{A_\epsilon^{(N,n)}} P(x^N, y^N) \overset{(b)}{\leq} |A_\epsilon^{(N,n)}| 2^{-nH(U,U')-dH(T,T')+N\epsilon}$$
$$\Rightarrow |A_\epsilon^{(N,n)}| \geq (1-\epsilon)2^{nH(U,U')+dH(T,T')-N\epsilon}.$$

Both inequalities (a) and (b) follow (A.3).

Part 3) To prove $(1-\epsilon)2^{-nI(U;U')-dI(T;T')-3N\epsilon} \leq \Pr((\tilde{X}^N, \tilde{Y}^N) \in A_\epsilon^{(N,n)}) \leq 2^{-nI(U;U')-dI(T;T')+3N\epsilon}$

Note that $\tilde{X}^N$ and $\tilde{Y}^N$ are independent and $Pr(\tilde{X}^N = x^N, \tilde{Y}^N = y^N) = P(x^N)P(y^N)$. Using (A.1), (A.2), and (A.3), we have

$$\Pr((\tilde{X}^N, \tilde{Y}^N) \in A_\epsilon^{(N,n)}) = \sum_{A_\epsilon^{(N,n)}} P(x^N)P(y^N)$$
$$\leq \left(2^{nH(U,U')+dH(T,T')+N\epsilon}\right)\left(2^{-nH(U)-dH(T)+N\epsilon}\right)\left(2^{-nH(U')-dH(T')+N\epsilon}\right)$$

$$= 2^{-nI(U;U')-dI(T;T')+3N\epsilon},$$

and

$$\Pr((\tilde{X}^N, \tilde{Y}^N) \in A_\epsilon^{(N,n)}) = \sum_{A_\epsilon^{(N,n)}} P(x^N)P(y^N)$$
$$\geq (1-\epsilon)\left(2^{nH(U,U')+dH(T,T')-N\epsilon}\right)\left(2^{-nH(U)-dH(T)-N\epsilon}\right)\left(2^{-nH(U')-dH(T')-N\epsilon}\right)$$
$$= (1-\epsilon)2^{-nI(U;U')-dI(T;T')-3N\epsilon}.$$

A.1.2 Proof of Lemma 11: Secure block code

The proof is based on a random coding argument. Given random variables W_2, W_1, X, Y, and Z as in the Lemma, let $R_c < I(W_1;Y)$, $R_2 = I(W_2;Y)$, $R_1 = R_c - R_2 < I(W_1;Y|W_2)$, $R_{sc} = I(W_1;Y|W_2) - I(W_1;Z|W_2)$, $M = 2^{nR_c}$ and $K = 2^{nR_{sc}}$. Assume that n is chosen sufficiently large such that nR_c, nR_2, nR_1, and nR_{sc} are all integers.

Define $\epsilon' = 2^{n(R_c - I(W_1;Y))}$ and $\epsilon = (2R_c+1)/R_{sc}\epsilon'$. Let $(\mathcal{B}_i)_{i=1}^{2^{\eta_2}}$ partition $[M]$ such that $\mathcal{B}_i = \{b_{i,j}\}_{j=1}^{2^{\eta_1}}$. Define $\mathfrak{b}_{indx} : [M] \to [2^{nR_2}] \times [2^{nR_1}]\}$ such that $\mathfrak{b}_{indx}(b) = (i,j)$, if b is labeled by $b_{i,j}$. Define the following two randomly generated codebooks.

(i) Define the codebook $\mathcal{C}_2$ as a the collection of 2^{η_2} codewords $\{w_{2,b_2}^n : \ b_2 \in [2^{\eta_2}]\}$, where each codeword w_{2,b_2}^n is of length n and is independently generated according to the distribution

$$\prod_{i=1}^{n} p(W_2 = w_{2,b_2}(i)).$$

(ii) For each w_{2,b_2}^n, define the codebook $\mathcal{C}_1(w_{2,b_2}^n)$ as the collection of $M = 2^{\eta_1}$ codewords $\{w_{1,b_2,b_1}^n : \ b_1 \in [2^{\eta_1}]\}$, where each codeword, w_{1,b_2,b_1}, is of length n and is independently generated according to the distribution

$$\prod_{i=1}^{n} p(W_1 = w_{1,b_2,b_1}(i)|W_2 = w_{2,b_2}(i)).$$

Encoding. The encoding function $Enc : [M] \to \mathcal{X}^n$ is defined such that $Enc(b)$ is the output of the DMC $(\mathcal{W}_1, \mathcal{X}, P_{X|W_1})$ for input w^n_{1,b_2,b_1} that is obtained using codebooks $\mathcal{C}_2$ and $\mathcal{C}_1$, where $(b_2, b_1) = \mathfrak{b}_{indx}(b)$.

Decoding. The decoding function $Dec : \mathcal{Y}^n \to [M]$ returns for $Y^n \in \mathcal{Y}^n$, a *unique* $b \in [M]$ such that the codeword $w^n_{1,b_2,b_1} \in \mathcal{C}_1$ for $(b_2, b_1) = \mathfrak{b}_{indx}(b)$ is ϵ-jointly typical to $Y_b^{n_b}$ (w.r.t. P_{W_1,Y_A}); she returns a NULL otherwise.

Key Derivation. The key derivation function $(\Phi_i)_{i=1}^K$ be a partition of $[M]$ into equal-sized parts of size $2^{n(R_c - R_{sc})}$. Define $\phi_{sk} : [M] \to [K]$ such that for $b \in \Phi_i$ we have $\phi_{sk}(b) = i$.

The reliability property of the block code follows from channel coding theorem (Theorem 2) over the DMC $(W_1, Y, P_{Y|W_1})$ and the fact that $R_c < I(W_1; Y)$ which gives decoding failure probability ϵ'. For the secrecy of $S = \Phi_{sk}(B)$, we have (letting $(B_2, B_1) = \mathfrak{b}_{indx}(B)$)

$$
\begin{aligned}
H(S|Z^n) &\geq H(S|w^n_{2,B_2}, Z^n) = H(S, w^n_{1,B_2,B_1}|w^n_{2,B_2}, Z^n) - H(w^n_{1,B_2,B_1}|S, w^n_{2,B_2}, Z^n) \\
&= H(w^n_{1,B_2,B_1}|w^n_{2,B_2}, Z^n) - H(w^n_{1,B_2,B_1}|S, w^n_{2,B_2}, Z^n) \\
&= H(w^n_{1,B_2,B_1}|w^n_{2,B_2}) - I(w^n_{1,B_2,B_1}; Z^n|w^n_{2,B_2}) - H(w^n_{1,B_2,B_1}|S, w^n_{2,B_2}, Z^n) \\
&\overset{(a)}{>} n[I(W_1; Y) - I(W_2; Y)] - nI(W_1; Z|W_2) - H(w^n_{1,B_2,B_1}|S, w^n_{2,B_2}, Z^n) \\
&= n[I(W_1; Y|W_2) - I(W_1; Z|W_2)] - H(w^n_{1,B_2,B_1}|S, w^n_{2,B_2}, Z^n) \\
&\overset{(b)}{\geq} n[I(W_1; Y|W_2) - I(W_1; Z|W_2)] - \epsilon \log(K). \\
\Rightarrow \quad & I(S; Z^n) \leq \epsilon \log(K).
\end{aligned}
$$

Inequality (a) follows from joint-AEP for (W_2, W_1, Z) as well as the fact that $M \leq 2^{nR_c} < 2^{nI(W_1;Y)}$. Inequality (b) holds because the knowledge of (S, w^n_{2,B_2}, Z^n) gives almost all the information about w^n_{1,B_2,B_1}; this is proved as follows. From key derivation, knowing S gives the partition Φ_S that B belongs to, and w^n_{2,B_2} shows the codeword chosen from $\mathcal{C}_2$. Define the codebook $\mathcal{C}^e_i(S, B_2) \triangleq \{w^n_{1,B_2,B_1} : B \in \Phi_S\}$ which is of size

$2^{n(R_c-R_{sc}-R_2)} = 2^{n(R_1-R_{sc})} < 2^{nI(W_1;Z|W_2)} \leq 2^{nI(W_1;Z)}$. The channel coding theorem (see Theorem 2) shows that Z^n can be used to recover $\hat{w}^n_{1,B_2,B_1}$ from $\mathcal{C}^e_i(S, B_2)$ with failure probability $\Pr(\hat{w}^n_{1,B_2,B_1} \neq w^n_{1,B_2,B_1}) \leq \epsilon'$. Applying Fano's inequality gives us

$$H(w^n_{1,B_2,B_1}|S, w^n_{2,B_2}, Z^n) \leq h(2\epsilon') + 2\epsilon' nR_c < (1 + 2R_c)/R_{sc}\epsilon' \log(K).$$

A.1.3 Proof of Lemma 12: Secure block codes

The existence of N secure block codes is proved similarly to the existence of one secure block code, by using N randomly generated codedbooks. Here, we only prove that a randomly selected typical X^n is in at least one of the codes with high probability. For given ϵ, for large enough n, each of the above codewords are ϵ-typical with high probability. From AEP for P_X, a randomly selected X^n equals to a codeword in a secure block code with probability at least $2^{-n(H(X)+\epsilon)}$. There are $M.N$ i.i.d. generated codewords for all the secure block codes. So, the probability that X^n does not match any of those codewords is at most

$$\begin{aligned}
(1 - 2^{-n(H(X)+\epsilon)})^{M.N} &= \left((1 - 2^{-n(H(X)+\epsilon)})^{n(H(X)+\epsilon)}\right)^{M.N-n(H(X)+\epsilon)} \\
&\leq \left(e^{-1}\right)^{M.N-n(H(X)+\epsilon)} \\
&= e^{-n(R'+R_c-H(X)-\epsilon)} = e^{-\gamma}.
\end{aligned}$$

A.1.4 Proof of Lemma 13: Secure equipartition

We prove the lemma for $R_{se} = H(Y|XZ) - \epsilon'$. This obviously implies the existence of secure equipartition with smallest rates R_{se}. In the proof, we assume that $|\mathcal{C}| \leq 2^{n(H(Y)-5\epsilon')}$.

Since $R_{se} < H(Y|XZ) \leq H(Y|Z)$ and $\epsilon \geq \epsilon' = 2^{n(R_{se}-H(Y|XZ))} \geq 2^{nR_{se}-H(Y|X)}$, Lemma 4 shows the existence of a (Γ, ϵ)-equipartition with Γ and ϵ defined in the statement of Lemma 13 such that each part has size at most $2^{n\epsilon'}.|\mathcal{C}|/\Gamma$. This existence is

implied by proving that a randomly generated partition function ψ serves as a (Γ, ϵ)-equipartition. We continue the proof by showing that such a randomly generate equipartition also satisfies the secrecy requirement (3.20). We write the conditional entropy of $T = \psi(Y^n)$ as

$$\begin{aligned} H(T|X^n = c, Z^n) &= H(Y^n, T|X^n = c, Z^n) - H(Y^n|X^n = c, Z^n, T) \\ &= H(Y^n|X^n = c, Z^n) - H(Y^n|X^n = c, Z^n, T) \\ &\overset{(a)}{\geq} n(H(Y|X, Z) - \epsilon') - H(Y^n|X^n = c, Z^n, T) \\ &\geq \log \Gamma - n\epsilon' - H(Y^n|X^n = c, Z^n, T) \\ &\overset{(b)}{\geq} \log \Gamma - n\epsilon'(I(Y; X, Z) + 1) - h(\epsilon') \\ &> \log \Gamma(1 - \epsilon), \end{aligned} \tag{A.4}$$

where

$$\epsilon = \frac{3nI(Y; X, Z)h(\epsilon')}{\log \Gamma} = \frac{3I(Y; X, Z)h(\epsilon')}{H(Y|XZ) - \epsilon'}.$$

Inequality (a) follows from joint AEP for (Y, X, Z) and inequality (b) is shown as follows. Knowing T reveals the part $\mathcal{C}(T)$ which Y^n belongs to. Consider $\mathcal{C}(T)$ as a codebook of size at most $2^{n\epsilon'}|\mathcal{C}|/\Gamma$. From joint AEP [23, Chaoter 8], if $\log(2^{n\epsilon'}|\mathcal{C}|/\Gamma)$ is less than $nI(Y; X, Z)$, then there exists such a partition with the corresponding encoding and decoding functions such that the error probability of decoding (X^n, Z^n) to Y^n is arbitrarily close to zero. We calculate $\log(2^{n\epsilon'}|\mathcal{C}|/\Gamma)$ as

$$\begin{aligned} \log(2^{n\epsilon'}|\mathcal{C}|/\Gamma) &= \log(|\mathcal{C}|) - \log(\Gamma) + n\epsilon' \\ &\leq n(H(Y) - 5\epsilon') - nR_{se} + n\epsilon' \\ &\leq n(H(Y) - 5\epsilon') - n(H(Y|X, Z) - \epsilon') + n\epsilon' \\ &\leq nI(Y; X, Z) - 3n\epsilon'. \end{aligned} \tag{A.5}$$

As a consequence, the error probability of the above decoding is less than ϵ', and Fano's

inequality gives that

$$H(Y^n|X^n = c, Z^n, T) \leq h(\epsilon') + n\epsilon' I(Y; X, Z). \qquad \square$$

A.2 Proof of Theorem 3: SK capacity lower bound for 2DMWC

We shall show a two-round SKE protocol, Π that achieves $Lbnd_1 + Lbnd_2$ in (3.23) for a given set of variables: μ, X_A,X_B, V_A,V_B, W_{2A},W_{2B},W_{1A}, and W_{1B}. The protocol proceeds in two parallel (and independent) instances: Instance 1 is initiated by Alice in round 1 and responded by Bob in round 2, and instance 2 is initiated by Bob and responded by Alice. Here we only describe instance 1 (3.24) and show how it achieves $Lbnd_1$; similarly, one can show that instance 2 achieves $Lbnd_2$ in (3.25).

Parameter definition. Also let n_1 and n_2 such that $n_1 = \mu n_2$ be sufficiently large integers that represent the number of 2DMWC uses in the first and the second round of the protocol, respectively. This implies that the protocol cost over the 2DMWC equals $Cost_{\Pi}^{2DMWC} = n_1 + n_2 = n_2(1 + \mu)$. We rephrase the constraint condition in (3.24) as

$$n_2 I(W_1; Y_A) \geq n_1\big(I(V; Y_B|X_A) + 3\alpha\big), \tag{A.6}$$

where $\alpha > 0$ is an small constant to be determined (later) from δ, and n_1 and n_2 are sufficiently large such that $2^{-\alpha \min\{n_1,n_2\}}$ approaches zero. Let us first define a number of integer parameters that are used in our SKE construction.

$$\begin{aligned}
&R_{1f} = H(X_A) - \alpha, \\
&R_{cf^{-1}} = I(V; X_A) - \alpha, \quad && R_{scf^{-1}} = I(V; X_A) - I(V; Y_{fE}) - 2\alpha, \\
&R_{cb} = I(W_1; Y_A) - \alpha, && R_{scb} = I(W_1; Y_A|W_2) - I(W_1; Y_{bE}|W_2) - 2\alpha, \\
&R_{ef} = H(V|X_A), && R_{ef}^{+} = H(V|X_A) + 2\alpha.
\end{aligned} \tag{A.7}$$

We informally describe each of the above quantities as follows. R_{1f} is the (highest) channel input rate for the forward channel. $R_{cf^{-1}}$ and $R_{scf^{-1}}$ are the reliable and secure

transmission rates over the inverse forward DMWC $(\mathcal{V}, \mathcal{X}_A, \mathcal{Y}_{fE}, P_{X_A,Y_{fE}|V})$, respectively. R_{cb} and R_{scb} are the reliable and secure transmission rates over the backward DMWC $(\mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_{bE}, P_{Y_A,Y_{bE}|X_B})$, respectively. R_{ef}/R_{ef}^+ shows the uncertainty rate of the forward channel. Using the above quantities, we define

$$\begin{aligned} M_1 &= \lfloor 2^{n_1 R_{cf^{-1}}} \rfloor, \quad & M_2 &= \lfloor 2^{n_2 R_{cb}} \rfloor, \\ K_1 &= \lfloor 2^{n_1 R_{scf^{-1}}} \rfloor, \quad & K_2 &= \lfloor 2^{n_2 [R_{scb}]^+} \rfloor, \\ N &= \lfloor 2^{n_1 R_{ef}^+} \rfloor, & & \\ L_1 &= \lfloor 2^{n_1 R_{1f}} \rfloor, & L_2 &= \lfloor 2^{n_2 R_{cb} - n_1 R_{ef}} \rfloor. \end{aligned} \tag{A.8}$$

Letting

$$\begin{aligned} &\epsilon = \max\big(\frac{2R_{cf^{-1}}+1}{R_{scf^{-1}}} 2^{-n_1\alpha} \ , \ \frac{2R_{cb}+1}{R_{scb}} 2^{-n_2\alpha}\big) \to 0, \quad \text{and} \\ &\gamma = 2^{n_1(R_{ef}^+ + R_{cf^{-1}} - H(V))} = 2^{n_1\alpha} \to \infty, \end{aligned}$$

and using Lemmas 11 and 12, we conclude the existence of the following secure-block codes to be used in our construction.

- For the inverse forward DMWC $(\mathcal{V}, \mathcal{X}_A, \mathcal{Y}_{fE}, P_{X_A,Y_{fE}|V})$, there exist N $(n_1, M_1, K_1, \epsilon)$-secure block codes $\{Enc'_j/Dec'_j : 1 \le j \le N\}$ over this channel with the key derivation functions $\phi_{j,sk}$, such that a randomly selected ϵ-typical sequence from $\mathcal{V}^n$ is in at least one of the codebooks with probability at least $1 - e^{-\gamma}$.

- For the backward DMWC $(\mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_{bE}, P_{Y_A,Y_{bE}|X_B})$, there exists an $(n_2, M_2, K_2, \epsilon)$-secure block code Enc/Dec with the key derivation function ϕ_{sk}.

Protocol description.

Common randomness generation. Let the set $\mathcal{X}_{A,\epsilon}^{n_1} = \{\mathbf{x}_{A,1}, \ldots, \mathbf{x}_{A,L_1}\}$ be obtained by independently selecting L_1 sequences in $\mathcal{X}_A^{n_1}$. Alice sends $\mathbf{X}_A = \mathbf{x}_{A,U_A}$ for uniformly

random $U_A \in [L_1]$, and Bob and Eve receive $\mathbf{Y}_B$ and $\mathbf{Y}_{fE}$, respectively. Bob obtains $\mathbf{V}$ by inputting $\mathbf{Y}_B$ to the DMC $(\mathcal{Y}_B, \mathcal{V}, P_{V|Y_B})$, and then finds (I_B, J_B) such that $\mathbf{V} = Enc'_{J_B}(I_B)$, i.e., the I_A-th codeword in the J_A-th secure block code over the inverse forward DMWC. This can be interpreted as follows: Bob has encoded $I_B \in [M_1]$ by the encoding function $Enc'_{J_B}(.)$, he has send the codeword over the inverse DMWC, but also needs to send the encoding function description. The second round is thus used for sending the block code index $J_B \in [N]$. This round is also used to send the randomness, $U_B \in [L_2]$.

Bob calculates $Q_B = L_2 J_B + U_B \in [M_2]$ (note that $M_2 = N.L_2$), and sends back $\mathbf{X}_B = Enc(Q_B)$, where Alice and Eve receive $\mathbf{Y}_A$ and $\mathbf{Y}_{bE}$, respectively. Using the secure block code for the backward DMWC, Alice obtains $\hat{Q}_B = Dec(\mathbf{Y}_A)$ and splits this to $\hat{U}_B$ and $\hat{J}_B$ as

$$\hat{U}_{2B} = \hat{Q}_B \mod (L_2), \qquad \hat{J}_B = (\hat{Q}_B - \hat{U}_{2B}^{:2r-2})/L_2.$$

$\hat{J}_B$ reveals which secure block code is used over inverse DMWC in round 1. Alice uses this knowledge to decode $\hat{I}_B = Dec'_{\hat{J}}(\mathbf{X}_A)$. The common randomness generated by Alice and Bob are indeed $(\hat{I}_B, \hat{Q}_B)$ and (I_B, Q_B), respectively.

Key derivation. Alice and Bob finally use the key derivation functions ϕ_{sk} and $\phi'_{j,sk}$ to calculate secret keys from their common randomness. The secret key is $S_1 = \big(\phi_{sk}(Q_B), \phi'_{J_B,sk}(I_B)\big)$. Alice and Bob calculate $S_{A1} = \big(\phi_{sk}(\hat{Q}_B), \phi'_{\hat{J}_B,sk}(\hat{I}_B)\big)$ and $S_{B1} = S_1$, respectively.

The above gives a description of instance 1 of the SKE protocol that is initiated by Alice. In a symmetric way, instance 2 of the protocol (initiated by Bob) is described. We denote the overall secret key and Alice's and Bob's estimates of this key by $S = (S_1, S_2)$, $S_A = (S_{A1}, S_{A2})$ and $S_B = (S_{B1}, S_{B2})$, respectively, where S_2, S_{A2}, and S_{B2} are resulted from instance 2.

Protocol analysis.

Reliability analysis: proving (3.3a). Instance 1 of the protocol fails if any of the following failures happens.

- *Failure in finding appropriate secure block code, $\mathcal{E}_1$:* Bob fails to find (I_B, J_B) such that $V = Enc'_{J_B}(I_B)$.
- *Decoding failure of secure block code, $\mathcal{E}_2$:* Alice calculates $\hat{Q}_B \neq Q_B$ or $\hat{I}_B \neq I_B$.

Following Lemmas 11-12, the probabilities of the above failures are upper bounded by $e^{-\gamma}$ and 2ϵ, respectively. Taking instance-2 failures into account the probability of the protocol's failure, denoted by $\mathcal{E}rr$ is upper-bounded by $2e^{-\gamma} + 4\epsilon$. This shows:

$$\Pr(S_A = S_B = S) \geq 1 - \Pr(\mathcal{E}rr) \leq 1 - 2e^{-\gamma} - 4\epsilon.$$

For any arbitrarily small $\delta > 0$, we can choose n_1 and n_2 sufficiently large such that $2e^{-\gamma} + 4\epsilon < \delta$.

Randomness analysis: proving (3.3c). The entropy of the secret key S can be bounded from below as

$$H(S) \geq \Pr(\overline{\mathcal{E}rr}) H(S|\overline{\mathcal{E}rr}) \geq (1-\delta) H(S|\overline{\mathcal{E}rr}). \tag{A.9}$$

We obtain $H(S|\overline{\mathcal{E}rr})$ by first discussing about I_B, J_B, and U_B. For all $i \in [M_1], j \in [N]$, we have

$$\Pr\left((I_B, J_B) = (i,j)\right) \leq \Pr(\mathbf{V} = Enc'_j(i)) \leq 2^{-n_1(H(V)-\epsilon)}, \tag{A.10}$$

where the last inequality follows from AEP and that the codeword $Enc'_j(i)$ is ϵ-typical w.r.t. V. On the other hand, $U_B \in [L_2]$ is uniform and independent of (I_B, J_B). We

conclude that, for all $i \in [M_1]$ and all $q \in [M_2]$, letting $u = q \mod (L_2)$ and $j = (q-u)/L_2$, we have (see (A.7), (A.8), and (A.36))

$$\begin{aligned}\Pr\left((I_B, Q_B) = (i,q)\right) &= \Pr\left((I_B, J_B, U_B) = (i,j,u)\right) = \Pr\left((I_B, J_B) = (i,j)\right).\Pr\left(U_B = u\right) \\ &\leq \frac{1}{L_2} 2^{-n_1(H(V)-\epsilon)} = 2^{-n_1 I(V;X_A) - n_2 I(W_1;Y_A) + n_2\alpha + n_1\epsilon} \\ &= \frac{2^{n_1(\epsilon-\alpha)}}{M_1 M_2}. \end{aligned} \tag{A.11}$$

The continuity of the entropy function gives

$$H(I_B, Q_B) \geq \log(M_1 M_2) - n_1(\epsilon - \alpha). \tag{A.12}$$

Using the property of functions $\phi_{sk}(.)$ and $\phi_{j,sk}(.)$, the above gives

$$\begin{aligned} H(S_1) &\geq \log(K_1 K_2) - n_1(\epsilon-\alpha) = n_1 R_{scf^{-1}} + n_2 [R_{scb}]_+ - n_1(\epsilon-\alpha) \\ &= n_2(\mu R_{scf^{-1}} + [R_{scb}]_+ - (\epsilon-\alpha)) \\ \Rightarrow \quad & \frac{H(S_1)}{Cost_{\Pi}^{2DMWC}} = \frac{\mu R_{scf^{-1}} + [R_{scb}]_+ - (\epsilon-\alpha)}{1+\mu} \end{aligned}$$

For the second instance of the protocol, one can show similarly that

$$\frac{H(S_2)}{Cost_{\Pi}^{2DMWC}} = \frac{\mu R_{scb^{-1}} + [R_{scf}]_+ + \epsilon - \alpha}{1+\mu}$$

Choosing ϵ and α such that $(\epsilon-\alpha)/(1+\mu) \leq \delta/2$ satisfies the randomness property.

Secrecy analysis: proving (3.3b). For instance 1, we show that $I(S_1; \mathbf{Y}_{fE}, \mathbf{Y}_{bE})$ remains negligible in rate. Letting $S_1 = (S_{11}, S_{12}) = \left(\phi_{sk}(Q_B), \phi'_{J_B,sk}(I_B)\right)$, we have

$$\begin{aligned} I(S_{11}, S_{12}; \mathbf{Y}_{fE}, \mathbf{Y}_{bE}) &= I(S_{11}; \mathbf{Y}_{fE}, \mathbf{Y}_{bE}) + I(S_{12}; \mathbf{Y}_{fE}, \mathbf{Y}_{bE} | S_{11}) \\ &\leq I(S_{11}; \mathbf{Y}_{fE}, \mathbf{Y}_{bE}, J_B) + I(S_{12}, \mathbf{X}_B; \mathbf{Y}_{fE}, \mathbf{Y}_{bE} | S_{11}) - I(\mathbf{X}_B; \mathbf{Y}_{fE}, \mathbf{Y}_{bE} | S_{11}, S_{12}) \\ &\overset{(a)}{=} I(S_{11}; \mathbf{Y}_{fE}, J_B) + I(S_{12}, \mathbf{X}_B; \mathbf{Y}_{bE} | S_{11}) - I(\mathbf{X}_B; \mathbf{Y}_{fE}, \mathbf{Y}_{bE} | S_{11}, S_{12}) \\ &\overset{(b)}{\leq} I(S_{11}; \mathbf{Y}_{fE}, J_B) + I(S_{12}, \mathbf{X}_B; \mathbf{Y}_{bE}) - I(\mathbf{X}_B; \mathbf{Y}_{bE} | S_{11}, S_{12}) \\ &\overset{(c)}{=} I(S_{11}; \mathbf{Y}_{fE}, J_B) + I(S_{12}, \mathbf{X}_B; \mathbf{Y}_{bE}) - I(\mathbf{X}_B; \mathbf{Y}_{bE} | S_{12}) \\ &= I(S_{11}; \mathbf{Y}_{fE}, J_B) + I(S_{12}; \mathbf{Y}_{bE}) \\ &\leq \epsilon \log(K_1.K_2). \end{aligned}$$

Equality (a) follows from the Markov chains $\mathbf{Y}_{bE} \leftrightarrow J_B \leftrightarrow (\mathbf{Y}_{fE}, S_{11})$ and $\mathbf{Y}_{fE} \leftrightarrow (S_{12}, \mathbf{X}_B) \leftrightarrow \mathbf{Y}_{bE}$. Inequality (b) follows from the Markov chains $S_{11} \leftrightarrow (S_{12}, \mathbf{X}_B) \leftrightarrow \mathbf{Y}_{bE}$ and the fact that removing $\mathbf{Y}_{fE}$ from the third mutual-information term decrease its value. Equality (c) holds since S_{11} is independent of $(S_{12}, \mathbf{X}_B, \mathbf{Y}_{bE})$.

The same result holds for the secret key S_2 from instance 2 of the protocol that is run independently of instance 1. This shows that for arbitrarily small $\delta > 0$, by choosing ϵ sufficiently small we can provide the secrecy as required by (3.3b).

A.3 Proof of Proposition 1: SK capacity for pd-2DMWC

In the pd-2DMWC setup, the DMWCs are degraded in either obverse or reverse directions. The SK capacity of the pd-2DMWC is upper bounded as (see Theorem 4)

$$C_{wsk}^{pd-2DMWC} \leq \max_{X_A, X_B} \{I(X_A; Y_B|Y_{fE}) + I(X_B; Y_A|Y_{bE})\}$$

We thus need to show the same lower bound on the capacity. We assume that both $I(X_A; Y_B)$ and $I(X_B; Y_A)$ are positive; otherwise, the proof can be easily modified to work. and We start by simplifying the expression (3.24) for $\mu = 0$ such that we can write

$$Lbnd_1 = [R_{scb}]_+ = [I(W_{1B}; Y_A|W_{2B}) - I(W_{1B}; Y_{bE}|W_{2B})]_+,$$

and the condition in (3.24) is satisfied when $I(W_{1B}; Y_A) > 0$. Letting $W_{2B} = 0$ and $W_{1B} = X_B$, we can simplify the above further as

$$Lbnd_1 = [I(X_B; Y_A) - I(XB; Y_{bE})]_+ = I(X_B; Y_A|Y_{bE}).$$

The above equality holds since if the backward channel is reversely degraded, both sides equal zero and if it is obversely degraded, the Markov chain $X_B \leftrightarrow Y_A \leftrightarrow Y_{bE}$ holds. Similarly when $\mu = 0$, by choosing $W_{2A} = 0$ and $W_{1A} = X_A$, we have

$$Lbnd_2 = I(X_A; Y_B|Y_{fE}).$$

Using the above for the lower bound expression (3.23) results in the following which completes the proof.

$$C_{wsk}^{pd-2DMWC} \geq \max_{X_A, X_B} \{I(X_A; Y_B|Y_{fE}) + I(X_B; Y_A|Y_{bE})\}.$$

A.4 Proof of Proposition 2: SK capacity bound for sd-2DMWC

From the Markov chain relations (3.21) and the independence of the two DMCs in the sd-2DMWC setup (see Definitions 35), $V_B \leftrightarrow Y_B \leftrightarrow X_A \leftrightarrow Y_{fE}$ forms a Markov chain, and so we write (3.22a) and (3.22c) as

$$R_{scf^{-1}} = I(V_B; X_A, Y_{fE}) - I(V_B; Y_{fE}) = I(V_B; X_A|Y_{fE}), \tag{A.13}$$

$$R_{scb^{-1}} = I(V_A; X_B, Y_{bE}) - I(V_A; Y_{bE}) = I(V_A; X_B|Y_{bE}). \tag{A.14}$$

From Definition 35 and the Markov chain relations in (3.21), there exist $\tilde{Y}_A$ and $\tilde{Y}_{bE}$ such that one of the Markov chains

$$W_{2A} \leftrightarrow W_{1A} \leftrightarrow X_B \leftrightarrow \tilde{Y}_A \leftrightarrow \tilde{Y}_{bE}, \text{ or} \tag{A.15a}$$

$$W_{2A} \leftrightarrow W_{1A} \leftrightarrow X_B \leftrightarrow \tilde{Y}_{bE} \leftrightarrow \tilde{Y}_A \tag{A.15b}$$

hold, and

$$I(X_B; Y_A) = I(X_B; \tilde{Y}_A), \qquad I(X_B; Y_{bE}) = I(X_B; \tilde{Y}_{bE})$$

$$I(W_{1A}; Y_A|W_{2A}) = I(W_{1A}; \tilde{Y}_A|W_{2A}), \quad I(W_{1A}; Y_{bE}|W_{2A}) = I(W_{1A}; \tilde{Y}_{bE}|W_{2A}).$$

Hence, we write (3.22d) as

$$\begin{aligned} R_{scb} &= I(W_{1A}; \tilde{Y}_A|W_{2A}) - I(W_{1A}; \tilde{Y}_{bE}|W_{2A}) \leq I(W_{1A}; \tilde{Y}_A|\tilde{Y}_{bE}, W_{2A}) \\ &\overset{(a)}{\geq} I(X_B; \tilde{Y}_A|\tilde{Y}_{bE}) = [I(X_B; \tilde{Y}_A) - I(X_B; \tilde{Y}_{bE})]_+ = [I(X_B; Y_A) - I(X_B; Y_{bE})]_+. \end{aligned} \tag{A.16}$$

Inequality (a) follows from (A.15). More precisely, if (A.15a) holds the inequality is easily satisfied, and if (A.15b) holds both sides equal zero. It is easy to see that equality

in (A.16) holds by choosing $W_{2A} = 1$ and W_{1A} to be X_B or 1, in the case of (A.15a) or (A.15b), respectively. In analogy to the above, we have

$$R_{scf} \geq [I(X_A; Y_B) - I(X_A; Y_{fE})]_+, \tag{A.17}$$

where the equality holds for some W_{2A} and W_{1A}. By replacing $R_{scf^{-1}}, R_{scb}, R_{scb^{-1}}$, and R_{scf} in (3.24) and (3.25) with the above-obtained quantities, (3.23) is simplified to (3.27).

