2015-07-24

Secure Communication over Adversarial Channel

wang, pengwei

UNIVERSITY OF CALGARY

Secure Communication over Adversarial Channel

by

Pengwei Wang

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

GRADUATE PROGRAM IN COMPUTER SCIENCE

CALGARY, ALBERTA

July, 2015

Abstract

Digital Communications play an important role in modern worlds, and it is crucial to consider the security problems associated with network communication. This dissertation explores the use of physical layer characteristics of communication channels and network multipath to build secure and reliable communication in adversarial setting. We investigate four adversarial models: *limited view adversary channel*, *adversarial wiretap channel*, *adversarial wiretap channel with public discussion*, and *Secure Message Transmission*. The first three models are about secure communication using physical layer characters, and the last is about using network multipath for communication.

We first consider secure and reliable communication over a wiretap channel with an active adversary. We consider on adversarial channel model, in which the adversary is able to eavesdrop the communication between the sender and the receiver, and also corrupt the communication by adding adversarial noise. The model of *limited view adversary* focuses on reliable communication over this channel, and the construction of *limited view adversary code* achieves reliable communication in this setting. *Adversarial wiretap channel* studies secure and reliable transmission over this adversarial channel. We obtain an upper bound on the capacity of this channel, and construct an *adversarial wiretap code* that provides secure and reliable communication over this channel. By allowing communicants to have access to a *public discussion channel*, secure communication becomes possible over adversarial wiretap channel for a wider range of parameters.

We then consider on *Secure Message Transmission* in networks. We propose a new construction for secure message transmission protocols using a *list decodable code* and a *message authentication code*. Our protocol has optimal transmission rate and provides the highest reliability among all known comparable protocols.

Acknowledgements

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

I would like to thank my examination committee: Dr. Payman Mohassel, Dr. Michael J. Jacobson, Dr. Gilad Gour, and Dr. Douglas Stinson, for their evaluation and comment on my work.

I would like to thank Hadi and Ashraful, who inspired my research on wiretap channel and secure message transmission problems. I have learned a lot from them about finding interesting research topic, scheduling work plan, communication skills, and research motivation.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Symbols, Abbreviations and Nomenclature

Symbol	Definition
AWTP	Adversarial Wiretap Channel
$\mathsf{AWTP}_{\mathsf{PD}}$	Adversarial Wiretap Channel with Public Discussion
FRS	Folded Reed-Solomon Code
LVAC	Limited View Adversarial Channel
LV-code	Limited View Adversarial Code
MAC	Message Authentication Code
PD	Public Discussion Channel
RMT	Reliable Message Transmission
SD	Statistical Distance
SMT	Secure Message Transmission
SMT-PD	Secure Message Transmission with Public Discussion

Chapter 1

Introduction

Network communication plays an important role in modern world. Computer networks allow users to connect to the Internet and access services from any part of the world. Many applications such as online banking system, online payment services, stock market services, social networks, and multimedia, can be accessed using the Internet. The new generation of wireless network technologies such as LTE allow fast access to the Internet services. Devices such as smart phones, touch pads, ultrabooks, and smart watches heavily depend on wireless communication to access Internet.

However, network communication, and in particular wireless communication, is sensitive to malicious attacks. It is possible for the adversary to implement eavesdropping and disrupting attacks. For instance, wireless devices broadcast electromagnetic signal. This makes it easier for the adversary to eavesdrop the packets that are transmitted in the channels. With low cost of antenna, adversary can emit a malicious signal to influence the original signal. Malicious attacks on network communication result in high loss to individuals and the society.

Traditional approaches to security have been considered in computational setting, and assume the adversary has limited computational power. Security of traditional cryptography depends on the hardness of computational problems such as integer factorization, discrete logarithm problem, and so on. With the increase in the CPU speed and the emergence of quantum computing, the computational problems which are hard nowadays may be easily solved in future. Cryptographic schemes, that are based on the hardness of computation, may be broken in future. Information theoretic security does not depend on any hardness assumption and so system with information theoretic security can provide security guarantee

for the future.

1.1 Security in Wireless Communication

Unlike wired networks, wireless network signals can be easily intercepted and tampered with by the adversary. First, wireless communication can suffer from the eavesdropping attacks. Since the wireless communication is broadcasted, the signal can be easily eavesdropped by the adversary. Second, wireless communication is susceptible to adversarial jamming. Openness of wireless communication allows the adversary to implement jamming attacks to disrupt the communication. It also allows the adversary to modify the signal and make the receiver decode wrong messages.

Physical Layer Security

Network communication is designed in layers and security solution are implemented at different layers of network. For instance, SSL (Secure Sockets Layer) is at the transport layer, and IPSec protocol is implemented at network layer.

Since wireless security is vulnerable to adversarial eavesdropping and jamming attack at physical layer, security solutions at this layer must be considered. We study noise channel model and study behaviour of adversary over physical layer. We give construction of protocols that achieve secure and reliable communication.

Wiretap Channel

Consider wireless communication. Alice (Sender $\mathcal{S}$) wants to transmit a message to Bob (Receiver $\mathcal{R}$). Eve (Adversary $\mathcal{A}$) eavesdrops the communication between Alice and Bob. We call the channel between Alice and Bob as the main channel, and the channel between Alice and Eve as the eavesdropper channel.

The signals that are observed by Bob and Eve are usually different. The difference can

be caused by the physical layer properties of wireless communication such as fading and path losses. If the channel noise over the main channel is much weaker than the noise over the eavesdropping channel, the signals received by Eve is expected to be weaker than Bob's signal. Since the degradation of signal makes it hard for Eve to decode the original signal sent by Alice, the security solution over wireless communication can take into account the differences of wireless communications over physical layer. It is different from the traditional cryptographic system which only considers the case that Eve receives the same signals as Bob.

Adversarial Jamming

Wireless communication can be easily corrupted by adversarial jamming attacks. Eve is able to add malicious signals to the original signals transmitted between Alice and Bob. This type of attack allows the adversary to modify the signals and messages during the transmission, and make Bob output an error message.

1.2 Security in Network Communication

In network communication, the computer devices are connected by devices, such as routers, switches, and cables. Network communication is vulnerable to adversarial eavesdropping and jamming attacks. Adversary can eavesdrop, and tamper with the packets that are transmitted in the network.

In this dissertation, we study *Secure Message Transmission* (SMT) and *Reliable Message Transmission* (RMT) which are abstractions of network communication problem. The sender and the receiver are abstracted as two nodes, and the network topology is abstracted as disjoint wires that each connects the sender node to the receiver node. The adversary can control a subset of wires and implement eavesdropping and jamming attacks on a subsets of wires, while the communication on the rest of wires are reliable and private to the adversary.

The aim of an SMT protocol is to achieve secure and reliable message communication between Alice and Bob.

1.3 Contributions

We study secure and reliable transmission of message problem over a channel with is partially eavesdropped and jammed by an adversary. Our contributions can be divided into two categories. The first contribution is on secure and reliable communication over wiretap channel with active adversary. We study *limited view adversary channel*, *adversarial wiretap channel*, and *adversarial wiretap channel with public discussion*. The second contribution is a new SMT protocol.

Limited View Adversary Channel

In Chapter 3, we define limited view adversary channels (LVAC) using a (ρ_r, ρ_w) wiretap adversary who can read a fraction ρ_r, and modify a fraction ρ_w, of a sent codeword. The code components that are read and/or modified, can be chosen adaptively, and the subsets of read and modified components could be different. Limited View Adversary Codes (LV codes) provide protection against an adversary who has partial view of the communication channel and can use this view to corrupt the sent codeword by constructing an adversarial error vector that will be added to the codeword. An LV code with δ reliability ensures correct recovery of the sent message with probability at least $1 - \delta$. The motivation for studying these codes models adversarial corruptions in wireless communications as well as networks that are partially controlled by an adversary, with the aim of providing reliable communication.

We have the following contributions. First we prove an upper bound on the rate of LV codes and extend it to a bound on the rate of a code family. Second, we give two explicit constructions of LV code family. The first construction of LV codes achieves the bound on

the condition that $S_r = S_w$, which means the reading set and writing set are same, and the second construction of LV codes relaxes the condition to $\rho_r + \rho_w < 1$, which means that the total fraction of read or write is no more than 1. Both constructions have efficient encoding and decoding algorithm. Finally we show the relationship between LV codes and a cryptographic primitive known as RMT, and use this relation to obtain a new bound on the transmission rate of 1-round δ-RMT protocols, and construct an optimal 1-round RMT protocol family.

Adversarial Wiretap Channel

In Chapter 4, we use the same adversary model as above, and define an adversarial wiretap channel (AWTP) that requires secrecy and reliability for communication over these channels. We define security and reliability for AWTP channels and use these definitions to evaluate security and reliability of codes for these channels.

We have three main contributions. First, we prove an upper bound on the rate of AWTP codes for (ρ_r, ρ_w)-AWTP channels. Second, we give an explicit construction of a perfectly secure AWTP code family with efficient decoding that achieves the bound, and hence obtain the secrecy capacity of the AWTP channel. Finally, we show the relationship between AWTP codes and SMT, and use this relation to obtain a new (and the only known) bound on the transmission rate of 1-round SMT protocols.

Adversarial Wiretap Channel with Public Discussion Protocol

In Chapter 5, we consider a model of adversarial wiretap channel with public discussion. For adversarial wiretap channel, we have shown that secure and reliable communication with arbitrary small ϵ and δ is possible if $\rho_r + \rho_w < 1$. For stronger adversary with reading and writing parameter $\rho_r + \rho_w > 1$, secure and reliable communication is still possible when the

communicants have access to a public discussion channel, and not all codeword components are accessible to the adversary (neither read, nor written to).

We, first, formalize the model of adversarial wiretap channel with public discussion ($\mathsf{AWTP_{PD}}$ protocol). We define secrecy and reliability of $\mathsf{AWTP_{PD}}$ protocols, and give two efficiency measures, rate of information transmission and round complexity. Second, we derive a tight upper bound on the rate, and a tight lower bound on the required number of rounds for an (ϵ, δ)-$\mathsf{AWTP_{PD}}$. We also give the construction of a rate optimal protocol with minimum number of rounds. Finally, we show implications of these results for *Secure Message Transmission with public discussion* (SMT-PD).

Secure Message Transmission Protocol

In Chapter 6, we study SMT and RMT problem. In SMT problem, Alice is connected to Bob through N node disjoint paths in the network, t of which are controlled by an adversary with *unlimited computational power*. Alice wants to send a message m to Bob in a *private* and *reliable* way.

We propose a new approach to the construction of 1-round $(0,\delta)$-SMT protocol for $2t+1 \leq N \leq 3t$ using an approach inspired by private codes that employs list decodable codes and message authentication codes. Our concrete construction uses Folded Reed-Solomon codes and multireceiver message authentication codes. The protocol has optimal transmission rate and gives the smallest δ among all known comparable protocols.

1.4 Organization

The thesis is organized as follow. In Chapter 2, we introduce the fundamentals of information theoretic security, the wiretap channel model, and SMT protocol. In Chapter 3, we study limited view adversary channel. Chapter 4 investigates adversarial wiretap channel. Chapter 5 presents adversarial wiretap channel with public discussion. Finally, in Chapter 6, we show

a construction of an SMT protocol.

Chapter 2

Preliminaries

This chapter provides the basic concepts and definitions. We give the notations used in this work, introduce the information theoretic security definitions, wiretap channel models, and adversarial channel models, and error correctable code. We also describe the model of SMT and SMT-PD.

2.1 Information Theoretic Security

2.1.1 Notions and Definitions

We use calligraphic symbols $\mathcal{X}$ to denote set of elements, X denote the random variable, and x denote an element over set. Let $\mathbf{x}$ denote the vector with length N, and x_i be the i^{th} element in $\mathbf{x}$. Let $\mathsf{Pr}(X)$ be a probability distribution of X, $\mathsf{Pr}(X,Y)$ be the joint distribution of (X,Y), and $\mathsf{Pr}(X|Y)$ be the condition distribution of X on Y. The expected value over distribution X is shown by $\mathsf{E}(X) = \sum_{x\in\mathcal{X}} x\mathsf{Pr}(x)$. We use $X \to Y \to Z$ to show the Markov chain between X, Y, Z. We use log() to denote logarithm in base two.

In information theory, Shannon entropy measures the amount of information contained in a variable [74].

Definition 1. *For a random variable $X \in \mathcal{X}$, the Shannon entropy is denoted by $\mathsf{H}(X)$ and is given by,*

$$\mathsf{H}(X) = -\sum_{x\in\mathcal{X}} \mathsf{Pr}(x)\log \mathsf{Pr}(x).$$

The entropy definition can be extended to a pair of random variables.

Definition 2. *The joint entropy $\mathsf{H}(X,Y)$ of a pair of random variables (X,Y) with a joint*

distribution $\mathsf{Pr}(x, y)$ *is defined by,*

$$\mathsf{H}(X, Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \mathsf{Pr}(x, y) \log \mathsf{Pr}(x, y).$$

We also define the conditional entropy of random variable X given Y.

Definition 3. *For a random variable* X *and* Y*, the conditional entropy of* X *given* Y *is given by,*

$$\mathsf{H}(X|Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \mathsf{Pr}(x, y) \log \mathsf{Pr}(x|y).$$

The mutual information entropy measures the amount of information that one random variable contains about another random variable. It defines the reduction of the uncertainty of one random variable due to the knowledge of the other.

Definition 4. *For a random variable* X *and* Y*, the mutual information entropy of* X *and* Y *is given as,*

$$\mathsf{I}(X; Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \mathsf{Pr}(x, y) \log \frac{\mathsf{Pr}(x)\mathsf{Pr}(y)}{\mathsf{Pr}(x, y)}.$$

We show the relationship between entropy, joint entropy, conditional entropy, and mutual informant entropy.

Lemma 1. *[16] The following relationship holds between Shannon information measaures.*

1.

$$\mathsf{H}(X, Y) = \mathsf{H}(X|Y) + \mathsf{H}(Y),$$

2.

$$\begin{aligned} \mathsf{I}(X; Y) &= \mathsf{H}(X) - \mathsf{H}(X|Y) \\ &= \mathsf{H}(Y) - \mathsf{H}(Y|X) \\ &= \mathsf{H}(X) + \mathsf{H}(Y) - \mathsf{H}(X, Y). \end{aligned}$$

A stochastic process $\{X_i\}$ is an indexed sequence of random variables. There can be arbitrary dependence among random variables. A simple example of stochastic process with dependence is the one in which each random variable only depends on the one that precedes it. Such stochastic process is call Markov chain.

Definition 5. *Random variables X, Y, Z are said to form a Markov chain (denoted by $X \to Y \to Z$) if the conditional distribution of Z depends only on Y, and is conditionally independent of X. Specifically, X, Y, and Z form a Markov chain $X \to Y \to Z$ if the joint probability mass function can be written as,*

$$\mathsf{Pr}(X, Y, Z) = \mathsf{Pr}(X)\mathsf{Pr}(Y|X)\mathsf{Pr}(Z|Y).$$

We use statistical distance between two random variables to measure how similar the two variables are distributed.

Definition 6. *For two random variables $X, X' \in \mathcal{X}$, the statistical distance between X and X' is obtained as $\mathbf{SD}(X, X') = \frac{1}{2}\sum_{x\in\mathcal{X}} |\mathsf{Pr}(X = x) - \mathsf{Pr}(X' = x)|$.*

The Shannon entropy measures the expected uncertainty of information contained in a random variable. In some security settings such as password guessing, the uncertainty of information should be measured in the worst-case. We use min-entropy to measure the minimum information contained in the variable.

Definition 7. *For a random variable $X \in \mathcal{X}$, the min-entropy is denoted as $\mathsf{H}_\infty(X) = -\log \max_x \mathsf{Pr}(x)$.*

Suppose we know a random variable Y and we wish to guess the value of a correlated random variable X. From Y, we calculate a function $g(Y) = X'$, where X' is an estimate of X. We observe that $X \to Y \to X'$ forms a Markov chain. The Fano's inequality relates the conditional entropy and probability of errors in guessing variable X. Fano's inequality is useful to get the bound on rate of channel from the decoding error probability.

Lemma 2. *(Theorem 2.10.1 [16]) For any estimator X' such that $X \to Y \to X'$, with $p_e = \mathsf{Pr}(X \neq X')$, it holds,*

$$\mathsf{H}(X|Y) \leq \mathsf{H}(X|X') \leq \mathsf{H}(p_e) + p_e \log |\mathcal{X}|,$$

This inequality can be weakened to,

$$\mathsf{H}(X|Y) \leq 1 + P_e \log |\mathcal{X}|.$$

2.1.2 Perfect Secrecy

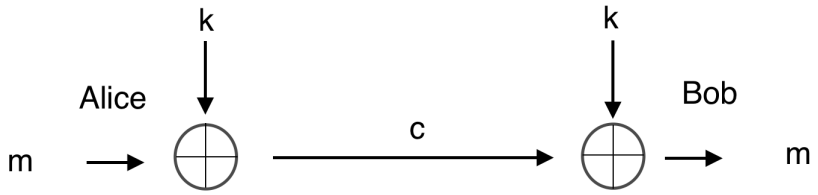
Let the plaintext be M and the ciphertext be C. Prefect security is defined as $\mathsf{H}(M|C) = \mathsf{H}(M)$. This implies the plaintext and ciphertext are statistically independent and the best strategy of an eavesdropping adversary to find the plaintext from a ciphertext is to query using apriori probability. The encryption scheme which is perfectly secure is immune to cryptanalysis, since there is no correlation between the ciphertext and the plaintext.

Shannon one-time pad is an encryption scheme that achieves prefect security. In one-time pad, Alice and Bob share a perfectly random secret key with size at least as long as the message. To encrypt the message, Alice adds over $\mathbb{F}_2$ each bit of the message and the key and transmits the ciphertext to Bob. Bob decrypts the ciphertext by subtracting each bits of key from the corresponding bit of the ciphertext each bits (Figure 2.1.2). One-time pad is information theoretically secure against eavesdropping adversary since every bits of the ciphertext and the plaintext are uncorrelated due to the random key. Though one-time pad achieves information theoretically secure, it needs a shared random key with the same length as the plaintext.

2.2 Wiretap Channel Model

In Shannon's model, the assumption is that the channel between sender and receiver is error-free. However, from the wireless physical layer communication, there exist communication

Figure 2.1: One-time pad



noise between the sender and receiver, as well as the sender and adversary. By allowing the transmission noise, it is possible to achieve communication of unconditional security without any secret key. Wyner [89] proposed wiretap channel model using a realistic communication model. Later Csiszár and Körner [18] extended this model to a more general broadcasting model. In wiretap channel model [18], there are two channels: one channel connects sender and receiver and is called main channel; the other channel connects sender and eavesdropping adversary and is called eavesdropping channel. Due to the noise of wireless communication, the observation of the main channel by the receiver maybe different from that of the eavesdropper. This is different from Shannon's one-time pad, where observation of receiver and eavesdropping adversary are exactly the same. The difference observation makes the decoding ability of the receiver stronger than the adversary if there is less noise in the main channel compared to the eavesdropping channel. Wiretap codes are used to achieve secure communication against unlimited computational eavesdropper over wiretap channel. Wiretap channel was initially studied over discrete memoryless channel [89, 18]. Later Leung-Yan-Cheong *et al.* [55] extended the wiretap channel model to Gaussian wiretap channel model; Ozarow *et al.* [66] extended it to erasure wiretap channel model. The wiretap channel model has also been considered for other communication setting such as fading channels [10] and MIMO channels [58]. All these models consider passive eavesdropping adversary only. Wiretap channel model with active adversary has been considered in [2, 64].

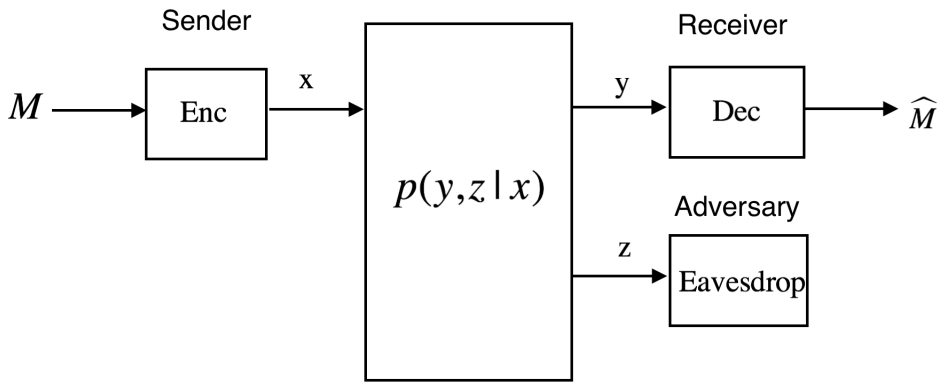
In the following, we formally introduce the Wyner's wiretap channel model, and wiretap

channel II. Then we introduce modeling active adversary using arbitrary varying wiretap channel model that models wiretap channel with an active jamming adversary. We also introduce the proposed security definitions of wiretap channel using information theoretic approach and cryptographic approach, and show the strongest security definition for wiretap channel.

2.2.1 Wyner's Wiretap Channel

Wyner wiretap model was initially proposed by Wyner [89], and later generalized by Csiszár and Körner [18]. The wiretap channel is illustrated in Fig. 2.2. For Wyner's wiretap channel, sender and receiver communicate over a discrete memoryless main channel, and the adversary eavesdrops over discrete memoryless eavesdropping channel. The wiretap channel of Csiszár and Körner [18] is a broadcast channel, which is characterized by a finite input alphabet $\mathcal{X}$, and two finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, and a transition probability matrix $\mathsf{Pr}(y, z|x)$ from $\mathcal{X}$ to $\mathcal{Y} \times \mathcal{Z}$. Wyner wiretap channel is over discrete memoryless channel.

Figure 2.2: The wiretap channel of Csiszár and Körner



Definition 8. *The transmission probability of N symbols over discrete memoryless channel for the input $\mathbf{x} = (x_1, \cdots, x_N)$ and the outputs $\mathbf{y} = (y_1, \cdots, y_N)$ and $\mathbf{z} = (z_1, \cdots, z_N)$ is given by,*

$$\mathsf{Pr}(\mathbf{y}, \mathbf{z}|\mathbf{x}) = \Pi_{i=1}^{N} \mathsf{Pr}(y_i, z_i|x_i)$$

Secure communication over wiretap channel is realized by wiretap code. There are two requirements for wiretap channel: secrecy and reliability. Secrecy guarantees the transmitted message will not be known by the adversary (eavesdropper); reliability guarantees the message is correctly decoded by the receiver.

Definition 9. *[89] The source emits a data sequence* $\mathbf{m} = (m_1, \cdots, m_k)$*, which consists of independent copies of binary random variable* M*, where* $\mathsf{Pr}(M_i = 1) = \mathsf{Pr}(M_i = 0) = \frac{1}{2}$ *for* $i = 1, \cdots, k$*, where* M_i *is the random variable representing the* i^{th} *bit of message. There are a pair of algorithms: an encoding algorithm* $f : \mathcal{M} \to \mathcal{X}$*, and a decoding algorithm* $\phi : \mathcal{X} \to \mathcal{M}$*. The sender encodes the message into the codeword* $\mathbf{x} = (x_1, \cdots, x_N)$*, and receiver receives a noise corrupted word* $\mathbf{y} = (y_1, \cdots, y_N)$*. The receiver outputs a data sequence* $\hat{\mathbf{m}} = (\hat{m}_1, \cdots, \hat{m}_k)$*. The secrecy of message* M *with respect to eavesdropper is measured by,*

$$\frac{1}{N}\mathsf{I}(M|Z) \leq \epsilon,$$

The reliability performance of the wiretap code is captured by the error probability δ *such that,*

$$\frac{1}{k}\sum_{i=1}^{k}\mathsf{Pr}(m_i \neq \hat{m}_i) \leq \delta.$$

The secrecy rate R is achievable over wiretap channel with $\mathsf{Pr}(y, z|x)$ if for any $\xi > 0$, there exists an wiretap code with length N such that,

$$\frac{1}{N}\log|\mathcal{M}| \geq R - \xi$$

and,

$$\frac{1}{N}\mathsf{I}(M|Z) \leq \xi$$

and,

$$\frac{1}{k}\sum_{i=1}^{k}\mathsf{Pr}(m_i \neq \hat{m}_i) \leq \xi.$$

The secrecy capacity C of wiretap channel is the supremum of all achievable secrecy rates. The secrecy capacity provides a counter part to the usual channel capacity, which only

considers the reliable communication over noisy channel without secrecy concerns. The secrecy capacity of wiretap channel has been established by Csiszár *et al.* [18], but based on a strong reliability definition. For any message $m \in \mathcal{M}$,

$$\sum_{x \in \mathcal{X}} f(x|m)\mathsf{Pr}(\phi(y) \neq m|x) \leq \delta.$$

Here the strong reliability means for any message $m \in \mathcal{M}$, the receiver outputs the correct message m with probability at least $1 - \delta$. This leads to the following result on secrecy capacity.

Theorem 1. *(Theorem 3 [18]) The secrecy capacity of discrete memoryless wiretap channel is,*

$$\mathsf{C} = \max_{V \to X \to Y,Z} (\mathsf{I}(V;Y) - \mathsf{I}(V;Z)),$$

where V is an auxiliary random variable satisfying the Markov chain $V \to X \to Y, Z$.

Efficient construction of Wyner's wiretap code over binary symmetric channel can be obtained by polar codes [43, 59], and by invertible randomness extractor and concatenated code [6].

2.2.2 Wiretap Channel II

Wiretap channel II was studied by Ozarow *et al.* [66]. The model of wiretap channel II is similar to the Wyner wiretap channel. But in wiretap channel II, the sender and the receiver are connected by an error-free main channel, and the sender and the eavesdropping adversary are connected by an erasure noisy channel.

Definition 10. *Let X be the random variable with alphabet $\{0, 1\}$, and Y be the variable with alphabet $\{0, 1, e\}$, where e is the erasure symbol. Erasure noise channel with erasure probability ρ is defined by probability that $\Pr(Y = e|X = 0) = \rho$, and $\Pr(Y = e|X = 1) = \rho$, and $\Pr(Y = 0|X = 0) = 1 - \rho$, and $\Pr(Y = 1|X = 1) = 1 - \rho$.*

In Wiretap channel II, the adversary's channel is an erasure noise channel where the eavesdropping components of the codeword are adaptively chosen by the adversary. The adversary with parameter ρ picks a subset $S \subseteq \{1, \cdots, N\}$ from a codeword of length N such that $|S| = \rho N$, and is allowed to observe x_i for $i \in S$.

Let $\mathbf{z} = (z_1, \cdots, z_N)$ be defined by,

$$z_i = \begin{cases} x_i & i \in S \\ ? & i \notin S \end{cases}$$

and denote the eavesdropper's information. The eavesdropping adversary, who can select the subset to examine, can be seen as adversarial erasure.

Secrecy and reliability of codes for wiretap channel II is defined similar to Wyner wiretap channel [89]. The code should satisfy secrecy, that is $\frac{1}{N}\mathsf{I}(M|Z) \leq \epsilon$, and the reliability, that is $\frac{1}{k}\sum_{i=1}^{k} \mathsf{Pr}(m_i \neq \hat{m}_i) \leq \delta$. The secrecy capacity of wiretap channel II is measured by the eavesdropping parameter ρ.

Theorem 2. *(Theorem 2.1 [66]) The secrecy capacity of wiretap channel II is,*

$$\mathsf{C} = 1 - \rho$$

The wiretap codes over wiretap channel II can be constructed using LDPC codes [5].

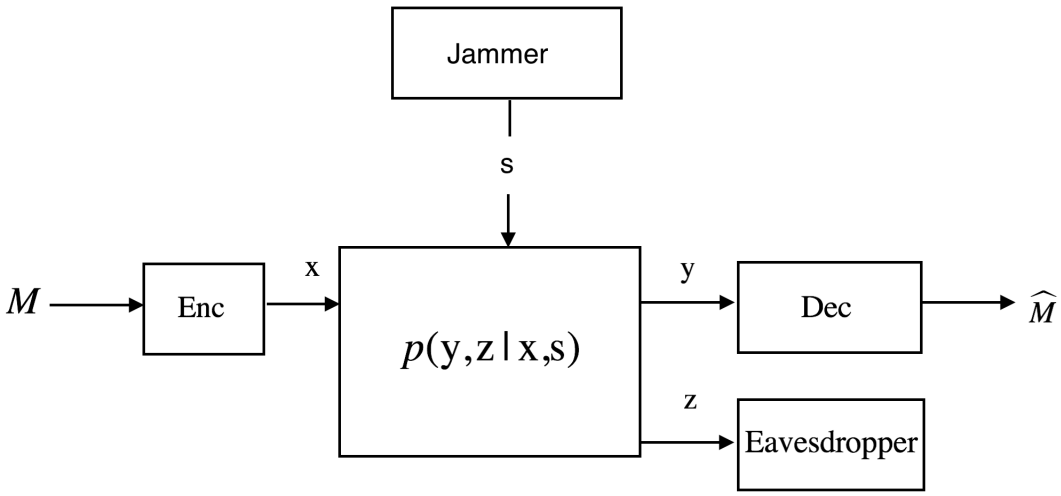
2.2.3 Active Adversary Arbitrarily Varying Wiretap Channels

The Wyner's wiretap channel model [89] and its follow up work [18, 55, 59, 66] only consider passive eavesdropping adversary model. In reality, passive adversary model is simplistic in wireless communication setting, the adversary can implement jamming attacks, and actively disrupt the communication. Active adversary model using arbitrarily varying wiretap channel model has been considered in [64, 12, 44]. In this model, the adversary not only implements eavesdropping attack, which is same as the wiretap channel model, but also actively changes the channel states. The impact of this jammer is modelled as the adversary's

capability of changing the state of the channel. The wiretap channel is characterized by a finite input alphabet $\mathcal{X}$, two finite output alphabet $\mathcal{Y} \times \mathcal{Z}$, an arbitrary state space $\mathcal{S}$, and a family of transmission probabilities from $\mathcal{X}$ to $\mathcal{Y} \times \mathcal{Z}$ indexed by $\mathcal{S}$. The transmission probability of an N-symbol input $\mathbf{x} = (x_1, \cdots, x_N)$ and outputs $\mathbf{y} = (y_1, \cdots, y_N)$ and $\mathbf{z} = (z_1, \cdots, z_N)$ is characterized by,

$$\mathsf{Pr}(\mathbf{y}, \mathbf{z}|\mathbf{x}, \mathbf{s}) = \Pi_{i=1}^{N} \mathsf{Pr}(y_i, z_i|x_i, s_i)$$

Figure 2.3: Active Adversary Arbitrarily Varying Wiretap Channels



Wiretap codes have been defined to combat the eavesdropping and jamming adversary over arbitrary varying wiretap channel. Similar to Wyner wiretap channel, wiretap code has two security requirements: secrecy and reliability.

Definition 11. *[64] An* (N, M) *wiretap code for active adversary wiretap channel consists of a message set* $\mathcal{M} = \{1, \cdots, \mathsf{M}\}$ *and a random variable* (F, Φ) *over family of wiretap code* (f, ϕ)*. The secrecy of wiretap code is measured as the average leakage rate of wiretap code such that*

$$\frac{1}{N}\mathsf{I}(M; Z|(F, \Phi)) \leq \epsilon,$$

and the reliability performance of wiretap code is,

$$\frac{1}{\mathsf{M}}\mathsf{E}_{(F,\Phi)}(\sum_{m\in\mathcal{M}}\sum_{\mathbf{z}}\mathsf{Pr}((\phi^{-1}(m))^c,\mathbf{z}|f(m)))\leq\delta.$$

Similar to wiretap codes, the rate R is achievable for active adversary arbitrary varying wiretap channel if for any $\xi>0$, there exists a wiretap code family such that,

$$\frac{1}{N}\log|\mathcal{M}|\geq R-\xi$$

and,

$$\frac{1}{N}\mathsf{I}(M;Z|(F,\Phi))\leq\xi$$

and,

$$\frac{1}{\mathsf{M}}\mathsf{E}_{(F,\Phi)}(\sum_{m\in\mathcal{M}}\sum_{\mathbf{z}}\mathsf{Pr}((\phi^{-1}(m))^c,\mathbf{z}|f(m)))\leq\xi$$

The upper bound on rate of active adversary arbitrary varying wiretap channel has been given by MolavianJazi *et al.* [64].

Theorem 3. *(Theorem 1 [64]) For active adversary arbitrary varying wiretap channel, the rate satisfies,*

$$R\leq\max_{\Pr(x)}(\min_{\overline{s}\in\overline{S}}\mathsf{I}(X;Y)-\min_{\overline{s}\in\overline{S}}\mathsf{I}(X;Z)),$$

where $\overline{S}=\{\overline{s}=\sum_{i=1}^{r}s_i\Pr(s_i):r\in\mathbb{N},s_i\in S,\Pr(s_i)\geq 0,\sum_{i=1}^{r}\mathsf{Pr}(s_i)=1\}$.

Currently there are only existence proof for active adversary arbitrary varying wiretap codes based on random code under certain assumptions. For instance, MolavianJazi *et al.* [64] show the existence of codes if the broadcast arbitrary varying wiretap channel satisfies degrade condition. That is random variables $X\to Y_s\to Z_s$ forms a Markov chain for all state s. Efficient construction of active adversary arbitrary varying wiretap code is an open problem.

2.2.4 Security and Reliability Definition

Wiretap codes should provide security and reliability. The reliability requires the wiretap code provide error correction for the receiver channel. This is measured by the probability of error for the receiver when decoding the received word Y^n. In coding theory, decoding error probability is required approach to zero as the length of code approaches to infinity, that is $\lim_{n\to\infty} \mathsf{Pr}(\mathsf{Dec}(Y^n) \neq M) = 0$ where probability is over the randomness of messages. This definition has been used in wiretap code schemes [2, 6, 9, 15, 42, 59, 64, 85].

We introduce the security definition of wiretap channels.

Mutual Information Security

The security of wiretap codes has been originally defined as the information rate of the secret message that adversary is tolerated to obtain,

$$\mathbf{Adv}(\mathsf{Enc}, \mathsf{View}_{\mathcal{A}}) = \frac{1}{N}\mathsf{I}(M; Z^N) \leq \epsilon$$

This is called weak security [62], and is used for the security definition of wiretap channel [89, 18, 66, 64].

Unfortunately, the total information that the adversary gains about the secret message is not necessarily bounded though the rate is arbitrarily small. The reason is that for any small ϵ by choosing large enough N, we can have ϵN to be a large value.

A stronger definition of security has been proposed by Maurer *et al.* [62] in the setting of key agreement protocol over wiretap channel. This definition requires the information that the adversary obtains about the secret key is negligible in absolute sense and not only in rate. That is,

$$\mathbf{Adv}(\mathsf{Enc}, \mathsf{View}_{\mathcal{A}}) = \mathsf{I}(M; Z^N) \leq \epsilon.$$

The definition provides a stronger definition key agreement protocols over wiretap channel. However, for secure message transmission over wiretap channel, this definition only provides security for uniformly distributed messages. In real world messages are not uniformly

distributed and may take values in some small and known set. An example is the set of messages in a voting system. So this definition cannot ensure security for secure message communication over wiretap channel. This leads to a stronger security definition, which is independent of the message distribution [6] and is called mutual information security, defined via $\max_M \mathsf{I}(M; Z^N)$. This is the definition of the information theoretic security for wiretap channel taking into account all distributions M over the message space,

$$\mathbf{Adv}^{\mathsf{mis}}(\mathsf{Enc}, \mathsf{View}_{\mathcal{A}}) = \max_{M} \mathsf{I}(M; Z^N) \leq \epsilon.$$

Semantic Security

In semantic security [37], the encryption algorithm must hide all partial information about the message. That is the adversary has little advantage to compute a function $f(\cdot)$ of the message given the ciphertext [37]. Semantic security definition can be extended to wiretap setting [6]. Let k be the length of message, and $\mathcal{S}$ be the simulator of adversary. Semantic security for wiretap channel is defined as follow,

$$\mathbf{Adv}^{\mathsf{ss}}(\mathsf{Enc}, \mathsf{View}_{\mathcal{A}}) = \max_{M}(\max_{\mathcal{A}}(\mathsf{Pr}(\mathsf{View}_{\mathcal{A}}(Z^N)) = f(M)) - \max_{\mathcal{S}} \mathsf{Pr}(\mathcal{S}(m) = f(M))) \leq \epsilon.$$

Here m is the length of message. This implies that the maximum probability that an adversary $\mathcal{A}$ having received information Z^N, can compute the result of function $f(\cdot)$ on the message, minus the maximum probability that a simulator $\mathcal{S}$ who only knows the message length, can do the same given only given the length of message.

Another measure of security is distinguishing security [46]. Distinguishing security is easy to use for security proofs in cryptographic systems and is given by,

$$\mathbf{Adv}^{\mathsf{ds}}(\mathsf{Enc}, \mathsf{View}_{\mathcal{A}}) = \max_{\mathcal{A}, m_1, m_2} 2\mathsf{Pr}(\mathcal{A}(m_1, m_2, Z^N) = b) - 1 \leq \epsilon,$$

where b is uniformly distributed over $\{0, 1\}$, and the maximum is over all message pairs $m_1, m_2 \in \mathcal{M}$ and all adversaries $\mathcal{A}$.

In wiretap channel setting, it is proved that semantic security is equivalent to distinguishing security [6].

Lemma 3. *(Theorem 1 [6]) Let* $\mathsf{Enc} : \{0,1\}^k \to \{0,1\}^N$ *be an encoding scheme and* Z^N *be adversarial observation. Then* $\mathbf{Adv}^{\mathsf{ss}}(\mathsf{Enc}; Z^N) \leq \mathbf{Adv}^{\mathsf{ds}}(\mathsf{Enc}; Z^N) \leq 2\mathbf{Adv}^{\mathsf{ss}}(\mathsf{Enc}; Z^N)$.

Equivalence between Mutual Information Security and Semantic Security

Mutual information security measures the difference between the adversary's uncertainty about the message before encoding and after eavesdropping. Bellare *et al.* [6] showed the equivalence of mutual information security and semantic security over wiretap channel. The equivalence is implied from the relations that the distinguishability security implies mutual information security (Theorem 4), and the relation that mutual information security implies distinguishable security over wiretap channel (Theorem 5).

Theorem 4. *(Theorem 5 [6]) Let* $\mathsf{Enc} : \{0,1\}^k \to \{0,1\}^N$ *be an encoding scheme, and* Z^N *be adversarial observation. Then* $\mathbf{Adv}^{\mathsf{ds}}(\mathsf{Enc}, Z^N) \leq \sqrt{2 \cdot \mathbf{Adv}^{\mathsf{mis}}(\mathsf{Enc}, Z^N)}$.

Theorem 5. *(Theorem 8 [6]) Let* $\mathsf{Enc} : \{0,1\}^k \to \{0,1\}^N$ *be an encoding scheme, and* Z^N *be adversarial observation, and* $\epsilon = \mathbf{Adv}^{\mathsf{ds}}(\mathsf{Enc}, Z^N)$. *Then* $\mathbf{Adv}^{\mathsf{mis}}(\mathsf{Enc}, Z^N) \leq 2\epsilon \cdot \log(\frac{2^N}{\epsilon})$.