A.5 Proof of Theorem 5: SK capacity for sd-2DMWC

We let Alice be the party who sends i.i.d. variables. The other case follows by symmetry. We use Lemma 24 to reduce a multi-round SKE protocol to a two-round one, and then give the highest rate that a two-round protocol can achieve.

Lemma 24. *When Alice can only send i.i.d. variables, the secret-key capacity is achieved by a two-round SKE protocol whose initiator is Alice.*

Proof. Let Π be a t-round SKE protocol that achieves the secret-key capacity under the above condition. In any (odd) round r, Alice's sent sequence $\mathbf{X}_A^{:r}$ is independent of her view in round $r-1$, and hence she could compute it in the first communication round. Besides, sending this sequence in the first round does not affect the distribution of Bob's and Eve's received sequences ($Y_B^{:r}$ and $Y_{fE}^{:r}$) since the channels are memoryless. Obviously Bob can compute $\mathbf{X}_B^{:r}$ for any even r as before. Hence, we can convert the protocol Π into Π' in which Alice sends the whole $||_{(odd)r\leq t}[\mathbf{X}_A^{:r}]$ in the first round and (following a similar argument) Bob sends the whole $||_{(even)r\leq t}[\mathbf{X}_B^{:r}]$ in the second round such that all communicated sequences and the final key in Π and Π' have the same joint probability distribution. Π' is is a two-round protocol with Alice as the initiator and with the same key distribution as in Π; hence, it achieves the SK capacity. □

Now, consider a two-round SKE protocol as depicted in Figure A.1 in which Alice sends a sequence of i.i.d. variables $\mathbf{X}_A$ of length n_1 in the first round. Since the channels are memoryless and independent, Bob and Eve receive sequences of i.i.d. variables $\mathbf{Y}_B$ and $\mathbf{Y}_{fE}$ and $\mathbf{Y}_B \leftrightarrow \mathbf{X}_A \leftrightarrow \mathbf{Y}_{fE}$ is a Markov chain. This setup can be seen as the DMMS $(\mathcal{Y}_B, \mathcal{X}_A, \mathcal{Y}_{fE}, P_{Y_B,X_A,Y_{fE}})$ between Bob, Alice, and Eve, respectively and the DMWC $(\mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_{bE}, P_{Y_A,Y_{fE}|X_B})$ from Bob to Alice and Bob. When the DMMS and DMWC satisfy the degradedness condition $Y_B \leftrightarrow X_A \leftrightarrow Y_{fE}$ and $X_B \leftrightarrow Y_A \leftrightarrow Y_{bE}$, [48] proves a tight expression for the secret-key capacity. The proof however can not be applied to our problem due to the "stochastic" degradedness of the (backward) DMWC. We give the following argument to upper bound the highest achievable rate R_{sk} for an arbitrarily small $\delta > 0$ as in (3.3).

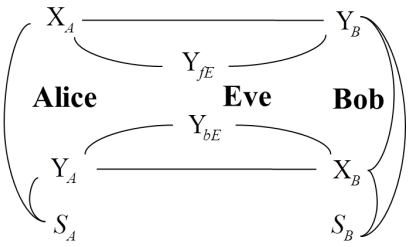


Figure A.1: Two-round SKE: Alice initiates the protocol and Bob calculates the key.

Assume that Bob sends $\mathbf{X}_B$ of length n_2 in the second round, where Alice and Eve receive $\mathbf{Y}_A$ and $\mathbf{Y}_{fE}$, respectively. The views of the parties at the end of the second round are $View_A = (\mathbf{X}_A, \mathbf{Y}_A)$, $View_B = (\mathbf{X}_B, \mathbf{Y}_B)$, and $View_E = (\mathbf{Y}_{fE}, \mathbf{Y}_{bE})$. Applying Fano's inequality to (3.3a) and using (3.3b) give the following results about secret key S.

$$H(S|View_A) \leq H(S|\hat{S}) < h(\delta) + \delta H(S), \tag{A.18}$$

$$I(S; View_E) = H(S) - H(S|View_E) \leq \delta H(S). \tag{A.19}$$

We upper bound the entropy of S as

$$\begin{aligned} H(S) &= I(S;View_A) + H(S|View_A) \\ &\overset{(a)}{\leq} I(S;View_A) - I(S;View_E) + h(\delta) + 2\delta H(S) \\ &\leq I(S;View_A|View_E) + h(\delta) + 2\delta H(S), \end{aligned} \tag{A.20}$$

which implies

$$\begin{aligned} (1-2\delta)H(S) - h(\delta) &\leq I(S;View_A) - I(S;View_E) \\ &= I(S;\mathbf{Y}_A) + I(S;\mathbf{X}_A|\mathbf{Y}_A) - I(S;\mathbf{Y}_{fE},\mathbf{Y}_{bE}) \\ &= I(S;\mathbf{Y}_A) + I(S;\mathbf{X}_A,\mathbf{Y}_{fE}|\mathbf{Y}_A) - I(S;\mathbf{Y}_{fE},\mathbf{Y}_{bE}) \\ &= I(S;\mathbf{Y}_A) + I(S;\mathbf{Y}_{fE}|\mathbf{Y}_A) + I(S;\mathbf{X}_A|\mathbf{Y}_{fE},\mathbf{Y}_A) - I(S;\mathbf{Y}_{fE},\mathbf{Y}_{bE}) \\ &= [I(S;\mathbf{Y}_{fE},\mathbf{Y}_A) - I(S;\mathbf{Y}_{fE},\mathbf{Y}_{bE})] + [I(S;\mathbf{X}_A|\mathbf{Y}_{fE},\mathbf{Y}_A)]. \end{aligned} \tag{A.21}$$

Inequality (a) follows from (A.18) and (A.19). We separately discuss the two terms in (A.68). Note that $(S,\mathbf{Y}_{fE}) \leftrightarrow \mathbf{X}_B \leftrightarrow (\mathbf{Y}_A,\mathbf{Y}_{bE})$ is a Markov chain. If the backward DMWC is stochastically degraded in favor of Y_{bE}, the first term is at most zero; otherwise, letting $X_B \leftrightarrow \tilde{Y}_A \leftrightarrow \tilde{Y}_{bE}$ (see Definition 35), we have

$$\begin{aligned} I(S;\mathbf{Y}_{fE},\mathbf{Y}_A) - I(S;\mathbf{Y}_{fE},\mathbf{Y}_{bE}) &= I(S;\mathbf{Y}_{fE},\tilde{\mathbf{Y}}_A) - I(S;\mathbf{Y}_{fE},\tilde{\mathbf{Y}}_{bE}) \\ &= I(S;\mathbf{Y}_{fE},\tilde{\mathbf{Y}}_A,\tilde{\mathbf{Y}}_{bE}) - I(S;\mathbf{Y}_{fE},\tilde{\mathbf{Y}}_{bE})I(S;\tilde{\mathbf{Y}}_A|\mathbf{Y}_{fE},\tilde{\mathbf{Y}}_{bE}) \\ &\leq I(S,\mathbf{Y}_{fE};\tilde{\mathbf{Y}}_A|\tilde{\mathbf{Y}}_{bE}) = I(S,\mathbf{Y}_{fE};\tilde{\mathbf{Y}}_A) - I(S,\mathbf{Y}_{fE};\tilde{\mathbf{Y}}_{bE}) \\ &= I(S,\mathbf{Y}_{fE};\mathbf{Y}_A) - I(S,\mathbf{Y}_{fE};\mathbf{Y}_{bE}) \overset{(a)}{\leq} n_2[I(W_{1B};Y_A) - I(W_{1B};Y_{bE})] \\ &\overset{(b)}{\leq} n_2[I(X_B;Y_A) - I(X_B;Y_{bE})]_+. \end{aligned} \tag{A.22}$$

Inequality (a) follows from the results of message transmission over single DMWCs (e.g., [26, Section V]), where the conditional distribution $P_{Y_A,Y_{bE}|X_B}$ corresponds to the backward DMWC and W_{1B} is an RV that satisfies the Markov chain $W_{1B} \leftrightarrow X_B \leftrightarrow (Y_A,Y_{bE})$. Inequality (b) is due to the degradedness of the backward DMWC. Letting J

be an independent random variable uniformly distributed over $[n_1]$, we write the second term in (A.68) as

$$\begin{aligned} I(S;\mathbf{X}_A|\mathbf{Y}_{fE},\mathbf{Y}_A) &\leq I(S,\mathbf{Y}_A;\mathbf{X}_A|\mathbf{Y}_{fE}) \\ &\overset{(a)}{=} I(S,\mathbf{Y}_A;\mathbf{X}_A) - I(S,\mathbf{Y}_A;\mathbf{Y}_{fE}) \\ &\overset{(b)}{=} \sum_{i=1}^{n_1} I(S,\mathbf{Y}_A;X_{A,i}|Y_{fE,i+1}^{n_1},X_A^{i-1}) - I(S,\mathbf{Y}_A;Y_{fE,i}|Y_{fE,i+1}^{n_1},Y_{fE}^{i-1}) \\ &\overset{(c)}{=} \sum_{i=1}^{n_1} I(S,\mathbf{Y}_A;X_{A,i}|Y_{fE,i},Y_{fE,i+1}^{n_1},X_A^{i-1}) \\ &= n_1 I(S,\mathbf{Y}_A;X_{A,J}|Y_{fE,J},Y_{fE,J+1}^{n_1},X_A^{J-1},J) \\ &\leq n_1 I(S,\mathbf{Y}_A,Y_{fE,J+1}^{n_1},X_A^{J-1},J;X_{A,J}|Y_{fE,J}). \end{aligned} \tag{A.23}$$

Equality (a) is due to the Makov chain $\mathbf{Y}_{fE} \leftrightarrow \mathbf{X}_A \leftrightarrow (S,\mathbf{Y}_A)$, equality (b) follows from the chain rule for difference between mutual information (see e.g., [26, Section V]), and equality (c) is due to the Markov chain $Y_{fE,i} \leftrightarrow X_{A,i} \leftrightarrow (S,\mathbf{Y}_A)$.

Now, letting $V_B = (S,\mathbf{Y}_A,Y_{fE,J+1}^{n_1},X_A^{J-1},J)$, $X_A = X_{A,J}$, $Y_B = Y_{B,J}$ and $Y_{fE} = Y_{fE,J}$, the conditional distribution $P_{Y_B.Y_{fE}|X_A}$ corresponds to the forward DMWC, the Markov chain $Y_{fE} \leftrightarrow X_A \leftrightarrow Y_B \leftrightarrow V_B$ is satisfied, and we have

$$I(S;\mathbf{X}_A|\mathbf{Y}_{fE},\mathbf{Y}_A) \leq n_1 I(V_B;X_A|Y_{fE}). \tag{A.24}$$

Using the quantities of (A.22) and (A.24) in the calculation of (A.68), $H(S)$ is upper bounded as

$$\begin{aligned} H(S) &\leq \frac{n_1 I(V_B;X_A|Y_{fE}) + n_2[I(X_B;Y_A) - I(X_B;Y_{bE})]_+ + h(\delta)}{(1-2\delta)} \\ &= n_1 I(V_B;X_A|Y_{fE}) + n_2[I(X_B;Y_A) - I(X_B;Y_{bE})]_+, \end{aligned} \tag{A.25}$$

where the last equality holds since δ is arbitrarily small. This together with (3.3c) proves

the argument and the condition in (3.28) is proven as follows.

$$
\begin{aligned}
n_2 I(X_B;Y_A) &\geq I(\mathbf{X}_B;\mathbf{Y}_A) \overset{(a)}{\geq} I(\mathbf{Y}_B;\mathbf{Y}_A) \\
&= I(\mathbf{Y}_A,S;\mathbf{Y}_B) - I(S;\mathbf{Y}_B|\mathbf{Y}_A) \geq I(\mathbf{Y}_A,S;\mathbf{Y}_B) - H(S|\mathbf{Y}_A) \\
&= I(\mathbf{Y}_A,S;\mathbf{Y}_B) - H(S|\mathbf{Y}_A,\mathbf{X}_A) - I(S;\mathbf{X}_A|\mathbf{Y}_A) \\
&\overset{(b)}{\geq} I(\mathbf{Y}_A,S;\mathbf{Y}_B) - h(\delta) - \delta H(S) - I(S;\mathbf{X}_A|\mathbf{Y}_A) \\
&\overset{(c)}{\geq} I(\mathbf{Y}_A,S;\mathbf{Y}_B) - I(\mathbf{Y}_A,S;\mathbf{X}_A) \\
&\overset{(d)}{=} \sum_{i=1}^{n_1} I(\mathbf{Y}_A,S,X_A^{i-1},Y_{B,i+1}^{n_1};Y_{B,i}) - I(\mathbf{Y}_A,S,X_A^{i-1},Y_{B,i+1}^{n_1};X_{A,i}) \\
&\overset{(e)}{=} \sum_{i=1}^{n_1} I(\mathbf{Y}_A,S,X_A^{i-1},Y_{B,i+1}^{n_1};Y_{B,i}|X_{A,i}) \\
&\overset{(f)}{\geq} \sum_{i=1}^{n_1} I(\mathbf{Y}_A,S,X_A^{i-1},Y_{fE,i+1}^{n_1};Y_{B,i}|X_{A,i}) \\
&= n_1 I(\mathbf{Y}_A,S,X_A^{J-1},Y_{fE,J+1}^{n_1};Y_{B,J}|X_{A,J},J) = n_1 I(V_B;Y_B|X_A) - n_1 I(J;Y_B|X_A) \\
&\overset{(g)}{=} n_1 I(V_B;Y_B|X_A). \qquad \text{(A.26)}
\end{aligned}
$$

Inequality (a) is due to the Markov chain $\mathbf{Y}_B \leftrightarrow \mathbf{X}_B \leftrightarrow \mathbf{Y}_A$; inequality (b) follows from (A.18); inequality (c) holds since δ is arbitrarily small and so $h(\delta) + \delta H(S)$ is negligible compared to the other quantities; equality (d) follows from the chain rule for difference between mutual information; equality (e) is due to the Markov chain $X_{A,i} \leftrightarrow Y_{B,i} \leftrightarrow (\mathbf{Y}_A, S, X_A^{i-1}, Y_{B,i+1}^{n_1})$; inequality (f) is due to the Markov chain $Y_{fE,i+1}^{n_1} \leftrightarrow Y_{B,i+1}^{n_1} \leftrightarrow Y_{B,i}$, and equality (g) holds since $Y_{B,J}$ is (i.i.d.) independent of J.

One can prove (3.29) by symmetry. This implies that, under the conditions of this theorem, equality in (3.27) holds.

A.6 Proof of Lemma 15: SK capacity bounds for 2BSWC

We show the lower bound by following that of (3.27) for sd-2DMWC. Considering (3.28). Let X_A and X_B have uniform distributions, and $V_B = Y_B$. We have

$$\begin{aligned} I(V_f; X_A|Y_{fE}) &= I(Y_B; X_A|Y_{fE}) = H(Y_B|Y_{fE}) - H(Y_B|X_A, Y_{fE}) \\ &\overset{(a)}{=} H(Y_B|Y_{fE}) - H(Y_B|X_A) = h(p_m \star p_e) - h(p_m), \\ I(X_B; Y_A) - I(X_B; Y_{bE}) &= H(X_B|Y_{bE}) - H(X_B|Y_A) = h(p_e) - h(p_m), \\ I(V_f; Y_B|X_A) &= H(Y_B|X_A) = h(p_m), \\ I(X_B; Y_A) &= H(X_B) - H(X_B|Y_A) = 1 - h(p_m). \end{aligned}$$

Equality (a) is due to the Markov chain $Y_B \leftrightarrow X_A \leftrightarrow Y_{fE}$. We write (3.28) as

$$Lnd_1' \geq \max_{\mu \geq 0} \{ \quad \tfrac{\mu[h(p_m \star p_e) - h(p_m)] + [h(p_e) - h(p_m)]_+}{1+\mu} \quad s.t. \quad \mu < \tfrac{1-h(p_m)}{h(p_m)} \}.$$

Since $[h(p_m \star p_e) - h(p_m)] \geq [h(p_e) - h(p_m)]_+$ always holds, the maximum above is achieved by the largest μ, i.e.,

$$\begin{aligned} Lnd_1' &\geq \frac{\frac{1-h(p_m)}{h(p_m)}[h(p_m \star p_e) - h(p_m)] + [h(p_e) - h(p_m)]_+}{1 + \frac{1-h(p_m)}{h(p_m)}} \\ &= (1 - h(p_m))[h(p_m \star p_e) - h(p_m)] + h(p_m)[h(p_e) - h(p_m)]_+. \end{aligned} \tag{A.27}$$

Due to the symmetry of noise parameters, the same holds for $Lbnd_2'$ and this completes the lower bound proof.

To prove the upper bound, we start by (3.26) and simplify it for the case of 2BSWC. For an arbitrary distribution X_A, we have

$$I(X_A; Y_B|Y_{fE}) = H(Y_B|Y_{fE}) - H(Y_B|X_A) = H(Y_B|Y_{fE}) - h(p_m),$$

where the first equality is due to the Markov chain $Y_B \leftrightarrow X_A \leftrightarrow Y_{fE}$. Using the joint probability distribution $P_{X_A, Y_B, Y_{fE}}$, one can show that the above quantity is maximized by letting X_A be uniformly distributed. Thus, to write the above as

$$I(X_A; Y_B|Y_{fE}) \leq h(p_m \star p_e) - h(p_m).$$

Due to symmetry again, we can show $I(X_B; Y_A|Y_{bE}) \leq h(p_m \star p_e) - h(p_m)$ when equality comes for uniform X_B. This completes the proof.

A.7 Proof of Theorem 6: SK capacity lower bound for 2DMWC^{-r}

We shall show a SKE protocol that achieves the rate $Lbnd_A^{-r} + Lbnd_B^{-r}$ for a given set of variables $(\mu, X_A, X_B, V_A, V_B, W_{2A}, W_{2B}, W_{1A}, W_{1B})$ that follow the conditions of the theorem. For the sake of simplicity, we only consider the case where the auxiliary variables are set to $V_A = Y_A$, $V_B = Y_B$, $W_{1A} = X_A$, $W_{1B} = X_B$, and $W_{2A} = W_{2B} = 0$. The proof for general auxiliary variables can be obtained via a straight-forward modification of the following argument (cf. the lower bound proof in Appendix A.2 for the 2DMWC setup).

Overview of the SKE protocol. The main SKE protocol has $2t + 1$ rounds and does not need any initial randomness. The protocol starts with an initialization round (round 0) that provides Alice and Bob with some amount of independent randomness. The initialization round is followed by t iterations of a two-round protocol, called the *basic protocol*. Each iteration of the basic protocol takes some independent randomness from Alice and Bob and returns to them a part of the secret key as well as new pieces of independent randomness. The independent randomness that is produced in iteration $1 \leq r \leq t - 1$ (resp. round 0) will be used in iteration $r + 1$ (resp. iteration 1). The secret key parts are finally concatenated to give the final secret key. In a deeper look, the basic protocol proceeds as two parallel instances of a key agreement sub-protocol, one initiated by Alice and one initiated by Bob. Each instance of the sub-protocol uses a part of the randomness provided by Alice and Bob, and partially contributes to the secret key.

Parameter definition. We rephrase the conditions (3.47) and (3.48) as

$$n_2 H(Y_A|X_B, Y_{bE}) \geq n_1(H(X_A) + \alpha), \qquad n_2 I(X_A; Y_B) \geq n_1(H(Y_A|X_B) + \alpha), \quad \text{(A.28)}$$

$$n_2 H(Y_B|X_A, Y_{fE}) \geq n_1(H(X_B) + \alpha), \qquad n_2 I(X_B; Y_A) \geq n_1(H(Y_B|X_A) + \alpha), \quad \text{(A.29)}$$

where $\alpha > 0$ is a sufficiently small real constant, to be determined from δ in the sequel, and n_1 and n_2 are sufficiently large positive integers such that $n_1 = \mu n_2$, and $1/\alpha = o(\min\{n_1, n_2\})$; in other words, $2^{-\alpha \min\{n_1, n_2\}}$ approaches zero.

In the following, we define a number of integer and set parameters and claim the existence of secure block codes and secure equipartitions using these parameters. Next, we describe the construction of the main protocol based on the given primitives. Define

$$\begin{aligned}
&R_{1f} = H(X_A) - \alpha, \quad R_{cf} = I(X_A; Y_B) - \alpha, \quad R_{scf} = I(X_A; Y_B) - I(X_A; Y_{fE}) - 2\alpha, \\
&R_{ef} = H(Y_B|X_A), \quad R_{ef}^{+} = H(Y_B|X_A) + 2\alpha, \quad R_{sef} = H(Y_B|X_A, Y_{fE}) - \alpha, \\
&R_{scf^{-1}} = I(Y_B; X_A) - I(Y_B; Y_{fE}) - 2\alpha.
\end{aligned} \quad \text{(A.30)}$$

We informally describe each of the above quantities as follows. For the forward DMWC, R_{1f} is the (highest) channel input rate, R_{cf} is the rate of reliable transmission, R_{scf} is the rate of secure transmission, R_{ef} is the equipartition rate (or the uncertainty rate of the channel), and R_{sef} is the secure equipartition rate. Note that R_{cf} can also be viewed as the rate of reliable transmission for the inverse forward DMWC (see Definition 7). Finally, $R_{scf^{-1}}$ is the secure transmission rate of the inverse forward DMWC. One can define similar quantities for the backward DMWC.

$$\begin{aligned}
&R_{1b} = H(X_B) - \alpha, \quad R_{cb} = I(X_B; Y_A) - \alpha, \quad R_{scb} = I(X_B; Y_A) - I(X_B; Y_{bE}) - 2\alpha, \\
&R_{eb} = H(Y_A|X_B), \quad R_{eb}^{+} = H(Y_A|X_B) + 2\alpha, \quad R_{seb} = H(Y_A|X_B, Y_{bE}) - \alpha, \\
&R_{scb^{-1}} = I(Y_A; X_B) - I(Y_A; Y_{bE}) - 2\alpha.
\end{aligned} \quad \text{(A.31)}$$

Each iteration of the two-round basic protocol uses the 2DMWC channel n_1 times in the first round and n_2 times in the second round; i.e. in total $n_1 + n_2$. In the second round,

Alice (resp. Bob) sends two sequences of lengths n_{21A} and n_{22A} (resp. n_{21B} and n_{22B}), where $n_{21A} + n_{22A} \, (= n_{21B} + n_{22B}) = n_2$ and,

$$n_{21A} = \frac{1}{R_{cf}} \min\{n_2 R_{cf}, n_2 R_{seb} + n_1 R_{eb} - n_1 R_{1f}\}, \tag{A.32}$$

$$n_{21B} = \frac{1}{R_{cb}} \min\{n_2 R_{cb}, n_2 R_{sef} + n_1 R_{ef} - n_1 R_{1b}\}. \tag{A.33}$$

Using the above quantities, we define,

$$\begin{aligned}
&M_{1A} = \lfloor 2^{n_1 R_{cb}} \rfloor, && M_{21A} = \lfloor 2^{n_{21A} R_{cf}} \rfloor, && \\
&K_{1A} = \lfloor 2^{n_1 R_{scb^{-1}}} \rfloor, && K_{21A} = \lfloor 2^{n_{21A} R_{scf}} \rfloor, && \\
&N_A = \lfloor 2^{n_1 R^{+}_{eb}} \rfloor, && && \\
&L_{1A} = \lfloor 2^{n_1 R_{1f}} \rfloor, && L_{2A} = \lfloor 2^{n_{21A} R_{cf} - n_1 R_{eb}} \rfloor, && L_A = L_{1A}.L_{2A}, \\
&\Gamma_{21A} = \min\{L_A, \lfloor 2^{n_{21B} R_{seb}} \rfloor\}, && \Gamma_{22A} = \lfloor 2^{n_{22B} R_{seb}} \rfloor, && \Gamma_A = \Gamma_{21A}.\Gamma_{22A}.
\end{aligned} \tag{A.34}$$

$$\begin{aligned}
&M_{1B} = \lfloor 2^{n_1 R_{cf}} \rfloor, && M_{21B} = \lfloor 2^{n_{21B} R_{cb}} \rfloor, && \\
&K_{1B} = \lfloor 2^{n_1 R_{scf^{-1}}} \rfloor, && K_{21B} = \lfloor 2^{n_{21B} R_{scb}} \rfloor, && \\
&N_B = \lfloor 2^{n_1 R^{+}_{ef}} \rfloor, && && \\
&L_{1B} = \lfloor 2^{n_1 R_{1b}} \rfloor, && L_{2B} = \lfloor 2^{n_{21B} R_{cb} - n_1 R_{ef}} \rfloor, && L_B = L_{1B}.L_{2B}, \\
&\Gamma_{21B} = \min\{L_B, \lfloor 2^{n_{21A} R_{sef}} \rfloor\}, && \Gamma_{22B} = \lfloor 2^{n_{22A} R_{sef}} \rfloor, && \Gamma_B = \Gamma_{21B}.\Gamma_{22B}.
\end{aligned} \tag{A.35}$$

Using (A.30)-(A.34), one can observe that $L_A = \Gamma_A$ and $L_B = \Gamma_B$ in the above. Let the set $\mathcal{X}^{n_1}_{A,\epsilon} = \{\mathbf{x}_{A,1}, \ldots, \mathbf{x}_{A,L_{1A}}\}$ be obtained by independently selecting L_{1A} sequences in $\mathcal{X}^{n_1}_A$. Similarly define $\mathcal{X}^{n_1}_{B,\epsilon} = \{\mathbf{x}_{B,1}, \ldots, \mathbf{x}_{B,L_{1B}}\} \subseteq \mathcal{X}^{n_1}_B$. Let Alice and Bob have two fixed public integers $u_a \in [\Gamma_{21A}]$ and $u_b \in [\Gamma_{21B}]$ as well as two fixed public sequences $\mathbf{a} \in \mathcal{X}^{n_{22A}}_A$ and $\mathbf{b} \in \mathcal{X}^{n_{22B}}_B$, respectively. Let $\mathfrak{u}_{A,split} : [\Gamma_{21A}] \times [\Gamma_{22A}] \to [L_{1A}] \times [L_{2A}]$ and $\mathfrak{u}_{B,split} : [\Gamma_{21B}] \times [\Gamma_{22B}] \to [L_{1B}] \times [L_{2B}]$ be arbitrary bijective mappings. For given P_{X_A} and P_{X_B}, define the inverse DMWCs $(\mathcal{Y}_B, \mathcal{X}_A, \mathcal{Y}_{fE}, P_{X_A, Y_{fE}|Y_B})$ and $(\mathcal{Y}_A, \mathcal{X}_B, \mathcal{Y}_{bE}, P_{X_B, Y_{bE}|Y_A})$ according to Definition 7.

Building blocks. Letting

$$\epsilon = 2^{-\min(n_1, n_{21A}, n_{21B})\alpha} \to 0 \qquad \text{and} \qquad \gamma = 2^{n_1(\alpha-\epsilon)} \to \infty,$$

and using Lemmas 11, 12, and 13 we arrive at the existence of the following primitives to be used in the main protocol.

Secure block codes for inverse channels (see Lemma 12).

- For the inverse forward DMWC $(\mathcal{Y}_B, \mathcal{X}_A, \mathcal{Y}_{fE}, P_{X_A, Y_{fE}|Y_B})$, there exist N_B $(n_1, M_{1B}, K_{1B}, \epsilon)$-secure block codes $\{Enc'_{B,j}/Dec'_{B,j} : \ 1 \leq j \leq N_B\}$ with the key derivation functions $\phi^j_{sk,B}$, such that a randomly selected ϵ-typical sequence in $\mathcal{Y}_B^n$ is in at least one of the codes with probability at least $1 - e^{-\gamma}$.

- For the inverse backward DMWC $(\mathcal{Y}_A, \mathcal{X}_B, \mathcal{Y}_{bE}, P_{X_B, Y_{bE}|Y_A})$, there exist N_A $(n_1, M_{1A}, K_{1A}, \epsilon)$-secure block codes $\{Enc'_{A,j}/Dec'_{A,j} : \ 1 \leq j \leq N_A\}$ with the key derivation functions $\phi^j_{sk,A}$, such that a randomly selected ϵ-typical sequence in $\mathcal{Y}_A^n$ is in at least one of the codes with probability at least $1 - e^{-\gamma}$.

Secure block codes and secure equipartitions (see Lemmas 11 and 13).

- For the forward DMWC $(\mathcal{X}_A, \mathcal{Y}_B, \mathcal{Y}_{fE}, P_{Y_B, Y_{fE}|X_A})$, there exists an $(n_{21A}, M_{21A}, K_{21A}, \epsilon)$-secure block code Enc_A/Dec_A with the key derivation function $\phi_{sk,A}$; furthermore, for each $i \in \mathcal{X}_A^{n_{21A}}$ there exists a (Γ_{21B}, ϵ)-secure equipartition ψ^i_B of $\mathcal{C}_{A,i} = Dec_A^{-1}(i) \subset \mathcal{Y}_B^{n_{21A}}$ w.r.t i.

- For the backward DMWC $(\mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_{bE}, P_{Y_A, Y_{bE}|X_B})$, there exists an $(n_{21B}, M_{21B}, K_{21B}, \epsilon)$-secure block code Enc_B/Dec_B with the key derivation function $\phi_{sk,B}$; furthermore, for each $i \in \mathcal{X}_A^{n_{21B}}$, there exists a (Γ_{21A}, ϵ)-secure equipartition ψ^i_A of $\mathcal{C}_{B,i} = Dec_B^{-1}(i) \subset \mathcal{Y}_A^{n_{21B}}$ w.r.t i.

Secure equipartitions for initialization phase (see Lemma 13):.

- For the forward DMWC $(\mathcal{X}_A, \mathcal{Y}_B, \mathcal{Y}_{fE}, P_{Y_B,Y_{fE}|X_A})$, there exists a (Γ_{22B}, ϵ)-secure equipartition ψ_B of $\mathcal{Y}_B^{n_{22A}}$ w.r.t. $\mathbf{a} \in \mathcal{X}_A^{n_{22A}}$.
- For the backward DMWC $(\mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_{bE}, P_{Y_A,Y_{bE}|X_B})$, there exists a (Γ_{22A}, ϵ)-secure equipartition ψ_A of $\mathcal{Y}_A^{n_{22B}}$ w.r.t. $\mathbf{b} \in \mathcal{Y}_A^{n_{22B}}$.

The initialization round (round 0). The initialization round proceeds as two parallel instances. The first and the second instances are to derive independent randomness for Bob and Alice, respectively; neither of them, however, produces a secret key. The first instance runs as follows. Alice sends the constant n_2-sequence $\mathbf{X}_A^{:0} = (Enc_A(u_a)||\mathbf{a})$ over the forward DMWC; Bob and Eve receive the noisy versions $\mathbf{Y}_B^{:0} = (\mathbf{Y}_{1B}||\mathbf{Y}_{2B})$ and $\mathbf{Y}_{fE}^{:0}$, respectively. Bob calculates $U_B^{:0} = (\psi_B^{u_a}(\mathbf{Y}_{1B})||\psi_B(\mathbf{Y}_{2B}))$ as independent randomness to be used in the first iteration of the basic protocol. He then splits this into two parts as $(U_{1B}^{:0}, U_{2B}^{:0}) = \mathfrak{u}_{B,split}(U_B^{:0})$. The first and the second parts are respectively used in the first and the second rounds of iteration 1.

In parallel to the above, the second instance runs as follows. Bob sends the constant n_2-sequence $\mathbf{X}_B^{:0} = (Enc_B(u_b)||\mathbf{b})$ over the backward DMWC; Alice and Eve receive $\mathbf{Y}_A^{:0} = (\mathbf{Y}_{1A}||\mathbf{Y}_{2A})$ and $\mathbf{Y}_{bE}^{:0}$, respectively. Alice calculates $U_A^{:0} = (\psi_A^{u_b}(\mathbf{Y}_{1B})||\psi_A(\mathbf{Y}_{2B}))$, as independent randomness, and splits it into $(U_{1A}^{:0}, U_{2A}^{:0}) = \mathfrak{u}_{A,split}(U_A^{:0})$, where the first and the second parts are respectively used in the first and the second rounds of iteration 1.

The basic protocol (iteration $1 \leq r \leq t$). Each iteration r of the basic protocol proceeds as two parallel instances of a two-round key agreement sub-protocol over the full-duplex communication channel. Each instance runs in two rounds, $2r-1$ and $2r$, where the 2DMWC is used n_1 and n_2 times, respectively. Each instance receives pieces of

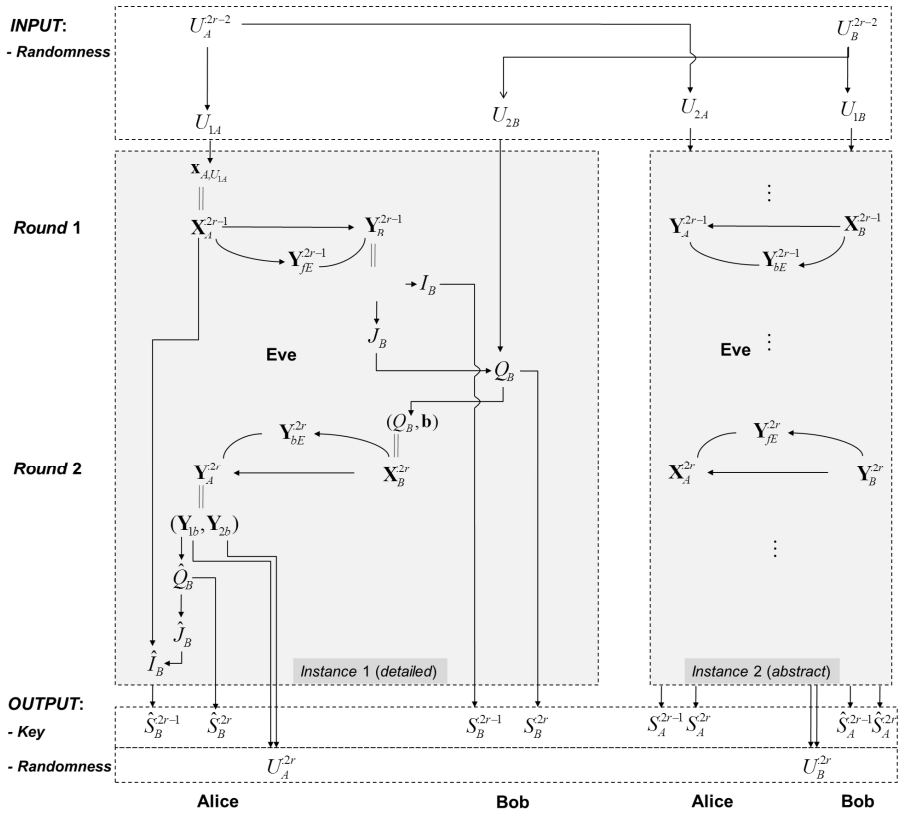


Figure A.2: The relationship between the variables in iteration r of the basic protocol.

randomness from Alice and Bob and returns to them a piece of secret key. Furthermore, the first and the second instances are initiated by Alice and Bob and return new pieces of independent randomness to Alice and Bob, respectively. The new randomness is used in the next iteration of the basic protocol. Figure A.2 summarizes the relationship between the random variables that are used in the first instance in iteration r of the basic protocol.

We describe the two instances of the key agreement sub-protocol together as follows. Alice and Bob send $\mathbf{X}_A^{:2r-1} = \mathbf{x}_{A,U_{1A}^{:2r-2}}$ and $\mathbf{X}_B^{:2r-1} = \mathbf{x}_{B,U_{1B}^{:2r-2}}$, and receive $\mathbf{Y}_A^{:2r-1}$ and $\mathbf{Y}_B^{:2r-1}$, respectively. Eve also receives $\mathbf{Y}_{fE}^{:2r-1}$ and $\mathbf{Y}_{bE}^{:2r-1}$.

Alice finds (I_A, J_A) such that $\mathbf{Y}_A^{:2r-1} = Enc'_{A,J_A}(I_A)$, i.e., the I_A-th codeword in the J_A-th secure block code over the inverse backward DMWC; similarly, Bob obtains (I_B, J_B) such that $\mathbf{Y}_B^{:2r-1} = Enc'_{B,J_B}(I_B)$. Round $2r-1$ may also be interpreted as follows. Alice

and Bob have encoded $I_A \in [M_{1A}]$ and $I_B \in [M_{1B}]$ to the codewords $Enc'_{A,J_A}(I_A)$ and $Enc'_{B,J_B}(I_B)$; they have sent them over the inverse DMWCs but have not included the information about which block code they belong to. Thus, round $2r$ is primarily used for sending the block code indices, i.e., $J_A \in [N_A]$ and $J_B \in [N_B]$. The round is also used to send the pieces of randomness, $U_{2A}^{:2r-2} \in [L_{2A}]$ and $U_{2B}^{:2r-2} \in [L_{2B}]$, as well as the deterministic sequences, $\mathbf{a}$ and $\mathbf{b}$.

In the beginning of round $2r$, Alice and Bob respectively calculate $Q_A \in [M_{21A}]$ and $Q_B \in [M_{21B}]$ as (note that $M_{21A} = N_A.L_{2A}$ and $M_{21B} = N_B.L_{2B}$)

$$Q_A = L_{2A}J_A + U_{2A}^{:2r-2}, \quad \text{and} \quad Q_B = L_{2B}J_B + U_{2B}^{:2r-2}. \tag{A.36}$$

They next use the key derivation functions (in the secure block code) to calculate key parts $S_A^{:2r} = \phi_{sk,A}(Q_A)$ and $S_B^{:2r} = \phi_{sk,B}(Q_B)$. In this round, Alice and Bob send the n_2-sequences $\mathbf{X}_A^{:2r} = (Enc_A(Q_A)||\mathbf{a})$ and $\mathbf{X}_B^{:2r} = (Enc_B(Q_B)||\mathbf{b})$ and receive $\mathbf{Y}_A^{:2r} = (\mathbf{Y}_{1A}||\mathbf{Y}_{2A})$ and $\mathbf{Y}_B^{:2r} = (\mathbf{Y}_{1B}||\mathbf{Y}_{2B})$, respectively. Eve also receives $\mathbf{Y}_{fE}^{:2r}$ and $\mathbf{Y}_{bE}^{:2r}$. Using the secure block code for the forward DMWC, Bob obtains $\hat{Q}_A$ such that $\mathbf{Y}_{1B} \in \mathcal{C}_{f,\hat{Q}_A}$ and calculates $\hat{S}_A^{:2r} = \phi_{sk,A}(\hat{Q}_A)$; similarly, Alice obtains $\hat{Q}_B$ such that $\mathbf{Y}_{1A} \in \mathcal{C}_{b,\hat{Q}_B}$ and calculates $\hat{S}_B^{:2r} = \phi_{sk,B}(\hat{Q}_B)$. To produce randomness for the next iteration, Alice and Bob use their secure equipartitions to calculate $U_A^{:2r} = (\psi_A^{\hat{Q}_B}(\mathbf{Y}_{1A})||\psi_A(\mathbf{Y}_{2A}))$ and $U_B^{:2r} = (\psi_B^{\hat{Q}_A}(\mathbf{Y}_{1B})||\psi_B(\mathbf{Y}_{2B}))$, respectively. The randomness pieces are then split into $(U_{1A}^{:2r}, U_{2B}^{:2r}) = \mathfrak{u}_{A,split}(U_A^{:2r})$ and $(U_{1B}^{:2r}, U_{2B}^{:2r}) = \mathfrak{u}_{B,split}(U_B^{:2r})$.

The above calculations are to derive independent randomness and secret key parts from round $2r$. The following is for deriving a key part out of round $2r-1$. Firstly, the parties calculate

$$\hat{U}_{2A}^{:2r-2} = \hat{Q}_A \mod (L_{2A}), \qquad \hat{J}_A = (\hat{Q}_A - \hat{U}_{2A}^{:2r-2})/L_{2A}, \tag{A.37}$$

$$\hat{U}_{2B}^{:2r-2} = \hat{Q}_B \mod (L_{2B}), \qquad \hat{J}_B = (\hat{Q}_B - \hat{U}_{2B}^{:2r-2})/L_{2B}. \tag{A.38}$$

The quantities $\hat{J}_A \in [N_A]$ and $\hat{J}_B \in [N_B]$ are used to find which secure block

codes need to be considered over the inverse DMWCs in round $2r-1$; More precisely, Alice decodes $\hat{I}_B = Dec'_{B,\hat{J}_B}(\mathbf{X}_A^{:2r-1})$ and Bob finds $\hat{I}_A = Dec'_{A,\hat{J}_A}(\mathbf{X}_B^{:2r-1})$. As for the establishment of the secret key part, Alice calculates $S_A^{:2r-1} = \phi_{sk,A}^{J_A}(Enc'_{A,J_A}(I_A))$ and $\hat{S}_B^{:2r-1} = \phi_{sk,B}^{\hat{J}_B}(Enc'_{B,\hat{J}_B}(\hat{I}_B))$, and Bob calculates $\hat{S}_A^{:2r-1} = \phi_{sk,A}^{\hat{J}_A}(Enc'_{A,\hat{J}_A}(\hat{I}_A))$ and $S_B^{:2r-1} = \phi_{sk,B}^{J_B}(Enc'_{B,J_B}(I_B))$.

The total secret key part in iteration r is $\left(S_A^{:2r-1}, S_A^{:2r}, S_B^{:2r-1}, S_B^{:2r}\right)$. Overall, the main protocol uses the 2DMWC $n = (2t+1)(n_1+n_2)$ times to establish $S = (S_A^{:r}, S_B^{:r})_{r=1}^{2t}$. By following this protocol, Alice calculates $S_A = (S_A^{:r}, \hat{S}_B^{:r})_{r=1}^{2t}$ and Bob calculates $S_B = (\hat{S}_A^{:r}, S_B^{:r})_{r=1}^{2t}$.

Protocol analysis. In what follows, we show that the main protocol satisfies reliability, secrecy, and randomness as in Definition 27 and achieves the lower bound in Theorem 6. Hereafter, we refer to the quantities I_A, J_A, I_B, J_B, Q_A, and Q_B in a certain iteration r by using $I_A^{:2r-1}$, $J_A^{:2r-1}$, $I_B^{:2r-1}$, $J_B^{:2r-1}$, $Q_A^{:2r-1}$, and $Q_B^{:2r-1}$, respectively.

Reliability analysis: proving (3.3a). We define the error event $\mathcal{E}rr$, which is true if at least one of the following happens.

- For an $1 \le r \le t$, at the end of round $2r-1$, Alice fails to find (I_A, J_A) such that $Y_A^{n_1:2r-1} = Enc'_{A,J_A}(I_A)$ or Bob fails to find (I_B, J_B) such that $Y_B^{n_1:2r-1} = Enc'_{B,J_B}(I_B)$. We refer to this event as $\mathcal{E}_r^1$, which indicates the failure in finding appropriate secure block codes over the inverse channels.

- For an $1 \le r \le t$, in round $2r$, Alice calculates $\hat{Q}_B^{:2r-1} \neq Q_B^{:2r-1}$ or $\hat{I}_B \neq I_B$ or Bob calculates $\hat{Q}_A^{:2r-1} \neq Q_A^{:2r-1}$ or $\hat{I}_A \neq I_A$. We refer to this event as $\mathcal{E}_r^2$, which indicates the decoding error in using the secure block codes.

- For an $0 \le r \le t-1$, at the end of round $2r$, Alice calculates $U_A^{:2r} = \perp$ or Bob calculates $U_B^{:2r} = \perp$. We refer to this event as $\mathcal{E}_r^3$, which shows the error in using the secure equipartitions.

The probability of each of the above events can be made arbitrarily small, thanks to the properties of the secure block codes and the secure equipartitions used in the protocol. In precise, we have the following upper bounds on the error event probabilities for each iteration $1 \leq r \leq t$ of the basic protocol, assuming that no error occurs in round 0 and all iterations up to $r-1$. Regarding the two sets of secure block codes for the inverse forward and backward channels, we have $\Pr(\mathcal{E}_r^1) \leq 2e^{-\gamma}$. The error event $\mathcal{E}_r^2$ corresponds to four decoding functions of the secure block codes of Alice and Bob over the channels, which implies $\Pr(\mathcal{E}_r^1) \leq 4\epsilon$. Finally, the secure partitions used by Alice and Bob give $\Pr(\mathcal{E}_r^3) \leq 2\epsilon$. The total error probability is calculated as follows. Let $\mathcal{E}_0^1$, $\mathcal{E}_0^2$, and $\mathcal{E}_t^3$ be always false.

$$
\begin{aligned}
\Pr(\mathcal{E}rr) &= \Pr\left(\bigcup_{r=0}^{t}(\mathcal{E}_r^1 \cup \mathcal{E}_r^2 \cup \mathcal{E}_r^3)\right) \\
&= \Pr\left(\mathcal{E}_0^1 \cup \mathcal{E}_0^2 \cup \mathcal{E}_0^3 \cup \bigcup_{r=1}^{t}\left[(\mathcal{E}_r^1 \cup \mathcal{E}_r^2 \cup \mathcal{E}_r^3) \cap \bigcap_{i=0}^{r-1}\overline{(\mathcal{E}_r^1 \cup \mathcal{E}_r^2 \cup \mathcal{E}_r^3)}\right]\right) \\
&= \Pr\left(\mathcal{E}_0^3\right) + \sum_{r=1}^{t}\Pr\left((\mathcal{E}_r^1 \cup \mathcal{E}_r^2 \cup \mathcal{E}_r^3) \cap \bigcap_{i=0}^{r-1}(\overline{\mathcal{E}_r^1} \cap \overline{\mathcal{E}_r^2} \cap \overline{\mathcal{E}_r^3})\right) \\
&\leq \Pr\left(\mathcal{E}_0^3\right) + \sum_{r=1}^{t}\Pr\left((\mathcal{E}_r^1 \cup \mathcal{E}_r^2 \cup \mathcal{E}_r^3)| \bigcap_{i=0}^{r-1}(\overline{\mathcal{E}_r^1} \cap \overline{\mathcal{E}_r^2} \cap \overline{\mathcal{E}_r^3})\right) \\
&\leq \Pr\left(\mathcal{E}_0^3\right) + \sum_{r=1}^{t}\Pr\left(\mathcal{E}_r^1| \bigcap_{i=0}^{r-1}(\overline{\mathcal{E}_r^1} \cap \overline{\mathcal{E}_r^2} \cap \overline{\mathcal{E}_r^3})\right) + \Pr\left(\mathcal{E}_r^2| \bigcap_{i=0}^{r-1}(\overline{\mathcal{E}_r^1} \cap \overline{\mathcal{E}_r^2} \cap \overline{\mathcal{E}_r^3})\right) \\
&\qquad + \sum_{r=1}^{t-1}\Pr\left(\mathcal{E}_r^3| \bigcap_{i=0}^{r-1}(\overline{\mathcal{E}_r^1} \cap \overline{\mathcal{E}_r^2} \cap \overline{\mathcal{E}_r^3})\right) \\
&\leq 2\epsilon + 2te^{-\gamma} + 4t\epsilon + 2(t-1)\epsilon \leq 6t\epsilon + 2te^{-2^{n_1\alpha/2}} \leq 7t\epsilon. \qquad \text{(A.39)}
\end{aligned}
$$

By selecting t to be polynomially increasing with $\min\{n_1, n_{21A}, n_{21B}\}$, $t\epsilon$ approaches zero for large enough n_1, n_{21A}, n_{2A}. This proves that for any arbitrarily $\delta > 0$ and sufficiently small α, we can find n_1 and n_2 such that $7t\epsilon < \delta$ and so

$$\Pr(S_A = S_B = S) \geq 1 - \Pr(\mathcal{E}rr) \geq 1 - 7t\epsilon > 1 - \delta. \qquad \text{(A.40)}$$

Randomness analysis: proving (3.3c). The entropy of the secret key S can be bounded from below as

$$H(S) \geq \Pr(\overline{\mathcal{E}rr})H(S|\overline{\mathcal{E}rr}) \geq (1 - 7t\epsilon)H(S|\overline{\mathcal{E}rr}). \tag{A.41}$$

We hereafter assume that no error has occurred and calculate the entropy of S based on this assumption. Assuming no error implies that each secure equipartition function gives an independent and uniform RV in the domain. In other words, ψ_A^j, ψ_A, ψ_B^j, and ψ_B return independent and uniform RVs in $[\Gamma_{21A}]$, $[\Gamma_{22A}]$, $[\Gamma_{21B}]$, and $[\Gamma_{22B}]$, respectively. So, for each iteration $1 \leq r \leq t$, the variables $U_A^{:2r-2}$ and $U_B^{:2r-2}$ are uniformly distributed and independent of the variables in any round less or equal to round $2r-2$. Since each execution of the basic protocol runs two key agreement procedures independently in parallel, the variables of these procedure are also independent. This implies that, for all $(i_A^{:2r-1}, q_A^{:2r-1}, i_B^{:2r-1}, q_B^{:2r-1})_{r=1}^t$ in $([M_{1A}] \times [M_{21A}] \times [M_{1B}] \times [M_{21B}])^t$,

$$\begin{aligned}
&\Pr\left(\bigcap_{r=1}^{t}(I_A^{:2r-1}, Q_A^{:2r-1}, I_B^{:2r-1}, Q_B^{:2r-1}) = (i_A^{:2r-1}, q_A^{:2r-1}, i_B^{:2r-1}, q_B^{:2r-1})\right) \\
&= \prod_{r=1}^{t} \Pr\left((I_A^{:2r-1}, Q_A^{:2r-1}, I_B^{:2r-1}, Q_B^{:2r-1}) = (i_A^{:2r-1}, q_A^{:2r-1}, i_B^{:2r-1}, q_B^{:2r-1})\right) \\
&= \prod_{r=1}^{t} \Pr\left((I_A^{:2r-1}, Q_A^{:2r-1}) = (i_A^{:2r-1}, q_A^{:2r-1})\right) . \Pr\left((I_B^{:2r-1}, Q_B^{:2r-1}) = (i_B^{:2r-1}, q_B^{:2r-1})\right) .
\end{aligned} \tag{A.42}$$

and hence, for all $(s_A^{:2r-1}, s_A^{:2r}, s_B^{:2r-1}, s_B^{:2r})_{r=1}^t$ in $([K_{1A}] \times [K_{21A}] \times [K_{1B}] \times [K_{21B}])^t$,

$$\begin{aligned}
&\Pr\left(\bigcap_{r=1}^{t}(S_A^{:2r-1}, S_A^{:2r}, S_B^{:2r-1}, S_B^{:2r}) = (s_A^{:2r-1}, s_A^{:2r}, s_B^{:2r-1}, s_B^{:2r})\right) \\
&= \prod_{r=1}^{t} \Pr\left((S_A^{:2r-1}, S_A^{:2r}) = (s_A^{:2r-1}, s_A^{:2r})\right) . \Pr\left((S_B^{:2r-1}, S_B^{:2r}) = (s_B^{:2r-1}, s_B^{:2r})\right) .
\end{aligned} \tag{A.43}$$

This leads to

$$H(S) = H\left((S_A^{:2r-1}, S_A^{:2r}, S_B^{:2r-1}, S_B^{:2r})_{r=1}^t\right) = \sum_{r=1}^{t} H(S_A^{:2r-1}, S_A^{:2r}) + H(S_B^{:2r-1}, S_B^{:2r}). \tag{A.44}$$

To continue the calculation above, we first discuss the RVs $I_A^{:2r-1}$, $J_A^{:2r-1}$, and $U_{2A}^{:2r-2}$. For all $i \in [M_{1A}]$ and all $j \in [N_A]$, we have

$$\Pr\left((I_A^{:2r-1}, J_A^{:2r-1}) = (i,j)\right) \leq \Pr(Y_A^{n_1:2r-1} = Enc'_{A,j}(i)) \leq 2^{-n_1(H(Y_A)-\epsilon)}, \tag{A.45}$$

where the last inequality follows from AEP and that $Enc'_{A,j}(i)$ is ϵ-typical w.r.t. Y_A. Since $U_A^{:2r-2} \in [\Gamma_{21A}] \times [\Gamma_{21B}]$ has a uniform distribution in, the two parts of it $U_{1A}^{:2r-2} \in [L_{1A}]$ and $U_{2A}^{:2r-2} \in [L_{2A}]$ are also uniformly distributed, i.e., specifically for $U_{2A}^{:2r-2}$,

$$\forall u \in [L_{2A}]: \quad \Pr\left(U_{2A}^{:2r-2} = u\right) = \frac{1}{L_{2A}}. \tag{A.46}$$

We conclude that, for all $i \in [M_{1A}]$ and all $q \in [M_{21A}]$, letting $u = q \mod (L_{2A})$ and $j = (q-u)/L_{2A}$, we have (see (A.30), (A.35), and (A.36))

$$\begin{aligned}
\Pr\left((I_A^{:2r-1}, Q_A^{:2r-1}) = (i,q)\right) &= \Pr\left((I_A^{:2r-1}, J_A^{:2r-1}, U_{2A}^{:2r-2}) = (i,j,u)\right) \\
&\overset{(a)}{=} \Pr\left((I_A^{:2r-1}, J_A^{:2r-1}) = (i,j)\right). \Pr\left(U_{2A}^{:2r-2} = u\right) \\
&= \frac{1}{L_{2A}} \Pr\left((I_A^{:2r-1}, J_A^{:2r-1}) = (i,j)\right) \\
&\leq \frac{1}{L_{2A}} 2^{-n_1(H(Y_A)-\epsilon)} = 2^{-n_1 I(X_B;Y_A) - n_{21A} I(X_A;Y_B) + n_1\epsilon} \\
&= \frac{2^{n_1\epsilon + n_{21A}\alpha}}{M_{1A}M_{21A}}.
\end{aligned} \tag{A.47}$$

Equality (a) holds since $(I_A^{:2r-1}, J_A^{:2r-1})$ and $U_{2A}^{:2r-2}$ are independent. The continuity of the entropy function gives

$$H(I_A^{:2r-1}, Q_A^{:2r-1}) \geq \log(M_{1A}M_{21A}) - n_{21A}\alpha - n_1\epsilon. \tag{A.48}$$

From the property of functions ϕ and ϕ^j (see Definition 32) and the description of the protocol, we can write

$$H(S_A^{:2r-1}, S_A^{:2r}) \geq \log(K_{1A}K_{21A}) - n_{21A}\alpha - n_1\epsilon = n_1 R_{scb^{-1}} + n_{21A} R_{scf} - n_{21A}\alpha - n_1\epsilon. \tag{A.49}$$

One can follow a similar approach to above to show

$$H(S_B^{:2r-1}, S_B^{:2r}) \geq \log(K_{1B}K_{21B}) - n_1\epsilon = n_1 R_{scf^{-1}} + n_{21B} R_{scb} - n_{21B}\alpha - n_1\epsilon. \tag{A.50}$$

Using (A.44) and (A.49) in (A.50), we can write

$$\begin{aligned}
\frac{H(S)}{n} &= \frac{t(n_1 R_{scb^{-1}} + n_{21A} R_{scf} - n_{21A}\alpha - n_1\epsilon) + t(n_1 R_{scf^{-1}} + n_{21B} R_{scb} - n_{21B}\alpha - n_1\epsilon)}{(t+1)(n_1+n_2)} \\
&\geq \frac{t}{(t+1)(\mu+1)} \left(\mu R_{scb^{-1}} + \frac{n_{21A}}{n_2} R_{scf} + \mu R_{scf^{-1}} + \frac{n_{21B}}{n_2} R_{scb} - 2\alpha - 2\mu\epsilon\right) \\
&\geq \frac{t}{(t+1)(1+\mu)} \left((\mu R_{scb^{-1}} + \gamma_1 R_{scf}) + (\mu R_{scf^{-1}} + \gamma_2 R_{scb}) - 2(1+\mu)\alpha\right)
\end{aligned} \tag{A.51}$$

where $\mu = \frac{n_1}{n_2}$ and γ_1 and γ_2 are as defined in the theorem. Thus, for an arbitrarily given $\delta > 0$, we can choose α, t, n_1, and n_2 such that

$$\frac{H(S)}{n} > Lbnd_A^{-r} + Lbnd_B^{-r} - \delta, \tag{A.52}$$

with $Lbnd_A^{-r}$ and $Lbnd_B^{-r}$ as defined in the theorem.

Secrecy analysis: proving (3.3b). Denote by $\mathbb{V}_E^{:r}$ and $SK^{:r}$ Eve's view and the total secret key established at the end of round r, respectively.

$$\begin{aligned}
H(S|\mathbb{V}_E^{:2t}) &= H(S) - I\left(SK^{:2t}; \mathbb{V}_E^{:2t}\right) \\
&= H(S) - I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; \mathbb{V}_E^{:2t}\right) - I\left(SK^{:2t-2}; \mathbb{V}_E^{:2t} | (S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}\right) \\
&= H(S) - I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; \mathbb{V}_E^{:2t}\right) - I\left(SK^{:2t-2}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t} | (S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}\right) \\
&\qquad - I\left(SK^{:2t-2}; \mathbb{V}_E^{:2t-2} | (S_A^{:r}, S_B^{:r}, \mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) \\
&\geq H(S) - I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; \mathbb{V}_E^{:2t}\right) - I\left(SK^{:2t-2}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t} | (S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}\right) \\
&\qquad - I\left(U_A^{:2t-2}, U_B^{:2t-2}; \mathbb{V}_E^{:2t-2} | SK^{:2t-2}\right) - I\left(SK^{:2t-2}; \mathbb{V}_E^{:2t-2}\right),
\end{aligned} \tag{A.53}$$

where the last inequality holds since

$$\begin{aligned}
&I\left(SK^{:2t-2}; \mathbb{V}_E^{:2t-2} | (S_A^{:r}, S_B^{:r}, \mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) \\
&\quad \leq I\left(SK^{:2t-2}, U_A^{:2t-2}, U_B^{:2t-2}; \mathbb{V}_E^{:2t-2} | (S_A^{:r}, S_B^{:r}, \mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) \\
&\quad \overset{(a)}{\leq} I\left(SK^{:2t-2}, U_A^{:2t-2}, U_B^{:2t-2}; \mathbb{V}_E^{:2t-2}\right) \\
&\quad = I\left(U_A^{:2t-2}, U_B^{:2t-2}; \mathbb{V}_E^{:2t-2} | SK^{:2t-2}\right) + I\left(SK^{:2t-2}; \mathbb{V}_E^{:2t-2}\right).
\end{aligned} \tag{A.54}$$

Inequality (a) is due to the Markov chain

$$(SK^{:2t-2}, \mathbb{V}_E^{:2t-2}) \leftrightarrow (U_A^{:2t-2}, U_B^{:2t-2}) \leftrightarrow (S_A^{:r}, S_B^{:r}, \mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}.$$

There are 5 terms on the right hand of (A.53). In the sequel, we calculate the second, the third, and the fourth terms separately and show that they are all arbitrarily small.

The second term in (A.53).

$$
\begin{aligned}
&I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; \mathbb{V}_E^{:2t}\right) \\
&\quad = I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) + I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; \mathbb{V}_E^{:2t-2} | (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) \\
&\quad \leq I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) \\
&\qquad\quad + I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}, U_A^{:2t-2}, U_B^{:2t-2}; \mathbb{V}_E^{:2t-2}, \mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2} | (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) \\
&\quad \overset{(a)}{\leq} I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) + I\left(U_A^{:2t-2}, U_B^{:2t-2}; \mathbb{V}_E^{:2t-2}, \mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}\right) \\
&\quad \overset{(b)}{=} I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) + I\left(U_A^{:2t-2}, U_B^{:2t-2}; \mathbf{Y}_{fE}^{:2t-2}, \mathbf{Y}_{bE}^{:2t-2}, \mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}\right) \\
&\quad \overset{(c)}{\leq} I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}\right) + (\log \Gamma_A + \log \Gamma_B)\epsilon \\
&\quad \overset{(d)}{=} I\left(S_A^{:2t-1}, S_A^{:2t}; \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t}\right) + I\left(S_B^{:2t-1}, S_B^{:2t}; \mathbf{Y}_{fE}^{:2t-1}, \mathbf{Y}_{bE}^{:2t}\right) + \log(\Gamma_A \Gamma_B)\epsilon. \qquad \text{(A.55)}
\end{aligned}
$$

Inequality (a) is due to the Markov chain

$$(\mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}, \mathbb{V}_E^{:2t-2}) \leftrightarrow (U_A^{:2t-2}, U_B^{:2t-2}) \leftrightarrow (S_A^{:r}, S_B^{:r}, \mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t},$$

equality (b) is due to

$$\mathbb{V}_E^{:2t-2} \leftrightarrow (\mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}, \mathbf{Y}_{fE}^{:2t-2}, \mathbf{Y}_{bE}^{:2t-2}) \leftrightarrow (U_A^{:2t-2}, U_B^{:2t-2}),$$

inequality (c) follows from the property of secure equipartitions (see (3.20)), and equality (d) holds due to the independency of the variables. We shall show that the first two terms of (A.55) are small. Using (A.30) and (A.34)),

$$
\begin{aligned}
&I\left(S_A^{:2t-1}, S_A^{:2t}; \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t}\right) \\
&\quad = I\left(S_A^{:2t-1}, S_A^{:2t}, \mathbf{Y}_A^{:2t-1}, \mathbf{X}_A^{:2t}; \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t}\right) - I\left(\mathbf{Y}_A^{:2t-1}, \mathbf{X}_A^{:2t}; \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t} | S_A^{:2t-1}, S_A^{:2t}\right) \\
&\quad = I\left(\mathbf{Y}_A^{:2t-1}, \mathbf{X}_A^{:2t}; \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t}\right) - I\left(\mathbf{Y}_A^{:2t-1}, \mathbf{X}_A^{:2t}; \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t} | S_A^{:2t-1}, S_A^{:2t}\right) \\
&\quad \leq I\left(\mathbf{Y}_A^{:2t-1}; \mathbf{Y}_{bE}^{:2t-1}\right) + I\left(\mathbf{X}_A^{:2t}; \mathbf{Y}_{fE}^{:2t}\right) - I\left(\mathbf{Y}_A^{:2t-1}, \mathbf{X}_A^{:2t}; \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t} | S_A^{:2t-1}, S_A^{:2t}\right) \\
&\quad \leq n_1(I(Y_A; Y_{bE}) + \epsilon) + n_{21A}(I(X_A; Y_{fE}) + \epsilon) - H\left(\mathbf{Y}_A^{:2t-1}, \mathbf{X}_A^{:2t} | S_A^{:2t-1}, S_A^{:2t}\right) \\
&\qquad\quad + H\left(\mathbf{Y}_A^{:2t-1}, \mathbf{X}_A^{:2t} | \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t}, S_A^{:2t-1}, S_A^{:2t}\right). \qquad \text{(A.56)}
\end{aligned}
$$

The last inequality follows from AEP. Using the proof for the existence of capacity achieving codes along with Fano's inequalities gives us that the last term in the above is

at most $(n_1 + n_{21A})\delta_1$ for some arbitrarily small δ_1. For the the rest we write

$$
\begin{aligned}
& I\left(S_A^{:2t-1}, S_A^{:2t}; \mathbf{Y}_{bE}^{:2t-1}, \mathbf{Y}_{fE}^{:2t}\right) \\
& \leq n_1 I(Y_A; Y_{bE}) + n_{21A} I(X_A; Y_{fE}) - H\left(\mathbf{Y}_A^{:2t-1}, \mathbf{X}_A^{:2t} | S_A^{:2t-1}, S_A^{:2t}\right) + (n_1 + n_{21A})(\epsilon + \delta_1) \\
& = n_1 I(Y_A; Y_{bE}) + n_{21A} I(X_A; Y_{fE}) - H\left(I_A^{:2t-1}, Q_A^{:2t-1} | S_A^{:2t-1}, S_A^{:2t}\right) + (n_1 + n_{21A})(\epsilon + \delta_1) \\
& = n_1 I(Y_A; Y_{bE}) + n_{21A} I(X_A; Y_{fE}) - H(I_A^{:2t-1}, Q_A^{:2t-1}) \\
& \qquad + H(S_A^{:2t-1}) + H(S_A^{:2t}) + (n_1 + n_{21A})(\epsilon + \delta_1) \\
& \leq n_1 I(Y_A; Y_{bE}) + n_{21A} I(X_A; Y_{fE}) - \log(M_1 M_{21A}) + \log(K_1 K_{21A}) + (n_1 + n_{21A})(\epsilon + \delta_1) \\
& = n_1 I(Y_A; Y_{bE}) + n_{21A} I(X_A; Y_{fE}) + n_1(R_{scb^{-1}} - R_{cb}) + n_{21A}(R_{scf} - R_{cf}) \\
& \qquad + (n_1 + n_{21A})(\epsilon + \delta_1) \\
& = n_1 I(Y_A; Y_{bE}) + n_{21A} I(X_A; Y_{fE}) - n_1(I(Y_A; Y_{bE}) + \alpha) \\
& \qquad - n_{21A}(I(X_A; Y_{fE}) + \alpha) + (n_1 + n_{21A})(\epsilon + \delta_1) \\
& = (n_1 + n_{21A})(\epsilon + \delta_1 - \alpha) \leq (n_1 + n_{21A})\delta_2,
\end{aligned} \tag{A.57}
$$

for an arbitrarily small δ_2. Similarly, one can show

$$
I\left(S_B^{:2t-1}, S_B^{:2t}; \mathbf{Y}_{fE}^{:2t-1}, \mathbf{Y}_{bE}^{:2t}\right) \leq (n_1 + n_{21B})\delta_3, \tag{A.58}
$$

for an arbitrarily small δ_3. This gives that (A.55) is bounded as

$$
I\left((S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}; \mathbb{V}_E^{:2t}\right) \leq (n_1 + n_2)\delta_4, \tag{A.59}
$$

for some arbitrarily small δ_4.