2.3 Codes for Reliability

In information theory, error detection and correction codes are used for reliable communication over noisy channels. Error detection allows to detect errors, while the error correction allows to reconstruct the original data from the error corrupted information. Error detection and correction codes have been widely used in network communication, wireless transmission, space telecommunication, and data storage.

Consider a sender $\mathcal{S}$ and receiver $\mathcal{R}$ that are connected by a noisy channel. $\mathcal{S}$ wants to transmit a message m reliably to $\mathcal{R}$. An error correcting code over alphabet Σ is a mapping $\mathsf{Enc} : \Sigma^k \to \Sigma^N$ from a string of length k over alphabet Σ to a string of length N. The length k is the length of message, and the length N is the block length of codeword. The rate of the code is defined as $R = \frac{\log |\mathcal{M}|}{N \log |\Sigma|}$. The set $\mathcal{C} = \{c : c \in \Sigma^N\} \subset \Sigma^N$ is called the code,

and the element $c \in \mathcal{C}$ is called a codeword. In general only a small fraction of all possible strings in Σ^N are valid codewords. The redundancy built into codewords is used to decode the message m even from a distorted version of the word.

Deterministic Encoding and Randomized (Stochastic) Encoding

The encoding algorithm can be deterministic or randomized. But the decoding algorithm is deterministic. For deterministic encoding algorithms, the input to the encoder is the message m. That is, the encoding algorithm is $\mathsf{Enc} : \mathcal{M} \to \mathcal{C}$. For randomized encoding algorithm, the input to the encoder is the message m and randomness r. That is, the encoding algorithm is $\mathsf{Enc} : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$.

2.3.1 Noisy Channel with Probabilistic Error

Communication channels are subject to channel noise, and the construction of error correction code depends on the channel error model. Historically, there are two channel noise models. The study of noisy channel with probabilistic error is due to Shannon [74]. Shannon demonstrated that it is possible to communicate information m nearly error free at a rate below a maximum rate depending on the channel noise. An example is binary symmetric channel, where the channel flips each transmitted bits with probability ρ. The flips of each bits are independent from other bits. Shannon characterized the largest rate (capacity) of reliable communication over such channels. He also showed the existence of codes with rates approaching the capacity and decoding error approaching to zero. However, the noisy channel with probabilistic error is too simple to model real world communication noise. There are many factors, which are generated by nature and mankind, may disturb the real world communication system.

2.3.2 Adversarial Channel

To address these issues, Hamming [41] considered adversarial error in communication channels. In Hamming model, the channel only has a limit on the fraction of errors for a block of data, which is bounded by the error rate ρ. Both location of corrupted symbols and actual errors are assumed to be adversarial. Hamming model is more pessimistic than Shannon's since it includes any arbitrary pattern of error. For adversarial channels, the code with length N which is able to correct error rate ρ requires the Hamming distance at least $2\rho N + 1$ in order that each codeword $c \in \mathcal{C}$ will not be confused with another codeword $c' \neq c$. This distance requirement limits the number of codeword $\mathcal{C} = \{c \in \mathcal{C}\}$ packing in space Σ^N, and the rate of code $\mathcal{C}$. For instance, in order to correctly decode the message in $\mathbb{F}_2$, the error rate must not exceed $\frac{1}{4}$ fraction of codeword in Hamming model, whereas the error probability is no more than $\frac{1}{2}$ fraction of codeword over probabilistic channel. Thus the rate over adversarial channel generally loss at the price of robustness of communication.

There are several models and techniques for reliable communication over adversarial channel with high rate of codeword.

2.3.3 List Decodable Code

List decodable code is proposed by Elias [30] and has the capability to decode more errors. For list decodable code, the receiver $\mathcal{R}$ outputs a list of messages instead of a unique message. The list of messages corresponds to all the codewords within ρN distance from the received word y. This relaxation of requirement on decoder enables to bridge the gap between error correcting capability of codes for adversarial error and probabilistic error.

Definition 12. *[30] A code $\mathcal{C}$ with the encoding function $\mathsf{LC} : \Sigma^k \to \Sigma^N$ is (ρ, ℓ)-list decodable if the number of codewords within distance ρN of any received word is at most ℓ. That is for every word $y \in \Sigma^N$, there are at most ℓ codewords at distance ρN or less from y.*

The existential results indicating potential for list decoding has been given by Zyablov *et al.* [90]. However, to achieve this potential decoding capability, one needs explicit construction of list decodable codes, and a polynomial time algorithm to perform list decoding. An explicit and efficient construction of list decodable code using Folded Reed-Solomon codes and Subspace Evasive Sets has been proposed in [39, 38, 29]. We will introduce the details of Folded Reed-Solomon code and Subspace Evasive Sets in Section 3.2.

2.3.4 Private Code

Langberg [50] described private codes in which the sender $\mathcal{S}$ and receiver $\mathcal{R}$ share a secret random key that is unknown to the adversary. A private code allows communication over a adversarial channel that meets the rate $1-\rho$, using $\mathcal{O}(\log N)$ size joint randomness.

Definition 13. *[50] Let k be the dimension of code, ℓ be the length of randomness, and N be the length of code. An (N, k, ℓ) private code is a pair of algorithm PC, PD, where $\mathsf{PC} : \Sigma^k \times \Sigma^\ell \to \Sigma^N$ and $\mathsf{PD} : \Sigma^N \times \Sigma^\ell \to \Sigma^k$. The code corrects ρN adversarial error with probability $1-\delta$ if for all messages $m \in \mathcal{M}$, we have $\mathsf{PD}(\mathsf{PC}(m, r), r) = m$ with probability at least $1-\delta$ where the probability is taken over all randomness r.*

Smith [78] gave a general construction of private code from list decodable code and message authentication code (MAC). The idea is that both $\mathcal{S}$ and $\mathcal{R}$ share the random secret key of MAC. In encoding algorithmn, $\mathcal{S}$ authenticates the message m, and constructs message authentication code (m, t) where t is the MAC tag calculated using the shared secret key. Then $\mathcal{S}$ encodes (m, t) using list decodable code. The decoding algorithm is inverse of encoding. $\mathcal{R}$ decodes the received word y using the list decoding algorithm, and then use MAC to verify each message in decoded list.

2.3.5 Computational Adversarial Channel

Hamming's adversarial channel is described in a computationally unbounded setting, Lipton *et al.* [57] proposed an adversarial channel where adversary is restricted to polynomial computation. The channel introduces adversarial error but the error is generated by a computationally bounded adversary. By limiting the adversary's computational power, it is possible to decode uniquely with high error rate [25, 76, 68]. Ding *et al.* proposed a scheme to achieve reliable communication over computational adversarial channel which requires $\mathcal{S}$ and $\mathcal{R}$ to share a secret random key [25]. A reliable communication scheme based on public key cryptosystem was shown in [68].

2.3.6 Error Detection Code

The error may happen in transmission or storage. In network transmission, error detection techniques are used to detect noise or impairments that are introduced to data is transmitted from the source to the destination. In storage systems, error detection techniques verify the integrity of data on disc or memory. Error detection codes are designed to achieve error detection in communication and storage systems. A simple example for error detection is parity check bits, which builds the $\mathbb{F}_2$ addition of bits with value 1. More sophisticated error detection codes are realized by hash function, or error correction code.

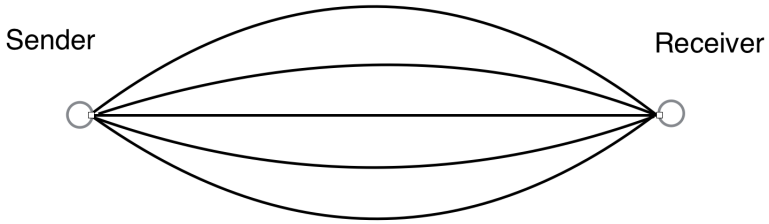
2.4 Secure Message Transmission

In *Secure Message Transmission* (SMT) problem, there is a synchronous network, that connects Alice (sender $\mathcal{S}$) and Bob (receiver $\mathcal{R}$). $\mathcal{S}$ and $\mathcal{R}$ are connected by N vertex-disjoint paths, also known as *wires* or channels. The network is undirected and communication on the wire are in both directions. $\mathcal{S}$ and $\mathcal{R}$ are both honest. The goal is to enable $\mathcal{S}$ to send a message $m_{\mathcal{S}}$, drawn from a message space $\mathcal{M}$ with a probability distribution $\Pr(m_{\mathcal{S}})$, to $\mathcal{R}$

such that $\mathcal{R}$ receives the message *reliably* and *securely*.

SMT protocols may have one or more rounds. In each protocol round, $\mathcal{S}$ or $\mathcal{R}$, constructs protocol messages that are sent over wires to the other party. Protocol messages are received by the recipient of the round, possibly in corrupted form, before the next round starts. At the end of the protocol, the receiver outputs a message $m_{\mathcal{R}}$.

Figure 2.4: Secure Message Transmission Protocol



We consider only 1-round protocols in which the sender selects a message m and uses the protocol description to construct protocol messages that are sent over each wire. The adversary $\mathcal{A}$ has unlimited computational power and can corrupt and control a subset of wires: the adversary can eavesdrop, block or modify communication that is sent over the corrupted wires. $\mathcal{A}$ is adaptive and can corrupt wires any time during the protocol execution and after observing communications over the wires corrupted so far. $\mathcal{A}$ is also rushing, that is it sees the messages sent by $\mathcal{S}$ over the corrupted wires before deciding on the messages to be sent over those wires. $\mathcal{A}$ can corrupt at most t out of the N wires and her selection of corrupted wires is unknown to $\mathcal{S}$ and $\mathcal{R}$.

Denote by $\mathsf{View}_{\mathcal{A}}(m_{\mathcal{S}}, r_{\mathcal{A}})$ the random variable that denotes the view of the adversary $\mathcal{A}$ when attacking the protocol assuming the sender has chosen $m_{\mathcal{S}}$ and $r_{\mathcal{A}}$, which is the random coins of the adversary.

Definition 14. *[33] A message transmission protocol between $\mathcal{S}$ and $\mathcal{R}$ is an (ε, δ)-Secure Message Transmission ((ε, δ)-SMT) protocol if the following two conditions are satisfied:*

- *Privacy: For every two messages $m_1, m_2 \in \mathcal{M}$ and every $r_{\mathcal{A}} \in \{0,1\}^*$ used by the adversary,*

$$\mathbf{SD}(\mathsf{View}_{\mathcal{A}}(m_1, r_{\mathcal{A}}), \mathsf{View}_{\mathcal{A}}(m_2, r_{\mathcal{A}})) \leq \varepsilon, \tag{2.1}$$

  where the probability is over the randomness of $\mathcal{S}$ and $\mathcal{R}$.

- *Reliability: $\mathcal{R}$ correctly receives the correct message m with probability $\geq 1-\delta$, and outputs the wrong message with probability $\leq \delta$. That is,*

$$\mathsf{Pr}(M_{\mathcal{S}} \neq M_{\mathcal{R}}) \leq \delta$$

Definition 15. *[33] A message transmission protocol between $\mathcal{S}$ and $\mathcal{R}$ is a δ-Reliable Message Transmission (δ-RMT) protocol if it only satisfies the reliability condition above.*

Kurosawa *et al.* proposed a stronger reliability definition [48]. It defines the receiver never outputs an incorrect message, and the probability that receiver outputs fail (denoted as $\perp$) is bounded by δ. That is,

$$\Pr[\text{Receiver outputs } \perp] \leq \delta$$

When $\varepsilon = 0$, the protocol is said to achieve *perfectly security*, and when $\delta = 0$, the protocol is said to achieve *perfect reliability*. The SMT protocol is called *perfect secure message transmission (PSMT)* if it achieves perfectly secure and perfectly reliable. The SMT protocol is called $(0, \delta)$-*SMT* if it achieves perfectly secure and δ reliable. The RMT protocol is called *perfect Reliable Message Transmission (PRMT)* if it achieves perfectly reliable. The RMT protocol is called δ-*RMT* if it achieves δ-reliable.

Communication efficiency of an SMT and RMT protocol is in terms of the *number of rounds*, and *transmission rate*.

The *number of rounds of an SMT and RMT protocol* is the number of interactions between $\mathcal{S}$ and $\mathcal{R}$. It was shown that 1-round PSMT is possible if and only if $N \geq 3t+1$ [28], and two or more rounds PSMT is possible if and only if $N \geq 2t+1$. For (0, δ)-SMT, it was shown

that 1-round (0, δ)-SMT protocol [33] is possible if and only if $N \geq 2t+1$. 1-round (0, δ)-SMT protocols are attractive because they guarantee perfect privacy and by allowing a small degradation in reliability (compared to perfect reliability), reduce the required connectivity and communication round. For RMT protocols, it was shown that it is possible if and only if $N \geq 2t+1$ [33].

Transmission rate of an SMT and RMT protocol is the ratio of the total communication to the length of the message. That is,

$$\tau = \frac{\mathsf{Total\ Length\ of\ Transcript}}{\mathsf{Length\ of\ Message}} = \frac{\sum_i \log |\mathcal{V}_i|}{\log |\mathcal{M}|}$$

In [79, 31, 67], lower bounds on transmission rates of (0, δ)-SMT protocols are derived. The lower bounds depend on the number of rounds. For PSMT, it was shown that the lower bound of transmission rate for two or more rounds PSMT is bounded by $\tau(\mathsf{SMT}) \geq \mathcal{O}(\frac{N}{N-2t})$ [79], and for 1-round PSMT is bounded by $\tau(\mathsf{SMT}) \geq \mathcal{O}(\frac{N}{N-3t})$ [31]. For (0, δ)-SMT, it was shown that for 1-round $(0, \delta)$-SMT, the transmission rate is bounded by $\tau(\mathsf{SMT}) \geq \mathcal{O}(\frac{N}{N-2t})$ [67]. For RMT, the lower bound on the transmission rate of 1-round PRMT is bounded by $\mathcal{O}(\frac{N}{N-2t})$ [79], and 1-round δ-RMT is given by $\mathcal{O}(\frac{N}{N-t})$ [67]. Protocols whose transmission rate asymptotically matches the lower bounds associated with their number of rounds, *are called optimal.* For 1-round (0, δ)-SMT protocols with $N = 2t+1$ and $N = (2+c)t$, optimal protocols must have transmission rates $\mathcal{O}(N)$ and $\mathcal{O}(1)$, respectively.

The *computational efficiency* of SMT and RMT protocols is the amount of computation that is required by the protocol. A protocol that needs exponential (in N) computation for $\mathcal{S}$ and $\mathcal{R}$, is called inefficient. Efficient protocols need polynomial (in N) computation.

2.4.1 Secure Message Transmission with Public Discussion

Public Discussion Channel

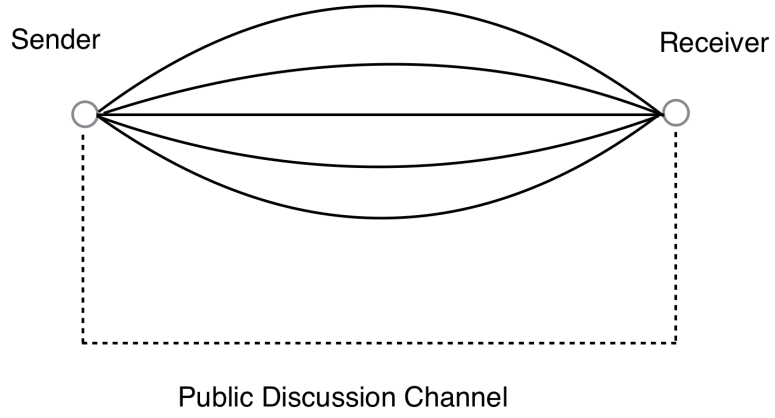
Maurer [61] and Ahlswede *et al.* [3] introduced public discussion channel first in the case of key agreement protocol over wiretap channel. $\mathcal{S}$ and $\mathcal{R}$ can use a public discussion (PD)

channel in addition to the wiretap channel. A public discussion channel is an authenticated communication channel that can be used by $\mathcal{S}$ and $\mathcal{R}$, and is readable by everyone including the adversary. They showed that in this model, secure communication is possible even if the noise in the eavesdropper's channel is lower than the main channel, thus showing the power of the PD channel as a resource for communicants.

Secure Message Transmission with Public Discussion

Garay *et al.* [35] studied the model of *Secure Message Transmission with public discussion* (SMT-PD). In this model, in addition to the wires in the standard SMT, $\mathcal{S}$ and $\mathcal{R}$ access to a public channel. The adversary can only read but not tamper the communication over public channel. In this new setting, SMT is achievable even if the adversary corrupts up to $t < N$ of the wires. In SMT-PD, there is an $\mathcal{S}$ and $\mathcal{R}$, that can interact over N node disjoint paths in a synchronous network, referred to as *wires*, and an authenticated public discussion channel (PD channel).

Figure 2.5: Secure Message Transmission with Public Discussion Protocol



Wires and the public discussion channel provide two-way communication. An SMT-PD protocol proceeds in rounds. In each round, $\mathcal{S}$ ($\mathcal{R}$) sends protocol messages over wires and/or the PD channel, which will be received by $\mathcal{R}$ ($\mathcal{S}$) before the end of the round. A computationally unbounded adversary $\mathcal{A}$ can corrupt up to t wires. $\mathcal{A}$ can eavesdrop, modify or block messages sent over a corrupted wire. $\mathcal{A}$ is adaptive and can corrupt wires any time

during the protocol execution and after observing communications over the wires corrupted so far. $\mathcal{A}$ can also observe the communication over public discussion channel, but can not tamper the information communicated over PD channel.

The security and reliability definition of SMT-PD protocol is same as definition of SMT. The efficiency of SMT-PD protocol is also measured by transmission rate, number of rounds, and computational efficiency.

Chapter 3

Limited View Adversary Code

3.1 Introduction

Reliable communication in presence of adversarial error is first considered in Hamming model [41] of error where the adversary sees the whole codeword and arbitrarily corrupts ρN symbols, where N is the length of the codeword and ρ is a constant. More recently weaker adversarial models have been introduced to capture real-life communication settings, where the adversary's access to the codeword (read, write or both) is limited because of reasons such as inadequate transceiver in wireless communications [51], or realtime nature of communication [24, 53]. A different line of work [40, 57, 76] models adversarial channels where the error is generated by a computationally bounded process.

We consider a model of adversarial channel introduced in [73] and called *Limited View Adversary Channel (LVAC)* in which the adversary is computationally unlimited but its access to the codeword is limited as follows: for a codeword of length N, the adversary can adaptively choose to "see" $\rho_r N$ components and modify $\rho_w N$ components of the codeword, and modification is by "adding" to the codevector an error vector of weight at most $\rho_w N$ where (ρ_r, ρ_w) is the pair of constants that specify the channel. A Limited View Adversary Codes (LV-code) provides reliable communication over an LVAC. There is no shared secret key between the communicants.

Hamming model of error with error fraction ρ can be seen as an LVAC with $\rho_r = 1$ and $\rho_w = \rho$. It is well known that unique decoding in Hamming model is only possible $\rho \leq \frac{1-R}{2}$. Using the same adversary model and allowing *list decoding* where the decoder outputs a list of possible codewords, one can increase the fraction of correctable errors to $\rho \leq 1 - R$. We

will show that for the same corruption[1] fraction ρ, an LV-code for a (ρ_r, ρ)-LVAC can provide unique decoding for $\rho \leq 1 - R$.

Motivation

The first motivation for studying LV-codes is from wireless adversary with a typical transceiver may not be able to "see" (correctly receive) the whole codeword or "write" (introduce strong noise) over the whole codeword. Moreover, the adversary's goal may in fact be to partially corrupt the codeword so that the decoder outputs a different message. This would be feasible by targeting and changing specific symbols in a codeword. By decoupling the read and the write sets of the adversary, one allows the adversary to use powerful strategies for modifying a codeword. Compared with the models in [24, 53], LV-codes do not require casuality and allow the adversary to select its read and write sets freely subject to the bound on their sizes.