The third term in (A.53).

$$
\begin{aligned}
& I\left(SK^{:2t-2}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t} | (S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}\right) \\
& \leq I\left(SK^{:2t-2}, \mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}; (\mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t}, U_A^{:2t-2}, U_B^{:2t-2} | (S_A^{:r}, S_B^{:r})_{r=2t-1}^{2t}\right) \\
& \overset{(a)}{\leq} I\left(\mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}; U_A^{:2t-2}, U_B^{:2t-2}\right) \\
& \overset{(b)}{=} I\left(\mathbf{X}_A^{:2t-2}; U_B^{:2t-2}\right) + I\left(\mathbf{X}_B^{:2t-2}; U_A^{:2t-2}\right) \\
& \leq \log(\Gamma_A . \Gamma_B)\epsilon.
\end{aligned} \tag{A.60}
$$

Inequality (a) is due to the Markov chain

$$SK^{:2t-2} \leftrightarrow (\mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}) \leftrightarrow (U_A^{:2t-2}, U_B^{:2t-2}) \leftrightarrow (S_A^{:r}, S_B^{:r}, \mathbf{Y}_{fE}^{:r}, \mathbf{Y}_{fB}^{:r})_{r=2t-1}^{2t},$$

and equality (b) follows from the independence of the variables.

The fourth term in (A.53).

$$\begin{aligned} & I\left(U_A^{:2t-2}, U_B^{:2t-2}; \mathbb{V}_E^{:2t-2} | SK^{:2t-2}\right) \\ & \quad \leq I\left(U_A^{:2t-2}, U_B^{:2t-2}; \mathbb{V}_E^{:2t-2}, \mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2} | SK^{:2t-2}\right) \\ & \quad \overset{(a)}{\leq} I\left(U_A^{:2t-2}, U_B^{:2t-2}; \mathbf{Y}_{fE}^{:2t-2}, \mathbf{Y}_{bE}^{:2t-2}, \mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}\right) \\ & \quad \overset{(b)}{=} I\left(U_A^{:2t-2}; \mathbf{Y}_{bE}^{:2t-2}, \mathbf{X}_B^{:2t-2}\right) + I\left(U_B^{:2t-2}; \mathbf{Y}_{fE}^{:2t-2}, \mathbf{X}_A^{:2t-2}\right) \\ & \quad \leq \log(\Gamma_A.\Gamma_B)\epsilon. \end{aligned} \tag{A.61}$$

Inequality (a) is due to the Markov chain

$$(SK^{:2t-2}, \mathbb{V}_E^{:2t-2}) \leftrightarrow (\mathbf{X}_A^{:2t-2}, \mathbf{X}_B^{:2t-2}, \mathbf{Y}_{fE}^{:2t-2}, \mathbf{Y}_{bE}^{:2t-2}) \leftrightarrow (U_A^{:2t-2}, U_B^{:2t-2}),$$

and equality (b) follows from the independence of the variables.

Using (A.59)-(A.61) in (A.53), we arrive at

$$H(S|\mathbb{V}_E^{:2t}) \geq H(S) - I\left(SK^{:t-2}; \mathbb{V}_E^{:t-2}\right) - (n_1 + n_2)\delta_5, \tag{A.62}$$

for some arbitrarily small δ_5. Repeating the above steps t times, lets us conclude

$$H(S|\mathbb{V}_E^{:2t}) \geq H(S) - t(n_1 + n_2)\delta_5, \tag{A.63}$$

which proves, for appropriate selection of parameters,

$$\frac{H(S|\mathbb{V}_E^{:2t})}{H(S)} \geq 1 - \frac{t(n_1 + n_2)\delta_5}{H(S)} > 1 - \delta. \tag{A.64}$$

A.8 Proof of Theorem 7: SK capacity upper bound for 2DMWC^{-r}

Let Π be an (R_{sk}, δ)-weakly secure t-round protocol that achieves the SK rate R_{sk} for an arbitrarily small $\delta > 0$. Using (3.3b) and Fano's inequality for (3.3a), we have

$$I(S; \mathbb{V}_E^{:t-1}) = H(S) - H(S|View_E) \leq \delta H(S), \tag{A.65a}$$

$$H(S|S_A) \leq h(\delta) + \delta H(S), \tag{A.65b}$$

$$H(S|S_B) \leq h(\delta) + \delta H(S) \tag{A.65c}$$

Considering (A.65), we write the entropy of S as

$$\begin{aligned} H(S) &= I(S; S_A) + H(S|S_A) + I(S; \mathbb{V}_E^{:t-1}) - I(S; \mathbb{V}_E^{:t-1}) \\ &\leq I(S; S_A|\mathbb{V}_E^{:t}) + H(S|S_A) + I(S; \mathbb{V}_E^{:t-1}) \qquad \text{(A.66)} \\ &\leq H(S_A|\mathbb{V}_E^{:t-1}) + h(\delta) + 2\delta H(S) \\ &\leq H(\mathbb{V}_A^{:t-1}|\mathbb{V}_E^{:t-1}) + h(\delta) + 2\delta H(S). \qquad \text{(A.67)} \end{aligned}$$

Similarly

$$H(S) \leq H(\mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t-1}) + h(\delta) + 2\delta H(S), \tag{A.68}$$

$$H(S) \leq H(\mathbb{V}_A^{:t-1}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t-1}) + h(\delta) + 2\delta H(S), \tag{A.69}$$

and, from (A.66),

$$\begin{aligned} H(S) &\leq I(S, S_B; S_A|\mathbb{V}_E^{:t-1}) + H(S|S_A) + I(S; \mathbb{V}_E^{:t-1}) \\ &= I(S_B; S_A|\mathbb{V}_E^{:t-1}) + I(S; S_A|S_B, \mathbb{V}_E^{:t-1}) + H(S|S_A) + I(S; \mathbb{V}_E^{:t-1}) \\ &\leq I(S_A; S_B|\mathbb{V}_E^{:t-1}) + H(S|S_B) + H(S|S_A) + I(S; \mathbb{V}_E^{:t-1}) \\ &\leq I(\mathbb{V}_A^{:t-1}; \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t-1}) + 2h(\delta) + 3\delta H(S). \qquad \text{(A.70)} \end{aligned}$$

Choose the RVs (X_A, Y_B, Y_{fE}) and (X_B, Y_A, Y_{bE}) such that they correspond to the 2DMWC probability distributions and

$$P_{X_A} = \frac{1}{n} \sum_{r=0}^{t-1} \sum_{i=1}^{n_r} P_{X_{A,i}^{:r}}, \qquad P_{X_B} = \frac{1}{n} \sum_{r=0}^{t-1} \sum_{i=1}^{n_r} P_{X_{B,i}^{:r}},$$

Below, we study each of the inequalities (A.67)-(A.70), respectively, to obtain four upper bounds on the entropy of the key S produced by the SKE protocol Π.

$$\begin{aligned} H(\mathbb{V}_A^{:t-1}|\mathbb{V}_E^{:t-1}) &\leq H(\mathbb{V}_A^{:t-1}|\mathbb{V}_E^{:t-1}) \\ &= \sum_{r=0}^{t-1} H(Y_A^{n_r:r}|\mathbb{V}_A^{:r-1}, \mathbb{V}_E^{:t-1}) \\ &\leq \sum_{r=0}^{t-1} H(Y_A^{n_r:r}|Y_{bE}^{n_r:r}) \\ &\leq nH(Y_A|Y_{bE}). \end{aligned} \tag{A.71}$$

Similarly

$$H(\mathbb{V}_A^{:t-1}|\mathbb{V}_E^{:t-1}) \leq nH(Y_B|Y_{fE}). \tag{A.72}$$

$$\begin{aligned} H(\mathbb{V}_A^{:t-1}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t-1}) &= \sum_{r=0}^{t-1} H(Y_B^{n_r:r}, Y_A^{n_r:r}|\mathbb{V}_A^{:r-1}, \mathbb{V}_B^{:r-1}, \mathbb{V}_E^{:t-1}) \\ &= \sum_{r=0}^{t-1} H(Y_B^{n_r:r}, Y_A^{n_r:r}|\mathbb{V}_A^{:r-1}, \mathbb{V}_B^{:r-1}, X_A^{n_r:r}, X_B^{n_r:r}, \mathbb{V}_E^{:t-1}) \\ &= \sum_{r=0}^{t-1} (H(Y_B^{n_r:r}|X_A^{n_r:r}, Y_{fE}^{n_r:r}, Y_{bE}^{n_r:r}) + H(Y_A^{n_r:r}|X_B^{n_r:r}, Y_{fE}^{n_r:r}, Y_{bE}^{n_r:r})) \\ &\leq n(H(Y_B|X_A, Y_{fE}) + H(Y_A|X_B, Y_{bE})). \end{aligned} \tag{A.73}$$

Finally,

$$\begin{aligned} I(\mathbb{V}_A^{:t-1}; \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t-1}) &= H(\mathbb{V}_A^{:t-1}|\mathbb{V}_E^{:t-1}) + H(\mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t-1}) - H(\mathbb{V}_A^{:t-1}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t-1}) \\ &\leq n(I(X_A; Y_B|Y_{fE}) + H(X_B; Y_A|Y_{bE})). \end{aligned} \tag{A.74}$$

Combining the above results gives

$$\begin{aligned} H(S) &\leq n \min \big(H(Y_B|Y_{fE}), H(Y_A|Y_{bE}), (H(Y_B|X_A, Y_{fE}) + H(Y_A|X_B, Y_{bE})) \ , \\ &\qquad (I(X_A; Y_B|Y_{fE}) + H(X_B; Y_A|Y_{bE}))\big) + 2h(\delta) + 3\delta H(S) \\ &= n(\min\{H(Y_B|X_A, Y_{fE}), I(X_B; Y_A|Y_{bE})\} \\ &\qquad + \min\{H(Y_A|X_B, Y_{bE}), I(X_A; Y_B|Y_{fE})\}) + 2h(\delta) + 3\delta H(S). \end{aligned} \tag{A.75}$$

From (3.3c) and (A.75), we conclude the following upper bound on R_{sk}

$$\begin{aligned} R_{sk} &< \frac{1}{n}H(S) + \delta \\ &< \min\{H(Y_B|X_A, Y_{fE}), I(X_B; Y_A|Y_{bE})\}] + \min\{H(Y_A|X_B, Y_{bE}), I(X_A; Y_B|Y_{fE})\} \\ &\quad +\delta + 2h(\delta) + 3\delta H(S) \\ &\leq \min\{H(Y_B|X_A, Y_{fE}), I(X_B; Y_A|Y_{bE})\}] + \min\{H(Y_A|X_B, Y_{bE}), I(X_A; Y_B|Y_{fE})\}. \end{aligned}$$

The last inequality holds since δ is arbitrarily small. □

A.9 Proof of Theorem 8: SK capacity for 2DMWC^{-r} without leakage

When the channel leaks zero information to Eve, we have $I(X_A, Y_B; Y_{fE}) = I(X_B, Y_B; Y_{bE}) = 0$. Following the lower bound (3.42), we choose $\mu = 00$ and lower bound the SK capacity as follows. Note that for this selection of μ the conditions (3.47) and (3.48) always hold.

$$C_{wsk}^{2DMWC} \geq \max_{X_A, X_B} \{Lbnd_A^{-r} + Lbnd_B^{-r}\}, \tag{A.76}$$

where

$$Lbnd_A^{-r} = (\gamma_1 I(X_A; Y_B)), \qquad \gamma_1 = \min\{1, \frac{H(Y_A|X_B)}{I(X_A; Y_B)}\}, \tag{A.77}$$

$$Lbnd_B^{-r} = (\gamma_2 I(X_B; Y_A)), \qquad \gamma_2 = \min\{1, \frac{H(Y_B|X_A)}{I(X_B; Y_A)}\}. \tag{A.78}$$

The above can be written as

$$Lbnd_A^{-r} = \min\{H(Y_A|X_B), I(X_A; Y_B)\}, \quad Lbnd_B^{-r} = \min\{H(Y_B|X_A), I(X_B; Y_A)\}. \tag{A.79}$$

The first and the second term above equal $Ubnd_A^{-r}$ and $Ubnd_B^{-r}$ in the upper bound (3.49). □

A.10 Proof of Lemma 16: SK capacity bounds for 2BSWC^{-r}

Following the lower bound expression (3.42) in Theorem 6, and letting X_A and X_B to be uniform binary RVs, we have

$$C_{wsk}^{BSWC^{-r}} \geq 2\max_{\mu\geq 0}\{Lbnd^{-r}\}, \text{ such that} \tag{A.80}$$

$$Lbnd^{-r} = \tfrac{1}{1+\mu}\left(\mu(h(p_m \star p_e) - h(p_m)) + \gamma(h(p_e) - h(p_m))_+\right), \tag{A.81}$$

$$\gamma = \min\{1, \tfrac{h(p_m)}{1-h(p_m)} - \mu\}, \tag{A.82}$$

$$\mu \leq \min\{h(p_m), \tfrac{1-h(p_m)}{h(p_m)}\}. \tag{A.83}$$

We show that the optimal choice of μ can be reduced to $\mu \in \{0, \mu_1^*, \mu_2^*\}$ (with μ_1^* and μ_2^* defined in (3.56)) can lead to the lower bound (A.80). We note that $\mu \leq \mu_2^*$ is an explicit condition of the lower bound and that (i) if $\mu \leq \mu_1^*$, then $\gamma = 1$; (ii) otherwise, $\gamma = \frac{h(p_m)}{1-h(p_m)} - \mu < 1$. Accordingly, we consider the following cases.

Case 1: $h(p_e) \leq h(p_m)$**.** In this case, $(h(p_e) - h(p_m))_+ = 0$ and so $Lbnd^{-r}$ is written as

$$\frac{\mu}{\mu+1}(h(p_m \star p_e) - h(p_m)). \tag{A.84}$$

This gives that, to maximize $Lbnd^{-r}$, the largest possible μ should be selected, i.e., $\mu = \mu_2^*$.

Case 2: $h(p_e) > h(p_m)$**.** We divide this into the following three subcases.

2.1) If $\mu_2^* \leq \mu_1^*$, for any $\mu \leq \mu_2^*$, the inequality $\mu \leq \mu_1^*$ also holds. From (i) above, $\gamma = 1$ and $Lbnd^{-r}$ can be expressed as the following weighted average

$$\frac{\mu}{1+\mu}((h(p_m \star p_e) - h(p_m))) + \frac{1}{1+\mu}(h(p_e) - h(p_m)). \tag{A.85}$$

Since the first term in the above average is greater or equal to the second term, the average is maximized by selecting the largest possible value for μ that is $\mu = \mu_2^*$.

2.2) If $\mu_2^* > \mu_1^* \geq 0$, then we may choose $\mu \leq \mu_1^*$ or $\mu_1^* < \mu \leq \mu_2^*$.

- For $\mu \leq \mu_1^*$, from (i), $\gamma = 1$ and so $Lbnd^{-r}$ is expressed the same way as (A.85). This implies that selecting $\mu = \mu_1^*$ (the largest possible value) leads to the maximization of the average.

- For $\mu_1^* < \mu \leq \mu_2^*$, from (ii), $Lbnd^{-r}$ can be written as the following weighted average

$$\frac{\mu}{\mu+1}(h(p_m \star p_e) - h(p_e)) + \frac{1}{\mu+1}(\frac{h(p_m)}{1-h(p_m)}(h(p_e) - h(p_m))). \tag{A.86}$$

Depending on the relationship between the first and the second terms of the above average, the maximum is achieved by selecting either the smallest or the largest possible μ in the range $\mu_1^* \leq \mu \leq \mu_2^*$, that is either μ_1^* or μ_2^*, respectively.

2.3) If $\mu_1^* < 0$, then for any $0 \leq \mu \leq \mu_2^*$, we have $\mu > \mu_1^*$. From (ii), $Lbnd^{-r}$ is written the same as (A.86). However, the smallest and the largest values of μ are 0 and μ_2^*, respectively.

In all cases above, either selection of $\mu \in \{0, \mu_1^*, \mu_2^*\}$ leads to the maximum achievable rate. i.e. the lower bound in (A.80) can be simplified to (A.80).

Following the upper bound (3.49) in Theorem 7 for the above setting, we arrive at

$$\begin{aligned}
&C_{wsk}^{BSWC^{-r}} \leq 2 \max_{X_A, X_B} \{Ubnd_A^{-r}, Ubnd_B^{-r}\}, \quad \text{where} \\
&Ubnd_A^{-r} = \min\{h(p_m), H(Y_B|Y_{fE}) - h(p_m)\}, \quad \text{and} \\
&Ubnd_B^{-r} = \min\{h(p_m), H(Y_A|Y_{bE}) - h(p_m)\}.
\end{aligned}$$

It is easy to show that by choosing uniformly random X_A and X_B, $Ubnd_A^{-r}$ and $Ubnd_B^{-r}$ reach their highest values, respectively. This proves the upper bound (3.57)

A.11 Proof of Theorem 9: SK capacity lower bound, TWDMWC

We provide a two-round SKE protocol, Π, that achieves

$$R_{sk} = \frac{\mu R_{stwc^{-1}} + [R_{stwc}]_+}{1+\mu} \tag{A.87}$$

for a given set of variables: μ, X_A,X_B, V_A,V_B, W_{2A},W_{2B},W_{1A}, and W_{1B} that satisfy the conditions of the theorem.

Parameter definition. Let n_1 and n_2 such that $n_1 = \mu n_2$ be sufficiently large integers that represent the number of TWDMWC uses in the first and the second round, respectively; hence the protocol cost equals $Cost_{\Pi}^{TWDMWC} = n \stackrel{\Delta}{=} n_1 + n_2 = n_2(1+\mu)$. We rephrase the conditions (3.63) and (3.64) as

$$n_1[I(V_A; X_A, Y_A|X_B, Y_B) + 3\alpha] \leq n_2 I(W_{1A}; X_B, Y_B), \tag{A.88}$$

$$n_1[I(V_B; X_B, Y_B|X_A, Y_A) + 3\alpha] \leq n_2 I(W_{1B}; X_A, Y_A), \tag{A.89}$$

where $\alpha > 0$ is a sufficiently small constant to be determined from the arbitrarily small δ. Let $n_{2,a1}$, $n_{2,a2}$, $n_{2,b1}$, and $n_{2,b2}$ be chosen such that $n_{2,a1} + n_{2,a2} = n_{2,b1} + n_{2,b2} = n_2$ and

$$n_{2,a2} I(W_{1A}; X_B, Y_B) = n_1[I(V_A; X_A, Y_A|X_B, Y_B) + 3\alpha], \tag{A.90}$$

$$n_{2,b2} I(W_{1B}; X_A, Y_A) = n_1[I(V_B; X_B, Y_B|X_A, Y_A) + 3\alpha]. \tag{A.91}$$

Also let ϵ and β be small constants such that $3n\epsilon < n_2\beta = n_1\alpha$. Define

$$\eta_{a,f} = n_1[I(V_A; X_A, Y_A) + \alpha] \tag{A.92a}$$

$$\eta_{a,g} = n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta], \quad \eta_{a,g,2} = n_{2,a1} I(W_{2A}; X_B, Y_B), \quad \eta_{a,g,1} = \eta_{a,g} - \eta_{a,g,2}, \tag{A.92b}$$

$$\eta_{a,t} = n_{2,a2}[I(W_{1A}; X_B, Y_B) - \beta], \quad \eta_{a,t,2} = n_{2,a2} I(W_{2A}; X_B, Y_B), \quad \eta_{a,t,1} = \eta_{a,t} - \eta_{a,t,2}, \tag{A.92c}$$

$$\eta_{b,f} = n_1[I(V_B; X_B, Y_B) + \alpha], \tag{A.92d}$$

$$\eta_{b,g} = n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta], \quad \eta_{b,g,2} = n_{2,b1} I(W_{2B}; X_A, Y_A), \quad \eta_{b,g,1} = \eta_{b,g} - \eta_{b,g,2}, \tag{A.92e}$$

$$\eta_{b,t} = n_{2,b2}[I(W_{1B}; X_A, Y_A) - \beta], \quad \eta_{b,t,2} = n_{2,b2} I(W_{2B}; X_A, Y_A), \quad \eta_{b,t,1} = \eta_{b,t} - \eta_{b,t,2}, \tag{A.92f}$$

$$\eta_{ab,f} = n_1[I(V_A, V_B; X_A, Y_A, X_B, Y_B) + 2\alpha], \qquad \eta = \eta_{a,g} + \eta_{b,g} + \eta_{ab,f}, \tag{A.92g}$$

$$\kappa = (n_1 + n_2) R_{sk}, \qquad \gamma = \eta - \kappa. \tag{A.92h}$$

Quantities in (A.92a)-(A.92c) (resp. (A.92d)-(A.92f)) are used in the calculation of what Alice (resp. Bob) needs to send during the communication. Although the quantities obtained in (A.90)-(A.92a) are real values, for sufficiently small β and sufficiently large n_1 and n_2, we can assume they are non-negative integers. Furthermore, we shall show that $\eta_{a,f} \geq \eta_{a,t}$, $\eta_{b,f} \geq \eta_{b,t}$, and $\eta \geq \kappa$. The former is shown below.

$$\begin{aligned}
\eta_{a,f} &= n_1[I(V_A; X_A, Y_A) + \alpha] \overset{(a)}{=} n_1[I(V_A; X_A, Y_A, X_B, Y_B) + \alpha] \\
&= n_1[I(V_A; X_B, Y_B) + I(V_A; X_A, Y_A|X_B, Y_B) + \alpha] \\
&\overset{(b)}{=} n_1 I(V_A; X_B, Y_B) + n_{2,a2} I(W_{1A}; X_B, Y_B) - 2n_1\alpha \\
&\geq n_{2,a2}[I(W_{1A}; X_B, Y_B) - \beta] - 2n_1\alpha \\
&\overset{(c)}{=} \eta_{a,t} - 2n_1\alpha.
\end{aligned}$$

Equality (a) is due to the Markov chain (3.60a), and equalities (b) and (c) follow from (A.90) and (A.92c), respectively. For sufficiently small α, we have $\eta_{a,f} \geq \eta_{a,t}$. Similarly, one can show $\eta_{b,f} \geq \eta_{b,t}$. To show $\eta \geq \kappa$, we calculate η as follows.

$$\begin{aligned}
\eta &= \eta_{a,g} + \eta_{b,g} + \eta_{ab,f} \\
&\overset{(a)}{=} n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] \\
&\quad + n_1[I(V_A, V_B; X_A, Y_A, X_B, Y_B) + 2\alpha] \\
&= n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_1 I(V_A; X_A, Y_A, X_B, Y_B) \\
&\quad + n_1 I(V_B; X_A, Y_A, X_B, Y_B|V_A) + 2n_1\alpha \\
&\overset{(b)}{=} n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_1 I(V_A; X_B, Y_B) \\
&\quad + n_1 I(V_A; X_A, Y_A|X_B, Y_B) + n_1 I(V_B; X_A, Y_A|V_A) + n_1 I(V_B; X_B, Y_B|X_A, Y_A) + 2n_1\alpha \\
&\overset{(c)}{=} n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_1 I(V_A; X_B, Y_B) \\
&\quad + n_{2,a2} I(W_{1A}; X_B, Y_B) + n_1 I(V_B; X_A, Y_A|V_A) + n_{2,b2} I(W_{1B}; X_A, Y_A) - 4n_1\alpha \\
&= n_2[I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A)] \\
&\quad + n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A)] - (n_{2,a1} + n_{2,b1})\beta - 4n_1\alpha.
\end{aligned} \tag{A.93}$$

Inequality (a) follows from (A.92a), equality (b) relies on the Markov chain (3.60a),

and equality (c) follows from (A.90) and (A.91). Comparing (A.93) with (A.87), for sufficiently small α and β, reveals $\eta \geq \kappa$.

The following is a list of sets, variables, and functions that are used in the SKE construction.

(i) Let $\mathcal{V}_{A,\epsilon}^{n_1}$ (resp. $\mathcal{V}_{B,\epsilon}^{n_1}$) be obtained by randomly and independently choosing $2^{\eta_{a,f}}$ (resp. $2^{\eta_{b,f}}$) ϵ-typical sequences from $\mathcal{V}_A^{n_1}$ (resp. $\mathcal{V}_B^{n_1}$).

(ii) Let $\mathfrak{f}_A : \mathcal{V}_{A,\epsilon}^{n_1} \to \mathcal{F}_A = [2^{\eta_{a,f}}]$ and $\mathfrak{f}_B : \mathcal{V}_{B,\epsilon}^{n_1} \to \mathcal{F}_B = [2^{\eta_{b,f}}]$ be arbitrary bijective mappings.

(iii) Let $\{\mathcal{V}_{A,\epsilon,i}^{n_1}\}_{i=1}^{2^{\eta_{a,t}}}$ be a partition of $\mathcal{V}_{A,\epsilon}^{n_1}$ into $2^{\eta_{a,t}}$ equal-sized parts. Define the function $\mathfrak{t}_A : \mathcal{V}_{A,\epsilon}^{n_1} \to \mathcal{T}_A = [2^{\eta_{a,t}}]$ such that, for any input in $\mathcal{V}_{A,\epsilon,i}^{n_1}$, it outputs i. Similarly define the partition $\{\mathcal{V}_{i,B,\epsilon}^{n_1}\}_{i=1}^{2^{\eta_{b,t}}}$ and the function $\mathfrak{t}_B$.

(iv) Let $\{\mathcal{T}_{A,i}\}_{i=1}^{2^{\eta_{a,t,2}}}$ be a partition of $\mathcal{T}_A$ into $2^{\eta_{a,t,2}}$ equal-sized parts; each of size $2^{\eta_{a,t,1}}$. Label elements of $\mathcal{T}_{A,i}$ by $\mathcal{T}_{A,i} = \{t_{A,i,j}\}_{j=1}^{\eta_{a,t,1}}$. Define the index function $\mathfrak{t}_{A,indx} : \mathcal{T}_A \to [2^{\eta_{a,t,2}}] \times [2^{\eta_{a,t,1}}]$ such that $\mathfrak{t}_{A,indx}(t) = (i,j)$, if t is labeled by $t_{A,i,j}$. Similarly define the partition $\{\mathcal{T}_{B,i}\}_{i=1}^{2^{\eta_{b,t,2}}}$ and the function $\mathfrak{t}_{B,indx}$.

(v) Let $\mathcal{G}_A = [2^{\eta_{a,g}}]$. In analogy to $\mathcal{T}_A$, let $\{\mathcal{G}_{A,i}\}_{i=1}^{2^{\eta_{a,g,2}}}$ be a partition of $\mathcal{G}_A$, where $\mathcal{G}_{A,i} = \{g_{A,i,j}\}_{j=1}^{2^{\eta_{a,g,1}}}$. Define the index function $\mathfrak{g}_{A,indx} : \mathcal{G}_A \to [2^{\eta_{a,g,2}}] \times [2^{\eta_{a,g,1}}]$ such that $\mathfrak{g}_{A,indx}(g) = (i,j)$, if g is labeled by $g_{A,i,j}$. Similarly, define $\mathcal{G}_B = [2^{\eta_{b,g}}]$, the partition $\{\mathcal{G}_{B,i}\}_{i=1}^{2^{\eta_{b,g,2}}}$, and the function $\mathfrak{g}_{B,indx}$.

(vi) Define the code book $\mathcal{C}_{2A}$ as the collection of $2^{\eta_{a,g,2}+\eta_{a,t,2}}$ codewords $\{w_{2A,i,i'}^{n_2} : i \in [2^{\eta_{a,g,2}}],\ i' \in [2^{\eta_{a,t,2}}]\}$, where each codeword $w_{2A,i,i'}^{n_2}$ is of length n_2 and is independently generated according to the distribution

$$\prod_{l=1}^{n_2} p(W_{2A} = w_{2A,i,i'}(l)).$$

Similarly, define the code book $\mathcal{C}_{2B} = \{w^{n_2}_{2B,i,i'} : \ i \in [2^{\eta_{b,g,2}}], \ i' \in [2^{\eta_{b,t,2}}]\}$.

(vii) For each codeword $w^{n_2}_{2A,i,i'}$, define the code book $\mathcal{C}_{1A}(w^{n_2}_{2A,i,i'})$ as the collection of $2^{\eta_{a,g,1}+\eta_{a,t,1}}$ words

$\{w^{n_2}_{1A,i,i',j,j'} : \ j \in [2^{\eta_{a,g,1}}], \ j' \in [2^{\eta_{a,t,1}}]\}$, where each codeword $w^{n_2}_{1A,i,i',j,j'}$ is of length n_2 and is independently generated according to the distribution

$$\prod_{l=1}^{n_2} p(W_{1A} = w_{1A,i,i',j,j'}(l) | W_{2A} = w_{2A,i,i'}(l)).$$

The code book $\mathcal{C}_{1A}$ is the set of all code books $\mathcal{C}_{1A}(w^{n_2}_{2A,i,j})$ and hence includes $2^{\eta_{a,g}+\eta_{a,t}}$ codewords. Similarly, define the code books $\mathcal{C}_{1B}(w^{n_2}_{2B,i,i'}) = \{w^{n_2}_{1B,i,i',j,j'} : \ j \in [2^{\eta_{b,g,1}}], \ j' \in [2^{\eta_{b,t,1}}]\}$ and the code book $\mathcal{C}_{1B}$ of size $2^{\eta_{b,g}+\eta_{b,t}}$.