A second motivation for the study of LV-codes is to establish their relationship with 1-round RMT as noted in [73]. However no precise relationship between the two was established. Reliable Message Transmission (RMT) [33] is a well studied cryptographic primitives for reliable communication in networks. In the RMT setting Alice is connected to Bob through a set of N node disjoint paths (wires) in a network, a subset of which is controlled by the adversary. A threshold adversary fully controls a subset of size t of the N wires. The goal of an RMT protocol is to provide reliability for communication. The relation between LV-codes and 1-round RMT allows a unified treatment of the two problems and relate and enrich results in the two settings.

Our Results

In this dissertation we consider (ρ_r, ρ_w)-LVACs and LV codes with δ reliability (δ-LV codes) that guarantee reliable message transmission over these channels with probability at least $1 - \delta$. We use a definition of reliability that allows the decoder to output an incorrect

[1] As we point out in Section 3.6 when $\rho_r = 1$, any general corruption can be modelled as an additive error.

message. We have the following results.

1) Upper bound on the code rate. For an LV code for a (ρ_r, ρ_w)-LVAC and an arbitrary message distribution $\Pr(M)$, we derive an upper bound on $\mathsf{H}(M)$ (See Eq. (3.17)), and use it to obtain an upper bound on the rate of LV codes. Using this bound for a code family results in an upper bound on the rate of a code families, and so the the following bound on the capacity of (ρ_r, ρ_w)-LVACs,

$$\mathsf{C} \leq 1 - \rho_w. \tag{3.1}$$

The bound is similar to the list decoding capacity of codes in Hamming error model. In LVAC model however, the decoder outputs a single codeword and not a list of codewords. The bound holds independent of the value of ρ_r and (intuitively) is the maximum possible rate because the corrupted fraction (ρ_w) of a codeword is not recoverable.

2) Two constructions LV-codes. We propose two constructions of LV-codes. *Our first construction is LV-codes over restricted LVAC.* We construct an δ-LV code that is non-linear, and uses two building blocks: a message authentication code and a Folded Reed-Solomon (FRS) code. To encode a message m, the sender first chooses N appropriately constructed secret keys, uses the keys to construct N authentication tags for the message using the chosen MAC (See MAC Construction II for details), and appends the tags to the message. The tagged message is then encoded using an FRS code. The i^{th} component of the final codeword which is sent to the receiver consists of the corresponding component of the FRS code and the MAC key. The decoder recovers the correct message in a conceptually two step process: using the list decoding algorithm of the FRS code to construct a list of possible codewords and then applying the MAC verification algorithm to output either the correct message, or $\perp$. This two step algorithm however can result in an exponential cost decoding because the output list of the FRS decoding algorithm can be of exponential size. To overcome this problem, we design a new decoding algorithm which combines the system of linear equations resulting from the algebraic list decoding algorithm [38] of FRS

codes, with a set of linear equations resulting from the verification algorithm of a specially constructed MAC, to have a single system of linear equation whose solution gives the correct message with a high probability. The MAC in this construction must be a key efficient MAC that can be used for different length messages and have appropriate verification algorithm suitable for efficient decoding. MAC Construction II satisfies these properties and could be of independent interest. *The final decoder complexity is polynomial.*

Our second construction is an efficient LV code family over LVAC with $\rho_r + \rho_w < 1$. We construct an efficient probabilistic LV code family whose rate R achieves the bound (Eq. 3.1) with equality, $R = 1 - \rho_w$, as the code length N approaches infinity, assuming $\rho_r + \rho_w < 1$. The construction thus achieves the channel capacity for $\rho_r < 1-\rho_w$. The capacity of (ρ_r, ρ_w)-LVAC for higher values of ρ_r remains an open question. The construction of the efficient LV code family uses three building blocks: a list decodable code [29], a message authentication code (referred to as authentication code) [77, 36] and a $(0, \delta)$-Adversarial Wiretap Code ($(0, \delta)$-AWTP code) [86]. To encode a message block $\mathbf{m}$, Alice (Sender) first authenticates the message $\mathbf{m}$ using a random key block $\mathbf{r}$ to generate a tagged message $(\mathbf{m}, \mathbf{t})$, which is then encoded using a list decodable code. The key block $\mathbf{r}$ is encoded by an AWTP code. Finally the i^{th} component of the LV code will consist of the i^{th} component of the AWTP code concatenated with the i^{th} component of the list decodable code. The receiver decodes the corrupted list decodable codeword and generates a list of possible codewords; it also decodes the corrupted codeword of the AWTP code to find the MAC key and uses it to identify the sent codeword in the list. Details of the construction is in Section 3.5. Note that the requirement $\rho_r < 1 - \rho_w$ is because of using a capacity achieving $(0, \delta)$-AWTP code. In [84] it is proved that non-zero rate for these codes implies $\rho_r + \rho_w < 1$ and so for this construction we will have $\rho_r < 1 - \rho_w$. It is however an open question to find capacity of the channel when $\rho_r > 1 - \rho_w$.

3) Relation with RMT. We show a one-to-one correspondence between *symmetric* 1-round RMTs and LV codes: a construction of an LV code gives a construction of a symmetric 1-round RMT with the same δ, and vice versa. Symmetric RMTs are RMTs with the added requirement that the set of transmissions on each wire is the same for all wires. All known RMTs are symmetric and so we simply refer to these protocols as RMT protocols. Efficiency of RMT protocols is measured by their *transmission rate* which is the number of transmitted bits for a single message bit. We give a new lower bound on the transmission rate of RMTs that holds for the more relaxed definition of reliability and allows the decoder to output incorrect messages also. Previous lower bound on transmission rate of RMT was for the stronger definition of reliability where the decoder outputs only correct messages. The relation between the bounds are discussed in Section 6.2.

We will also use the LV code construction in Section 3.5 to construct a family of 1-RMT protocols when $N = (2 + c)t$, for which error probability δ decreases exponentially with the number of wires. The field size in the two constructions satisfy the requirements of the underlying FRS codes and are of similar size.

3.2 Preliminary

3.2.1 Folded Reed-Solomon Code (FRS code)

An error correcting code $\mathcal{C}$ over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^N$. A code $\mathcal{C}$ of length N and *rate* R is $(\rho, \ell_{\mathsf{List}})$-list decodable if the number of codewords within distance ρN from any received word is at most ℓ_{List}. It is assumed that ℓ_{List} is a polynomial function of code length. It can be proved that for list decodable codes $\rho \leq 1 - R$. An explicit construction of a list decodable code that achieves the list decoding capacity $\rho = 1 - R$, is given by Guruswami et al. [38]. The code is called *Folded Reed-Solomon code (FRS code)*, and can be seen as a Reed-Solomon code with extra structure. The code has polynomial time encoding and list

decoding algorithms.

Definition 16. *[38] A u-Folded Reed-Solomon code is an error correcting code with block length N over $\mathbb{F}_q^u$ where $q > Nu$. The message of an FRS code is written as a polynomial $f(x)$ of degree k over $\mathbb{F}_q$. The FRS codeword corresponding to the message is a vector over $\mathbb{F}_q^u$ where each component is a u-tuple $(f(\gamma^{ju}), f(\gamma^{ju+1}), \cdots, f(\gamma^{ju+u-1}))$, $0 \leq j < N$, and γ is a generator of $\mathbb{F}_q^*$, the multiplicative group of $\mathbb{F}_q$. A codeword of a u-Folded Reed-Solomon code of length N is in one-to-one correspondence with a codeword c of a Reed-Solomon code of length uN, and is obtained by grouping u consecutive components of c. We use* FRSenc *to denote the encoding algorithm of the FRS code. u is called the* folding parameter *of the FRS code.*

We will use the *linear algebraic FRS decoding algorithm* of these codes [38]. The detail of linear algebraic FRS decoding algorithm is in Section 3.7.1.

Lemma 4. *[38] For a Folded Reed-Solomon code of block length N and rate $R = \frac{k}{uN}$, the following holds for all integers $1 \leq v \leq u$. Given a received word $y \in (\mathbb{F}_q^u)^N$ agreeing with c in at least a fraction*

$$N - \rho N > N(\frac{1}{v+1} + \frac{v}{v+1}\frac{uR}{u-v+1}),$$

one can compute a matrix $\mathbf{M} \in \mathbb{F}_q^{k \times v}$ and a vector $\mathbf{z} \in \mathbb{F}_q^k$, such that the message polynomials $f \in \mathbb{F}_q[X]$ in the decoded list are contained in the affine space $\mathbf{Mb} + \mathbf{z}$ where $\mathbf{b} \in \mathbb{F}_q^v$. The computation is in time $\mathcal{O}((Nu \log q)^2)$.

3.2.2 Subspace Evasive Set

Subspace evasive sets are used to reduce the list size of list decodable code [29].

Definition 17 (Subspace Evasive Set[29, 38])**.** *Let $\mathcal{S} \subset \mathbb{F}_q^n$. We say $\mathcal{S}$ is a (v, ℓ)-subspace evasive if for all v-dimensional affine subspaces $\mathcal{H} \subset \mathbb{F}_q^n$, we have $|\mathcal{S} \cap \mathcal{H}| \leq \ell$.*

Dvir *et al.* [29] gave an efficient explicit construction of subspace evasive set $\mathcal{S} \subset \mathbb{F}_q^n$, with an efficient *intersection algorithm* that computes $\mathcal{S} \cap \mathcal{H}$ for any v-dimensional subspace $\mathcal{H} \subset \mathbb{F}_q^n$. Theorem 1 in [29] states the following.

Theorem 6 ([29])**.** *For any finite field $\mathbb{F}_q$ and parameters $v \geq 1$, $\xi > 0$ there exists an explicit construction of a set $\mathcal{S} \subset \mathbb{F}_q^n$ of size $|\mathcal{S}| > \mathbb{F}_q^{(1-\xi)n}$ that is $(v, c(v,\xi))$-subspace evasive set with $c(v,\xi) = (v/\xi)^v$.*

We use the following construction of a $(v, (d_1)^v)$-subspace evasive set, with $|\mathcal{S}| = |\mathbb{F}_q|^{(1-\xi)n}$, given in Section 3 of [29]. A $v \times w$ matrix is called *strongly-regular* [29] if all its $r \times r$ sub-matrixs are regular (have non-zero determinant) for all $1 \leq r \leq v$.

Lemma 5. *(Theorem 3.2 [29]) Let $v \geq 1, \xi > 0$ and $\mathbb{F}_q$ be a finite field. Let $w = v/\xi$ and, assume w divides n. Let A be a $v \times w$ matrix with coefficients in $\mathbb{F}_q$ which is strongly-regular. Let $d_1 > \cdots > d_w$ be integers. For $i \in [v]$ let*

$$f_i(x_1, \cdots, x_w) = \sum_{j=1}^{w} A_{i,j} x_j^{d_j},$$

and define the subspace evasive set $\mathcal{S} \in \mathbb{F}_q^n$ to be (n/w) times cartesian product of $\mathbf{V}_{\mathbb{F}_q}(f_1, \cdots, f_v) \subset \mathbb{F}_q^w$. That is,

$$\begin{aligned}\mathcal{S} &= \mathbf{V}_{\mathbb{F}_q}(f_1, \cdots, f_v) \times \cdots \times \mathbf{V}_{\mathbb{F}_q}(f_1, \cdots, f_v) \\ &= \{\mathbf{x} \in \mathbb{F}_q^n : f_i(x_{tw+1}, \cdots, x_{tw+w}) = 0, \forall 0 \leq t < n/w, 1 \leq i \leq v\}.\end{aligned}$$

Then $\mathcal{S}$ is $(v, (d_1)^v)$-subspace evasive set, and $|\mathcal{S}| = |\mathbb{F}_q|^{(1-\xi)n}$.

In above, $\mathbf{V}_{\mathbb{F}_q}$ is defined as follows.

Let $\overline{\mathbb{F}}_q$ denote its algebraic closure of $\mathbb{F}_q$. A *variety* in $\overline{\mathbb{F}}_q^n$ is the set of common zeros of one or more polynomials. For v polynomials $f_1 \cdots f_v \in \mathbb{F}_q[x_1 \cdots x_w]$, the variety defined by the polynomial is denoted by

$$\mathbf{V}(f_1, \cdots, f_v) = \{x \in \overline{\mathbb{F}}_q^w | f_1(x) = \cdots f_v(x) = 0\}.$$

For polynomials $f_1 \cdots f_v \in \mathbb{F}_q[x_1 \cdots x_w]$ define the common solution in $\mathbb{F}_q^w$ as

$$\mathbf{V}_{\mathbb{F}_q}(f_1, \cdots f_v) = \mathbf{V}(f_1 \cdots f_v) \cap \mathbb{F}_q^w = \{x \in \mathbb{F}_q^w : f_1(x) = \cdots f_v(x) = 0\}.$$

Claim 4.3 in [29] proves that the construction gives a $(v, v^{D \cdot v \log\log v})$-subspace evasive set, with the field size satisfying $q < nv^{D \cdot v \log\log v}$.

To use subspace evasive set for efficient list decoding of FRS codes, two efficient algorithms are needed: (i) a bijection mapping that maps a message of the message space into an element of the subspace evasive set $\mathcal{S}$, and (ii) an intersection algorithm that computes the intersection between $\mathcal{S}$ and an affine subspace $\mathcal{H}$ with dimension at most v. This latter algorithm allows the FRS decoder output list, that can be expressed as an affine space, be pruned to a constant size. The lemmas below show that for these two tasks efficient algorithms exist for the subspace evasive set above.

Lemma 6. *[29] Let $v, w, n_1 \in \mathbb{N}$, $b = \frac{n_1}{w-v}$, $n = bw$, and $\mathbb{F}_q$ be a finite field. For any vector $\mathbf{v} \in \mathbb{F}_q^{n(1-\epsilon)}$, there is a bijection which maps $\mathbf{v}$ into an element of the subspace evasive set $\mathcal{S} \subset \mathbb{F}_q^n$. That is, $\mathsf{SE} : \mathbf{v} \to \mathbf{s} \in \mathcal{S}$. The encoding algorithm is $\mathsf{Poly}(n)$.*

Lemma 7. *[29] Let $\mathcal{S} \subset \mathbb{F}_q^n$ be the (v, ℓ)-subspace evasive set (described above). Then there exists an algorithm that, given a basis for any $\mathcal{H}$, outputs $\mathcal{S} \cap \mathcal{H}$ in time $\mathsf{Poly}(v^{v \cdot \log\log v})$.*

FRS codes have efficient polynomial time encoding and decoding algorithms. The list size of FRS codes however is exponential in the code length N. A construction of FRS codes that uses subspace evasive sets [29] has constant list size while maintaining efficient encoding and decoding.

Lemma 8. *[29] There exists an explicit family of codes $\{\mathcal{C}^N \subset \Sigma^N\}^{N \in \mathbb{N}}$ such that for every ξ there exists N_0 and codes of length $N > N_0$ and rate $R(\mathcal{C}^N)$ over alphabet $\Sigma = \mathbb{F}_q^{\frac{1}{\xi^2}}$, that can list decode a fraction $\rho = 1 - R(\mathcal{C}^N) - \xi$ of errors in quadratic time. The list size is at most $\mathcal{O}((1/\xi)^{1/\xi})$.*

3.2.3 Adversarial Wiretap Code (AWTP Code)

Adversarial wiretap codes (Chapter 4) provide secure and reliable transmission from Alice to Bob over a (ρ_r, ρ_w)-adversarial wiretap channel. The adversary in an adversarial wiretap channel can read a fraction ρ_r of a codeword components, and add error to a fraction ρ_w of the components. This adversary has the same reading and writing capability of the adversary in LV adversarial channels, however the goal of the communicants in adversarial wiretap channel is to achieve secure and reliable transmission, while in LV channels only reliability is required. It is proved that capacity of these channels is $1 - \rho_r - \rho_w$. Wang *et al.* [86] gave an explicit construction of a capacity achieving code for adversarial wiretap channels with polynomial time encoding and decoding time. In Chapter 4, we show an explicit construction of a capacity achieving code for adversarial wiretap channels with polynomial time encoding and decoding. This AWTP code achieves perfect security and bounds decoding error probability to δ.

Lemma 9. *(Theorem 3 [85]) For any sufficient small $\xi > 0$, there is a perfectly secure adversarial wiretap code $\mathcal{C}^N$ with length N over a (ρ_r, ρ_w) adversarial wiretap channel, such that the information rate is $R(\mathcal{C}^N) = 1 - \rho_r - \rho_w - \xi$, the alphabet is $\Sigma = \mathbb{F}_q^{\frac{1}{\xi^2}}$, and the decoding error satisfies $\delta \leq \frac{(1/\xi)^{D/\xi \log\log(1/\xi)}}{q^N}$.*

3.2.4 Message Authentication Code (MAC)

A message authentication code (MAC)[77] is a cryptographic primitive that allows a sender who shares a secret key with the receiver to construct authenticated messages to be sent over a channel that is tampered by an adversary, and the receiver to be able to verify the integrity of the received message.

Definition 18. *A message authentication code consists of two algorithms* $(\mathsf{MAC}, \mathsf{Ver})$ *that are used for authentication and verification, respectively. For a message m an* authentication

tag, *or simply a* tag, *is computed,*

$$t = \mathsf{MAC}(m, r),$$

and a tagged message (m, t) *is constructed. The verifier accepts a tagged pair* (m, t) *if* $\mathsf{Ver}((m, t), r)) = 1$. *Security of a one-time MAC is defined as,*

$$\Pr[(m', t'), \mathsf{Ver}((m', t'), r) = 1 | (m, t), t = \mathsf{MAC}(m, r)] \leq \delta.$$

MAC Construction I

We use a MAC construction that uses polynomials over $\mathbb{F}_q$. This construction has been previously used in [8]. We use the same construction over an extension field. Let $\mathbf{m}$ be a vector of length ℓN, and $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2)$ be vector with $\mathbf{r}_1$ and $\mathbf{r}_2$ of length N respectively, and $\mathbf{t}$ be vector of length N over $\mathbb{F}_q$. Let ϕ be a bijection between vectors of length N over $\mathbb{F}_q$, and elements of $\mathbb{F}_{q^N}$. Define the MAC generation function $\mathsf{MAC} : \mathbb{F}_q^{\ell N} \times \mathbb{F}_q^{2N} \to \mathbb{F}_q^N$, where $\mathsf{MAC}(\mathbf{m}, \mathbf{r}) = \mathbf{t}$ as,

$$\mathbf{t} = \mathsf{MAC}(\mathbf{m}, \mathbf{r}) = \phi^{-1}(\sum_{i=0}^{\ell-1} \phi(\mathbf{x}_i)\phi(\mathbf{r}_1)^i + \phi(\mathbf{r}_2)).$$

Lemma 10. *For the MAC construction above, the success probability of the adversary in forging a tagged message* $(\mathbf{m}', \mathbf{r}')$ *that pass MAC verification is no more than* $\frac{\ell}{q^N}$.

The proof is a direct extension of the proof in [60].

MAC Construction II

We show a new construction of MAC that can be used for randomized LVAC code I. This MAC is specially designed to make the decoding algorithm of LVAC code in polynomial time. The MAC construction shares the similar form of the MAC in follow,

$$t = \mathsf{MAC}(\mathbf{x}, \mathbf{r}) = \sum_{1 \leq m \leq d} x_m r_m + \sum_{d+1 \leq m \leq \ell} x_m r_m + r_{\ell+1} \mod q^N.$$

But we change the form of message, randomness, and tag into vector and matrix.

The function $\mathsf{MAC} : \mathbb{F}_q^{\ell N} \times \mathbb{F}_q^{dN+3N-2} \to \mathbb{F}_q^{3N-2}$ can be considered as system of linear equations over $\mathbb{F}_q$.

1. The message of the MAC is a vector of length ℓN with $\ell \leq \binom{d+2}{2} - 1$,

$$\mathbf{x} = (x_{1,0}, \cdots, x_{1,N-1}, \cdots, x_{\ell,0}, \cdots, x_{\ell,N-1}).$$

2. The *randomness* of the MAC is a vector of length $dN + 3N - 2$ over $\mathbb{F}_q$,

$$\mathbf{r} = (r_{1,0}, \cdots, r_{1,N-1}, r_{d,0} \cdots, r_{d,N-1}, r_{d+1,0}, \cdots, r_{d+1,3N-3}).$$

We write the key in the form of a $(3N-2) \times (\ell N + 1)$ matrix:

$$\mathbf{R} = \Big[\mathbf{R}_1 \mid \cdots \mid \ \mathbf{R}_d \mid \ \mathbf{R}_{d+1} \mid \cdots \mid \ \mathbf{R}_l \mid \ \mathbf{R}_{l+1},\Big]$$

where $\mathbf{R}_m$ is a matrix that, depending on the value of the index m, can take the following forms. For $1 \leq m \leq d$,

$$\mathbf{R}_m = \begin{bmatrix} r_{m,0} & 0 & \cdots & 0 \\ r_{m,1} & r_{m,0} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ r_{m,N-1} & r_{m,N-2} & \cdots & r_{m,0} \\ 0 & r_{m,N-1} & \cdots & r_{m,1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r_{m,N-1} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

For $d+1 \leq m \leq \ell$,

$$\mathbf{R}_m = \begin{bmatrix} r_{i,j,0} & 0 & \cdots & 0 \\ r_{i,j,1} & r_{i,j,0} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ r_{i,j,N-1} & r_{i,j,N-2} & \cdots & r_{i,j,0} \\ r_{i,j,N} & r_{i,j,N-1} & \cdots & r_{i,j,1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{i,j,2N-1} & r_{i,j,2N-2} & \cdots & r_{i,N-1} \\ 0 & r_{i,j,2N-1} & \cdots & r_{i,j,N} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r_{i,j,2N-1} \end{bmatrix}.$$

Here $m = id + j - \frac{i(i-1)}{2}$ if $d+1 \leq m \leq \ell$ and $1 \leq i \leq j \leq d$. Each entry $r_{i,j,k} = \sum_{\substack{0 \leq a_1, a_2 \\ a_1 + a_2 = k}} r_{i,a_1} r_{j,a_2}$ for $0 \leq k \leq 2N-1$.

and,

$$\mathbf{R}_{\ell+1} = [r_{d+1,0}, \cdots, r_{d+1,3N-3}]^T.$$

3. The *tag* of MAC is a vector of length $3N-2$,

$$\mathbf{t} = (t_0, \cdots, t_{3N-3}).$$

4. $\mathsf{MAC}(\cdot)$ algorithm: The message $\mathbf{x}$ is encoded to the message $(\mathbf{x}, \mathbf{t})$ using the MAC algorithm $\mathbf{t} = \mathsf{MAC}(\mathbf{x}, \mathbf{r})$. Let $\mathbf{x}_i = (x_{i,0}, \cdots, x_{i,N-1})$ for $i = 1, \cdots, \ell$. The $\mathsf{MAC}(\cdot)$ function is as following:

$$\mathsf{MAC}(\mathbf{x},\mathbf{r}) = \sum_{1\le m\le d} \mathbf{R}_m\mathbf{x}_m + \sum_{d+1\le m\le \ell} \mathbf{R}_m\mathbf{x}_m + \mathbf{R}_{\ell+1}$$

$$= [\mathbf{R}_1 \mid \cdots \mid \mathbf{R}_\ell \mid \mathbf{R}_{\ell+1}] \times \begin{bmatrix} x_{1,0} \\ \vdots \\ x_{1,N-1} \\ \vdots \\ x_{\ell,0} \\ \vdots \\ x_{\ell,N-1} \\ 1 \end{bmatrix} = \begin{bmatrix} \mathbf{t} \end{bmatrix} \tag{3.2}$$

5. $\mathsf{Ver}((\mathbf{x}',\mathbf{t}'),\mathbf{r})$ algorithm: The verification algorithm $\mathsf{Ver}((\mathbf{x}',\mathbf{t}'),\mathbf{r})$ for a key $\mathbf{r}$ is by calculating $\mathsf{MAC}(\mathbf{x}',\mathbf{r})$, and comparing it with the received $\mathbf{t}'$.

Lemma 11. *The probability that a computationally unlimited adversary can forge a message* $(\mathbf{x}',\mathbf{t}')$ *with* $\mathbf{x}' \neq \mathbf{x}$ *that passes the verification is no more than* $\frac{2}{q^N}$.

Proof. We need to find the following probability:

$$\mathsf{Pr}(\mathsf{MAC}(\mathbf{x}',\mathbf{r}) = \mathbf{t}').$$

The MAC function given by Eqs. (3.2), is equivalent to the MAC of the polynomial form in Eq. (3.3). For $0 \le i \le 3N-3$, the coefficients of X^i in both sides of Eq. (3.3) form the same equation as the i^{th} equation in Eqs. (3.2),

$$\begin{aligned} t(X) &= \mathsf{MAC}(\mathbf{x},\mathbf{r}) \\ &= \sum_{1\le m\le d} x_m(X)r_m(X) + \sum_{\substack{d+1\le m\le \ell \\ m=id+j-\frac{i(i-1)}{2}}} x_m(X)r_i(X)r_j(X) + r_{d+1}(X) \mod q. \end{aligned} \tag{3.3}$$

Here each polynomial is in following,

$$x_m(X) = x_{m,0} + \cdots + x_{m,N-1}X^{N-1} \mod q \quad \text{for} \quad 1 \le i \le \ell$$

$$r_m(X) = r_{m,0} + \cdots + r_{m,N-1}X^{N-1} \mod q \quad \text{for} \quad 1 \le m \le d$$

$$r_m(X) = r_{i,j,0} + \cdots + r_{i,j,2N-2}X^{2N-2} = r_i(X)r_j(X) \mod q$$
$$\text{for} \quad d+1 \le m \le \ell,\ m = id + j - \frac{i(i-1)}{2}$$

$$r_{d+1}(X) = r_{d+1,0} + \cdots + r_{d+1,3N-3}X^{3N-3} \mod q$$

$$t(X) = t_0 + \cdots + t_{3N-3}X^{3N-3} \mod q$$

So if we can show the probability that the adversary forged MAC code $(\mathbf{x}', \mathbf{t}')$ pass MAC function Eq. (3.3), then the adversary forged MAC $(\mathbf{x}', \mathbf{t}')$ pass MAC function given by Eqs. (3.2) is bounded by the same probability.

Assume the adversary forges a message $(\mathbf{x}', \mathbf{t}')$ with $\mathbf{x}' \neq \mathbf{x}$, that passes the verification. We write the MAC in polynomial form.

$$\begin{aligned} t'(X) &= \mathsf{MAC}(\mathbf{x}', \mathbf{r}) \\ &= \sum_{1 \le m \le d} x'_m(X) r_m(X) + \sum_{\substack{d+1 \le m \le \ell \\ m = id + j - \frac{i(i-1)}{2}}} x'_m(X) r_i(X) r_j(X) + r_{d+1}(X) \mod q. \end{aligned} \tag{3.4}$$

Since the correct MAC code satisfies verification, it implies,

$$\begin{aligned} t(X) &= \mathsf{MAC}(\mathbf{x}, \mathbf{r}) \\ &= \sum_{1 \le m \le d} x_m(X) r_m(X) + \sum_{\substack{d+1 \le m \le \ell \\ m = id + j - \frac{i(i-1)}{2}}} x_m(X) r_i(X) r_j(X) + r_{d+1}(X) \mod q. \end{aligned} \tag{3.5}$$

By subtracting the two equations we will have,

$$\sum_{\substack{d+1 \le m \le \ell \\ m = id + j - \frac{i(i-1)}{2}}} \Delta x_m(X) r_i(X) r_j(X) + \sum_{1 \le m \le d} \Delta x_m(X) r_m(X) = \Delta t(X) \mod q.$$

The above equation has at most $2q^{(d-1)N}$ solutions for $(r_1(X), \cdots, r_d(X))$. This means that there are at most $2q^{(d-1)N}$ keys $\mathbf{r}$ that satisfy $\mathsf{MAC}(\mathbf{x}, \mathbf{r}) = \mathbf{t}$ and $\mathsf{MAC}(\mathbf{x}', \mathbf{r}) = \mathbf{t}'$. However, there are q^{dN} possible values for $\mathbf{r}$ satisfying $\mathsf{MAC}(\mathbf{x}, \mathbf{r}) = \mathbf{t}$.

It implies that the success probability of the forgery attack is,

$$\mathsf{Pr}(\mathsf{MAC}(\mathbf{x}', \mathbf{r}) = \mathbf{t}') \leq \frac{2q^{N(d-1)}}{q^{Nd}} = \frac{2}{q^N}.$$

□

3.3 Model and definitions

3.3.1 Limited View Adversarial Channels

Let $[N] = \{1, \cdots, N\}$, and $S_r = \{i_1, \cdots, i_{\rho_r N}\} \subset [N]$ and $S_w = \{j_1, \cdots, j_{\rho_w N}\} \subset [N]$ denote two subsets of $[N]$, and $\mathsf{SUPP}(x)$ of vector $x \in \Sigma^N$ be the set of positions where the component $x_i \neq 0$.

Definition 19. *A (ρ_r, ρ_w)-*Limited View Adversarial channel (or a (ρ_r, ρ_w)-LVAC)*, is a communication channel between Alice and Bob, that is partially controlled by Eve with two capabilities: Reading and Writing. For a codeword $c \in \Sigma^N$ where Σ is an additive group, the capabilities of Eve are,*

- *Reading: Eve can select a subset $S_r \subseteq [N]$ of size at most $\rho_r N$ and read the components of the codeword c on positions associated with S_r. Eve's view of the codeword is given by, $\mathsf{View}_{\mathcal{A}}(\mathsf{LVACenc}(m), r_{\mathcal{A}}) = \{c_{i_1}, \cdots, c_{i_{\rho_r N}}\}$, and consists of all the components that are read (observed).*
- *Writing: Eve can choose a subset $S_w \subseteq [N]$ of size at most $\rho_w N$, for "writing". This is by adding an error vector e to the codeword c, where the addition is component-wise over Σ and $\mathsf{SUPP}(e) \subseteq S_w$. The corrupted components of c are $\{y_{j_1}, \cdots, y_{j_{\rho_w N}}\}$ and $y_{j_\ell} = c_{j_\ell} + e_{j_\ell}$. The error e is generated according to Eve's best strategy for making Bob's decoder to output in error.*

We assume the adversary is *adaptive* and can select the components for reading and writing one by one, at each step using their knowledge of the codeword at that time.

The LVAC is called *restricted* if the reading and writing sets of the adversary are same, that is $S_r = S_w$. For a restricted ρ-LV adversary channel the reading and writing parameters satisfy $\rho = \rho_r = \rho_w$.

3.3.2 Limited View Adversary Code

Alice and Bob will use a *limited view adversary code* to provide reliability for communication.

Definition 20. *A Limited View Adversary Code (or LV code) for a (ρ_r, ρ_w)-LV adversary channel ((ρ_r, ρ_w)-LVAC) consists of an encoding $\mathsf{LVACenc} : \mathcal{M} \to \mathcal{C}^N$ from the message space $\mathcal{M}$ to the codeword space $\mathcal{C}^N \subset \Sigma^N$, and a deterministic decoding algorithm $\mathsf{LVACdec} : \Sigma^N \to \mathcal{M}$. For a message m that is encoded to c by the sender and corrupted to $y = c + e$ by the (ρ_r, ρ_w)-LVAC, the probability that the receiver outputs the message $m' \neq m$ with probability is no more than δ. That is for any $m \in \mathcal{M}$, and adversary's observation z we have,*

$$\mathsf{Pr}(\mathsf{LVACdec}(\mathsf{LVACenc}(m) + \mathbf{Adv}(z)) \neq m) \leq \delta.$$

The above definition of reliability is for strong LV codes. *In* weak LV codes *the decoding error probability is averaged over all messages in the message space, and the reliability requirement is,*

$$\mathsf{Pr}(M_{\mathcal{S}} \neq M_{\mathcal{R}}) \leq \delta.$$

In other words the reliability requirement is for a random message $m \in \mathcal{M}$.

An LV code with δ decoding error is called δ-LV code. An LV code is deterministic if the $\mathsf{LVACenc}(\cdot)$ is deterministic, and LV code is probabilistic if the $\mathsf{LVACenc}(\cdot)$ is probabilistic. A LV code family $\mathbb{C} = \{\mathcal{C}^N\}_{N \in \mathbb{N}}$ for (ρ_r, ρ_w)-LVAC is a family of LV codes indexed by the code length $N \in \mathbb{N}$.

Definition 21. *The rate $R(\mathbb{C})$ is achievable by a code family $\mathbb{C}$ if for any $\xi > 0$ there exists N_0 such that for any $N > N_0$, we have $\frac{1}{N} \log_{|\Sigma|} |\mathcal{M}| \geq R(\mathbb{C}) - \xi$, and the probability of decoding error satisfies $\delta \leq \xi$.*

We use achievable rate of LV code families over a LVAC to define capacity of these channels.

Definition 22. *The capacity* C *of a* (ρ_r, ρ_w) *LVAC is the highest achievable rate of all LV code families* $\mathbb{C}$ *for the channel.*

3.4 An upper bound on the rate of LV codes

We derive an upper bound on the rate of an LV code and use the bound to find an upper bound on the highest achievable rate of a code family for a (ρ_r, ρ_w)-LV adversary channel. The rate upper bound only depends on the parameter ρ_w. However achieving the bound would impose condition on ρ_r.

Theorem 7. *The rate of an LV code* $\mathcal{C}^N$ *over a* (ρ_r, ρ_w)*-LVAC is bounded as,*

$$R(\mathcal{C}^N) = \frac{\mathsf{H}(M)}{N \log |\Sigma|} \leq 1 - \rho_w + 2\mathsf{H}(\delta). \tag{3.6}$$

The highest achievable rate of an LV code family for a (ρ_r, ρ_w)*-LVAC is bounded as,*

$$\mathsf{C} \leq 1 - \rho_w. \tag{3.7}$$

Proof is in Section 3.7.2.

In restricted LVACs, the adversary is restricted in their choice of S_r and S_w and so one may expect a different upper bound. However we prove the same upper bound holds in this case also.

Proposition 1. *The rate of an LV code family for a* restricted ρ-LVAC *is bounded as,*

$$\mathsf{C} \leq 1 - \rho_w.$$

Note that this proposition does not follow from Theorem 7 as the adversary in restricted LVAC is less powerful and one may expect a different upper bound. One however can use the same proof method to derive the bound for codes over restricted LVACs.

3.5 LV-codes Construction

We show two constructions of randomized LV-code. The first LV-code is over restricted ρ-LVAC.

3.5.1 LV-codes Construction I

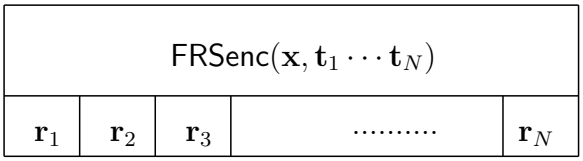
In this section we show the first efficient construction of randomized LV-codes family over restricted ρ-restricted LVAC. In ρ-restricted LVAC, the adversary reading and writing sets are same, that is $S_r = S_w$, and $\rho = \rho_r = \rho_w$. The LV-code is constructed over $\mathbb{F}_q^u$. The construction of randomized LV-codes makes use of the MAC and FRS code with appropriately chosen parameters.

1. MAC: we use the MAC Construction II in Section 3.2.4: The MAC function is in the form of $\mathsf{MAC} : \mathbb{F}_q^{\ell N} \times \mathbb{F}_q^{dN+3d-2} \to \mathbb{F}_q^{3d-2}$ with $\ell = \lceil uR(\mathcal{C}^N) \rceil$ and $d = \lceil \sqrt{2u_1} \rceil$.

2. Folded Reed-Solomon Code: The FRS code has length N over $\mathbb{F}_q^{u_1}$.

Let N and $R(\mathcal{C}^N)$ denote the code length and information rate, respectively. Let the randomness vector $\mathbf{r}_i$ for $i = 1, \cdots, N$ with length u_2. Let $u_2 = Nd + 3N - 2 = N\lceil \sqrt{2u_1} \rceil + 3N - 2$ and $u = u_1 + u_2$. The randomized LV-codes is over $\mathbb{F}_q^u$ with $u = u_1 + u_2$. Sender wishes to send the information block $\mathbf{m} = (m_0, \cdots, m_{uR(\mathcal{C}^N)N-1}), m_i \in \mathbb{F}_q$, to the receiver.

LV code I



LV codes I

Encoding: Alice performs the following steps:

1. Append vector $\{\mathbf{0}\}$ over $\mathbb{F}_q$ with length $N(\ell - uR(\mathcal{C}^N))$ to message $\mathbf{m} = (m_0, \cdots, m_{uR(\mathcal{C}^N)N-1})$, and forms the vector $\mathbf{x} = (\mathbf{m}, \mathbf{0})$ of length ℓN.

2. Randomly generate the key $\mathbf{r}_i$ for $1 \leq i \leq N$ of the MAC Construction II. Each key is written as a $(3N-2) \times (\ell N + 1)$ matrix of MAC Construction II,

$$\mathbf{R}_i = [\mathbf{R}_{i,1} \mid \cdots \mid \mathbf{R}_{i,\ell} \mid \mathbf{R}_{i,d+1}].$$

3. Generate tag $\mathbf{t}_i = \mathsf{MAC}(\mathbf{x}, \mathbf{r}_i)$ for $i = 1, \cdots, N$ using MAC Construction II.

   The dimension of FRS code is $k = \ell N + N(3N-2)$. The message block of FRS code is,

$$(\mathbf{x}, \mathbf{t}_1 \cdots \mathbf{t}_N).$$

4. Encode the message block to the codeword using FRS encoding algorithm,

$$c^{\mathsf{FRS}} = \mathsf{FRSenc}(\mathbf{x}, \mathbf{t}_1 \cdots \mathbf{t}_N).$$

   The codeword c of the LV-codes is obtained by appending randomness $\mathbf{r}_i$ to the i^{th} component of the FRS code c_i^{FRS}. Each component of the codeword c is,

$$c_i = (c_i^{\mathsf{FRS}}, \mathbf{r}_i).$$

Decoding: Bob performs the following steps:

1. Receive a corrupted word y with the i^{th} component of the word $y_i = (y_i^{\mathsf{FRS}}, \hat{\mathbf{r}}_i)$. Here y_i^{FRS} and $\hat{\mathbf{r}}_i$ is the corrupted i^{th} component of the FRS code and the randomness, respectively.