(viii) Let $Enc_A : \mathcal{G}_A \times \mathcal{T}_A \to \mathcal{W}^{n_2}_{1A}$ be an encoding function such that $Enc(g,t) = w^{n_2}_{1A,i,i',j,j'}$, using the above code books, where $(i,j) = \mathfrak{g}_{indx}(g)$ and $(i',j') = \mathfrak{t}_{A,indx}(t)$. Similarly, define the encoding function $Enc_B : \mathcal{G}_B \times \mathcal{T}_B \to \mathcal{W}^{n_2}_{1B}$.

(ix) Let DMC_{W_A} and DMC_{W_B} be DMCs, representing $W_{1A} \to X_A$ and $W_{1B} \to X_B$, which are specified by $P_{X_A|W_{1A}}$ and $P_{X_B|W_{1B}}$, respectively.

(x) Let $\{\mathcal{K}_s\}_{s=1}^{2^\kappa}$ be a partition of $\mathcal{F}_A \times \mathcal{G}_A \times \mathcal{F}_B \times \mathcal{G}_B$ into equal-sized parts of size 2^γ. Define the key derivation function $\phi : \mathcal{F}_A \times \mathcal{G}_A \times \mathcal{F}_B \times \mathcal{G}_B \to [2^\kappa]$ such that, for any input in $\mathcal{K}_s$, it outputs s.

Protocol description.

Common randomness generation. Alice and Bob generate i.i.d. n_1-sequences $\mathbf{X}_A^{:1}$ and $\mathbf{X}_B^{:1}$ according to the distributions P_{X_A} and P_{X_B}, respectively, and send them in the first communication round. They receive the n_1-sequences $\mathbf{Y}_A^{:1}$ and $\mathbf{Y}_B^{:1}$, respectively, while Eve receives $\mathbf{Y}_E^{:1}$. Alice searches in $\mathcal{V}^{n_1}_{A,\epsilon}$ to find a (not necessarily unique) sequence $V_A^{n_1}$ such

that $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $V_A^{n_1}$ are ϵ-jointly typical w.r.t. $P_{(X_A,Y_A),V_A}$. Similarly, Bob searches for a sequence $V_B^{n_1}$ such that $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ and $V_B^{n_1}$ are ϵ-jointly typical w.r.t. $P_{(X_B,Y_B),V_B}$. A party that fails in finding such a sequence returns a NULL.

Assuming no NULL is returned, Alice computes $T_A = \mathfrak{t}_A(V_A^{n_1})$ and selects uniformly at random $G_A \in \mathcal{G}_A$. She calculates $(T_{A,2}, T_{A,1}) = \mathfrak{t}_{A,indx}(T_A)$ and $(G_{A,2}, G_{A,1}) = \mathfrak{g}_{A,indx}(G_A)$, and uses them to calculate $W_{1A}^{n_2} = Enc(G_A, T_A)$. Similarly Bob computes $T_B = \mathfrak{t}_B(V_B^{n_1})$, selects uniformly at random $G_B \in \mathcal{G}_B$, calculates $(T_{B,2}, T_{B,1}) = \mathfrak{t}_{B,indx}(T_B)$, $(G_{B,2}, G_{B,1}) = \mathfrak{g}_{B,indx}(G_B)$, and then $W_{1B}^{n_2} = Enc(G_B, T_B)$. Alice and Bob input $W_{1A}^{n_2}$ and $W_{1B}^{n_2}$ to the DMCs DMC_{W_A} and DMC_{W_B} to obtain and send the n_2 sequences $\mathbf{X}_A^{:2}$ and $\mathbf{X}_B^{:2}$ in the second communication round, respectively. Alice, Bob, and Eve receive the n_2-sequences $\mathbf{Y}_A^{:2}$, $\mathbf{Y}_B^{:2}$, and $\mathbf{Y}_E^{:2}$, respectively.

Alice searches for a "unique" codeword $\hat{W}_{1B}^{n_2} \in \mathcal{C}_{1B}$ such that $(\mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})$ and $\hat{W}_{1B}^{n_2}$ are ϵ-jointly typical w.r.t. $P_{(X_A,Y_A),W_{1B}}$. Alice returns a NULL if no such a sequence is found; otherwise, she obtains $(\hat{G}_B, \hat{T}_B)$ such that $Enc_B(\hat{G}_B, \hat{T}_B) = \hat{W}_{1B}^{n_2}$, and then searches for a "unique" codeword $\hat{V}_B^{n_1} \in \mathcal{V}_{\hat{T}_B,\epsilon}^{n_1}$ such that $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $\hat{V}_B^{n_1}$ are ϵ-jointly typical w.r.t. $P_{(X_A,Y_A),V_B}$; she returns a NULL if no such a sequence is found. Bob follows a similar approach to obtain $\hat{W}_{1A}^{n_2}$, $(\hat{G}_A, \hat{T}_A)$, and $\hat{V}_A^{n_1}$.

Key derivation. The secret key is $S = \phi(F_A, G_A, F_B, G_B)$. Alice computes $S_A = \phi(F_A, G_A, \hat{F}_B, \hat{G}_B)$, where $F_A = \mathfrak{f}_A(V_A^{n_1})$ and $\hat{F}_B = \mathfrak{f}_B(\hat{V}_B^{n_1})$. Similarly, Bob computes $S_A = \phi(\hat{F}_A, \hat{G}_A, F_B, G_B)$, where $\hat{F}_A = \mathfrak{f}_A(\hat{V}_A^{n_1})$ and $F_B = \mathfrak{f}_B(V_A^{n_1})$. Note that $\hat{G}_A$ and $\hat{G}_B$ have been obtained in the decoding phase.

Protocol analysis.

Randomness analysis, proving (3.3c). First we calculate the quantity $H(V_A^{n_1}, V_B^{n_1})$ to be

used in the sequel. From AEP for V_A, for every $\mathbf{u} \in \mathcal{V}_{A,\epsilon}^{n_1}$, we have

$$\begin{aligned}\Pr\{V_A^{n_1} = \mathbf{u}\} &\leq \sum_{((\mathbf{x},\mathbf{y}),\mathbf{u}):\ \epsilon-\text{jointly-typical}} \Pr\{(X_A^{n_1}, Y_A^{n_1}) = (\mathbf{x},\mathbf{y})\} \\ &\leq 2^{n_1[H(X_A,Y_A|V_A)+2\epsilon]} 2^{-n_1[H(X_A,Y_A)-\epsilon]} = 2^{-n_1[I(V_A;X_A,Y_A)-3\epsilon]}. \quad \text{(A.94)}\end{aligned}$$

Note that $V_A^{n_1}$ and $V_B^{n_1}$ are chosen to be ϵ-jointly-typical to $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$, respectively. On the other hand, due to AEP, for large enough n_1, $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ are ϵ-jointly-typical with probability arbitrarily close to 1. This implies that $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ and $V_A^{n_1}$ are ϵ-jointly-typical with probability arbitrarily close to 1. So, for every $\mathbf{u} \in \mathcal{V}_{A,\epsilon}^{n_1}$ and $\mathbf{u}' \in \mathcal{V}_{B,\epsilon}^{n_1}$, we can write

$$\begin{aligned}\Pr\{V_B^{n_1} = \mathbf{u}'|V_A^{n_1} = \mathbf{u}\} &\leq \sum_{((\mathbf{x},\mathbf{y}),\mathbf{u}',\mathbf{u}'):\ \epsilon-\text{jointly-typical}} \Pr\{(X_B^{n_1}, Y_B^{n_1}) = (\mathbf{x},\mathbf{y})|V_A^{n_1} = \mathbf{u})\} \\ &\leq 2^{n_1[H(X_B,Y_B|V_B,V_A)+2\epsilon]} 2^{-n_1[H(X_B,Y_B|V_A)-\epsilon]} = 2^{-n_1[I(V_B;X_B,Y_B|V_A)-3\epsilon]}. \quad \text{(A.95)}\end{aligned}$$

From (A.94) and (A.95), we have for all $\mathbf{u}$ and $\mathbf{u}'$

$$\begin{aligned}\Pr\{V_A^{n_1} = \mathbf{u} \wedge V_B^{n_1} = \mathbf{u}'\} &\leq 2^{-n_1[I(V_A;X_A,Y_A)+I(V_B;X_B,Y_B|V_A)-6\epsilon]} \\ &\overset{(a)}{=} 2^{-n_1[I(V_A,V_B;X_A,Y_A,X_B,Y_B)-6\epsilon]} \\ &\overset{(b)}{=} 2^{-\eta_{ab,f}+2n_1\alpha+6n_1\epsilon} \\ &< 2^{-\eta_{ab,f}+4n_1\alpha} \quad \text{(A.96)} \\ \Rightarrow H(V_A^{n_1}, V_B^{n_1}) &> \eta_{ab,f} - 4n_1\alpha. \quad \text{(A.97)}\end{aligned}$$

Equality (a) is due to the Markov chain (3.60a), and equality (b) follows from (A.92g). Furthermore, for large enough n_1, with probability arbitrarily close to 1 the following happens. $V_A^{n_1}$ and $V_B^{n_1}$ become jointly typical and since the sets $\mathcal{V}_{A,\epsilon}^{n_1}$ and $\mathcal{V}_{B,\epsilon}^{n_1}$ are obtained independently according to distributions P_{V_A} and P_{V_B}, respectively, at most $2^{\eta_{a,f}+\eta_{b,f}-n_1[I(V_A;V_B)-3\epsilon]}$ ϵ-jointly typical sequences exist in $\mathcal{V}_{A,\epsilon}^{n_1} \times \mathcal{V}_{B,\epsilon}^{n_1}$, and this implies

that

$$\begin{aligned} H(V_A^{n_1}, V_B^{n_1}) &\leq \eta_{a,f} + \eta_{b,f} - n_1[I(V_A;V_B) - 3\epsilon] \\ &\overset{(a)}{=} n_1[I(V_A;X_A,Y_A) + \alpha] + n_1[I(V_B;X_B,Y_B) + \alpha] - n_1[I(V_A;V_B) - 3\epsilon] \\ &\overset{(b)}{=} n_1[I(V_A,V_B;X_A,Y_A,X_B,Y_B) + 2\alpha + 3\epsilon] \\ &\overset{(c)}{=} \eta_{ab,f} + 3n_1\epsilon. \end{aligned} \tag{A.98}$$

Inequality (a) and equality (c) follow from (A.92a), and equality (b) is due to the Markov chain (3.60a). Since F_A and F_B are bijective functions of $V_A^{n_1}$ and $V_B^{n_1}$ (see (ii) and the encoding phase), we can write for all f_A and f_B

$$\Pr\{F_A = f_A \wedge F_B = f_B\} < 2^{-\eta_{ab,f}+4n_1\alpha}, \tag{A.99}$$

$$\eta_{ab,f} - 4n_1\alpha \leq H(F_A, F_B) \leq \eta_{ab,f} - 3n_1\epsilon. \tag{A.100}$$

In addition, G_A and G_B are selected uniformly at random from the sets $\mathcal{G}_A$ and $\mathcal{G}_B$, respectively. Hence,

$$\forall g_A \in \mathcal{G}_A: \quad \Pr\{G_A = g_A\} = 2^{-\eta_{a,g}} \Rightarrow H(G_A) = \eta_{a,g}, \tag{A.101}$$

$$\forall g_B \in \mathcal{G}_B: \quad \Pr\{G_B = g_B\} = 2^{-\eta_{b,g}} \Rightarrow H(G_B) = \eta_{b,g}. \tag{A.102}$$

There are 2^κ choices for the key S (see (x) and the key derivation phase) and, for every $s \in [2^\kappa]$, the probability that $S = s$ equals to the probability that $(F_A, G_A, F_B, G_B) \in \mathcal{K}_s$, i.e.,

$$\begin{aligned} \Pr(S = s) &= \sum_{(f_A,g_A,f_B,g_B)\in\mathcal{K}_s} \Pr\{F_A = f_A \wedge F_B = f_B \wedge G_A = g_A \wedge G_B = g_B\} \\ &\overset{(a)}{=} \sum_{(f_A,g_A,f_B,g_B)\in\mathcal{K}_s} \Pr\{G_A = g_A\} \Pr\{G_B = g_B\} \Pr\{F_A = f_A \wedge F_B = f_B\} \\ &\leq 2^\gamma . 2^{-\eta_{a,g}} . 2^{-\eta_{b,g}} . 2^{-\eta_{ab,f}+4n_1\alpha} \\ &= 2^{\gamma-\eta+4n_1\alpha} \\ \Rightarrow H(S) &\geq \eta - \gamma - 4n_1\alpha = \kappa - 4n_1\alpha. \end{aligned}$$

Equality (a) follows from the fact that G_A and G_B are chosen independently by Alice and Bob, respectively, and the rest follows from (A.92a). We conclude that

$$\frac{H(S)}{n} = \frac{H(S)}{n_1+n_2} \geq \frac{\kappa - 4n_1\alpha}{n_1+n_2} \geq R_{sk} - 4\alpha > R_{sk} - \delta.$$

by selecting $\alpha < \delta/4$.

Reliability analysis, proving (3.3a). To prove reliability means to prove that Alice and Bob will calculate the same valid shared key with probability arbitrarily close to 1. This happens if both encoding and decoding phases are successful without any party returning a NULL. We discuss each phase separately as follows.

Since $\log|\mathcal{V}_{A,\epsilon}| = \eta_{a,f} = n_1[I(V_A; X_A, Y_A) + \alpha]$, for $\epsilon > 0$ and large enough n_1, by choosing α to be small but sufficiently larger than ϵ, from AEP both $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ and $V_A^{n_1}$ are ϵ-jointly-typical with probability arbitrarily close to 1; similarly $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ and $V_B^{n_1}$ are ϵ-jointly-typical, and so the encoding phase is successful. The decoding phase includes two levels of decoding. In the first level, Alice decodes $(\mathbf{X}_A^{:2}, \mathbf{Y}_A^{:2})$ to $\hat{W}_{1B}^{n_2} \in \mathcal{C}_{1B}$ and Bob decodes $(\mathbf{X}_B^{:2}, \mathbf{Y}_B^{:2})$ to $\hat{W}_{1A}^{n_2} \in \mathcal{C}_{1A}$. If $\log|\mathcal{C}_{1B}|$ (resp. $\log|\mathcal{C}_{1A}|$) is less than $n_2 I(W_{1B}; X_A, Y_A)$ (resp. $n_2 I(W_{1A}; X_B, Y_B)$) then, from joint-AEP, the decoding error probabilities are arbitrarily close to zero. The two inequalities are shown below (see (vii) and (A.92a)).

$$\begin{aligned}
\log|\mathcal{C}_{1B}| &= \eta_{b,g} + \eta_{b,t} = n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] + n_{2,b2}[I(W_{1B}; X_A, Y_A) - \beta] \\
&= n_2[I(W_{1B}; X_A, Y_A) - \beta] < n_2[I(W_{1B}; X_A, Y_A) - 3\epsilon], \\
\log|\mathcal{C}_{1A}| &= \eta_{a,g} + \eta_{a,t} = n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] + n_{2,a2}[I(W_{1A}; X_B, Y_B) - \beta] \\
&= n_2[I(W_{1A}; X_B, Y_B) - \beta] < n_2[I(W_{1A}; X_B, Y_B) - 3\epsilon].
\end{aligned}$$

In the second level of decoding, Alice decodes $(\mathbf{X}_A^{:1}, \mathbf{Y}_A^{:1})$ to $\hat{V}_B^{n_1} \in \mathcal{V}_{\hat{T}_B,\epsilon}^{n_1}$ and Bob decodes $(\mathbf{X}_B^{:1}, \mathbf{Y}_B^{:1})$ to $\hat{V}_A^{n_1} \in \mathcal{V}_{\hat{T}_A,\epsilon}^{n_1}$. Given that the first level of decoding is successful, if $\log|\mathcal{V}_{\hat{T}_B,\epsilon}^{n_1}|$ (resp. $\log|\mathcal{V}_{\hat{T}_A,\epsilon}^{n_1}|$) is less than $n_1 I(V_B; X_A, Y_A)$ (resp. $n_2 I(V_A; X_B, Y_B)$) then,

again from joint-AEP, the decoding error probabilities are arbitrarily close to zero. We have (see (iv) and (A.92a))

$$\begin{aligned}
\log|\mathcal{V}^{n_1}_{\hat{T}_A,\epsilon}| = \eta_{a,f} - \eta_{a,t} &= n_1[I(V_A;X_A,Y_A)+\alpha] - n_{2,a2}[I(W_{1A};X_B,Y_B)-\beta] \\
&\overset{(a)}{=} n_1[I(V_A;X_B,Y_B)+I(V_A;X_A,Y_A|X_B,Y_B)+\alpha] - n_{2,a2}[I(W_{1A};X_B,Y_B)-\beta] \\
&\overset{(b)}{=} n_1 I(V_A;X_B,Y_B) + n_{2,a2}I(W_{1A};X_B,Y_B) - n_{2,a2}I(W_{1A};X_B,Y_B) - 2n_1\alpha + n_{2,a2}\beta \\
&= n_1 I(V_A;X_B,Y_B) - 2n_1\alpha + n_{2,a2}\beta \\
&\leq n_1 I(V_A;X_B,Y_B) - n_1\alpha \\
&< n_1[I(V_A;X_B,Y_B)-3\epsilon].
\end{aligned}$$

Equality (a) is due to the Markov chain (3.60a), and equality (b) follows from (A.90). Similarly, we can show that

$$\log|\mathcal{V}^{n_1}_{\hat{T}_B,\epsilon}| \quad < n_1[I(V_B;X_A,Y_A)-3\epsilon].$$

Hence, for sufficiently small ϵ we conclude that

$$\Pr(S_A = S_B = S) \geq \Pr\left(\hat{F}_A = F_A \wedge \hat{G}_A = G_A \wedge \hat{F}_B = F_B \wedge \hat{G}_B = G_B\right) > 1-\phi \quad \text{(A.103)}$$

Secrecy analysis, proving (3.3b). We shall show that $H(S|\mathbf{Y}^{:1}_E, \mathbf{Y}^{:2}_E)/H(S)$ is arbitrarily close to 1. First, we discuss the quantities $H(T_A,T_B)$, $H(T_{A,2},T_{B,2})$, $H(G_{A,2})$ and $H(G_{B,2})$ that are used in the proof. From the encoding phase, for all $(t,t') \in \mathcal{T}_A \times \mathcal{T}_B$

(see (iv) and (A.92a)),

$$\begin{aligned}
\Pr\{T_A = t \wedge T_B = t'\} &= \sum_{\mathbf{u}\in\mathcal{V}^{n_1}_{t,A,\epsilon},\ \mathbf{u}'\in\mathcal{V}^{n_1}_{t',B,\epsilon}} \Pr(V_A^{n_1} = \mathbf{u} \wedge V_B^{n_1} = \mathbf{u}') \\
&\overset{(a)}{\leq} 2^{\eta_{a,f}-\eta_{a,t}} 2^{\eta_{b,f}-\eta_{b,t}} 2^{-\eta_{ab,f}+4n_1\alpha} \\
&= 2^{\eta_{a,f}+\eta_{b,f}-\eta ab,f}.2^{-\eta_{a,t}-\eta_{b,t}+4n_1\alpha} \\
&= 2^{n_1[I(V_A;X_A,Y_A)+\alpha]+n_1[I(V_B;X_B,Y_B)+\alpha]-n_1[I(V_A,V_B;X_A,Y_A,X_B,X_B)+2\alpha]}.2^{-\eta_{a,t}-\eta_{b,t}+4n_1\alpha} \\
&\overset{(b)}{=} 2^{n_1[I(V_A;X_A,Y_A)+I(V_B;X_B,Y_B)-I(V_A;X_A,Y_A)-I(V_B;X_B,X_B|V_A)]}.2^{-\eta_{a,t}-\eta_{b,t}+4n_1\alpha} \\
&= 2^{-\eta_{a,t}-\eta_{b,t}+n_1 I(V_A;V_B)+4n_1\alpha}. \qquad \text{(A.104)}
\end{aligned}$$

Inequality (a) is obtained from (A.96) and equality (b) is due to the Markov chain (3.60a). This follows that

$$\eta_{a,t} + \eta_{b,t} - n_1 I(V_A;V_B) - 4n_1\alpha \leq H(T_A,T_B) \leq \eta_{a,t} + \eta_{b,t} - n_1 I(V_A;V_B) + 3n_1\epsilon, \quad \text{(A.105)}$$

where the upper bound holds since following the argument before (A.98), there are at most $2^{\eta_{a,t}+\eta_{b,t}-n_1 I(V_A;V_B)+3n_1\epsilon}$ sequences in $\mathcal{T}_A \times \mathcal{T}_B$ that correspond to the ϵ-jointly typical sequences in $\mathcal{V}^{n_1}_{A,\epsilon} \times \mathcal{V}^{n_1}_{B,\epsilon}$. Similarly, for all $(i,i') \in [2^{\eta_{a,t,2}}] \times [2^{\eta_{b,t,2}}]$ (see (v) and (A.92a)),

$$\begin{aligned}
\Pr\{T_{A,2} = i \wedge T_{B,2} = i'\} &= \Pr\{T_A \in \mathcal{T}_{A,i} \wedge T_B \in \mathcal{T}_{B,i'}\} \\
&= \sum_{j=1}^{\eta_{a,t,1}} \sum_{j'=1}^{\eta_{b,t,1}} \Pr\{T_A = t_{A,i,j} \wedge T_B = t_{B,i',j'}\} \\
&\leq 2^{\eta_{a,t,1}+\eta_{b,t,1}} 2^{-\eta_{a,t}-\eta_{b,t}+n_1 I(V_A;V_B)+4n_1\alpha} \\
&= 2^{-\eta_{a,t,2}-\eta_{b,t,2}+n_1 I(V_A;V_B)+4n_1\alpha} \qquad \text{(A.106)} \\
\Rightarrow H(T_{A,2},T_{B,2}) &\geq \eta_{a,t,2} + \eta_{b,t,2} - n_1 I(V_A;V_B) - 4n_1\alpha \qquad \text{(A.107)}
\end{aligned}$$

Since G_A and G_B have uniform distributions, $G_{A,2}$ and $G_{B,2}$ are uniformly distributed in the sets $[2^{\eta_{a,g,2}}]$ and $[2^{\eta_{b,g,2}}]$, respectively, and we can write

$$H(G_{A,2}) = \eta_{a,g,2}, \qquad H(G_{B,2}) = \eta_{b,g,2}. \qquad \text{(A.108)}$$

In the following, we prove that $H(S|\mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2})$ is close to $H(S)$. We calculate a lower bound on $H(S|\mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2})$ and next we use this to find a lower bound on $H(S|\mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2})/H(S)$ that is arbitrarily close to 1.

$$\begin{aligned}
H(S|\mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) &\geq H(S|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) \\
&= H(S, F_A, G_A, F_B, G_B|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) \\
&\quad -H(F_A, G_A, F_B, G_B|S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) \\
&= H(F_A, G_A, F_B, G_B|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) \\
&\quad -H(F_A, G_A, F_B, G_B|S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) \\
&= H(F_A, G_A, F_B, G_B|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad -I(F_A, G_A, F_B, G_B; \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}|T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad -H(F_A, G_A, F_B, G_B|S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}). \qquad \text{(A.109)}
\end{aligned}$$

We calculate each of the above three terms separately in the following. The first term

in (A.109) is written as

$$
\begin{aligned}
H(F_A, G_A, F_B, G_B | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) &\overset{(a)}{=} H(F_A, F_B | T_{A,2}, T_{B,2}) + H(G_A | G_{A,2}) + H(G_B | G_{B,2}) \\
&\overset{(b)}{=} H(F_A, F_B) + H(G_A) + H(G_B) - H(T_{A,2}, T_{B,2}) - H(G_{A,2}) - H(G_{B,2}) \qquad \text{(A.110)} \\
&\overset{(c)}{\geq} \eta_{ab,f} - 4n_1\alpha + \eta_{a,g} + \eta_{b,g} - [\eta_{a,t,2} + \eta_{b,t,2}] - \eta_{a,g,2} - \eta_{b,g,2} \\
&\overset{(d)}{\geq} n_1 I(V_A, V_B; X_A, Y_A, X_B, Y_B) - 2n_1\alpha + n_{2,a1}[I(W_{1A}; X_B, Y_B) - \beta] \\
&\quad + n_{2,b1}[I(W_{1B}; X_A, Y_A) - \beta] - [n_{2,a2} I(W_{2A}; X_B, Y_B) + n_{2,b2} I(W_{2B}; X_A, Y_A)] \\
&\quad - n_{2,a1} I(W_{2A}; X_B, Y_B) - n_{2,b1} I(W_{2B}; X_A, Y_A) \\
&= n_1 I(V_A, V_B; X_A, Y_A, X_B, Y_B) + n_{2,a1} I(W_{1A}; X_B, Y_B) + n_{2,b1} I(W_{1B}; X_A, Y_A) \\
&\quad - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) - 2n_1\alpha - 2n_2\beta \\
&\overset{(e)}{=} n_1[I(V_A; X_B, Y_B) + I(V_A; X_A, Y_A | X_B, Y_B) + I(V_B; X_A, Y_A | V_A) \\
&\quad + I(V_B; X_B, Y_B | X_A, Y_A)] + n_{2,a1} I(W_{1A}; X_B, Y_B) + n_{2,b1} I(W_{1B}; X_A, Y_A) \\
&\quad - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) - 4n_1\alpha \\
&\overset{(f)}{=} n_1 I(V_A; X_B, Y_B) + n_{2,a2} I(W_{1A}; X_B, Y_B) + n_1 I(V_B; X_A, Y_A | V_A) \\
&\quad + n_{2,b2} I(W_{1B}; X_A, Y_A) - 6n_1\alpha + n_{2,a1} I(W_{1A}; X_B, Y_B) \\
&\quad + n_{2,b1} I(W_{1B}; X_A, Y_A) - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) - 4n_1\alpha \\
&= n_1 I(V_A; X_B, Y_B) + n_1 I(V_B; X_A, Y_A | V_A) + n_2 I(W_{1A}; X_B, Y_B) + n_2 I(W_{1B}; X_A, Y_A) \\
&\quad - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) - 10n_1\alpha \\
&\overset{(g)}{=} n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A | V_A)] \\
&\quad + n_2[I(W_{1A}; X_B, Y_B | W_{2A}) + I(W_{1B}; X_A, Y_A | W_{2B})] - 10n_1\alpha. \qquad \text{(A.111)}
\end{aligned}
$$

Equality (a) holds since $(F_A, F_B, T_{A,2}, T_{B,2})$, $(G_A, G_{A,2})$, and $(G_B, G_{B,2})$ are independent of each other, and equality (b) is due to the fact that $T_{A,2}$, $T_{B,2}$, $G_{A,2}$, $G_{B,2}$ are deterministic functions of F_A, F_B, G_A, G_B, respectively (see the encoding phase). Inequality (c) follows from (A.100), (A.101), (A.102), (A.107), and (A.108). Inequality (d) follows from (A.92a), equality (e) relies on the Markov chain (3.60a), equality (f) follows from (A.90) and (A.91), and equality (g) is due to the Markov chains (3.60b) and (3.60c). The

second term in (A.109) can be written as

$$
\begin{aligned}
&I(F_A, G_A, F_B, G_B; \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&= I(F_A, G_A, F_B, G_B; \mathbf{Y}_E^{:1} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad + I(F_A, G_A, F_B, G_B; \mathbf{Y}_E^{:2} | \mathbf{Y}_E^{:1}, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\overset{(a)}{=} I(V_A^{n_1}, G_A, V_B^{n_1}, G_B; \mathbf{Y}_E^{:1} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad + I(V_A^{n_1}, T_A, G_A, V_B^{n_1}, T_B, G_B; \mathbf{Y}_E^{:2} | \mathbf{Y}_E^{:1}, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\overset{(b)}{=} I(V_A^{n_1}, G_A, V_B^{n_1}, G_B; \mathbf{Y}_E^{:1} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad + I(T_A, G_A, T_B, G_B; \mathbf{Y}_E^{:2} | \mathbf{Y}_E^{:1}, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\overset{(c)}{\leq} I(V_A^{n_1}, G_A, V_B^{n_1}, G_B; \mathbf{Y}_E^{:1} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad + I(T_A, G_A, T_B, G_B; \mathbf{Y}_E^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\overset{(d)}{\leq} I(V_A^{n_1}, V_B^{n_1}; \mathbf{Y}_E^{:1}) + I(T_A, G_A, T_B, G_B; \mathbf{Y}_E^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&= I(V_A^{n_1}, V_B^{n_1}; \mathbf{Y}_E^{:1}) + \min\{H(T_A, G_A, T_B, G_B | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) \\
&\quad , I(T_A, G_A, T_B, G_B; \mathbf{Y}_E^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2})\} \\
&\overset{(e)}{=} I(V_A^{n_1}, V_B^{n_1}; \mathbf{Y}_E^{:1}) + \min\{[H(T_A, T_B | T_{A,2}, T_{B,2}) + H(G_A | G_{A,2}) + H(G_B | G_{B,2})] \\
&\quad , [H(\mathbf{Y}_E^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - H(\mathbf{Y}_E^{:2} | T_A, G_A, T_B, G_B, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2})]\} \\
&\overset{(f)}{=} I(V_A^{n_1}, V_B^{n_1}; \mathbf{Y}_E^{:1}) + \min\{[H(T_A, T_B) - H(T_{A,2}, T_{B,2}) + H(G_A) - H(G_{A,2}) \\
&\quad + H(G_B) - H(G_{B,2})] \, , [H(\mathbf{Y}_E^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - H(\mathbf{Y}_E^{:2} | T_A, G_A, T_B, G_B)]\} \\
&\overset{(g)}{\leq} I(V_A^{n_1}, V_B^{n_1}; \mathbf{Y}_E^{:1}) + \min\{[(\eta_{a,t} + \eta_{b,t} - n_1 I(V_A; V_B) + 3n_1\epsilon) \\
&\qquad -(\eta_{a,t,2} + \eta_{b,t,2} - n_1 I(V_A; V_B) - 4n_1\alpha) + \eta_{a,g} - \eta_{a,g,2} + \eta_{b,g} - \eta_{b,g,2}] \\
&\quad , [H(\mathbf{Y}_E^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - H(\mathbf{Y}_E^{:2} | T_A, G_A, T_B, G_B)]\} \\
&\overset{(h)}{=} I(V_A^{n_1}, V_B^{n_1}; \mathbf{Y}_E^{:1}) + \min\{[n_2 \left(I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A) - 2\beta\right) \\
&\quad -n_2 \left(I(W_{2A}; X_B, Y_B) + I(W_{2B}; X_A, Y_A)\right) + 5n_1\alpha] \\
&\qquad , [H(\mathbf{Y}_E^{:2} | T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}) - H(\mathbf{Y}_E^{:2} | T_A, G_A, T_B, G_B)]\} \\
&\overset{(i)}{\leq} n_1 I(V_A, V_B; Y_E) + \min\{[n_2(I(W_{1A}; X_B, Y_B | W_{2A}) + I(W_{1B}; X_A, Y_A | W_{2B})) + 3n_1\alpha] \\
&\qquad , [n_2 H(Y_E | W_{2A}, W_{2B}) - n_2 H(Y_E | W_{1A}, W_{1B})]\} \\
&\overset{(j)}{\leq} n_1 I(V_A, V_B; Y_E) + \min\{[n_2(I(W_{1A}; X_B, Y_B | W_{2A}) + I(W_{1B}; X_A, Y_A | W_{2B})) + 3n_1\alpha] \\
&\qquad , [n_2 I(W_{1A}, W_{1B}; Y_E | W_{2A}, W_{2B})]\}. \qquad \text{(A.112)}
\end{aligned}
$$

Equality (a) holds since F_A and F_B (resp. T_A and T_B) are bijective (resp. deterministic) functions of $V_A^{n_1}$ and $V_B^{n_1}$, respectively. Equality (b) and inequality (c) are due to $(\mathbf{Y}_E^{:1}, V_A^{n_1}, V_B^{n_1}) \leftrightarrow (T_A, G_A, T_B, G_B) \leftrightarrow \mathbf{Y}_E^{:2}$, and inequality (d) is due to

$$(T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, G_A, G_B) \leftrightarrow (V_A^{n_1}, V_B^{n_1}) \leftrightarrow \mathbf{Y}_E^{:1}.$$

Equality (e) holds since $(T_A, T_B, T_{A,2}, T_{B,2})$, $(G_A, G_{A,2})$, and $(G_B, G_{B,2})$ are independent of each other, and equality (b) holds since $T_{A,2}$, $T_{B,2}$, $G_{A,2}$, $G_{B,2}$ are deterministic functions of T_A, T_B, G_A, G_B, respectively. Inequality (g) follows from (A.101), (A.102), (A.105), (A.107), and (A.108), and equality (h) follows from (A.92a). Inequality (i) follows from AEP and the Markov chains (3.60b) and (3.60c), and inequality (j) is due to $(W_{2A}, W_{2B}) \leftrightarrow (W_{1A}, W_{1B}) \leftrightarrow Y_E$.