2. Use the FRS decoding algorithm to decode the FRS codeword y^{FRS} and get Eqs. (3.11).

3. Generate N system of linear equations. Each system of linear equations is generated by FRS decoding algorithm and MAC key $\mathbf{r}_i$. The i^{th} system of linear equation is in the form

$$\begin{bmatrix} \mathbf{B}_0 & \mathbf{B}_1 & \cdots & \mathbf{B}_i & \cdots & \mathbf{B}_N \\ \mathbf{R}'_i & \mathbf{0} & \cdots & -\mathbf{I} & \cdots & \mathbf{0} \end{bmatrix} \times \begin{bmatrix} \mathbf{x} \\ \mathbf{t}_1 \\ \vdots \\ \mathbf{t}_i \\ \vdots \\ \mathbf{t}_N \end{bmatrix} = \begin{bmatrix} -\mathbf{a}' \\ -\mathbf{R}_{i,d+1} \end{bmatrix} \tag{3.8}$$

Here the first $\ell N + N(3N-2)$ equations are generated by the FRS decoding algorithm of Eq. (3.11): the first ℓN columns of the matrix of coefficients of these equations forms $\mathbf{B}_0$, and for $1 \leq i \leq N$, columns $(\ell N + (i-1)(3N-2))^{th}$ to $(\ell N + i(3N-2) - 1)^{th}$ of this matrix specify $\mathbf{B}_i$. Finally, $-\mathbf{a}'$ is the right hand side vector. The last $3N-2$ equations are from MAC Construction II using key $\mathbf{r}_i$, with $\mathbf{R}'_i = [\mathbf{R}_{i,1} \mid \cdots \mid \mathbf{R}_{i,\ell}]$, and $\mathbf{I}$ is identity matrix.

4. Bob outputs $\mathbf{m}$, if this is the unique message output by the system of $N - \rho N$ linear equations; Otherwise Bob randomly outputs $\perp$.

We show the reliability and rate of randomized LV-codes.

Reliability

Lemma 12. *If the adversary does not choose position i^{th} to read and write, the probability that the i^{th} system of linear equations Eqs. (3.8) does not produce the unique and correct* $\mathbf{m}$ *is at most* $\frac{2}{q^{N-v+1}}$. *That is,*

$$\mathsf{Pr}(\mathbf{m}' : \mathbf{m}' \neq \mathbf{m} \quad \textit{and} \quad \mathbf{m}' \textit{ is solution of Eqs. (3.8) }) \leq \frac{2}{q^{N-v+1}}.$$

Proof. Firstly, if any $\mathbf{m}'$, which is not equal to $\mathbf{m}$, is a solution Eqs. (3.8), then its associated vector $(\mathbf{x}', \mathbf{t}')$ must satisfy the last $3N-2$ equations in Eqs. (3.8). Since these equations generated by MAC, that is,

$$\begin{bmatrix} \mathbf{R}'_i & -\mathbf{I} \end{bmatrix} \times \begin{bmatrix} \mathbf{x}' \\ \\ \mathbf{t}'_i \end{bmatrix} = \begin{bmatrix} -\mathbf{R}_{i,v+2} \end{bmatrix}.$$

It implies,

$$\mathsf{MAC}(\mathbf{x}', \mathbf{r}_i) = \mathbf{t}'_i.$$

Using lemma 11, the probability that $\mathsf{MAC}(\mathbf{x}', \mathbf{r}_i) = \mathbf{t}'_i$ is at most $\frac{2}{q^N}$.

Secondly, from the decoding algorithm of the FRS code, there are at most q^{v-1} vectors $(\mathbf{x}', \mathbf{t}')$ which satisfy the first k equations in Eqs. (3.8). So by union the probability that $(\mathbf{x}', \mathbf{t}')$ is the solution of first k equations in Eqs. (3.8), and still be a solution of last $3N-2$ equations in Eqs. (3.8), the probability that the Eqs. (3.8) contain any solutions $(\mathbf{x}', \mathbf{t}')$ associated with $\mathbf{m}' \neq \mathbf{m}$, is at most $\frac{2q^{v-1}}{q^N} = \frac{2}{q^{N-v+1}}$. □

Lemma 13. *The decoding error of the LV-codes is at most* $\delta \leq \frac{2N}{q^{N-v+1}}$ *if* $\rho \leq \frac{1}{2} - \frac{1}{2N}$.

Proof. Firstly, we show the correct message $\mathbf{m}$ is always output by Bob. Since the correct message $\mathbf{m}$ is always contained in decoded list of FRS decoding algorithm, and associated with the correct MAC code $(\mathbf{x}, \mathbf{t})$, it is always the solution of Eqs. (3.8) if the i^{th} component of codeword is not corrupted. Since there are $N - \rho N$ components of codeword, it implies that $\mathbf{m}$ will always be output by Bob.

Secondly, we show that the probability of any message $\mathbf{m}' \neq \mathbf{m}$ output by Bob is bounded by $\frac{2N}{q^{N-v+1}}$, and so the probability of decoding error is bounded by $\delta \leq \frac{2N}{q^{N-v+1}}$. The adversary can corrupt at most ρN components on set $S = S_r = S_w = \{i_1, \cdots, i_{\rho N}\}$ of codeword, and make $\mathbf{m}'$ be the solution of Eqs. (3.8) on components in set S. Since $\rho N < N/2$, if the corrupted message $\mathbf{m}'$ output by Bob, it must be the solution of at least one Eqs. (3.8) on set $[N] \setminus S$. From Lemma 12, the probability of any $\mathbf{m}' \neq \mathbf{m}$ is the solution of the i^{th} Eqs. (3.8) with $i \in [N] \setminus S$ is bounded by $\frac{2}{q^{N-v+1}}$. It implies that the probability of any $\mathbf{m}' \neq \mathbf{m}$ is the solution of any i^{th} Eqs. (3.8) with $i \in [N] \setminus S$ is bounded by $\frac{2N}{q^{N-v+1}}$. So the probability that $\mathbf{m}'$ output by Bob bounded by $\frac{2N}{q^{N-v+1}}$.

It implies for any message $\mathbf{m}$, the probability of decoding error is,

$$\mathsf{Pr}(\mathsf{LVACdec}(\mathsf{LVACenc}(\mathbf{m}) + e) = \mathbf{m}' \neq \mathbf{m}) \leq \frac{2N}{q^{N-v+1}}. \tag{3.9}$$

□

Rate of LV-codes

First we study the decoding condition of LV-codes $\mathcal{C}^N$ with length N. We show the decoding condition LV-codes in Lemma 14.

Lemma 14. *The LV-codes over $\mathbb{F}_q^u$ can correctly decode if there is,*

$$\rho \leq \min(\frac{1}{2} - \frac{1}{2N}, \frac{v}{v+1} - \frac{v}{v+1}\frac{uR(\mathcal{C}^N) + 3N}{N^2 + u - N(\sqrt{N^2 + 2u} + 3) - v}).$$

Proof is in Section 3.7.3.

Then we show the rate of LV-code family $\mathbb{C} = \{\mathcal{C}^N\}$.

Theorem 8. *For any small $\xi > 0$, there is an LV-code $\mathcal{C}^N$ with length N over ρ-restricted LVAC with $\rho < \frac{1}{2}$. The rate of LV-code $\mathcal{C}^N$ is $R(\mathcal{C}^N) = 1 - \rho - 4\xi$. The alphabet of LV-code is $\Sigma = \mathbb{F}_q^{\frac{2N^2}{\xi^4} + \frac{2N^2}{\xi^2}}$, and the decoding error is $\delta \leq \xi$. The required computational time of encoding and decoding algorithm of LV-code is polynomial in N. The LV-code family $\mathbb{C} = \{\mathcal{C}^N\}$ for ρ-restricted LVAC channel achieves rate $R(\mathbb{C}) = 1 - \rho$ for ρ-restricted LVAC with $\rho < \frac{1}{2}$.*

Proof. First, from the decoding condition $\rho = \rho_r = \rho_w \leq \frac{1}{2} - \frac{1}{2N}$, it implies, $\rho < 1/2$.

Second, let $1/2 > \xi > 0$ is a small constant, $v = \frac{1}{\xi}$, $u = \frac{2N^2}{\xi^4} + \frac{2N^2}{\xi^2}$, $N_0 > \frac{2}{\xi}$. From Lemma 14, the decoding condition of LV-codes of length N is satisfied if,

$$\begin{aligned}\rho &\leq \frac{1}{1+\xi} - \frac{1}{1+\xi}\frac{(\frac{2N^2}{\xi^4} + \frac{2N^2}{\xi^2})R(\mathcal{C}^N) + 3N^2}{N^2 + (\frac{2N^2}{\xi^4} + \frac{2N^2}{\xi^2}) - N(\sqrt{N^2 + \frac{4N^2}{\xi^4} + \frac{4N^2}{\xi^2}})} \\ &= \frac{1}{1+\xi} - \frac{1}{1+\xi}((1+\xi^2)R(\mathcal{C}^N) + \frac{3}{2}\xi^4).\end{aligned}$$

It implies the decoding condition should satisfies if,

$$\rho \leq 1 - R(\mathcal{C}^N) - 3\xi. \tag{3.10}$$

So if we choose the rate of LV-codes is equal to,

$$R(\mathcal{C}^N) = 1 - \rho - 4\xi.$$

The decoding condition Eq. (3.10) of LV-codes will be satisfied. It implies if $N > N_0$, there is,

$$R(\mathcal{C}^N) = 1 - \rho - 4\xi \geq R(\mathbb{C}) - 4\xi,$$

and the decoding error is bounded by,

$$\delta \leq q^{\frac{1}{\xi} - N} \leq q^{-\frac{N}{2}} \leq \xi.$$

So it implies the rate of LV-codes family $\mathbb{C}$ is $R(\mathbb{C}) = 1 - \rho$.

The encoding algorithm is efficient from the polynomial time in N of FRS encoding algorithm and MAC function MAC. The decoding algorithm is efficient from the polynomial time in N of FRS decoding algorithm and solving N Eqs. (3.8).

□

3.5.2 LV-codes Construction II

We construct an efficient LV code family $\mathbb{C} = \{\mathcal{C}^N\}_{N\in\mathbb{N}}$ for a (ρ_r, ρ_w)-LVAC. The encoding and decoding algorithms of the LV code family $\mathbb{C}$ are denoted by $\mathsf{LVACenc}$ and $\mathsf{LVACdec}$,

respectively. The construction employs a construction of Folded Reed-Solomon codes that uses subspace evasive sets, a message authentication code, and an adversarial wiretap code, with the following parameters:

- FRS codes using subspace evasive sets: From Lemma 8, there is an FRS code $\mathcal{C}_{\mathsf{FRS}}$ over alphabet $\Sigma_{\mathsf{FRS}} = \mathbb{F}_q^{\frac{1}{\xi^4}}$, with rate $R_{\mathsf{FRS}} = 1 - \rho_w - \xi^2$. The construction uses subspace evasive sets has the decoder list size bounded by $(1/\xi^2)^{\frac{D}{\xi^2}\log\log\frac{1}{\xi^2}}$.
- MAC: From Lemma 10, there is a MAC function $\mathsf{MAC} : \mathbb{F}_q^{uR(\mathcal{C}^N)N} \times \mathbb{F}_q^{2N} \to \mathbb{F}_q^N$, with the probability of failure to detect a forged tagged message bounded by $\delta_{\mathsf{MAC}} \leq \frac{uR(\mathcal{C}^N)}{q^N}$.
- AWTP code: From Lemma 9, there is an AWTP code $\mathcal{C}_{\mathsf{AWTP}}$ over alphabet $\Sigma_{\mathsf{AWTP}} = \mathbb{F}_q^{\frac{1}{\xi^2}}$, whose rate is $R_{\mathsf{AWTP}} = 1 - \rho_r - \rho_w - \xi$, and has decoding error bounded by $\delta_{\mathsf{AWTP}} \leq \frac{(1/\xi)^{\frac{D}{\xi}\log\log(\frac{1}{\xi})}}{q^N}$.

The construction of the LV code is as follows.

LV code II

Encoding: Alice does the following:

1. For an information block $\mathbf{m}$ of length $uR(\mathcal{C}^N)N$ with $u = \log|\Sigma|$ and $\Sigma = \mathbb{F}_q^{\frac{1}{\xi^2}+\frac{1}{\xi^4}}$, do the following. Generate random vectors $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2)$ with $\mathbf{r}_i \in \mathbb{F}_q^N$, $i = 1, 2$, and use it to find the MAC tag for the message $\mathbf{m}$, using the MAC construction in Section 5.2.1,

$$\mathsf{MAC}(\mathbf{m}, \mathbf{r}) = \mathbf{t}.$$

   The tagged message is of length $uR(\mathcal{C}^N)N + N$ over $\mathbb{F}_q$.

2. Encode the randomness $\mathbf{r}$ into a codeword c_{AWTP} of an AWTP code of length N,

$$c_{\mathsf{AWTP}} = \mathsf{AWTPenc}(\mathbf{r}).$$

3. Encode the vector $(\mathbf{m}, \mathbf{t})$ into a codeword c_{FRS} of an Folded Reed-Solomon of length N that uses subspace evasive sets for efficient decoding. That is,

$$c_{\mathsf{FRS}} = \mathsf{FRSenc}(\mathbf{m}, \mathbf{t}).$$

4. The codeword c of the LV code has the i^{th} component, $c_i = (c_{\mathsf{AWTP},i}, c_{\mathsf{FRS},i}) \in \Sigma, i = 1, \cdots, N$.

   Alice sends c to Bob over the LVAC.

Decoding: Bob does the following:

1. Bob receives a corrupted word y. Each component of y is broken into two parts to reconstruct the (corrupted) AWTP codeword y_{AWTP}, and the (corrupted) FRS codeword y_{FRS}, of the sender.

2. Bob uses AWTP decoding algorithm to decode y_{AWTP} and obtain the randomness vector $\mathbf{r}$. The decoding error of AWTP code is bounded by δ_{AWTP}.

3. Bob uses the FRS codeword decoding algorithm to decode y_{FRS}, and outputs a list $\mathcal{L}_{\mathsf{FRS}}$ of size $|\mathcal{L}_{\mathsf{FRS}}| \leq (1/\xi^2)^{\frac{D}{\xi^2} \log\log \frac{1}{\xi^2}}$. Each element in the list $\mathcal{L}_{\mathsf{FRS}}$ is a potential tagged message $(\mathbf{m}_i, \mathbf{t}_i)$.

4. Bob checks whether the $(\mathbf{m}_i, \mathbf{t}_i) \in \mathcal{L}_{\mathsf{FRS}}$ is a correctly formed tagged message by verifying,

$$\mathbf{t}_i = \mathsf{MAC}(\mathbf{m}_i, \mathbf{r}).$$

   If there is a unique valid tagged message, then Bob outputs the message $\mathbf{m}$ corresponding to the tagged message. Otherwise, outputs $\perp$.

Reliability of LV codes

Lemma 15. *The probability of decoding error (strong reliability) for the LV code is bounded by* $\delta \leq \frac{2(1/\xi^2)^{(2+\frac{D}{\xi^2}\log\log\frac{1}{\xi^2})}}{q^N}$.

Proof. The decoding error happens in the following two cases.

1. The AWTP decoding algorithm outputs the wrong randomness vector $\mathbf{r}'$. This probability is bounded by $\delta_{\mathsf{AWTP}} \leq \frac{(1/\xi)^{\frac{D}{\xi}\log\log(\frac{1}{\xi})}}{q^N}$.

2. If the AWTP decoding algorithm outputs the correct randomness $\mathbf{r}'$, there exists a tagged message $(\mathbf{m}', \mathbf{t}')$ in the decoding list $\mathcal{L}_{\mathsf{FRS}}$ with $\mathbf{m}' \neq \mathbf{m}$ that passes the MAC verification algorithm. Since the AWTP code is perfectly secure, the randomness $\mathbf{r}$ is received by Bob with perfect security. So Bob can use $\mathbf{r}$ to verify the validity of the tagged message $(\mathbf{m}', \mathbf{t}')$. For each $(\mathbf{m}', \mathbf{t}')$ with $\mathbf{m}' \neq \mathbf{m}$, the probability of passing MAC verification is bounded by $\delta_{\mathsf{MAC}} \leq \frac{uR(\mathcal{C}^N)}{q^N}$. Since the size of the list containing $(\mathbf{m}', \mathbf{r}') \in \mathcal{L}_{\mathsf{FRS}}$ is bounded by $|\mathcal{L}_{\mathsf{FRS}}| \leq (1/\xi^2)^{\frac{D}{\xi^2}\log\log\frac{1}{\xi^2}}$, the probability that the decoder outputs the message $\mathbf{m}'$, such that the corresponding tagged message $(\mathbf{m}', \mathbf{r}')$ passes the MAC verification and $(\mathbf{m}', \mathbf{r}') \in \mathcal{L}_{\mathsf{FRS}}$, is bounded by $\delta_{\mathsf{FRS}} \leq \frac{uR(\mathcal{C}^N)|\mathcal{L}|}{q^N} \leq \frac{uR(\mathcal{C}^N)(1/\xi^2)^{\frac{D}{\xi^2}\log\log\frac{1}{\xi^2}}}{q^N}$.

So the total probability of decoding error is bounded as follows,

$$\delta = \delta_{\mathsf{AWTP}} + \delta_{\mathsf{FRS}} \leq \frac{2(1/\xi^2)^{(2+\frac{D}{\xi^2}\log\log\frac{1}{\xi^2})}}{q^N}.$$

□

Rate of an LV code family

Theorem 9. *The information rate of the probabilistic LV code family* $\mathbb{C} = \{\mathcal{C}^N\}^{N\in\mathbb{N}}$ *over a* (ρ_r, ρ_w)*-LVAC is* $R(\mathbb{C}) = 1 - \rho_w$. *The read and write parameters must satisfy* $\rho_r + \rho_w < 1$. *The encoding and decoding algorithms are polynomial time in* N.

Proof. 1). First we show that the rate of the LV code family is $R(\mathbb{C}) = 1 - \rho_w$.

Let $0 \leq \xi \leq \frac{1}{2}$, u be the length of alphabet Σ, u_{AWTP} be the length of alphabet Σ_{AWTP}, u_{FRS} be the length of alphabet Σ_{FRS}, and $N_0 \geq (2 + \frac{D}{\xi^2} \log\log \frac{1}{\xi^2})(1 + 2\log \frac{1}{\xi}) + \log \frac{1}{\xi}$. From $u_{\mathsf{FRS}} R_{\mathsf{FRS}} N = uR(\mathcal{C}^N)N$ and $u = u_{\mathsf{AWTP}} + u_{\mathsf{FRS}}$, we have,

$$R_{\mathsf{FRS}} = \frac{u}{u_{\mathsf{FRS}}} R(\mathcal{C}^N) = (1 + \frac{1}{u_{\mathsf{FRS}}}) R(\mathcal{C}^N) \leq R(\mathcal{C}^N) + \xi^4.$$

Since $R_{\mathsf{FRS}} = 1 - \rho_w - \xi^2$, we have,

$$R(\mathcal{C}^N) \geq R_{\mathsf{FRS}} - \xi^4 \geq 1 - \rho_w - 2\xi^2 \geq 1 - \rho_w - \xi,$$

and,

$$\delta \leq \frac{2(1/\xi^2)^{(2+\frac{D}{\xi^2}\log\log\frac{1}{\xi^2})}}{q^N} \leq \xi.$$

So the rate of LV code family is $R(\mathbb{C}) = 1 - \rho_w$.

2). Second we show that the reading and writing parameter must satisfy $\rho_r + \rho_w < 1$.

To transmit the randomness $\mathbf{r}$ securely and reliably, the maximum length of $\mathbf{r}$ must be no more than the maximum information that can be transmitted by the AWTP code. Lemma 9 implies that the length of the randomness $\mathbf{r}$ is bounded as,

$$N \leq (1 - \rho_r - \rho_w - \xi) \log |\Sigma_{\mathsf{AWTP}}| N.$$

Since $\Sigma_{\mathsf{AWTP}} = \mathbb{F}_q^{\frac{1}{\xi_1^2}}$, we have,

$$1 - \xi - \xi^2 \geq \rho_r + \rho_w.$$

So the reading and writing sets must satisfy $1 - \xi - \xi^2 \geq \rho_r + \rho_w$. Since ξ approaches zero as N goes to infinity, we have $\rho_r + \rho_w < 1$.