The third term in (A.109), i.e., $H(F_A, G_A, F_B, G_B | S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2})$ is discussed as follows. The knowledge of $S = s$ determines $\mathcal{K}_s$ where (F_A, G_A, F_B, G_B) is located. Furthermore, the knowledge of $(T_{A,2}, G_{A,2}) = (i, i')$ and $(T_{B,2}, G_{B,2}) = (j, j')$ gives respectively the codewords $w_{2A,i,i'}^{n_2} \in \mathcal{C}_{2A}$ and $w_{2B,j,j'}^{n_2} \in \mathcal{C}_{2B}$ that are used in the encoding phase. Define the code book

$$\mathcal{C}_s^e = \{(u_A^{n_1}, u_B^{n_1}, w_{1A}^{n_2}, w_{1B}^{n_2}) : (\mathfrak{f}_A(u_A^{n_1}), g_A, \mathfrak{f}_B(u_B^{n_1}), g_B) \in \mathcal{K}_s, w_{1A}^{n_2} = Enc_A(\mathfrak{t}_A(u_A^{n_1}), g_A),$$
$$w_{1B}^{n_2} = Enc_B(\mathfrak{t}_B(u_B^{n_1}), g_B), \;\; t_{A,2} = i, g_{A,2} = i', \;\; t_{B,2} = j, g_{B,2} = j'\}.$$

Given $(\mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2})$, one can search in $\mathcal{C}_s^e$ for a unique codeword $(\check{V}_A^{n_1}, \check{V}_B^{n_1}, \check{W}_{1A}^{n_2}, \check{W}_{1B}^{n_2})$ that is (ϵ, n_1)-bipartite jointly typical to $(\mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2})$ w.r.t. $(P_{(V_A,V_B),Y_E}, P_{(W_{1A},W_{1B}),Y_E})$; and return a NULL if no such a codeword is found. We have

$$|\mathcal{C}_s^e| = \frac{|\mathcal{K}_s|}{2^{\eta_{a,g,2}+\eta_{a,t,2}+\eta_{b,g,2}+\eta_{b,t,2}}} = 2^{\gamma-\eta_2},$$

where $\eta_2 = \eta_{a,g,2} + \eta_{a,t,2} + \eta_{b,g,2} + \eta_{b,t,2}$. If $\gamma - \eta_2 < n_1 I(V_A, V_B; Y_E) + n_2 I(W_{1A}, W_{1B}; Y_E)$ holds, then from bipartite joint-AEP, the error probability in the above jointly-typical decoding becomes arbitrarily small. We use the expression for η in (A.93) to calculate

$\eta - \eta_2$ as follows.

$$\begin{aligned}
\eta - \eta_2 &= \eta - \eta_{a,g,2} - \eta_{a,t,2} - \eta_{b,g,2} - \eta_{b,t,2} \\
&\overset{(a)}{\leq} n_2[I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A)] + n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A)] - 4n_1\alpha \\
&\quad - n_{2,a1} I(W_{2A}; X_B, Y_B) - n_{2,a2} I(W_{2A}; X_B, Y_B) - n_{2,b1} I(W_{2B}; X_A, Y_A) - n_{2,b2} I(W_{2B}; X_A, Y_A) \\
&= n_2[I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A)] + n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A)] - 4n_1\alpha \\
&\quad - n_2 I(W_{2A}; X_B, Y_B) - n_2 I(W_{2B}; X_A, Y_A) \\
&\overset{(b)}{=} n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})] \\
&\quad + n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A)] - 4n_1\alpha.
\end{aligned}$$

Inequality (a) follows from (A.92a) and (A.93), and equality (b) is due to the Markov chains (3.60b) and (3.60c). We use the above to calculate $\gamma - \eta_2$ as follows.

$$\begin{aligned}
\gamma - \eta_2 &= \eta - \kappa - \eta_2 = [\eta - \eta_2] - (n_1 + n_2) R_{sk} \\
&\overset{(a)}{=} n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})] + n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A)] \\
&\quad - n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A) - I(V_A, V_B; Y_E)] - 4n_1\alpha \\
&\quad - n_2[I(W_{1B}; X_A, Y_A|W_{2B}) + I(W_{1A}; X_B, Y_B|W_{2A}) - I(W_{1A}, W_{1B}; Y_E|W_{2A}, W_{2B})]_+ \\
&\leq n_1 I(V_A, V_B; Y_E) + n_2 I(W_{1A}, W_{1B}; Y_E|W_{2A}, W_{2B}) - 4n_1\alpha \\
&\overset{(b)}{<} n_1 I(V_A, V_B; Y_E) + n_2 I(W_{1A}, W_{1B}; Y_E) - 12n\epsilon. \qquad \text{(A.113)}
\end{aligned}$$

The second and the third lines in equality (a) come from (A.87), and inequality (b) is due to $(W_{2A}, W_{2B}) \leftrightarrow (W_{1A}, W_{1B}) \leftrightarrow Y_E$. Let $\check{F}_A = \mathfrak{f}_A(\check{V}_A^{n_1})$, $\check{F}_B = \mathfrak{f}_B(\check{V}_B^{n_1})$, and $\check{G}_A$ and $\check{G}_B$ be chosen such that

$$\check{W}_{1A}^{n_2} = Enc_A(\mathfrak{t}_A(\check{V}_A^{n_1}), \check{G}_A), \qquad \text{and} \qquad \check{W}_{1B}^{n_2} = Enc_B(\mathfrak{t}_B(\check{V}_B^{n_1}), \check{G}_B).$$

From (A.113), we conclude that given $(S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2})$,

$$\Pr\{(\check{F}_A, \check{F}_B, \check{G}_A, \check{G}_B) \neq (F_A, G_A, F_B, G_B)\} \leq 2\epsilon,$$

and Fano's inequality gives

$$\begin{aligned}
H(F_A, G_A, F_B, G_B|S, T_{A,2}, G_{A,2}, T_{B,2}, G_{B,2}, \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) &\leq H(F_A, G_A, F_B, G_B|\check{F}_A, \check{F}_B, \check{G}_A, \check{G}_B) \\
&\leq h(2\epsilon) + 2\epsilon\eta = h(2\epsilon) + 2\epsilon\eta, \qquad \text{(A.114)}
\end{aligned}$$

where $h(\epsilon) = -\epsilon \log(\epsilon) - (1-\epsilon)\log(1-\epsilon)$ is the binary entropy function. Combining (A.109), (A.111), (A.112), and (A.114), one can write

$$
\begin{aligned}
H(S|\mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) &\geq n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A)] \\
&\quad + n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})] - n_1 I(V_A, V_B; Y_E) - 8n_1\alpha \\
&\quad - \min\{[n_2(I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B})) + 3n_1\alpha], \\
&\qquad\qquad [n_2 I(W_{1A}, W_{1B}; Y_E|W_{2A}, W_{2B})]\} - h(2\epsilon) - 2\epsilon\eta \\
&\geq n_1[I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A|V_A) - I(V_A, V_B; Y_E)] \\
&\quad + n_2[I(W_{1A}; X_B, Y_B|W_{2A}) + I(W_{1B}; X_A, Y_A|W_{2B}) - I(W_{1A}, W_{1B}; Y_E|W_{2A}, W_{2B})]_+ \\
&\quad - 11n_1\alpha - h(2\epsilon) - 2\epsilon\eta \\
&\overset{(a)}{=} (n_1 + n_2)R_{sk} - 11n_1\alpha - h(2\epsilon) - 2\epsilon\eta \\
&\overset{(b)}{=} \kappa - 11n_1\alpha - h(2\epsilon) - 2\epsilon\eta \\
&\geq H(S) - 11n_1\alpha - h(2\epsilon) - 2\epsilon\eta.
\end{aligned}
$$

Equalities (a) and (b) are due to (A.87) and (A.92h), respectively. The above implies that for arbitrarily small $\delta > 0$, by appropriately selecting the small constants α and ϵ we have $I(S; \mathbf{Y}_E^{:1}, \mathbf{Y}_E^{:2}) < \delta H(S)$. $\square$

A.12 Proof of Theorem 10: SK capacity upper bound, TWDMWC

We provide an upper bound on the SK rate that any possible SKE protocol can achieve. For arbitrary $\delta > 0$, let Π be an (R_{sk}, δ) t-round SKE protocol over TWDMWC, where in each communication round $1 \leq r \leq t$, Alice and Bob send sequences $\mathbf{X}_A^{:r}$, $\mathbf{X}_B^{:r}$ of length n_r over the channel and receive n_r-sequences $\mathbf{Y}_A^{:r}$, and $\mathbf{Y}_B^{:r}$ in return, respectively. Eve also receives the n_r-sequence $\mathbf{Y}_E^{:r}$. We denote the total number of channel uses by

$$
n = \sum_{r=1}^{t} n_r. \tag{A.115}
$$

According to Definition 27, the three conditions (3.3c)-(3.3b) are satisfied. Using Fano's inequality for (3.3a), we have

$$H(S|S_A) \leq h(\delta) + \delta H(S), \qquad H(S|S_B) \leq h(\delta) + \delta H(S) \tag{A.116}$$

Furthermore, the secrecy condition in (3.3b) can be written as

$$I(S; \mathbb{V}_E^{:t}) = H(S) - H(S|\mathbb{V}_E^{:t}) \leq \delta H(S). \tag{A.117}$$

Considering (A.116) and (A.117), we write the entropy of S as

$$\begin{aligned}
H(S) &= I(S; S_B) + H(S|S_B) + I(S; \mathbb{V}_E^{:t}) - I(S; \mathbb{V}_E^{:t}) \\
&\leq I(S; S_B|\mathbb{V}_E^{:t}) + H(S|S_B) + I(S; \mathbb{V}_E^{:t}) \\
&\leq I(S, S_A; S_B|\mathbb{V}_E^{:t}) + H(S|S_B) + I(S; \mathbb{V}_E^{:t}) \\
&= I(S_A; S_B|\mathbb{V}_E^{:t}) + I(S; S_B|S_A, \mathbb{V}_E^{:t}) + H(S|S_B) + I(S; \mathbb{V}_E^{:t}) \\
&\leq I(S_A; S_B|\mathbb{V}_E^{:t}) + H(S|S_A) + H(S|S_B) + I(S; \mathbb{V}_E^{:t}) \\
&\leq I(\mathbb{V}_A^{:t}; \mathbb{V}_B^{:t}|\mathbb{V}_E^{:t}) + 2h(\delta) + 3\delta H(S).
\end{aligned} \tag{A.118}$$

The first term above is written as follows (see 3.1 and Figure 3.1).

$$\begin{aligned}
&I(\mathbb{V}_A^{:t}; \mathbb{V}_B^{:t}|\mathbb{V}_E^{:t}) = I(\mathbf{X}_A^{:t}, \mathbf{Y}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t}) \\
&= I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, \mathbb{V}_B^{:t-1}|\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}, \mathbb{V}_E^{:t}) \\
&\overset{(a)}{\leq} I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{Y}_E^{:t}) \\
&= I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t}) + I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{Y}_B^{:t}|\mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1}, \mathbb{V}_E^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{Y}_E^{:t}) \\
&\overset{(b)}{\leq} I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t}) + I(\mathbf{X}_A^{:t}; \mathbf{Y}_B^{:t}|\mathbf{X}_B^{:t}, \mathbf{Y}_E^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{Y}_E^{:t}) \\
&= I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1}|\mathbb{V}_E^{:t}) + I(\mathbf{X}_A^{:t}; \mathbf{Y}_B^{:t}|\mathbf{X}_B^{:t}, \mathbf{Y}_E^{:t}) \\
&\quad + I(\mathbf{Y}_A^{:t}; \mathbf{X}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{Y}_E^{:t}) + I(\mathbf{Y}_A^{:t}; \mathbf{Y}_B^{:t}|\mathbf{X}_A^{:t}, \mathbf{X}_B^{:t}, \mathbf{Y}_E^{:t}).
\end{aligned} \tag{A.119}$$

Inequalities (a) and (b) are respectively due to the Markov chains

$$(\mathbb{V}_A^{:t-1}, \mathbb{V}_B^{:t-1}, \mathbb{V}_E^{:t-1}) \leftrightarrow (\mathbf{X}_A^{:t}, \mathbf{X}_B^{:t}, \mathbf{Y}_B^{:t}, \mathbf{Y}_E^{:t}) \leftrightarrow \mathbf{Y}_A^{:t},$$

$$(\mathbb{V}_A^{:t-1}, \mathbb{V}_B^{:t-1}, \mathbb{V}_E^{:t-1}) \leftrightarrow (\mathbf{X}_A^{:t}, \mathbf{X}_B^{:t}, \mathbf{Y}_E^{:t}) \leftrightarrow \mathbf{Y}_B^{:t}.$$

The first term in (A.119) can be rephrased as the following three terms

$$
\begin{aligned}
&I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1} | \mathbb{V}_E^{:t}) = I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1} | \mathbb{V}_E^{:t-1}, \mathbf{Y}_E^{:t}) \\
&\quad = I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1}, \mathbf{Y}_E^{:t} | \mathbb{V}_E^{:t-1}) - I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{Y}_E^{:t} | \mathbb{V}_E^{:t-1}) \\
&\quad = I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1} | \mathbb{V}_E^{:t-1}) + I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{Y}_E^{:t} | \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1}, \mathbb{V}_E^{:t-1}) \\
&\qquad\quad - I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{Y}_E^{:t} | \mathbb{V}_E^{:t-1}) \\
&\quad \overset{(a)}{=} I(\mathbb{V}_A^{:t-1}; \mathbb{V}_B^{:t-1} | \mathbb{V}_E^{:t-1}) + I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{Y}_E^{:t} | \mathbf{X}_B^{:t}, \mathbb{V}_B^{:t-1}, \mathbb{V}_E^{:t-1}) - I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{Y}_E^{:t} | \mathbb{V}_E^{:t-1}) \\
&\quad \overset{(b)}{\leq} I(\mathbb{V}_A^{:t-1}; \mathbb{V}_B^{:t-1} | \mathbb{V}_E^{:t-1}) + I(\mathbf{X}_A^{:t}; \mathbf{Y}_E^{:t} | \mathbf{X}_B^{:t}, \mathbb{V}_E^{:t-1}) - I(\mathbf{X}_A^{:t}, \mathbb{V}_A^{:t-1}; \mathbf{Y}_E^{:t} | \mathbb{V}_E^{:t-1}) \\
&\quad \leq I(\mathbb{V}_A^{:t-1}; \mathbb{V}_B^{:t-1} | \mathbb{V}_E^{:t-1}) + I(\mathbf{X}_A^{:t}; \mathbf{Y}_E^{:t} | \mathbf{X}_B^{:t}, \mathbb{V}_E^{:t-1}) - I(\mathbf{X}_A^{:t}; \mathbf{Y}_E^{:t} | \mathbb{V}_E^{:t-1}) \qquad \text{(A.120)}
\end{aligned}
$$

Equality (a) is due to the Markov chains $\mathbf{X}_A^{:t} \leftrightarrow \mathbb{V}_A^{:t-1} \leftrightarrow \mathbb{V}_B^{:t-1}$ and $\mathbf{X}_B^{:t} \leftrightarrow \mathbb{V}_B^{:t-1} \leftrightarrow \mathbb{V}_A^{:t-1}$, and inequality (b) is due to $(\mathbb{V}_A^{:t-1}, \mathbb{V}_B^{:t-1}) \leftrightarrow (\mathbf{X}_A^{:t}, \mathbf{X}_B^{:t}) \leftrightarrow \mathbf{Y}_E^{:t}$. By recursively continuing the above steps in (A.119) and (A.120) t times, we reach

$$
\begin{aligned}
I(\mathbb{V}_A^{:t}; \mathbb{V}_B^{:t} | \mathbb{V}_E^{:t}) &\leq \sum_{r=1}^{t} I(\mathbf{X}_A^{:r}; \mathbf{Y}_B^{:r} | \mathbf{X}_B^{:r}, \mathbf{Y}_E^{:r}) + I(\mathbf{X}_B^{:r}; \mathbf{Y}_A^{:r} | \mathbf{X}_A^{:r}, \mathbf{Y}_E^{:r}) + I(\mathbf{Y}_A^{:r}; \mathbf{Y}_B^{:r} | \mathbf{X}_A^{:r}, \mathbf{X}_B^{:r}, \mathbf{Y}_E^{:r}) \\
&\qquad + I(\mathbf{X}_A^{:r}; \mathbf{Y}_E^{:r} | \mathbf{X}_B^{:r}, \mathbb{V}_E^{:r-1}) - I(\mathbf{X}_A^{:r}; \mathbf{Y}_E^{:r} | \mathbb{V}_E^{:r-1}) \\
&\leq \sum_{r=1}^{t} \sum_{i=1}^{n_r} I(X_{A,i}^{:r}; Y_{B,i}^{:r} | X_{B,i}^{:r}, Y_{E,i}^{:r}) + I(X_{B,i}^{:r}; Y_{B,i}^{:r} | X_{A,i}^{:r}, Y_{E,i}^{:r}) + I(Y_{A,i}^{:r}; Y_{B,i}^{:r} | X_{A,i}^{:r}, X_{B,i}^{:r}, Y_{E,i}^{:r}) \\
&\qquad + I(X_{A,i}^{:r}; Y_{E,i}^{:r} | X_{B,i}^{:r}, \mathbb{V}_E^{:r-1}, Y_{E,1}^{i-1:r}) - I(X_{A,i}^{:r}; Y_{E,i}^{:r} | \mathbb{V}_E^{:r-1}, Y_{E,1}^{i-1:r}), \qquad \text{(A.121)}
\end{aligned}
$$

where the last inequality holds since the channel is memoryless. Let $Q_i^{:r} = (\mathbb{V}_E^{:r-1}, Y_{E,1}^{i-1:r})$. We choose the RVs $X_A = X_{A,\tilde{i}}^{:\tilde{r}}$, $X_B = X_{B,\tilde{i}}^{:\tilde{r}}$, $Y_A = Y_{A,\tilde{i}}^{:\tilde{r}}$, $Y_B = Y_{B,\tilde{i}}^{:\tilde{r}}$, $Y_E = Y_{E,\tilde{i}}^{:\tilde{r}}$ and $Q = Q_{\tilde{i}}^{:\tilde{r}}$, where $\tilde{i}$ and $\tilde{j}$ are chosen such that

$$
\begin{aligned}
&I(X_A; Y_B | X_B, Y_E) + I(X_B; Y_A | X_A, Y_E) + I(Y_A; Y_B | X_A, X_B, Y_E) + I(X_A; Y_E | X_B, Q) - I(X_A; Y_E | Q) = \\
&\max_{1 \leq r \leq t,\ 1 \leq i \leq n} [I(X_{A,i}^{:r}; Y_{B,i}^{:r} | X_{B,i}^{:r}, Y_{E,i}^{:r}) + I(X_{B,i}^{:r}; Y_{B,i}^{:r} | X_{A,i}^{:r}, Y_{E,i}^{:r}) + I(Y_{A,i}^{:r}; Y_{B,i}^{:r} | X_{A,i}^{:r}, X_{B,i}^{:r}, Y_{E,i}^{:r}) \\
&\qquad + I(X_{A,i}^{:r}; Y_{E,i}^{:r} | X_{B,i}^{:r}, Q_i^{:r}) - I(X_{A,i}^{:r}; Y_{E,i}^{:r} | Q_i^{:r})].
\end{aligned}
$$

It is easy to see that X_A, X_B, Y_A, Y_B, and Y_E correspond to the TWDMC distribution $(P_{Y_A,Y_B,Y_E|X_A,X_B})$, and the Markov chain

$$Q \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B, Y_E)$$

holds. We continue (A.121) as

$$\begin{aligned}\frac{1}{n}I(\mathbb{V}_A^{:t};\mathbb{V}_B^{:t}|\mathbb{V}_E^{:t}) &\leq I(X_A;Y_B|X_B,Y_E)+I(X_B;Y_A|X_A,Y_E)\\ &\quad +I(Y_A;Y_B|X_A,X_B,Y_E)+I(X_A;Y_E|X_B,Q)-I(X_A;Y_E|Q)\\ &= I(X_A;Y_B|X_B,Y_E)+I(X_B;Y_A|X_A,Y_E)+I(Y_A;Y_B|X_A,X_B,Y_E)\\ &\quad +H(X_A|X_B,Q)-H(X_A|X_B,Q,Y_E)-H(X_A|Q)+H(X_A|Q,Y_E)\\ &= I(X_A;Y_B|X_B,Y_E)+I(X_B;Y_A|X_A,Y_E)+I(Y_A;Y_B|X_A,X_B,Y_E)\\ &\quad +I(X_A;X_B|Y_E,Q)-I(X_A;X_B|Q). \end{aligned} \tag{A.122}$$

Using (3.3c), (A.118) and (A.122), we have the following upper bound on R_{sk}

$$\begin{aligned}R_{sk} \;<\; \frac{1}{n}H(S)+\delta &\leq I(X_A;Y_B|X_B,Y_E)+I(X_B;Y_A|X_A,Y_E)+I(Y_A;Y_B|X_A,X_B,Y_E)\\ &\quad +I(X_A;X_B|Y_E,Q)-I(X_A;X_B|Q),\end{aligned}$$

where the last inequality follows from the fact that δ is arbitrarily small. This proves the upper bound in (3.65). □

A.13 Proof of Lemma 14: Cascade error probability

We shall prove the two inequalities (3.32) and (3.33). Depending on the values of x and y, we consider the following four cases, and prove these two inequalities in each case separately.

Case 1: $x \leq 0.5, y \leq 0.5$**.**

In this case, $x \star y \leq 0.5$ also holds. This is shown below.

$$x \star y = x + y - 2xy = x + 2y(0.5 - x) \leq x + (0.5 - x) \leq 0.5, \tag{A.123}$$

where the first inequality holds since $y \leq 0.5$. This allows us to rewrite the claimed inequality (3.32) as

$$0.5 - x \star y \leq \min\{0.5 - x, 0.5 - y\}. \tag{A.124}$$

To prove this, we shall show that $x \star y$ is greater then or equal to both x and y. We show the former as

$$x \star y = x + y - 2xy = x + y(1 - 2x) \geq x, \tag{A.125}$$

where the inequality holds since $x \leq 0.5$. Similarly, one can show

$$x \star y = x + y - 2xy = y + x(1 - 2y) \geq y. \tag{A.126}$$

This completes the proof of (3.32) for Case 1. Since the binary entropy function $h(p)$ is increasing for $0 \leq p \leq 0.5$, we have from (A.125)-(A.126) that

$$h(x \star y) \geq \max\{h(x), h(y)\}. \tag{A.127}$$

Case 2: $x \leq 0.5, y \geq 0.5$**.**

In this case, we show $x \star y \geq 0.5$ as follows.

$$x \star y = x + y - 2xy = x + 2y(0.5 - x) \geq x + (0.5 - x) \geq 0.5, \tag{A.128}$$

where the first inequality holds since $y \geq 0.5$. Therefore, we write (3.32) as

$$x \star y - 0.5 \leq \min\{0.5 - x, y - 0.5\}, \tag{A.129}$$

which is equivalent to proving $x \star y + x \leq 1$ and $x \star y \leq y$. The former is shown as

$$x \star y + x = x + y - 2xy + x = 2x + y(1 - 2x) \leq 2x + (1 - 2x) \leq 1, \tag{A.130}$$

where the first inequality holds since $y \leq 1$. The latter is shown as

$$x \star y = x + y - 2xy = y + x(1 - 2y) \leq y, \tag{A.131}$$

where the inequality holds since $y \geq 0.5$. This completes the proof of (3.32) in Case 2. We prove (3.33) as follows. The binary entropy function $h(p)$ is decreasing for $0.5 \leq p \leq 1$. This gives that, using (A.131),

$$h(x \star y) \geq h(y). \tag{A.132}$$

Similarly, since $1 - x \geq 0.5$, we use (A.130) to write $x \star y \leq 1 - x$; hence,

$$h(x \star y) \geq h(1 - x) = h(x), \tag{A.133}$$

since $h(p) = h(1 - p)$ holds for all $0 \leq p \leq 1$.

Case 3: $x \geq 0.5, y \leq 0.5$**.**

Proving inequalities (3.32) and (3.33) in this case follows from that in Case 2, by symmetry.

Case 4: $x \geq 0.5, y \geq 0.5$**.**

We can always write $x \star y$ as

$$x \star y = x + y - 2xy = (1 - x) + (1 - y) - 2(1 - x)(1 - y) = x' + y' - 2x'y' = x' \star y', \tag{A.134}$$

where $x' = 1 - x$ and $y' = 1 - y$. Observe that x' and y' are both less than or equal to 0.5. Thus, we can use the lemma results proved for Case 1 (above), and write

$$|0.5 - x' \star y'| \leq \min\{|0.5 - x'|, |0.5 - y'|\}. \tag{A.135}$$

The fact that $x' \star y' = x \star y$, $|0.5 - x'| = |0.5 - x|$, and $|0.5 - y'| = |0.5 - y|$ proves (3.32) as

$$|0.5 - x \star y| \leq \min\{|0.5 - x|, |0.5 - y|\}. \tag{A.136}$$

To prove (3.33),

$$h(x \star y) = h(x' \star y') \overset{(a)}{\geq} \max\{h(x'), h(y')\} \overset{(b)}{=} \max\{h(x), h(y)\}. \tag{A.137}$$

Inequality (a) follows from (A.127), and equality (b) holds since, for any $0 \leq p \leq 1$, we have that $h(p) = h(1 - p)$. $\square$

A.14 Proof of Lemma 17: SK capacity lower bound for TWBSWC

For the TWBWC setup, we follow the lower bound (3.62) by letting $W_{2A} = W_{2B} = 0$ and X_A and X_B be independent, uniformly-distributed bits; hence, to write the lower bound as

$$C_{wsk}^{TWBWC} \geq \max_{\mu \geq 0, X_A, X_B, V_A, V_B, W_{2A}, W_{2B}, W_{1A}, W_{1B}} [\frac{n_1 Lbd_1^{tw} + n_2 [Lbd_2^{tw}]_+}{n_1 + n_2}, \quad \text{s.t.} \tag{A.138}$$

$$n_1 I(V_A; X_A, Y_A | X_B, Y_B) < n_2 I(W_{1A}; X_B, Y_B), \tag{A.139}$$

$$n_1 I(V_B; X_B, Y_B | X_A, Y_A) < n_2 I(W_{1B}; X_A, Y_A)], \tag{A.140}$$

where

$$Lbd_1^{tw} = I(V_A; X_B, Y_B) + I(V_B; X_A, Y_A | V_A) - I(V_A, V_B; Y_E), \tag{A.141}$$

$$Lbd_2^{tw} = I(W_{1A}; X_B, Y_B) + I(W_{1B}; X_A, Y_A) - I(W_{1A}, W_{1B}; Y_E). \tag{A.142}$$

The two terms, Lbd_1^{tw} and Lbd_2^{tw}, in the lower bound argument depend on the distributions of (V_A, V_B) and (W_{1A}, W_{1B}), respectively. In the following, we continue the lower bound only for the following case among all possible distributions of (see (3.60a)-(3.60c))

$$[(V_A, V_B), (W_{1A}, W_{1B})] \in \{[(X_A + Y_A + N'_{sA}, X_B + Y_B + N'_{sB}), (X_A + N_{sA}, X_B + N_{sB})] : 0 \leq p_1, p_2 \leq 1\},$$

where N_{sA}, N_{sB}, N'_{sA}, and N'_{sB} are independent BSC noises with error probabilities

$$\Pr(N'_{sA} = 1) = \Pr(N_{sB} = 1) = p_1, \qquad \Pr(N'_{sB} = 1) = \Pr(N_{sA} = 1) = p_2.$$

In this case, we calculate the first term Lbd_1^{tw}, given noise variables N'_{sA} and N'_{sB} as follows.

$$\begin{aligned}
Lbd_1^{tw} \triangleq Lbd_1^{tw*} &= I(X_A + Y_A + N'_{sA}; X_B, Y_B) + I(X_B + Y_B + N'_{sB}; X_A, Y_A) \\
&\quad - I(X_A + Y_A + N'_{sA}, X_B + Y_B + N'_{sB}; Y_E) \\
&\overset{(a)}{=} 1 - H(X_A + Y_A + N'_{sA}|X_B, Y_B) + 1 - H(X_B + Y_B + N'_{sB}|X_A, Y_A) \\
&\quad - (1 - H(Y_E|X_A + Y_A + N'_{sA}, X_B + Y_B + N'_{sB})) \\
&\overset{(b)}{=} 1 - H(X_B + N_{rA} + N'_{sA}|X_B, Y_B) - H(X_A + N_{rB} + N'_{sB}|X_A, Y_A) \\
&\quad + H(X_A + X_B + N_E|X_B + N_{rA} + N'_{sA}, X_A + N_{rB} + N'_{sB}) \\
&\overset{(c)}{=} 1 - H(X_B + N_{rA} + N'_{sA}|X_B) - H(X_A + N_{rB} + N'_{sB}|X_A) \\
&\quad + H(X_A + X_B + N_E|X_A + X_B + N_{rA} + N_{rB} + N'_{sA} + N'_{sB}) \\
&\overset{(d)}{=} 1 - h(p_1 \star p_{r_a}) - h(p_2 \star p_{r_b}) + h(p_1 \star p_2 \star p_{r_a} \star p_{r_b} \star p_e). \qquad \text{(A.143)}
\end{aligned}$$

Equalities (a)-(d) hold due to the following: (a) holds since X_A, X_B, and Y_E have uniform distributions, (b) follows from (3.67), (c) holds because Y_B is independent of $(X_B, X_B + N_{rA} + N'_{sA})$ and Y_A is independent of $(X_A, X_A + N_{rB} + N'_{sB})$, and (d) is due to the BSC property. Similarly, we obtain the second term Lbd_2^{tw} given noise variables N_{sA}, and N_{sB} as

$$\begin{aligned}
Lbd_2^{tw} \triangleq Lbd_2^{tw*} &= I(X_A + N_{sA}; X_B, Y_B) + I(X_B + N_{sB}; X_A, Y_A) - I(X_A + N_{sA}, X_B + N_{sB}; Y_E) \\
&= 1 - H(X_A + N_{sA}|X_B, Y_B) - H(X_B + N_{sB}|X_A, Y_A) + H(Y_E|X_A + N_{sA}, X_B + N_{sB}) \\
&= 1 - H(X_A + N_{sA}|X_B, X_B + Y_B) + 1 - H(X_B + N_{sB}|X_A, X_A + Y_A) \\
&\quad + H(Y_E|X_A + N_{sA}, X_B + N_{sB}) \\
&= 1 - H(X_A + N_{sA}|X_B, X_A + N_{rB}) - H(X_B + N_{sB}|X_A, X_B + N_{rA}) \\
&\quad + H(X_A + X_B + N_E|X_A + N_{sA}, X_B + N_{sB}) \\
&= 1 - H(X_A + N_{sA}|X_A + N_{rB}) - H(X_B + N_{sB}|X_B + N_{rA}) \\
&\quad + H(X_A + X_B + N_E|X_A + X_B + N_{sA} + N_{sB}) \\
&= 1 - h(p_2 \star p_{r_b}) - h(p_1 \star p_{r_a}) + h(p_1 \star p_2 \star p_e). \qquad \text{(A.144)}
\end{aligned}$$