3). The encoding algorithm is efficient since both adversarial wiretap codes and FRS codes (with subspace evasive set message coding), have polynomial (in N) time encoding algorithms (in Poly(N)); also the MAC function MAC is polynomial time Poly(N). The decoding algorithm is efficient because decoding function of the first two primitives are efficient, and the output list size of the FRS code with subspace evasive set message coding is constant size. Finally, the MAC verification algorithm is in Poly(N). □

A comparison of LV code constructions

We compare the LV code construction. LV code [73] is deterministic while the latter two are probabilistic. All LV codes are capacity achieving. LV code [73] and LV code III both allow $S_r \neq S_w$, while LV code II needs $S_r = S_w$. LV code [73] has $\rho_r + \rho_w < 1 - 1/N$ and has the restriction that $\rho_r = \rho_w$. LV code III has efficient decoding and has the requirement that $\rho_r + \rho_w < 1$

Table 3.1: LV-Code Construction

Code	**Rate** $R(\mathcal{C}^N)$	**Comp.**	Σ	**Adversary capability**
LV code [73]	$1 - \rho_w - \xi$	Exp(N)	$\mathbb{F}_q^2$	$\rho_r = \rho_w =$ $\min(R(\mathcal{C}^N) - \frac{1}{2N}, 1 - R(\mathcal{C}^N) - \frac{1}{2N})$
LV code I	$1 - \rho_w - \xi$	Poly(N)	$\mathcal{O}(\mathbb{F}_q^{\frac{N^2}{\xi^4}})$	$S_r = S_w$, $\rho < 1/2$
LV code II	$1 - \rho_w - \xi$	Poly(N)	$\mathcal{O}(\mathbb{F}_q^{\frac{1}{\xi^4}})$	$\rho_r + \rho_w < 1$

3.6 LV-codes and RMT

3.6.1 LV codes and 1-round RMT

LV codes are defined over an alphabet Σ and so all components of a codeword are elements of Σ. In RMT protocols however, the set of transmissions over each wire may be different.

Definition 23 (Symmetric RMT)**.** *Let $\mathcal{W}_j^i, j = 1 \cdots N, i = 1 \cdots r$, denote the set of possible transmissions over wire j in an r-round RMT protocol. An RMT protocol is called a* symmetric RMT protocol *if $\mathcal{W}_j^i = \mathcal{W}^i$ is independent of j.*

All known constructions of threshold RMT protocols are symmetric.

Proposition 2. *There is a one-to-one correspondence between LV codes $\mathcal{C}^N$ of length N that provide δ-reliability for restricted ρ-LVACs, and 1-round symmetric δ_{RMT}-RMT protocols for N wires with security against a (t, N) threshold adversary, where $t = \rho N$.*

An LV code can be used to construct a 1-round symmetric δ_{RMT}-RMT, where $\delta_{\mathsf{RMT}} = \delta$. The converse is also true.

Proof. Consider an LV code $\mathcal{C}^N$ with decoding error δ for a restricted ρ-LVAC. By associating each component of a codeword with a distinct wire, one can construct a 1-round symmetric δ_{RMT}-RMT protocol for N wires. The protocol security is against a threshold (t, N) adversary with $t = \rho N$. The RMT encoding and decoding are obtained from the corresponding functions in the LV code; that is, $\mathsf{RMTenc}(m) = \mathsf{LVACenc}(m)$ and $\mathsf{RMTdec}(y) = \mathsf{LVACdec}(y)$. To relate the reliability of the RMT protocol to that of the LVAC-code, we note the following:

1. Decoding error is both cases requires the decoder to output the correct message with probability at least $1 - \delta$.
2. The corruption of a codeword in a restricted ρ-LVAC is by additive error while in RMT the adversary can arbitrarily modify the $|S| = t$ corrupted wires. However in restricted ρ-LVACs, $S = S_r = S_w, |S| = \rho N$ and so modifying the components $(c_{i_1}, \cdots c_{i_t})$ to $(c'_{i_1}, \cdots c'_{i_t})$ is equivalent to calculating an error e with $\mathsf{SUPP}(e) = S$ and $(e_{i_1}, \cdots e_{i_t}) = ((c'_{i_1} - c_{i_1}), \cdots (c'_{i_t} - c_{i_t}))$, and adding it to the codeword. This means that for these channels additive error can be used to generate all possible adversarial tamperings.

The theorem follows by constructing a restricted LV code with $S = S_r = S_w$ from a 1-round symmetric δ_{RMT}-RMT, using the same correspondence between the code components and the wires. We will have $\delta = \delta_{\mathsf{RMT}}$. □

The upper bound on the rate (Theorem 7) of LV codes for ρ-restricted LVAC, gives a lower bound on the transmission rate of 1-round symmetric δ-RMT protocols.

Theorem 10. *Transmission rate of 1-round symmetric δ-RMT protocols is lower bounded by,*

$$\tau(\mathsf{RMT}) \geq \frac{N}{N - t + 2N\mathsf{H}(\delta)}.$$

Proof. Let $R(\mathcal{C}^N)$ be the rate of a δ-LV code $\mathcal{C}^N$ for a restricted ρ-LVAC. From Proposition 13, the transmission rate of the associated 1-round symmetric δ-RMT is given by, $\tau(\mathsf{RMT}) = \frac{N \log |\mathcal{V}|}{\log |\mathcal{M}|} = \frac{1}{R(\mathcal{C}^N)}$.

Now consider a 1-round symmetric δ-RMT for N wires and $t = \rho N$. Using Theorem 7, we have an LV code for a restricted LVAC with $S = S_r = S_w$ whose information rate is upper bounded by,

$$R(\mathcal{C}^N) \leq 1 - \rho + 2\mathsf{H}(\delta).$$

Since the transmission rate of a symmetric δ-RMT protocol is the inverse of the information rate of the corresponding LV code, we have,

$$\tau(\mathsf{RMT}) = \frac{1}{R(\mathcal{C}^N)} \geq \frac{1}{1 - \rho + 2\mathsf{H}(\delta)} = \frac{N}{N - t + 2N\mathsf{H}(\delta)}.$$

□

Since $\delta \geq 0$, the right hand side of the bound is smaller than the known bound $\frac{N}{N-t}$. This is expected as the definition of reliability used here weaker than the one used derivation of this latter bound (Theorem 4, [67]) requiring decoder to output correct messages only.

Corollary 1. *For $N = 2t + 1$, we have,*

$$\tau(\mathsf{RMT}) = \frac{1}{R(\mathcal{C}^N)} \geq \frac{2t + 1}{t + 1 + 2(2t + 1)\mathsf{H}(\delta)}.$$

Since $\delta \geq 0$, the right hand side of the bound is less than the known bound $\frac{2t+1}{1+t}$ that is for the stronger definition of reliability. An explanation similar to what is given for Theorem (14) applies here also.

Corollary 2. *For $N = 2t + ct$, we will have the following.*

1.

$$\tau(\mathsf{RMT}) = \frac{1}{R(\mathcal{C}^N)} \geq \frac{2+c}{1+c+2(2+c)\mathsf{H}(\delta)}.$$

2. The RMT construction obtained from the LV code in Section 4.5 is efficient and optimal, and the failure probability $\delta \leq \mathcal{O}(\frac{1}{q^N})$.

Proof is in Section 3.7.4.

3.7 Proof of Chapter 3

3.7.1 Detail of Linear Algebraic FRS Decoding Algorithm

Proof. Linear algebraic list decoding [38] has two main steps: interpolation and message finding as outlined below. Let γ be a primitive element for $\mathbb{F}_q$.

- Find a polynomial, $Q(X, Y_1, \cdots, Y_v) = A_0(X) + A_1(X)Y_1 + \cdots + A_v(X)Y_v$ over $\mathbb{F}_q$, such that $\deg(A_i(X)) \leq D$ for $i = 1 \cdots v$ and $\deg(A_0(X)) \leq D + k - 1$, satisfying $Q(\alpha_i, y_{i_1}, y_{i_2}, \cdots, y_{i_v}) = 0$ for $1 \leq i \leq n_0$, where $n_0 = (u - v + 1)N$.
- Find all polynomials $f(X) \in \mathbb{F}_q[X]$ of degree at most $k-1$ and coefficients $f_0, f_1 \cdots f_{k-1}$, that satisfy, $A_0(X) + A_1(X)f(X) + A_2(X)f(\gamma X) + \cdots + A_v(X)f(\gamma^{v-1}X) = 0$.

The two above requirements are satisfied if $f \in \mathbb{F}_q[X]$ is a polynomial of degree at most $k-1$ whose FRS encoding agrees with the received word $\mathbf{y}$ in at least t components where,

$$t > N(\frac{1}{v+1} + \frac{v}{v+1}\frac{uR}{u-v+1}).$$

This means we need to find all polynomials $f(X) \in \mathbb{F}_q[X]$ of degree at most $k-1$ and coefficients $f_0, f_1, \cdots, f_{k-1}$, that satisfy,

$$A_0(X) + A_1(X)f(X) + A_2(X)f(\gamma X) + \cdots + A_v(X)f(\gamma^{v-1}X) = 0.$$

Let $A_i(X) = \sum_{j=0}^{D+k-1} a_{i,j} X^j$ for $0 \leq i \leq v$. Note that $a_{i,j} = 0$ for $i \geq 1$ and $j \geq D$. Define the polynomials,

$$\begin{cases} B_0(X) = a_{1,0} + a_{2,0}X + a_{3,0}X^2 + \cdots + a_{v,0}X^{v-1}, \\ \quad \vdots \\ B_{k-1}(X) = a_{1,k-1} + a_{2,k-1}X + a_{3,k-1}X^2 + \cdots + a_{v,k-1}X^{v-1}. \end{cases}$$

Requiring that the coefficients of $X^i, i = 0 \cdots k-1$, in the polynomial $Q(X) = A_0(X) + A_1(X)f(X) + A_2(X)f(\gamma X) + \cdots + A_v(X)f(\gamma^{v-1}X) = 0$ be equal to 0, is equivalent to the following system of linear equations for $f_0 \cdots f_{k-1}$.

$$\begin{bmatrix} B_0(\gamma^0) & 0 & 0 & \cdots & 0 \\ B_1(\gamma^0) & B_0(\gamma^1) & 0 & \cdots & 0 \\ B_2(\gamma^0) & B_1(\gamma^1) & B_0(\gamma^2) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ B_{k-1}(\gamma^0) & B_{k-2}(\gamma^1) & B_{k-3}(\gamma^2) & \cdots & B_0(\gamma^{k-1}) \end{bmatrix} \times \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_{k-1} \end{bmatrix} = \begin{bmatrix} -a_{0,0} \\ -a_{0,1} \\ -a_{0,2} \\ \vdots \\ -a_{0,k-1} \end{bmatrix} \tag{3.11}$$

The rank of the coefficient matrix in (Eqs. 3.11) is at least $k - v + 1$. This is because there are at most $v - 1$ solutions for the equation $B_0(X) = 0$ and so at most $v - 1$ possible γ^i satisfying $B_0(\gamma^i) = 0$, resulting in the rank of the matrix of (Eqs. 3.11) to be at least $k - v + 1$. This means that the dimension of the solution space is at most $v - 1$ and there are at most q^{v-1} solutions to (Eqs. 3.11). This gives the list size to be equal to q^{v-1}.

□

3.7.2 Proof of Theorem 7

Proof. We prove an upper bound on the rate of weak LV codes for (ρ_r, ρ_w)-LVACs. For these codes error probability is averaged over all codewords. The rate upper bound for strong LV codes cannot be more than this upper bound as for these latter codes error probability of decoding for any message is bounded by δ.

The bound is for the rate of an arbitrary code and is derived for a special strategy of the adversary given below. Noting that the adversary can always use this strategy, it follows that the code rate cannot be higher than the bound that is derived for this special strategy. The adversary's strategy is the following.

1. Adversary selects a reading set S_r and a writing set S_w before the LV code transmission.
2. After the codeword is transmitted, the adversary 1) reads the $\rho_r N$ components of the codeword on the set S_r; 2) chooses an error vector e with $\mathsf{SUPP}(e) \in S_w$, randomly and with uniform distribution, and adds it component-wise to the codeword.

Let M denote the random variable associated with the message space, C denote the random variable associated with the LV codeword sent by Alice, Y denote the random variable associated with the received word of Bob, and E denote the random variable associated with the error generated by the Adversary. We associate a random variable C_i to the i^{th} component of the code. Distribution of this variable can be obtained from the distribution of C. Let Y_{S_w} and $Y_{\overline{S_w}}$ denote the components of a codeword on the sets S_w and $\overline{S_w} = [N]/S_w$ of a word Y, respectively. The proof has three steps.

STEP 1. First, we give an upper bound on $\mathsf{H}(M|Y)$.

From the weak LV codes we have,

$$\mathsf{Pr}(M_{\mathcal{S}} \neq M_{\mathcal{R}}) \leq \delta.$$

From Fano's inequality (Theorem 2.10.1, Page 38, [16]), the decoding error probability δ implies,

$$\mathsf{H}(M|Y) \leq \mathsf{H}(M_{\mathcal{R}}|M_{\mathcal{S}}) \leq \mathsf{H}(\delta) + \delta \log |\mathcal{M}|. \tag{3.12}$$

Since $\log |\mathcal{M}| \leq N \log |\Sigma|$, we have

$$\mathsf{H}(M|Y) \leq \mathsf{H}(\delta) + \delta N \log |\Sigma|. \tag{3.13}$$

STEP 2. We give an upper bound on the rate $R(\mathcal{C}^N)$ of an LV code $\mathcal{C}^N$ of length N. We have,

$$\mathsf{H}(M) = \mathsf{H}(M|Y) + \mathsf{H}(Y) - \mathsf{H}(Y|M). \tag{3.14}$$

In the following, we will bound the three terms on the right side of Eq. (3.14).

The first term has been bounded by Eq. (3.13). The second term is bounded by,

$$\mathsf{H}(Y) \leq \log|\mathcal{Y}| \leq N \log|\Sigma|. \tag{3.15}$$

The last term is bounded as follow,

$$\begin{aligned} \mathsf{H}(Y|M) &= \mathsf{H}(Y_{S_w}, Y_{\overline{S_w}}|M) \\ &\geq \mathsf{H}(Y_{S_w}|M) \\ &\geq \mathsf{H}(Y_{S_w}|M, C) \\ &\overset{(1)}{=} \mathsf{H}(E) \\ &= \rho_w N \log|\Sigma|. \end{aligned} \tag{3.16}$$

Here (1) is because the adversary's error is selected uniformly and independent of the message and the codeword.

From Eq. (3.13) (3.15) (3.16), we have,

$$\mathsf{H}(M) \leq (1-\rho_w) N \log|\Sigma| + \mathsf{H}(\delta) + \delta N \log|\Sigma|. \tag{3.17}$$

The bound (3.17) holds for any distribution on $\mathcal{M}$. In particular for uniform message distribution, we have the bound $R(\mathcal{C}^N)$ on the code rate,

$$R(\mathcal{C}^N) = \frac{\mathsf{H}(M)}{N \log|\Sigma|} \leq 1 - \rho_w + 2\mathsf{H}(\delta). \tag{3.18}$$

STEP 3. Let C denote the highest achievable rate of an LV code family for a (ρ_r, ρ_w)-LVAC. We show the upper bound on C. Suppose there is an LV code family $\mathbb{C}$ for a (ρ_r, ρ_w)-LVAC with rate $R(\mathbb{C}) = 1 - \rho_w + \hat{\xi}$, for some small constant $0 < \hat{\xi} < \frac{1}{2}$.

Let $\mathsf{H}(p_0) = \frac{\hat{\xi}}{4}$. So for any $\hat{\xi}' \leq p_0$, we have $2\mathsf{H}(\hat{\xi}') \leq \frac{\hat{\xi}}{2}$ and $\hat{\xi}' \leq \mathsf{H}(\hat{\xi}') \leq \frac{\hat{\xi}}{4}$. From Definition 21, for any $0 < \hat{\xi}' \leq p_0$, there is an N_0 such that for any $N > N_0$, we have $\delta < \hat{\xi}'$ and,

$$\begin{aligned} R(\mathcal{C}^N) &\geq R(\mathbb{C}) - \hat{\xi}' \\ &= 1 - \rho_w + \hat{\xi} - \hat{\xi}' \\ &\overset{(1)}{=} 1 - \rho_w + 2\mathsf{H}(\delta) + \frac{\hat{\xi}}{2} - \hat{\xi}' \\ &\overset{(2)}{>} 1 - \rho_w + 2\mathsf{H}(\delta). \end{aligned}$$

Here (1) is from $\mathsf{H}(\delta) \leq \mathsf{H}(\hat{\xi}') < \frac{\hat{\xi}}{2}$; and (2) is from $\hat{\xi}' < \frac{\hat{\xi}}{2}$.

This contradicts the bound on $R(\mathcal{C}^N)$ in Eq. (3.18). So the upper bound on the rate of an LV code family over a (ρ_r, ρ_w)-LVAC is,

$$\mathbf{C} = \max_{\mathbb{C}} R(\mathbb{C}) \leq 1 - \rho_w.$$

□

3.7.3 Proof of Lemma 14

Proof. Firstly, the adversary cannot corrupt $\rho \geq \frac{1}{2}$ fraction of a codeword: If the adversary can read and write on half of the components of a codeword c, they can choose another codeword c' and add appropriate error vector to replace components of c on the controlled positions to obtain y which is equal to c' on the controlled components. The decoder can not decode y and fail because half of the components of y is the same as c and the other half the same as c'. It implies, $\rho \leq \frac{1}{2} - \frac{1}{2N}$.

Secondly, let R_{FRS} be the information rate of the FRS code. The decoding algorithm of LVAC adversary code need to satisfy the decoding condition of FRS code. According to Lemma 4, the FRS code with length N and information rate R_{FRS} can decode ρN adversary errors if satisfying the condition:

$$N - \rho N \geq N(\frac{1}{v+1} + \frac{v}{v+1}\frac{u_1 R_{\mathsf{FRS}}}{u_1 - v + 1}). \tag{3.19}$$

The equation is satisfied if,

$$N - \rho N \geq \frac{N}{v+1} + \frac{v}{v+1}\frac{(N(uR(\mathcal{C}^N)+1) + N(3N-2))}{u_1 - v + 1}.$$

It implies that the maximum error that the adversary can add is,

$$\rho \leq \frac{v}{v+1} - \frac{v}{v+1}\frac{uR(\mathcal{C}^N) + 3N - 1}{u_1 - v + 1}.$$

Since $u = u_1 + u_2 = u_1 + \lceil\sqrt{2u_1}\rceil N + 3N - 2$, it implies,

$$u_1 \geq N^2 + u - 3N + 1 - N\sqrt{N^2 + 2u - 2(3N-1)}.$$

So the decoding condition of FRS code is satisfied if the following inequality is met:

$$\rho \leq \frac{v}{v+1} - \frac{v}{v+1}\frac{uR(\mathcal{C}^N) + 3N - 1}{N^2 + u - 3N + 2 - N\sqrt{N^2 + 2u - 2(3N-1)} - v + 1}.$$

It implies,

$$\rho \leq \frac{v}{v+1} - \frac{v}{v+1}\frac{uR(\mathcal{C}^N) + 3N}{N^2 + u - N(\sqrt{N^2 + 2u} - 3) - v}.$$

□

3.7.4 Proof of Corollary 2

Proof. Item 1, follows directly from Theorem 14 by substituting $N = (2+c)t$.

For item 2, we need to choose parameters $R(\mathcal{C}^N), \rho, \xi$ of the LV code such that the corresponding 1-round RMT is optimal. The selection is as follows.

1. We choose $\rho_r = \rho_w = \rho = \frac{1}{2+c}$.
2. Rate $R(\mathcal{C}^N)$: we have the LV code rate $R(\mathcal{C}^N) = \frac{1}{2+c}$. The transmission rate τ of the corresponding RMT is $\tau = \frac{1}{R(\mathcal{C}^N)} = 2 + c = \mathcal{O}(\frac{N}{N-t})$ which is a constant and so the RMT protocol is optimal.
3. Parameter ξ: the code family is capacity achieving and parameter ξ determines that the code rate is at most ξ less than the capacity.