We write the conditions (A.139) and (A.140), respectively, as

$$\begin{aligned} n_1 < n_1' &\triangleq n_2 \frac{I(X_A + N_{sA}; X_B, Y_B)}{I(X_A + Y_A + N_{sA}'; X_A, Y_A | X_B, Y_B)} = n_2 \frac{1 - H(X_A + N_{sA} | X_B, Y_B)}{H(X_A + Y_A + N_{sA}' | X_B, Y_B)} \\ &= n_2 \frac{1 - H(X_A + N_{sA} | X_A + N_{rB})}{H(X_B + N_{rA} + N_{sA}' | X_B, Y_B)} = n_2 \frac{1 - h(p_2 \star p_{r_b})}{h(p_1 \star p_{r_a})}, \end{aligned} \tag{A.145}$$

and

$$\begin{aligned} n_1 < n_1'' &\triangleq n_2 \frac{I(X_B + N_{sB}; X_A, Y_A)}{I(X_B + Y_B + N_{sB}'; X_B, Y_B | X_A, Y_A)} = n_2 \frac{1 - H(X_B + N_{sB} | X_A, Y_A)}{H(X_B + Y_B + N_{sB}' | X_A, Y_A)} \\ &= n_2 \frac{1 - H(X_B + N_{sB} | X_B + N_{rA})}{H(X_A + N_{rB} + N_{sB}' | X_A, Y_A)} = n_2 \frac{1 - h(p_1 \star p_{r_a})}{h(p_2 \star p_{r_b})}. \end{aligned} \tag{A.146}$$

By letting $n_1^* = \min\{n_1', n_1''\}$ and following the lower bound (A.138) for this case, we arrive at

$$\max_{n_1, n_2, p_1, p_2} [\frac{n_1 Lbd_1^{tw*} + n_2 [Lbd_2^{tw*}]_+}{n_1 + n_2}, \quad \text{s.t.} \quad n_1 \leq n_1^*]. \tag{A.147}$$

Using the result of Lemma 14 for (A.143), we have that $Lbd_1^{tw*} \geq 0$ holds for any $0 \leq p_1, p_2 \leq 1$. On the other hand, comparing (A.143) and (A.144) reveals that $Lbd_1^{tw*} \geq Lbd_2^{tw*}$. These together imply $Lbd_1^{tw*} \geq [Lbd_2^{tw*}]_+$. Thus, the maximum in (A.147) is achieved by selecting $n_1 = n_1^*$, i.e.,

$$Lbnd_N^{tw} \triangleq \max_{p_1, p_2} [\frac{n_1^* Lbd_1^{tw*} + n_2 [Lbd_2^{tw*}]_+}{n_1^* + n_2}] = \max_{p_1, p_2} [\mu Lbd_1^{tw*} + (1 - \mu)[Lbd_2^{tw*}]_+], \tag{A.148}$$

where

$$\mu = \frac{n_1^*}{n_1^* + n_2} = \min\{\frac{1 - h(p_1 \star p_{r_a})}{1 - h(p_1 \star p_{r_a}) + h(p_2 \star p_{r_b})}, \frac{1 - h(p_2 \star p_{r_b})}{1 - h(p_2 \star p_{r_b}) + h(p_1 \star p_{r_a})}\}. \tag{A.149}$$

Furthermore, (A.148) clearly shows that

$$Lbnd_N^{tw} \geq \max_{p_1, p_2} [Lbd_2^{tw*}]_+,$$

since $Lbd_1^{tw} \geq [Lbd_2^{tw}]_+$ holds for any $0 \leq p_1, p_2 \leq 1$. $\square$

A.15 Proof of Lemma 19: Uniform and strong SK capacity equality

Prerequisites. We shall show that the protocol Π_s is a $(C^{\mathfrak{S}}_{usk}, \delta)$-strongly-secure SKE protocol, i.e., it satisfies reliability, strong secrecy, and strong uniformity as in Definition 29. The following analysis is given assuming that "Alice" sends the $2L$ bits of information for reconciliation. Similar analysis works when Bob sends information reconciliation bits. Using the reliability property of Π_u, we write

$$\forall 1 \leq i \leq N, 1 \leq j \leq 2: \quad \Pr(S_{uAj,i} \neq S_{uAj,i}) \leq \delta'.$$

Fano's inequality (cf. [23, Ch 2]) and the independence of Π_u repetitions give us

$$\forall 1 \leq j \leq 2: \quad H(S^N_{uAj}|S^N_{uBj}) \leq N\left(\delta' K + 1\right).$$

We combine the above with Lemma 9 to reach the following. For any $\delta_1 > 0$, by choosing ϵ_1 sufficiently small, there exists L satisfying

$$L \leq (1+\epsilon_1)N\left(\delta' K + 1\right) \leq \delta_1 NK, \tag{A.150}$$

for which information reconciliation succeeds with probability $\geq 1 - 2\epsilon_1$, i.e.,

$$\Pr(S'^N_{uA1} = S'^N_{uB1}) \geq 1 - \epsilon_1 \qquad \text{and} \qquad \Pr(S'^N_{uA2} = S'^N_{uB2}) \geq 1 - \epsilon_1. \tag{A.151}$$

The secrecy and uniformity properties of Π_u (see (3.3b) and (3.4)) imply

$$\forall 1 \leq i \leq N, 1 \leq j \leq 2: \quad H(S_{uAj,i}|\mathbb{V}_{uEj,i}) \geq (1-\delta')\left(K - \delta' Cost^{\mathfrak{S}}_{\Pi_u}\right). \tag{A.152}$$

Strong secrecy: Proving (3.5b). Eve's view $View_E$ of the protocol originates from the first two steps of the above construction, where resources in the setup are used. In step (i), she observes $(\mathbb{V}^N_{uE1}, \mathbb{V}^N_{uE2})$. We use Lemma 25, as a simplified version of [60, Lemma 6], which shows that the min-entropy of long i.i.d. sequences becomes close to their Shannon entropy.

Lemma 25. *For any joint distribution P_{XZ}, let X^n and Y^n be drawn i.i.d. according to P_{XZ}. For any $\epsilon > 0$, for sufficiently large n, there exists an event $\mathcal{E}$ such that $\Pr(\mathcal{E}) \geq 1 - \epsilon/n$, and furthermore, for all $z \in \mathcal{Z}^n$,*

$$H_\infty(X^n|Z^n = z, \mathcal{E}) \geq n\left(H(X|Y) - \epsilon\right).$$

Letting $\epsilon_2 \leq 1/(NK^2)$, the above implies that there is an event $\mathcal{E}_j$ with probability $\Pr(\mathcal{E}_j) \geq 1 - \epsilon_2 \geq 1 - \frac{1}{NK^2}$, such that for all views v_j,

$$\begin{aligned} H_\infty(\tilde{S}_{jA}|\mathbb{V}_{uEj}^N = v_j, \mathcal{E}_j) &\overset{(a)}{=} H_\infty(S_{uAj}^N|\mathbb{V}_{uEj}^N = v_j, \mathcal{E}_j) \\ &\overset{(b)}{\geq} N\left((1-\delta')(K - \delta' Cost_{\Pi_u}^{\mathfrak{S}}) - \epsilon_2\right) \\ &\geq NK(1-\delta_2), \end{aligned} \tag{A.153}$$

for some $\delta_2 > 0$ that can be made arbitrarily small based on δ' and ϵ_2 when N and K are sufficiently large. Equality (a) is due to the injective binary mapping function and inequality (b) follows from (A.152).

In step (ii), Eve observes the independent variables $\mathbb{V}_{rEj}$, for $1 \leq j \leq 2$, each of which reveals some information about the information reconciliation (error-correction) bits $h_j(S_{uAj}^N)$. This implies the Markov chain $\mathbb{V}_{rEj} \leftrightarrow h_j(S_{uAj,i}) \leftrightarrow (S_{uAj}^N, \mathbb{V}_{uEj}^N)$, which lets us write the following. For any instance of Eve's view v_j' there exists an L-bit string w such that, for $\epsilon_3 > 0$ and $1 \leq j \leq 2$, we have

$$\begin{aligned} H_\infty(\tilde{S}_{jA}|\mathbb{V}_{uEj}^N = v_j, \mathbb{V}_{rEj} = v_j', \mathcal{E}_j) &\geq H_\infty(\tilde{S}_{jA}|\mathbb{V}_{uEj}^N = v_j, h_j(S_{uAj}^N) = w, \mathcal{E}_j) \\ &\overset{(a)}{\geq} H_\infty(\tilde{S}_{jA}|\mathbb{V}_{uEj}^N = v_j, \mathcal{E}_j) - L - \epsilon_3 \qquad \text{(with prob. } \geq 1 - 2^{-\epsilon_3}) \\ &\overset{(b)}{\geq} NK(1 - \delta_1 - \delta_2) - \epsilon_3 \qquad \text{(with prob. } \geq 1 - 2^{-\epsilon_3}). \end{aligned}$$

Inequality (a) follows from the property of the min-entropy function (cf. [60]), and inequality (b) is due to (A.150), (A.153), and Lemma 9. We continue, by choosing $\epsilon_3 = \log(NK^2)$, which leads to

$$H_\infty(\tilde{S}_{jA}|\mathbb{V}_{uEj}^N = v_j, \mathbb{V}_{rEj} = v_j', \mathcal{E}_j) \geq NK(1-\delta_3) \qquad \text{(with prob. } \geq 1 - \tfrac{1}{NK^2}),$$

for arbitrarily small $\delta_3 > 0$, by choosing N and K sufficiently large. The above inequality shows that, with high probability for any instance of Eve's view, each $\tilde{S}_{jA}$ is arbitrarily close to uniform in rate. Applying the two-source extractor makes the output arbitrarily close to uniform in terms of its absolute value. This is shown in the following. For sufficiently small $\epsilon_4 > 0$, let $\gamma = 2^{-\epsilon_4 NK}$ and the extractor output length r satisfy

$$r \;=\; 3NK(1-\delta_3) - NK - 4\log(1/\epsilon) \geq 2NK(1-\delta_4),$$

for $\delta_4 > 0$ which can be made arbitrarily small by choosing N and K sufficiently large. According to Lemma 7, the output $\tilde{S}_A$ of the two-source extractor given $View_E = v_e$, $\mathcal{E}_1$, and $\mathcal{E}_2$ is γ-close to uniform with probability $1 - \frac{1}{NK}$. Similarly to [60, Lemma 6], the above implies

$$H(\tilde{S}_A|View_E = v_e, \mathcal{E}_1, \mathcal{E}_2) \geq r - 2^{\epsilon_4 NK} \qquad (\text{with prob. } \geq 1 - \tfrac{1}{NK^2}).$$

By taking into consideration the probabilities of $\mathcal{E}_1$ and $\mathcal{E}_2$, we arrive at

$$\begin{aligned} H(\tilde{S}_A|View_E) &\geq (1 - \frac{1}{NK^2} + \Pr(\overline{\mathcal{E}}_1) + \Pr(\overline{\mathcal{E}}_2))(r - 2^{\epsilon_4 NK}) \\ &\geq (1 - \frac{3}{NK^2})(r - 2^{\epsilon_4 NK}) \geq r - \delta_5, \end{aligned} \tag{A.154}$$

for $\delta_5 < \delta$, by choosing N and K sufficiently large. This proves strong secrecy as $r = \log|\mathcal{S}|$.

Reliability: Proving (3.5a). We first note that (A.154) also shows $H(\tilde{S}_A) \geq r - \delta_5$, i.e., the absolute entropy of $\tilde{S}_A$ can be made arbitrarily close to uniform. Similarly to [60], the uniformization step converts $\tilde{S}_A$ to a completely uniform variable S_A with error probability $\Pr(S_A \neq \tilde{S}_A) \leq \epsilon_5$ for arbitrarily small $\epsilon_5 > 0$. The following steps eventually prove the reliability property by using (A.151).

$$\begin{aligned} \Pr(S_A \neq S_B) &\leq \Pr(S_A \neq \tilde{S}_A \;\vee\; \tilde{S}_A \neq S_B) \leq \Pr(S_A \neq \tilde{S}_A) + \Pr(\tilde{S}_A \neq S_B) \\ &\leq \Pr(S_A \neq \tilde{S}_A) + \Pr(S'^N_{uA1} \neq S'^N_{uB1}) + \Pr(S'^N_{uA2} \neq S'^N_{uB2}) \leq \epsilon_5 + 2\epsilon_1 < \delta, \end{aligned}$$

for appropriately small ϵ_1 and ϵ_5 when N and K are sufficiently large.

Strong uniformity: Proving (3.5c). The protocol Π_s provides r-bit secret key. Obviously perfect uniformity holds as S_A is uniformly distributed thanks to the uniformization step. The rest is to analyze the key rate and show that it is arbitrarily close to the uniform SK capacity $C_{usk}^{\mathfrak{S}}$. Before all, note that the protocol Π_u satisfies the randomness condition (3.3c), i.e., $K/Cost_{\Pi_u}^{\mathfrak{S}} \geq C_{usk}^{\mathfrak{S}} - \delta'$.

The cost $Cost_{\Pi_s}^{\mathfrak{S}}$ of the protocol Π_s equals those of steps (i) and (ii), i.e., $2NCost_{\Pi_u}^{\mathfrak{S}}$ plus the cost of sending $2L$ information bits by either party. We note that other steps do not use any communication resource and hence have no effect on the total cost. Assuming that the setup allows for reliable transmission in at least one direction, we denote by $C_m^{\mathfrak{S}}$ the reliability capacity of the setup (maximized over forward and backward directions). This gives that for any $\epsilon_6 > 0$ and large enough N and K (hence L), there exists a protocol that sends $2L$ information bits in either (forward or backward) direction with error probability ϵ_6 and cost at most $\frac{2L}{C_m^{\mathfrak{S}} - \epsilon_6}$. The SK rate achieved by the protocol Π_s is obtained as follows.

$$\begin{aligned}
\frac{H(S_A)}{Cost_{\Pi_s}^{\mathfrak{S}}} &= \frac{r}{Cost_{\Pi_s}^{\mathfrak{S}}} \geq \frac{2NK(1-\delta_4)}{2NCost_{\Pi_u}^{\mathfrak{S}} + 2L/(C_m^{\mathfrak{S}} - \epsilon_6)} \geq \frac{2NK(1-\delta_4)}{2NCost_{\Pi_u}^{\mathfrak{S}} + 2\delta_1 NK/(C_m^{\mathfrak{S}} - \epsilon_6)} \\
&\geq \frac{Cost_{\Pi_u}^{\mathfrak{S}}(C_{usk}^{\mathfrak{S}} - \delta')(1-\delta_4)}{Cost_{\Pi_u}^{\mathfrak{S}} + \delta_1 Cost_{\Pi_u}^{\mathfrak{S}} C_{usk}^{\mathfrak{S}}/(C_m^{\mathfrak{S}} - \epsilon_6)} = \frac{(C_{usk}^{\mathfrak{S}} - \delta')(1-\delta_4)}{1 + \delta_1 C_{usk}^{\mathfrak{S}}/(C_m^{\mathfrak{S}} - \epsilon_6)} \geq C_{usk}^{\mathfrak{S}}(1-\delta),
\end{aligned}$$

The last inequality is attained by choosing $\epsilon_6, \delta_1, \delta_4$, and δ' suitably small for sufficiently large N and K. This proves that the strong SK capacity equals to the uniform SK capacity.

Appendix B

Proof Results on Manipulation Detection

B.1 Proof of Theorem 11: effective tag length

The proof mainly relies on the results of the following lemma.

Lemma 26. *For any weak, resp. strong, LR-AMD code the failure probability is lower bounded as*

$$\epsilon \geq \max\{\left((1-e^{-1})\frac{\mathfrak{M}-1}{\mathfrak{X}-1}\right)^{1-\alpha}\ ,\ (1-e^{-1})\mathfrak{M}^{\alpha}\frac{\mathfrak{M}-1}{\mathfrak{X}-1}\},\quad \textit{resp.} \tag{B.1}$$

$$\epsilon \geq \left((1-e^{-1})\frac{\mathfrak{M}-1}{\mathfrak{X}-1}\right)^{(1-\alpha)/2}. \tag{B.2}$$

Proof. We start by the $(\mathfrak{M}, \mathfrak{X}, \alpha, \epsilon)$-weak LR-AMD code. We shall show that for any such code there exist a message distribution $M \in \mathcal{M}$, a leakage variable Z with $\tilde{H}_{\infty}(M|Z) \geq (1-\alpha)\log\mathfrak{M}$, and an adversary whose success chance in changing M is lower bounded by (B.1).

Let M be uniformly distributed and Z be an $\alpha\log\mathfrak{M}$-bit string that represents the adversary's $\alpha\log\mathfrak{M}$ questions about the codeword. The variable Z is such that each bit Z_i is defined by $Z_i = Query_i(Z_1^{i-1}, M)$, where $Query_i$ shows the i-th question. Let $X = Enc(M)$ be the codeword for M. The adversary can choose any non-zero adversarial noise $\delta \in \mathcal{X}/\{0\}$ to be added to the X. There are $n = \mathfrak{X}-1$ values for δ, at least $t = M-1$ of which lead to valid codewords $X+\delta$. Let $\mathcal{X}^+$ be the set of such valid δ values. If the adversary picks δ randomly, their success chance will be thus at least t/n.

We now describe the adversary's strategy as follows. She first chooses a random subset $\mathcal{H}_0 \subseteq \mathcal{X}/\{0\}$ of size $k = n/t$ and runs Algorithm B.1. The size of $\mathcal{H}$ at the end of

Algorithm 1 Adversary's strategy

$\mathcal{H} \leftarrow \mathcal{H}_0$.

for $i = 1$ to $\alpha \log \mathfrak{M}$ **do**

Partition $\mathcal{H}$ arbitrarily into equal sized $\mathcal{H}_1$ and $\mathcal{H}_2$.

Ask whether $|\mathcal{H}_1 \cap \mathcal{X}^+| > 0$.

if Yes **then**

$\mathcal{H} \leftarrow \mathcal{H}_1$.

else

$\mathcal{H} \leftarrow \mathcal{H}_2$.

end if

end for

Choose δ randomly from H.

return δ.

the algorithm decreases to $k/\mathfrak{M}^\alpha$. The adversary succeeds with probability $\mathfrak{M}^\alpha/k$ only if $\mathcal{H}_0 \cap \mathcal{X}^+$ is not empty, whose probability is obtained as

$$\Pr(|\mathcal{H}_0 \cap \mathcal{X}^+| > 0) = 1 - \Pr(|\mathcal{H}_0 \cap \mathcal{X}^+| = 0) = 1 - \frac{\binom{n-t}{k}}{\binom{n}{k}} = 1 - \frac{(n-t)!(n-k)!}{n!(n-k-t)!}$$
$$= 1 - \frac{(n-k) \times \cdots \times (n-k-t)}{n \times \cdots \times (n-t)} \geq 1 - (1-k/n)^t = 1 - (1-1/t)^t \geq 1 - e^{-1}.$$

This concludes that the adversary's success probability is at least

$$\epsilon \geq (1-e^{-1})\mathfrak{M}^\alpha/k = (1-e^{-1})\mathfrak{M}^\alpha \frac{\mathfrak{M}-1}{\mathfrak{X}-1},$$

which is the second term of (B.1). For the first term, we use the fact that the message size $\mathfrak{M}$ is such that after $\alpha \log \mathfrak{M}$ questions the adversary cannot guess the correct message with probability more than ϵ, and this implies $\mathfrak{M}^{1-\alpha} \geq 1/\epsilon$. We use this to write (noting that $0 \leq \alpha \leq 1$)

$$\epsilon^{1/(1-\alpha)} \geq (1-e^{-1})\frac{\mathfrak{M}-1}{\mathfrak{M}\mathfrak{T}-1} \implies \epsilon \geq \left((1-e^{-1})\frac{\mathfrak{M}-1}{\mathfrak{X}-1}\right)^{1-\alpha}.$$

A similar argument can be used for the $(\mathfrak{M}, \mathfrak{X}, \mathfrak{R}, \alpha, \epsilon)$-strong LR-AMD code: For uniform randomness R and the variable Z such that $\tilde{H}_\infty(R|Z) \geq (1-\alpha)\log\mathfrak{R}$, the adversary can use a similar strategy to Algorithm B.1 with $\alpha\log\mathfrak{R}$ questions to achieve the success chance of (noting that there are at least $\mathfrak{R}(\mathfrak{M}-1)$ valid δ values in $\mathcal{H}_0$)

$$\epsilon \geq (1-e^{-1})\mathfrak{R}^{\alpha}\frac{\mathfrak{R}(\mathfrak{M}-1)}{\mathfrak{X}-1}.$$

In a strong LR-AMD code, the adversary is assumed to know the message. So the randomness size $\mathfrak{R}$ should be large enough to satisfy $\mathfrak{R}^{1-\alpha} \geq 1/\epsilon$. Combining this with the above shows that $(0 \leq \alpha \leq 1)$

$$\epsilon^{2/(1-\alpha)} \geq (1-e^{-1})\frac{\mathfrak{M}-1}{\mathfrak{X}-1} \quad\Longrightarrow\quad \epsilon \geq \left((1-e^{-1})\frac{\mathfrak{M}-1}{\mathfrak{X}-1}\right)^{(1-\alpha)/2},$$

which gives (B.2). □ □

We now use (B.1) to lower bound the effective tag length of weak AMD code families as

$$\begin{aligned}
\log\mathfrak{X}-\nu &\geq \log\frac{\mathfrak{X}}{\mathfrak{M}} = \log\left(\frac{\mathfrak{X}}{\mathfrak{M}-1}\times\frac{\mathfrak{M}-1}{\mathfrak{M}}\right) \geq \log\frac{\mathfrak{X}-1}{\mathfrak{M}-1} + \log(1-\mathfrak{M}^{-1}) \\
&\geq \max\{\frac{1}{1-\alpha}\log\frac{1}{\epsilon}\ ,\ \log\frac{1}{\epsilon}+\alpha\log\mathfrak{M}\} + \log(1-e^{-1}) + \log(1-\mathfrak{M}^{-1}) \\
&\geq \max\{\frac{\kappa}{1-\alpha}\ ,\ \kappa+\alpha\nu\} - 2.
\end{aligned}$$

Similarly, (B.2) can be used to lower bound the effective tag length of strong AMD code families as

$$\begin{aligned}
\log\mathfrak{X}-\nu &\geq \log\frac{\mathfrak{X}-1}{\mathfrak{M}-1} + \log(1-\mathfrak{M}^{-1}) \\
&\geq \frac{2}{1-\alpha}\log\frac{1}{\epsilon} + \log(1-e^{-1}) + \log(1-\mathfrak{M}^{-1}) \geq \frac{2\kappa}{1-\alpha} - 2.
\end{aligned}$$

B.2 Proof of Theorem 12: weak AMD code

We need to show that for the uniformly random message $M \in \mathbb{F}^d$ and any $(\delta_m, \delta_t) \in \mathbb{F}^d \times \mathbb{F}$ such that $\delta_m \neq 0$, it holds

$$\Pr_M(f_{w2}(M+\delta_m) = f_{w2}(M) + \delta_t) \leq \frac{t-1}{q}. \tag{B.3}$$

Since $\delta_m = (\delta_{m,1}, \ldots, \delta_{m,d}) \neq 0$, there exists at least non-zero one element $\delta_{m,o} \neq 0$ for $1 \leq o \leq d$. This lets us write the term $f_{w2}(M+\delta_m) - f_{w2}(M) - \delta_t$ as a polynomial of degree $t-1$ with respect to the variable M_o, i.e.,

$$\begin{aligned} Poly(M_o) \quad &\triangleq f_{w2}(M+\delta_m) - f_{w2}(M) - \delta_t = \left[\sum_{i=1}^{d} (M_i + \delta_{m,i})^t - M_i^t\right] - \delta_t \\ &= \sum_{j=1}^{t} \binom{t}{j} \delta_{m,o}^j M_o^{t-j} + a_0, \end{aligned} \tag{B.4}$$

where $a_0 = \left[\sum_{i=1, i\neq o}^{d} (M_i + \delta_{m,i})^t - M_i^t\right] - \delta_t$ is the constant term of the polynomial (w.r.t. M_o). For any values of $(M_i)_{i\neq o}$, hence fixed a_0, the polynomial $Poly(M_o)$ evaluates to zero for at most $t-1 \leq 2$ (out of q) values of M_o. The polynomial thus becomes zero with probability at most $2/q$, implying (B.3).

The effective tag length of this code family is obtained as follows. For integers $\kappa, \nu \in \mathbb{N}$, let $q = 2^{\kappa+1}$ and $d = \lceil \nu / \log q \rceil$ so that both $\epsilon = 2/q \leq 2^{-\kappa}$ and $|\mathcal{F}^d| = q^d \geq 2^\nu$ are satisfied. By restricting the source space $\mathcal{F}^d$ to only $\mathfrak{M} = 2^\nu$ elements the code range will also reduce to $\mathfrak{X} = q2^\nu$ elements in $\mathcal{F}^{d+1}$. This fact gives

$$\log \mathfrak{X} - \nu = \nu + \log q - \nu = \kappa + 1.$$

B.3 Proof of Theorem 13: strong LR-AMD code

Let Enc/Dec denote a $(\mathfrak{M}, \mathfrak{X}, \mathfrak{R}, \epsilon)$-strong AMD code. The security property implies (when there is no leakage)

$$\forall m: \quad \max_{\delta} \Pr_R(Dec(Enc(R;m) + \delta) \notin \{m, \perp\}) \leq \epsilon, \tag{B.5}$$

where R is the uniformly distributed randomness of the encoder. For any m and any δ, define $\mathcal{R}_{fail}(m,\delta) \subseteq \mathcal{R}$ as the set of r values that lead to the verification failure, by satisfying $Dec(Enc(R;m)+\delta) \notin \{m, \perp\}$. Since R has uniform distribution, the probability that $R \in \mathcal{R}_{fail}(m,\delta)$ equals to $|\mathcal{R}_{fail}(m,\delta)|/\mathfrak{R}$; thus, to write (B.5) as $\forall m: \ \max_\delta |\mathcal{R}_{fail}(m,\delta)| \leq \epsilon\mathfrak{R}$.

Let Z be any random variable such that the randomness R is $(1-\alpha)$-weak conditioned on Z for $0 \leq \alpha \leq 1$, i.e., $E_z \max_r \Pr(R=r|Z=z) \leq \mathfrak{R}^{\alpha-1}$. For any message m, the probability of failure when Z is leaked to the adversary $\mathcal{A}dv$ is upper bounded as

$$
\begin{aligned}
&\Pr(Dec(Enc(R;m)+\mathcal{A}dv(Z)) \notin \{m,\perp\}) \\
&\quad = E_z \Pr(Dec(Enc(R;m)+\mathcal{A}dv(z)) \notin \{m,\perp\}|Z=z) \\
&\quad \leq E_z \max_\delta \Pr(R \in \mathcal{R}_{fail}(m,\delta) \mid Z=z) = E_z \max_\delta \sum_{r\in\mathcal{R}_{fail}(m,\delta)} \Pr(R=r|Z=z) \\
&\quad \leq E_z \max_\delta |\mathcal{R}_{fail}(m,\delta)| \max_r \Pr(R=r|Z=z) \\
&\quad = \max_\delta |\mathcal{R}_{fail}(m,\delta)| \ \ E_z \max_r \Pr(R=r|Z=z) \leq \epsilon\mathfrak{R}^\alpha.
\end{aligned}
$$

B.4 Proof of Theorem 14: weak BLR-AMD code

The code construction is systematic, so we only need to show the security property. Let the message $M \in \mathbb{F}^d$ come from a $(1-\alpha)$-block-source, the codeword be $X=(M,G) \in \mathbb{F}^{d+1}$ where $G=f_{dlr}(M)$, and the leakage information be $Z=f(X)$ for some $(d-1)$-block-leakage function $f: \mathbb{F}^{d+1} \to \mathcal{L}$. Letting Enc_{dlr}/Dec_{dlr} denote the encoding and decoding functions, the decoding failure probability when Z is leaked to the adversary

$\mathcal{A}dv$ is upper bounded as

$$\begin{aligned}
&\Pr(Dec_{dlr}(Enc_{dlr}(M) + \mathcal{A}dv(Z)) \notin \{m, \perp\}) \\
&= E_z \Pr(Dec_{dlr}(Enc_{dlr}(M) + \mathcal{A}dv(z)) \notin \{m, \perp\} | Z = z) \\
&\leq E_z \max_{\delta} \Pr(Dec_{dlr}(Enc_{dlr}(M) + \delta) \notin \{m, \perp\} | Z = z)
\end{aligned}$$

We thus need to show that for any $\delta = (\delta_m, \delta_t) \in \mathbb{F}^d \times \mathbb{F}$ such that $\delta_m \neq 0$, it holds

$$E_z \max_{\delta_m \neq 0, \delta_t} \Pr_{M}(f_{dlr}(M + \delta_m) = f_{dlr}(M) + \delta_t \mid Z = z) \leq \frac{\psi d}{q^{1-\alpha}}. \tag{B.6}$$

Since $f(.)$ is $(d-1)$-block-leakage, there is a set $I \subset \{1, 2, \ldots, d+1\}$ of size at most $d-1$ such that we have $Z = f'(X_I)$ for some $f' : \mathbb{F}^{d-1} \to \mathcal{L}$. Let s and t such that $0 \leq s < t \leq d+1$ be two indices not in I. Certainly $X_s = M_s$ is a message element since $0 \leq s \leq d$, but there are two cases for X_t, i.e., either $t \leq d$ and $X_t = M_t$ is a message element, or $t = d+1$ and $X_t = f_{dlr}(M)$ is the tag. Both cases imply that there is one message element M_o (where o is either s or t) remains $(1-\alpha)$-weak conditioned on Z, i.e., $\tilde{H}_\infty(M_o|Z) \geq (1-\alpha)\log q$, noting that M is a $(1-\alpha)$-block-source.

We now write the term $f_{dlr}(M + \delta_m) - f_{dlr}(M) - \delta_t$ as

$$\begin{aligned}
f_{dlr}(M + \delta_m) - f_{dlr}(M) - \delta_t &= \sum_{i=1}^{d} \left[\tau^{\sum_j g_{i,j}(M_j + \delta_{m,j})} - \tau^{\sum_j g_{i,j} M_j} \right] - \delta_t \\
&= \sum_{i=1}^{d} \left[\left(\tau^{\sum_j g_{i,j}\delta_{m,j}} - 1 \right) \tau^{\sum_{j \neq o} g_{i,j} M_j} \tau^{g_{i,o} M_o} \right] - \delta_t
\end{aligned}$$

Letting $a_0 = -\delta_t$, $Y = \tau^{M_o}$, and a_i be the coefficient of $Y^{g_{i,o}}$ in the summation, i.e.,

$$a_i = \left(\tau^{\sum_j g_{i,j}\delta_{m,j}} - 1 \right) \tau^{\sum_{j \neq o} g_{i,j} M_j},$$

one can write the above as a polynomial

$$P(Y) \stackrel{\triangle}{=} f_{dlr}(M + \delta_m) - f_{dlr}(M) - \delta_t = \sum_{i=1}^{d} [a_i Y^{g_{i,o}}] + a_0 \tag{B.7}$$

which is of degree at most $\max_i(g_{i,o}) = \psi d$ over $\mathbb{F}$. Lemma 27 shows that the polynomial has degree is at least 1 since the polynomial has at least one non-zero coefficient, with high probability.

Lemma 27. *For any $\delta = (\delta_m, \delta_t)$ such that $\delta_m \neq 0$, the polynomial $p(Y)$ has at least one non-zero coefficient.*

Proof. We prove the claim by contradiction. Assume that all a_i's are zero, implying (τ is a primitive element in $\mathbb{F}_q$)

$$\forall 1 \leq i \leq d: \quad \Big(\tau^{\sum_j g_{i,j}\delta_{m,j}} - 1\Big)\tau^{\sum_{j\neq o} g_{i,j}M_j} = 0 \;\Rightarrow\; \tau^{\sum_j g_{i,j}\delta_{m,j}} = 1$$
$$\Rightarrow \sum_{j=1}^{d} g_{i,j}\delta_{m,j} = 0 \mod q-1.$$

The above can be written as $\delta_m.G = 0$ over $\mathbb{Z}_{q-1}$, which holds only if $\delta_m = 0$ as G is non-singular. This contradicts the adversarial assumption $\delta_m \neq 0$. □ □

The polynomial $P(Y)$ is a non-constant polynomial with degree at most ψd, hence there are at most ψd values of Y that make the polynomial evaluate to zero. On the other hand, there are at most $\psi d + 1$ values of M_o corresponding to these Y values (the additional 1 is for when the roots include $Y = 1$ which corresponds to $M_o \in \{0, q-1\}$). Let $\mathcal{M}_{o,fail}(\delta)$ of size at most $\psi d+1$ be the set of such M_o values that lead to verification failure. The security property (B.8) is proved as

$$\begin{aligned} &E_z \max_{\delta_m\neq 0,\delta_t} \Pr_M(f_{dlr}(M+\delta_m) = f_{dlr}(M) + \delta_t \mid Z = z) \\ &\quad \leq E_z \max_{\delta_m\neq 0,\delta_t,(m_j)_{j\neq o}} \Pr(M_o \in \mathcal{M}_{o,fail}(\delta) \mid Z = z) \\ &\quad \leq \max_{\delta_m\neq 0,\delta_t,(m_j)_{j\neq o}} |\mathcal{M}_{o,fail}(\delta)| \;.\; E_z \max_{m_o} \Pr(M_o = m_o \mid Z = z) \leq \frac{\psi d}{q^{1-\alpha}}. \end{aligned}$$

B.5 Proof of Theorem 15: robust SSS

For the $(1-\alpha)$-block-source secret $S \in \mathcal{U}^d$ let $X = Enc(S) \in \mathcal{F}^l$, $Sh = (Sh_i)_{i=1}^t = \mathbf{Share}^*(S) = (\mathbf{Share}(X_1^n), \ldots, \mathbf{Share}(X_{(t-1)n+1}^d))$, and $Sh' = (Sh'_i)_{i=1}^t$ be the manipulated share vector as in Deification 46. We define $\delta_{sh} = Sh' - Sh$ whose elements are

zero for honest players, Λ for absent players, and adversarially chosen values for the unqualified or intermediate subset $\mathcal{B}$ of dishonest players. The linearity of the SSS lets us write for any $1 \leq i \leq t$,

$$\mathbf{Rec}(Sh'_i) = \begin{cases} \perp, & \text{if } \mathbf{Rec}(\delta_{sh,i}) = \perp \\ (X^{in}_{(i-1)n+1} + \delta_i), & \text{else} \end{cases},$$

where $\delta_i = \mathbf{Rec}(\delta_{sh,i})$ is determined arbitrarily by an adversary whose knowledge of the secret is $Z = Sh^{\mathcal{B}}$. We hence write $\delta = \mathcal{A}dv(Z)$ for some adversary function. The definition of the somewhere-perfect SSS implies that the overall leakage can be written as $Z = f(X)$ for some t-block-leakage function f, where $t = w(n-1) = l - w \geq l - 2$. The BLR-AMD code security property hence promises that

$$\Pr(\mathbf{Rec}^*(Sh') \notin \{S, \perp\}) \leq \Pr_{S,\mathcal{A}dv}(Dec(Enc(S) + \mathcal{A}dv(Z) \notin \{S, \perp\}) \leq \epsilon.$$

B.6 Proof of Theorem 16: AMD over EWC

For uniform message $M = (M_1, M_2, \ldots, M_d) \in \mathbb{F}_q^d$, we denote its tag by $T = f_{dlr}(M) \in \mathbb{F}_q$. The codeword $X = (M, T) \in \mathbb{F}_q^{d+1}$ is transmitted over the (u, p)-EWC as a sequence of u-ary symbols: letting $q = u^\eta$ each codeword element $X_i \in \mathbb{F}_q$ consists of η such symbols. The wiretapping adversary observes each u-ary symbol independently with probability $1 - p$; in other words each symbol is erased by the channel with probability p. The probability that one codeword element is completely erased is thus $p' = p^\eta = p^{\log_u(q)} = q^{\log_u(p)} = q^{\zeta - 1}$, where $\zeta = \log_u(pu)$. We shall prove that with high probability $(\geq 1 - \exp\left(-\frac{(d+1)}{8q^{1-\zeta}}\right))$ the wiretap channel leakage matches a $(l-2)$-block-leakage, for which the BLR-AMD code can detect algebraic manipulation except with probability $\frac{\psi d+1}{q}$. Let $Erase^{2+}$ denote the event that the wiretap channel leakage Z misses at least

two elements the codeword X. We obtain the probability of this events as

$$\begin{aligned}\Pr(Erase^{2+}) &= 1-\sum_{i=0}^{1}\binom{d+1}{i}p'^{i}(1-p')^{d+1-i} \overset{(a)}{\geq} 1-e^{-\frac{((d+1)p'-1)^2}{2(d+1)p'}} \\ &\geq 1-e^{-\frac{((d+1)p')^2}{8(d+1)p'}} = 1-e^{-\frac{(d+1)p'}{8}} = 1-e^{-\frac{(d+1)}{8q^{1-\zeta}}}. \end{aligned} \tag{B.8}$$

Inequality (a) uses the Chernoff bound. The overall detection failure probability is upper bounded by the summation of the probability that $Erase^{2+}$ does not occur and the probability that the BLR-AMD constriction fails, which equals $exp\left(-\frac{(d+1)}{8q^{1-\zeta}}\right)+\frac{\psi d+1}{q}$.

B.7 Proof of Proposition 3: bitwise manipulation detection

The code rate is simply the product of the rates of the Manchester code, 0.5, and the BLR-AMD code, $\frac{d}{d+1}$. We moreover prove that failure probability of the code Enc_b/Dec_b equals that the BLR-AMD code over p-BEWC (or $p/2$-BSWC), which equals

$$\frac{\psi d+1}{2^v}+\exp\left(-\frac{(d+1)p^v}{8}\right), \tag{B.9}$$

for uniform message. We show this by discussing that using on-off keying and Manchester coding causes a bitwise manipulation adversary to be either detected or behave like an additive (keep and flip) adversary, whose manipulation is detected by the BLR-AMD code from Theorem 16. For message M, we denote the n-bit codeword $X=Enc(M)$, where $n=2(d+1)v$, by $X=(X_1,X_2,\ldots,X_n)$. The on-off keying transmission makes the adversary only choose from keep, flip, and set-to-1 functions. Assume such an adversary wants to tamper with the codeword and let $Tamp_A=(t_1,t_2,\ldots,t_n)$ be the sequence of bit-manipulation functions over the set of keep, flip, and set-to-1. We claim that $Dec_{mn}(Tamp_A(X))\in\{\perp, Dec_{mn}(Tamp_S(X))\}$, where $Tamp_S=(t'_1,t'_2,\ldots,t'_n)$ is an "additive" manipulation sequence such that $\forall 1\leq i\leq n/2$:

$$(t'_{2i-1},t'_{2i})=\begin{cases}\text{(keep, keep)}, & (t_{2i-1},t_{2i})\in\{\text{(keep, set-to-1)},\text{(set-to-1, keep)},\text{(set-to-1, set-to-1)}\}\\ \text{(flip, flip)}, & (t_{2i-1},t_{2i})\in\{\text{(flip, set-to-1)},\text{(set-to-1, flip)}\}\\ (t_{2i-1},t_{2i}), & \text{else}\end{cases} \tag{B.10}$$

We consider the case where $Dec_{mn}(Tamp_A(X)) \neq \perp$ since otherwise we are done with the proof. For every $1 \leq i \leq n/2$, the pair of codeword bits (X_{2i-1}, X_{2i}) are either 01 or 10. We can prove the above claim by showing that, in both of these cases,

$$(t'_{2i-1}(X_{2i-1}), t'_{2i}(X_{2i})) = (t_{2i-1}(X_{2i-1}), t_{2i}(X_{2i})). \tag{B.11}$$

We do this for $(X_{2i-1}, X_{2i}) = 01$ and the other case can be argued similarly. Note that the equality (B.11) holds trivially from (B.10) if the pair (t_{2i-1}, t_{2i}) does not include any set-to-1 function. Otherwise, the only valid options are $(t_{2i-1}, t_{2i}) \in \{$ (keep, set-to-1), (set-to-1, flip) $\}$. It is easy to see that the equality (B.11) holds for both options.

B.8 Proof of Proposition 4: manipulation detection and privacy

Let $n = 2(d+1)v$ and $k = dv$. The codeword $C = Enc_{wb}(M) \in \{0,1\}^n$ is obtained by applying three encoding functions sequentially. The first (wiretap) encoding gives $X = Enc_w(M) \in \{0,1\}^k$ which is uniform for the uniform message $M \in \{0,1\}^t$. The second (BLR-AMD) encoding gives $Y = (X, f_{dlr}(X)) \in \{0,1\}^{n/2}$, and the third (Manchester) encoding results in $C = Enc_{mn}(Y)$. The code rate is simply $t/n = (td)/(2k(d+1))$. The bitwise manipulation detection failure probability also equals that of the code Enc_b/Dec_b and uniformity of X (see Proposition 3). It remains to prove the privacy property of the code.

We only show privacy over p-BEWC, noting that it also implies privacy over p-BSWC since the latter channel output can be constructed by the former. Manchester encoding Enc_{mn} appends to each bit of $Y = (X, f_{dlr}(X))$ its negation, which has the same amount of information as the bit itself. If both a bit and its negation are erased by p-BEWC (which occurs with probability $p' = p^2$), the Eve cannot discover the bit. This implies that Eve's view $Z = BEC_p(C)$ can be constructed by $Z' = BEC_{p'}(Y)$ that is the view of an eavesdropper over the p'-BEC without Manchester coding. This allows us to

remove the role of Manchester coding and assume that Eve's view is $Z' = (Z'_1, Z'_2)$, where $Z'_1 = BEC_{p'}(X)$ and $Z'_2 = BSC_{p'}(f_{dlr}(X))$. We conclude

$$\begin{aligned} I(M;Z) = I(M;Z'_1,Z'_2) &= I(M;Z'_1) + I(M;Z'_2|Z'_1) \leq I(M;Z'_1) + H(Z'_2) \\ &\leq I(M;Z'_1) + (n/2-k) \leq I(M;Z'_1) + v \\ \Rightarrow I(M;Z)/t &\leq \epsilon + v/t \leq 2\epsilon. \end{aligned}$$

B.9 Proof of Proposition 5: AMD for linear-delay adversary

We start by considering the linear-delay adversarial case. For message any $m \in \mathbb{F}^d$ and uniform randomness $R \in \mathbb{F}$, the codeword $X = (m, R, f_s(R;M)) \in \mathbb{F}^{d+2}$ is transmitted over the channel. Let $n = (d+2)u$ denote the code length. When $d \geq \lceil \frac{2}{\gamma} - 2 \rceil$, the success probability of the γ-linear-delay adversary $\mathcal{A}dv_{\mathbf{ldo},\gamma}$ is upper bounded by that of an adversary $\mathcal{A}dv^*$ whose view of the transmission equals $Z = m$, i.e., $\mathcal{A}dv^*$ only sees the message. This is true because the view of $\mathcal{A}dv_{\mathbf{ldo},\gamma}$ at any time can be constructed using the view of $\mathcal{A}dv^*$, since for all $1 \leq i \leq n$:

$$i - \gamma n \leq (1-\gamma)(d+2)u = du + 2u - \gamma(d+2)u \leq du + 2u - \gamma\frac{2}{\gamma}u = du.$$

From lemma 20, the success probability $\mathcal{A}dv^*$ is upper bounded by $(d+1)/q$ for $q = 2^v$; this completer the proof.

A similar proof can be used for the Γ-constant-delay adversary $\mathcal{A}_{\mathbf{cdo},\Gamma}$ when $v \leq \lfloor \Gamma/2 \rfloor$ because again, the view of this adversary can be constructed by that of $\mathcal{A}dv^*$ since

$$i - \Gamma \leq (d+2)u - \Gamma = du + (2u - \Gamma) \leq du.$$

B.10 Proof of Theorem 17: unary coding for constant-delay adversary

Let p_n denote the success probability of the 1-constant-delay adversary, Eve, when the n-unary code is used for algebraic manipulation detection. We prove $p_n \leq 2/(n+1)$ by induction over the code length. The claim for the base case $n = 1$ follows trivially from the fact that the success probability is upper bounded by 1. Assuming that for all integers $i \leq k$, $p_n \leq i/(n+1)$ holds, we shall show that it also holds for $i = k+1$. Let M be uniformly selected from $\{0, 1, \ldots, k+1\}$ and $\mathbf{X} = Enc_u(M)$. Eve aims at choosing the first adversarial noise bit such that her success chance p_{k+1} is maximized. Depending on the first codeword bit X_1, the following cases need to be considered.

Case 1: Eve chooses $\delta_1 = 0$. If we have $X_1 = 0$, Eve will fail since the only valid codeword with this zero prefix is $\underline{0}^{k+1}$ and there is no chance left for her to change it. If $X_1 = 1$, there are $k+1$ codeword with such prefix in the codebook. Removing this bit one from all remaining codewords results in a k-unary code which Eve needs to attack. Using the induction hypothesis, her success chance in this step cannot be more than $2/(k+1)$. Noting that $X_1 = 0$ and $X_1 = 1$ occur with probabilities $1/(k+2)$ and $(k+1)/(k+2)$, respectively, we upper bound Eve's success probability in this case as $\frac{2}{k+2}$.

Case 2: Eve chooses $\delta_1 = 1$. If $X_1 = 0$, Eve will certainly win since she knows that the transmitted codeword must be $\mathbf{X} = \underline{0}^{k+1}$ and the first bit of the forged codeword is $X_1' = 1$. This lets her change $\mathbf{X}$ to any codeword of her choice in the codebook. However, if $X_1 = 1$ there are $k+1$ codewords with such prefix in the codebook while the only choice for a forged codeword is $\mathbf{X}' = \underline{0}^{k+1}$. Using another similar induction argument, it is not hard to show that this leads to a success chance of $1/(k+1)$ for Eve. Eventually, Eve's success chance in this case is upper bounded by $\frac{2}{k+2}$.

The above shows $p_{k+1} \leq \frac{2}{k+2}$, and this proves the Theorem.

B.11 Non-singular $d \times d$ matrix construction over $\mathbb{Z}_p$

Let H be a $d \times d$ diagonal matrix over $\mathbb{Z}_p$, where p is prime and $d < 3p$, with entries $H_{i,i} = i$ for $1 \leq i \leq d$. The following algorithm converts H into a non-singular matrix G that has non-identical entries in each and every column. It is easy to show that the value of s is always upper bounded by $2i$ and thus at the end, all entries in G are less or equal to $2d + d = 3d$.

$G \leftarrow H$

for $j = 1$ to $d - 1$ **do**

  Add column j of G to its column $j + 1$

end for

$s \leftarrow 2$

for $i = 2$ to d **do**

  while s equals any entry of G up to row $i - 1$ **do**

    $s \leftarrow s + 1$

  end while

  Add s times the first row of G to row i

end for

return G

B.12 On-off keying

On-off keying is the simplest form of amplitude-shift keying (ASK) modulation that transmits the bit "1" as the presence a carrier wave signal and the bit "0" as the absence of the signal. The career wave is usually a high frequency sinusoidal signal that is trimmed for a relatively short time interval. We assume that the career wave is deterministic and

publicly known to all the parties (including Eve). Although on-off keying is in essence a binary modulation, it can work with any underlying modulation scheme by letting "0" be the absence of signal and "1" be transmitted as a publicly known (fixed) modulated signal. Manipulation of a bit (transmitted by on-off keying) is by injecting an adversarial

Transmission		Tampering	
bit abstraction	signal	bit abstraction	signal
0	—	keep	—
		flip	
1		set-to-0	×
		set-to-1	

Table B.1: Bitwise manipulation realization for on-off keying.

signal to the channel. Assume that the career wave is one period of the sine signal. As illustrated in Table B.1, there are appropriately-shaped signals to realize the keep, flip, and set-to-1 functions. However, there is no signal to realize a (deterministic) set-to-0 for a bit unless the adversary knows the bit, under which condition she could realize set-to-0 by either keeping or flipping the bit. This property lets us replace, without loss of generality, the unlimited bitwise manipulation adversary with an additive-and-set-to-1 adversary.

Appendix C

Proof Results on Distance Bounding Verification

C.1 Proof of Lemma 22: averaging sampler

For any $m \in \{0,1\}^k$ and sampling sequence $(S_1, \ldots, S_k) = Samp(U_r)$ and define $x \in \{0,1\}^n$ such that

$$\forall i \in [n]: \; x_i = \begin{cases} m_j, & \text{if} \exists j: \; i = S_j \\ 0, & \text{else} \end{cases}.$$

Since X is (μ, δ)-almost-secure conditioned on Y, we have $E_y \max_x \Pr(d_H(X,x) \leq \mu n | Y = y) \leq 2^{-\delta n}$. Define $\Delta_x = X \oplus x \in \{0,1\}^n$ and the event $\mathcal{E}_x$ to be true when $\frac{1}{n}\sum_{i=1}^n \Delta_{x,i} > \mu$; this gives $E_y \max_x \Pr(\overline{\mathcal{E}}_x | Y = y) \leq 2^{-\delta n}$. Conditioned on $\mathcal{E}_x$, the averaging sampler guarantees that

$$\Pr(\frac{1}{k}\sum_{j=1}^k \Delta_{x,S_j} \leq \mu - \theta | \mathcal{E}_x) \leq \gamma.$$

We complete the proof as

$$\begin{aligned}
&E_{y,u} \max_m \Pr(d_H(M,m) \leq (\mu - theta)k | Y = y, U_r = u) \\
&= E_{y,u} \max_m \Pr(\frac{1}{k}\sum_{i=1}^k \Delta_{x,S_j} \leq \mu - \theta | Y = y, U_r = u) \\
&\leq E_{y,u} \max_m \Pr(\frac{1}{k}\sum_{i=1}^k \Delta_{x,S_j} \leq \mu - \theta | \mathcal{E}_x, Y = y, U_r = u) + \Pr(\overline{\mathcal{E}}_x | Y = y, U_r = u) \\
&= E_{y,u} \max_m \Pr(\frac{1}{k}\sum_{i=1}^k \Delta_{x,S_j} \leq \mu - \theta | \mathcal{E}_x) + \Pr(\overline{\mathcal{E}}_x | Y = y) \leq \gamma + 2^{-\delta n}. \square
\end{aligned}$$

C.2 Proof of Lemma 23: BSWC representation of PLAN

Let $S \in \{0,1\}$ be a bit to be delivered to an intended distance d over the $\texttt{PLAN}^{\xi,\alpha,\Sigma}$ environment using $Mod_E/Demod$ functions. Applying the modulator function to S gives $X = Mod_E(S)$, where $E = \left(\frac{d}{d_0}\right)^{\alpha} E_0$. When X is transmitted, the signals received at distances d and ψd are respectively denoted by $Y = X' + N_y$ and $Z = X'' + N_z$, where $X' = (\xi d^{\alpha})^{-0.5} X$, $X'' = (\xi(\psi d)^{\alpha})^{-0.5} X$, and N_y and N_z are noise variables generated by independent sources both with Gaussian distribution $\sim \mathcal{N}(0, \sqrt{\Sigma})$. Let $p_{\mathbf{i}}$ and $p_{\mathbf{b}}$ be errors in estimating S in the intended and the blocked receivers at distances d and ψd, respectively.

We obtain $p_{\mathbf{i}}$ by noting that the intended receiver can calculate $S' = Demod(Y)$, which implies $p_{\mathbf{i}} = \Pr(S' \neq S)$. We have

$$\begin{aligned}\Pr(S'=1|S=0) &= \Pr(Y>0|X=-\sqrt{E}) = \Pr(Y>0|X'=-\sqrt{\frac{E}{\xi d^{\alpha}}}) \\ &= \Pr(N_y > \sqrt{\frac{E_0}{\xi d_0^{\alpha}}}) = \frac{1}{2}\text{erfc}(\sqrt{SNR^*}),\end{aligned}$$

and due to symmetry $\Pr(S'=0|S=1) = \frac{1}{2}\text{erfc}(\sqrt{SNR^*})$. This concludes that

$$p_{\mathbf{i}} = \frac{1}{2}\text{erfc}(\sqrt{SNR^*}).$$

We obtain the bit error probability $p_{\mathbf{b}}$ at the blocked receiver by calculating its com-

plement, i.e., the success chance in guessing S using the knowledge of Z.

$$\begin{aligned}
1-p_{\mathbf{b}} &= E_z \max_s \Pr(S=s|Z=z) = \int_{-\infty}^{\infty} \max_s f_Z(z|S=s).\Pr(S=s)\ dz \\
&= \int_{-\infty}^{0} f_Z(z|S=0).\Pr(S=0)\ dz + \int_{0}^{\infty} f_Z(z|S=1).\Pr(S=1)\ dz \\
&= \Pr(S=0)\left(\int_{-\infty}^{0} f_Z(z|X=-\sqrt{E})\ dz\right) + \Pr(S=1)\left(\int_{0}^{\infty} f_Z(z|X=\sqrt{E})\ dz\right) \\
&= \Pr(S=0)\left(\int_{-\infty}^{\sqrt{\frac{E_0}{\xi(d_0\psi)^\alpha}}} f_N(n)\ dn\right) + \Pr(S=1)\left(\int_{-\sqrt{\frac{E_0}{\xi(d_0\psi)^\alpha}}}^{\infty} f_N(n)\ dn\right) \\
&= \left(1-\frac{1}{2}\mathrm{erfc}(\sqrt{\frac{SNR^*}{\psi^\alpha}})\right)\Big(\Pr(S=0)+\Pr(S=1)\Big) \\
&= 1-\frac{1}{2}\mathrm{erfc}(\sqrt{\frac{SNR^*}{\psi^\alpha}}).
\end{aligned}$$

This shows that

$$p_{\mathbf{b}} = \frac{1}{2}\mathrm{erfc}(\sqrt{\frac{SNR^*}{\psi^\alpha}}).$$

C.3 Proof of Proposition 6: basic DBV

For any choice of $E_0 \leq E_{max}$, the error probabilities $p_{\mathbf{i}}$ and $p_{\mathbf{b}} > p_{\mathbf{i}}$ (at distances $d_{\mathbf{c}}$ and $\psi d_{\mathbf{c}}$, respectively) are determined by Lemma 23. For uniform challenge $M \in bset^k$, let $X = Mod_E(M)$ be transmitted and Y and Z be received at distances $d_{\mathbf{c}}$ and $\psi d_{\mathbf{c}}$, respectively. For an honest prover at distance $d_{\mathbf{c}}$, the probability of being rejected equals to the probability that there are more than βk errors in $\hat{M} = Demod(Y)$. The completeness condition of Definition 56 requires

$$\sum_{i>\beta k} \binom{k}{i} p_{\mathbf{i}}^i (1-p_{\mathbf{i}})^{k-i} \leq \epsilon_{\mathtt{FR}}. \tag{C.1}$$

For a dishonest prover at distance $\psi d_{\mathbf{c}}$, the best probability of being accepted is obtained by choosing $Demod(Z)$ as response, noting that $p_{\mathbf{b}} < 0.5$, the communication channel is memoryless, and the challenge is uniform. The acceptance probability hence equals to the probability that there are at most βk errors in $Demod(Z)$. The completeness

condition of Definition 56 requires

$$\sum_{i \leq \beta k} \binom{k}{i} p_{\mathbf{b}}^{i} (1 - p_{\mathbf{b}})^{k-i} \leq \epsilon_{\mathtt{FA}}. \tag{C.2}$$

We let $p_{\mathbf{i}} < \beta < p_{\mathbf{b}}$ and apply Chernoff's inequality to simplify (C.1)-(C.2) as

$$\exp\left(-\frac{(\beta - p_{\mathbf{i}})^2}{\beta + p_{\mathbf{i}}} k\right) \leq \epsilon_{\mathtt{FR}}, \text{ and } \exp\left(-\frac{(p_{\mathbf{b}} - \beta)^2}{2p_{\mathbf{b}}} k\right) \leq \epsilon_{\mathtt{FA}}. \tag{C.3}$$

These inequalities suggest

$$k \geq \max\{\frac{(p_{\mathbf{i}} + \beta)\ln(1/\epsilon_{\mathtt{FR}})}{(\beta - p_{\mathbf{i}})^2}\ ,\ \frac{(2p_{\mathbf{b}})\ln(1/\epsilon_{\mathtt{FA}})}{(p_{\mathbf{b}} - \beta)^2}\}. \tag{C.4}$$

C.4 Proof of Theorem 18: BRM-DBV for general intruder

We shall show that the BRM-DBV protocol is complete and is sound against all three attacks. The completeness follows directly from the DBV protocol Π_2. Soundness against DFA and MFA is also implied by TFA-security, because these two attacks against the DBV protocols becomes special cases of terrorist fraud: DFA can be realized when $\mathbb{I}$ does not do any activity, and MFA can be realized when $\mathbb{P}$ follows the protocol honestly. Thus, we only focus on TFA-security, for which we should assume that $\mathbb{P}$ is really located at a distance $d_{\mathbf{r}} \geq \psi d_{\mathbf{c}}$.

Without loss of generality, we consider the strongest TFA scenario where all communication to and from $\mathbb{I}$ is error-free (it is literally located pretty close to $\mathbb{V}$) and $\mathbb{P}$'s distance is the $d_{\mathbf{r}} = \psi d_{\mathbf{c}}$. $\mathbb{V}$'s BRM oracle sends X_O over the PLAN environment, $\mathbb{P}$ observes Y_O, and $\mathbb{I}$ observes (with no error) X_O; however, each party can only retrieve $k = \lambda n$ bits from what they observe.

Upon receiving X_O (or its binary equivalent O), $\mathbb{I}$ retrieves $f_{\text{adv}}(O)$ for some function $f_{\text{adv}} : \{0,1\}^n \to \{0,1\}^k$ which is chosen based on the leaked knowledge W about SK_e, which is given by $\mathbb{P}$ to $\mathbb{I}$. The definition of TFA requires that W does not increase $\mathbb{I}$'s

success chance in impersonation. We give a proof sketch to argue that W cannot help improve the TFA's success chance either. (We do not provide a formal proof due to lack of space.) The above requirement on W implies the independence of W and the averaging sampler output $Samp(\mathsf{SK}_e)$; otherwise, knowing about the indices of X selected by the sampler would increase $\mathbb{I}$'s chance in impersonation. We can thus replace the key SK_e with a new variable SK'_e that is independent of W and whose values determine all possible outputs from $Samp(\mathsf{SK}_e)$. This suggests that either SK_e is independent of W or it can be replaced by SK'_e that is independent of W. Hereon, we assume that W and hence $f_{\text{adv}}(.)$ are independent of SK_e.

On the prover's side, there is the noisy signal Y_O as well as the secret key SK. Letting $V = (f_{\text{adv}}(X_O), Y_O, \mathsf{SK})$ we shall prove:

$$E_v \max_m \Pr(d_H(M, m) \leq \beta k | V = v) \leq \epsilon_{\mathtt{FA}}. \tag{C.5}$$

For fixed E_0, let $p_{\mathbf{b}}$ be the bit error probability in $\mathbb{P}$'s receiver (at distance $d_{\mathbf{r}}$) which is obtained from Lemma 23. Using Chernoff's inequality shows that for any $\mu < p_{\mathbf{b}}$,

$$E_y \max_o \Pr(d_H(O, o) \leq \mu n | Y_O = y) = \sum_{i \leq \mu n} \binom{n}{i} p_{\mathbf{b}}^i (1 - p_{\mathbf{b}})^{n-i} \leq \exp\left(-\frac{(p_{\mathbf{b}} - \mu)^2}{2p_{\mathbf{b}}} n\right). \tag{C.6}$$

That is O is (μ, δ_1)-almost-secure conditioned on Y_O, where $\delta_1 = \frac{(p_{\mathbf{b}} - \mu)^2}{2\ln(2) p_{\mathbf{b}}}$. Using Lemma 21 shows us that O is (μ, δ_2)-almost-secure conditioned on $(Y_O, f_{\text{adv}}(X_O))$, where $\delta_2 = \delta_1 - \lambda$ is positive because $\mu + \ln(2)\lambda + \sqrt{(\ln(2)\lambda)^2 + 2\ln(2)\mu\lambda} < p_{\mathbf{b}}$ holds by the theorem. We now apply Lemma 22 which gives us that M is (β, δ')-almost-secure conditioned on $(Y_O, f_{\text{adv}}(X_O), \mathsf{SK})$, where $\beta = \mu - \theta$ and $\delta' = \log(\gamma + 2^{-\delta_2 n})/k = \log(\epsilon_{\mathtt{FA}})/k$ as mentioned by the theorem. This completes the proof.

C.5 Proof of Theorem 19: BRM-DBV for sampling intruder

The proof here requires one step modification compared to that of Appendix C.4 (for Theorem 18), which relies on the sampling intruder assumption. For this intruder, the

retrieval function $f_{\text{adv}} : \{0,1\}^n \to \{0,1\}^k$ is a sampling function, i.e., $f_{\text{adv}}(O) = O_I$ for some fixed set of k indices $I = \{i_1, \ldots, i_k\} \subseteq [n]$, which is selected independently of SK. Let $\bar{I} = [n] - I$ denote the complement of I. Given $(Y_O, f_{\text{adv}}(O))$, the adversary first determines O_I, calculates $O' = Demod(Y_O)$, and uses each bit of $O'_{\bar{I}}$ to obtain some information about the corresponding bit of $O_{\bar{I}}$.

For fixed E_0, let $p_{\mathbf{b}}$ be the bit error probability at distance $d_{\mathbf{r}}$, obtained from Lemma 23. We calculate δ such that O is (μ, δ)-almost secure conditioned on $(Y_O, f_{\text{adv}}(O))$ as follows (we use Chernoff's inequality since $\mu < (1-\lambda)p_{\mathbf{b}}$).

$$
\begin{aligned}
E_{a,y} \max_o \Pr(d_H(O,o) \le \mu n | Y_O = y, f_{\text{adv}}(O) = a) &= E_{o'_{\bar{I}}} \max_{o_I} \Pr(d_H(O_I, o_I) \le \mu n | O'_{\bar{I}} = o'_{\bar{I}}) \\
&= \sum_{i \le \mu n} \binom{(1-\lambda)n}{i} p_{\mathbf{b}}^i (1-p_{\mathbf{b}})^{n-i} \le \exp\left(-\frac{((1-\lambda)p_{\mathbf{b}} - \mu)^2}{2(1-\lambda)p_{\mathbf{b}}} n \right) \\
\Rightarrow \quad \delta &\le \frac{((1-\lambda)p_{\mathbf{b}} - \mu)^2}{2\ln(2)(1-\lambda)p_{\mathbf{b}}}
\end{aligned}
$$

Applying Lemma 22 lets us conclude that M is (β, δ')-almost-secure conditioned on $(Y_O, f_{\text{adv}}(X_O), \mathsf{SK})$, where $\beta = \mu - \theta$ and $\delta' = \log(\gamma + 2^{-\delta n})/k$ which equals $\log(\epsilon_{\mathtt{FA}})/k$ according to the theorem.