The parameter must be chosen with two considerations: the FRS code with the subspace evasive set used for the encoding of the message (appended with MAC), and the AWTP code used for transfering the MAC key.

(a) FRS with subspace evasive set message coding: From Section 4.5, for the LV code we have $\Sigma_{\mathsf{FRS}} = \mathbb{F}_q^{\frac{1}{\xi^4}}$ and $\Sigma = \mathbb{F}_q^{\frac{1}{\xi^4}+\frac{1}{\xi^2}}$. Let $\rho = \frac{1}{2+c}$ and $R(\mathcal{C}^N) = \frac{1}{2+c}$. From,

$$\log|\mathcal{M}| = R_{\mathsf{FRS}}(\mathcal{C}^N) N \log|\Sigma_{\mathsf{FRS}}| = R(\mathcal{C}^N) N \log|\Sigma|,$$

we have,

$$R(\mathcal{C}^N) \leq R_{\mathsf{FRS}}(\mathcal{C}^N).$$

Since $R_{\mathsf{FRS}}(\mathcal{C}^N) = 1 - \rho - \xi$, it implies that,

$$R(\mathcal{C}^N) \leq R_{\mathsf{FRS}}(\mathcal{C}^N) = 1 - \rho - \xi,$$

and so ξ must satisfy,

$$\xi \leq 1 - \rho - R(\mathcal{C}^N) = 1 - \frac{1}{2+c} - \frac{1}{2+c} = \frac{c}{2+c}. \tag{3.20}$$

(b) AWTP code: We have $R_{\mathsf{AWTP}}(\mathcal{C}^N) = 1 - \rho - \rho - \xi$ and $\rho = \frac{1}{2+c}$, and so,

$$R_{\mathsf{AWTP}}(\mathcal{C}^N) = 1 - 2\rho - \xi.$$

Let

$$\xi \leq \frac{c}{2(2+c)}. \tag{3.21}$$

From Section 4.5 the alphabet of AWTP is $\Sigma_{\mathsf{AWTP}} = \mathbb{F}_q^{\frac{1}{\xi^2}}$ and so the rate of the AWTP code is,

$$R_{\mathsf{AWTP}}(\mathcal{C}^N) = 1 - 2\rho - \xi = \frac{c}{2+c} - \xi = \frac{c}{2(2+c)}. \tag{3.22}$$

The required randomness vector $\mathbf{r}$ h for the LV code has length N. Since,

$$\frac{\log|\mathbf{r}|}{N \log|\Sigma_{\mathsf{AWTP}}|} = \frac{N}{N \log|\Sigma_{\mathsf{AWTP}}|} = (\frac{c}{2(2+c)})^2$$

is less than the information rate of the AWTP code with the chosen parameters, if we choose $\xi = \frac{c}{2(2+c)}$, then $\mathbf{r}$ can be sent securely and reliably using the AWTP code.

To satisfy both above conditions, Eq. (3.20) and AWTP code Eq. (3.21), we will choose,

$$\xi \leq \frac{c}{2(2+c)}.$$

From the LV code parameter $R(\mathcal{C}^N), \rho, \xi$ above, we can determine the parameters of the δ-RMT scheme obtained from the LV code:

1. Transmission rate: $\tau = \mathcal{O}(\frac{N}{N-t})$ and so the RMT is optimal.
2. Computational time: Since $\xi = \frac{c}{2(2+c)}$ is constant, the list size of the FRS code with subspace evasive set encoding is constant and so the decoding algorithms of the AWTP code and the FRS code with subspace evasive set encoding, are polynomial in N and so the decoding algorithm of the RMT is polynomial time.
3. Decoding error: the LV code decoding error is $\delta \leq \frac{2(1/\xi^2)^{(2+\frac{D}{\xi^2}\log\log\frac{1}{\xi^2})}}{q^N}$ and ξ is constant. This means that the decoding error of RMT is bounded by $\delta \leq \mathcal{O}(\frac{1}{q^N})$.

□

Chapter 4

Adversarial Wiretap Channel

4.1 Introduction

Wyner [89] made the seminal observation that noise in the channel can be used as a resource for cryptographers, and proposed wiretap channel model to provide (asymptotic) perfect secrecy and reliability against a computationally unbounded adversary without requiring a shared key. In Wyner's original model and its generalization to *broadcast channel* [18], the sender is connected to, the receiver over a noisy channel referred to as the *main channel*, and to the eavesdropper over a second noisy channel referred to as the *wiretap channel*.

The goal is to provide (asymptotic) perfect secrecy and reliability for message transmission from Alice to Bob. Wyner and Ozarow [66] introduced *wiretap II model* in which the main channels is noiseless and the wiretap channel is an erasure channel where the erasures are controlled by the adversary: the adversary can select the subset of codeword components that they would like to see. The goal is to provide perfect secrecy for the communicants (the channel is reliable). *Secrecy capacity* of a wiretap channel is the highest possible rate of communication with perfect secrecy and reliability. Wyner derived secrecy capacity of a *degraded* wiretap channel where the wiretapper channel is a concatenation of the main channel and a second noisy channel, and showed the existence of codes that achieve secrecy capacity. Similar results have been proved for wiretap II, and broadcast channel in [66] and [18], respectively.

Wiretap model naturally captures physical layer wireless communication where the sender's transmission can be intercepted (eavesdropped) by a third party who is within the reception distance of the transmitter. There is a large body of research [9, 15, 20, 55, 56, 66, 61, 63,

62, 64, 49, 59, 20] on variations of the basic wiretap model including extending the goal of communication to key agreement. There have also been numerous implementations based on this model [6, 9].

Considering active adversaries in wiretap model is well motivated by real life application scenarios. In wireless communication it is relatively easy to inject signals in the channel resulting in the transmitted symbols to be erased, or selectively modified [69]. Recent proposals [64, 12, 2] for physical layer active adversaries in wiretap setting consider an adversary that is modelled using general arbitrarily varying channels and fall short of one or more of the following, (i) considering adaptive adversaries that use their current knowledge to perform their next actions, (ii) using strong security definition, (iii) deriving an expression, or a tight upper-bound, for secrecy capacity, and (iv) providing an efficient explicit construction.

In this dissertation we propose a model for a wiretap channel with active adversary, that we call *Adversarial Wiretap Channel (AWTP Channel).* The model has a coding theory approach and well captures active adversaries for a large class of real-life channel corruptions. We achieve all the properties (i) to (iv) for this model.

Our Results

1). AWTP Channels and AWTP Codes. An AWTP channel is specified by a pair of parameters (ρ_r, ρ_w): for a codeword of length N, the adversary can choose a subset S_r of size up to $\rho_r N$ components to read, and a subset S_w of size up to $\rho_w N$ components to write to, and *writing is by adding an error vector with non-zero components in S_w, to the codeword.* The goal is to provide secrecy and reliability for communication in presence of the above adversary. Secrecy is defined as the indistinguishability of the adversary's view of communication for any two messages, and is measured by the statistical distance between the two views. Reliability is given by the receiver's probability of correctly decoding a sent message that has been chosen by the adversary (See Definition 26).

An AWTP code provides security and reliability for message transmission over (ρ_r, ρ_w)-

AWTP channels. An *AWTP code is specified by a tuple* $(\mathcal{M}, N, \Sigma, \epsilon, \delta)$, denoting the message space, code length, alphabet set, and upper bounds on secrecy loss and error probability, respectively. Σ is an additive group and corruption of a codeword is by adding (component wise) an error vector to it. A code has a pair of algorithms $(\mathsf{AWTPenc}(\cdot), \mathsf{AWTPdec}(\cdot))$ for encoding and decoding, respectively. Encoding is probabilistic and decoding is deterministic. The adversary is allowed to choose the message distribution and the best tampering error using their view of the communication. When other parameters are clear from the context, we refer to the code as an (ϵ, δ)-AWTP code. In an (ϵ, δ)-AWTP code the information leaked about the message and the probability of decoding error, are upper bounded by ϵ and δ, respectively.

The *rate of an AWTP code* $\mathcal{C}^N$ of length N is denoted by $R(\mathcal{C}^N)$, and is defined as $R(\mathcal{C}^N) = \frac{\log_2 |\mathcal{M}|}{N \log_2 |\Sigma|} = \frac{1}{N} \log_{|\Sigma|} |\mathcal{M}|$. An *$\epsilon$-AWTP code family* $\mathbb{C}^\epsilon$ is a family $\{\mathcal{C}^N\}_{N \in \mathbb{N}}$ of (ϵ, δ_N)-AWTP codes, indexed by the code length N. A *rate $R(\mathbb{C}^\epsilon)$ is achievable* by an ϵ-AWTP code family $\mathbb{C}^\epsilon$, if for any sufficiently small $\xi > 0$ there exists an N_0 such that for all $N \geq N_0$ we have $\frac{1}{N} \log_{|\Sigma|} |\mathcal{M}| \geq R(\mathbb{C}^\epsilon) - \xi$, and the decoding error probability satisfies $\delta_N \leq \xi$. The ϵ-secrecy capacity of an AWTP channel, denoted by C^ϵ (C^0 for perfect secrecy), is the highest achievable rate of all ϵ-AWTP code families for the channel.

2). Rate Upper Bound of AWTP channels. For any (ϵ, δ)-AWTP code over a (ρ_r, ρ_w)-AWTP channel, and any message distribution, we prove an upper bound on $\mathsf{H}(M)$ (See Eq. 4.18) and use it to obtain an upper bound on the rate of (ϵ, δ)-AWTP codes. Using this bound for a code family results in the following upper bound on the secrecy capacity of a (ρ_r, ρ_w)-AWTP channel,

$$\mathsf{C}^\epsilon \leq 1 - \rho_r - \rho_w + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon}). \tag{4.1}$$

For $\epsilon = 0$, we have $\mathsf{C}^0 \leq 1 - \rho_r - \rho_w$.

This last bound can be explained by noting that the components of a codeword that are either read or written to, cannot contribute to secure and reliable transmission of information.

Since the capacity result must hold for *all* adversaries, that is all choices of S_r and S_w (subject to the restrictions on the sizes of the sets), for an adversary that uses $S_r \cap S_w = \emptyset$, the rate will be bounded by $1 - \rho_r - \rho_w$. The bound implies that perfect secrecy for (ρ_r, ρ_w)-AWTP channels is possible if $\rho_r + \rho_w < 1$. When the adversary is almost oblivious (ρ_r is small), the rate can be positive even when the adversary writes over a large fraction $< 1 - \rho_r$ of the codeword, and on the other extreme when ρ_r is close to 1, fewer than $< 1 - \rho_r$ corrupted components could be tolerated.

This bound is achieved by the construction in Section 4.5 (Theorem 12), and so we obtain the perfect secrecy capacity of a (ρ_r, ρ_w)-AWTP channel,

$$\mathsf{C}^0 = 1 - \rho_r - \rho_w. \tag{4.2}$$

3). A Capacity Achieving AWTP Code Family. We construct a capacity achieving $(0, \delta)$-AWTP code family $\mathbb{C} = \{\mathcal{C}^N : N \in \mathbb{N}\}$, for a (ρ_r, ρ_w)-AWTP channel. For any sufficiently small $\xi > 0$, the code $\mathcal{C}^N$ has $R(\mathcal{C}^N) = 1 - \rho_r - \rho_w - \xi$ and uses an alphabet of size $|\Sigma| = \mathcal{O}(q^{1/\xi^2})$. Decoding algorithm is efficient and decoding error probability satisfies $\delta \leq \mathcal{O}(q^{-N})$. The decoding algorithm satisfies *strong reliability* condition which means that the decoder always outputs a correct message, or outputs $\perp$. The construction gives a code family that achieves the capacity C^0.

The construction uses three building blocks: an *Algebraic Manipulation Detection Code* (AMD code), a *Subspace Evasive Set*, and a *Folded Reed-Solomon code (FRS code)*, all defined in Section 4.2. The intuition behind the construction is as follows.

To correct adversarial errors we use a list decodable code (FRS code) that can correct up to $\rho_w N$ errors in the codeword. The message of the FRS code however, is prepared with a number of considerations. Firstly, we note that the decoder outputs a list of codewords that includes the sent codeword. To identify the sent codeword in the list, we embed the message in a codeword of an AMD code. This allows Bob to identity the sent message (codeword) in the list, by applying the decoding algorithm of the AMD code on the message

part of the codewords in the list. In constructing LV codes we used AWTP codes to send the secret key of a MAC over the adversarial channel. To construct AWTP code we will use a cryptographic primitive that does not require key, and yet allows detection of algebraic manipulations. Secondly, to have an efficient decoding algorithm, the decoded list size must be constant. This will be obtained by mapping the AMD codeword, to an element of subspace evasive set. Finally, to guarantee perfect secrecy, the view of the adversary (given by the $\rho_r N$ read components of the codeword) must be independent of the sent message. This is achieved by appending sufficient number ($\rho_r N$) of random elements to the element in subspace evasive set. The FRS code encodes the resulting vector into AWTP codeword. By carefully choosing the parameters of the above building blocks, the rate of the resulting code family will achieve the rate upper bound of (ρ_r, ρ_w)-AWTP channels, and so the code family is capacity achieving. Details of the encoding and decoding algorithms are given in Section 4.5.

4). Relations with SMT. AWTP model of secure and reliable communication is closely related to 1-round SMT [28], a model proposed for secure and reliable communication in networks. In the SMT setting Alice is connected to Bob through a set of N node disjoint paths (*wires*) in a network, a subset of which is controlled by the adversary. The most widely studied adversary model for SMT is a *threshold adversary* that fully controls a subset of size t of the N wires. The goal of an SMT protocol is to provide secrecy and reliability for communication: an (ϵ, δ)-SMT protocol ensures that the secrecy loss (statistical distance of the adversary's view for any two messages) is bounded by ϵ, and the probability of error in decoding is bounded by δ [33]. We note that in an AWTP channel the error is *added to the codeword*, while an SMT adversary can replace their chosen codeword components by any value of its choice. In Section 4.6, we show a direct relationship between the two primitives and use it to obtain a new bound on the efficiency parameter of SMT protocols.

Related Work

Adversarial wiretap definitions. Wiretap model and its extensions have attracted considerable attentions in recent years. There is a large body of excellent works on extensions of wiretap model [18, 66, 61, 63, 49, 15], construction of capacity achieving codes [42, 6], and implementation of codes in practice [11, 9]. We only consider the works that are directly related to active adversaries considered here. Active adversaries in wiretap channels was first considered in Wyner wiretap II [66] model in which the adversary selects its view of the communication channel. The adversary however does not modify the transmission over the main channel which is assumed to be noise-free. Physical layer active adversaries for wiretap channels that tamper with the transmission, have been considered more recently [64, 12, 2]. These works model active adversaries as an arbitrarily varying channel. An *arbitrarily varying channel (AVC)* [21, 4, 19, 44] is specified by two finite sets $\mathcal{X}$ and $\mathcal{Y}$ of input and output alphabets, a finite set $\mathcal{A}$ of *channel states*, and a set of channels specified by transition probabilities $\mathsf{Pr}(y|x,a), x \in \mathcal{X}, y \in \mathcal{Y}, a \in \mathcal{A}$. The channel state in general varies with each channel use (possibly with memory) and,

$$\mathsf{Pr}(y^n|x^n,a^n) = \Pi_{i=1}^{n}\mathsf{Pr}(y_i|x_i,a_i),$$

where $a^n = (a_1 \cdots a_n)$, $a^n \in \mathcal{A}^n$, is the sequence of channel states. An *arbitrarily varying wiretap channel (AVWC)* is specified by an input alphabet set $\mathcal{X}$, two sets of output alphabets, $\mathcal{Y}$ and $\mathcal{Z}$, representing the *legitimate receiver's* and *the wiretapper's* received values, respectively, and a family of channels, each given by a transition probability $\mathsf{Pr}(y,z|x,a), x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}, a \in \mathcal{A})$ indexed by the channel state a. In [64], the *jammer* chooses the state a_i (jamming signal) independent of the eavesdroppers' observation z. Transmitter and receiver know the state space, but not the state chosen by the adversary. The message is chosen randomly, with uniform distribution. *Encoding and decoding is randomized*; that is the system uses a family of encoder and decoder pairs, that is known to the eavesdropper and the jammer. The pair used by the sender and receiver is specified

by a random value (also called key) that is known to the eavesdropper but *not the jammer*. Security is measured by the *rate of the mutual information between the message and the adversary's observation*, and reliability for a pair of encoder and decoder is in terms of the expected error probability over all messages. For randomized codes security and reliability are averaged over all realizations of the code.
In summary, the model, (i) assumes common randomness between the sender and the receiver that is unknown to the jammer but is known to the eavesdropper, (ii) uses weak definition of secrecy and average error probability, and (iii) the jammer's corruption does not depend on the eavesdropper view.

Our adversarial channel model can be seen as a special arbitrarily varying channel where the adversary's eavesdropping and tampering subsets are bounded, and the type of tampering is additive. For this special class however we remove the above restrictions: (i) we do not assume shared randomness between the sender and the receiver, (ii) we use a strong definition of secrecy in terms of the statistical distance between the adversary's views of any two messages, and for reliability allow the adversary to choose the message distribution that causes the worst case error; and (iii) consider an adaptive adversary that uses all the information at each point to choose the next component to be read or written to.

Arbitrarily varying channels are also used in [12], where secrecy measured by the mutual information of a *random message* (uniform distribution on messages) and the adversary's view. Our security definition using statistical distance is equivalent to *the mutual information security when the message distribution is adversarially chosen* [6]. In [2] wiretap II model is extended to include an active adversary, and two possible types of corruptions have been considered. In the first, the adversary erases symbols that are observed, and in the second, corrupts them. In our notations, the adversary in both cases [2] has $S_r = S_w$. The adversary in our model however does not have this limitation on the choice of S_r and S_w.

Security Definitions. Wyner [89] quantified security of wiretap channels by the adver-

sary's equivocation, defined as the average (per message symbol) uncertainty about the message, given the adversary's view of the sent codeword. This definition is strengthened in [62, 15, 42, 6]. In [6], the relationship among security notions used in wiretap channels is studied, and it is shown that defining security as the statistical distance between adversary's views of two messages, is equivalent to a security notion that is called *mutual information security* and maximizes the mutual information between the message and adversary's view, over all message distributions. It follows that this latter is stronger than the strong security notion in [62], as the adversary can choose the message distribution.

Adversarial Channels. Adversarial channels have been widely studied in the literature [19, 40, 52]. A good survey can be found in [54]. An adversarial channel that is closely related to this work is *limited view (LV) adversary channel*. An LV adversary is identical to the adversary in AWTP channel, however the goal of the communication in the former is reliability only, while transmission over AWTP channels requires secrecy and reliability both.

Computationally unlimited active adversaries at the network layer of communication, have been considered in [61, 63, 71, 45, 26]. Such adversaries can view, or tamper with, the whole message, and providing protection against them requires access to extra resources such as shared randomness [36, 77], close secrets [45], or extra channels [65]. The adversary in AWTP setting is at the physical layer of communication, and without having access to any other resource, the only advantage of communicants over the adversary is the limited access of the adversary to the channel.

4.2 Preliminaries

4.2.1 Algebraic Manipulation Detection Code (AMD code)

Consider a storage device $\Sigma(\mathcal{G})$ that holds an element x from a group $\mathcal{G}$. The storage $\Sigma(\mathcal{G})$ is private but can be manipulated by the adversary by adding $\Delta \in \mathcal{G}$. AMD codes allow the manipulation to be detected.

Definition 24 (AMD Code[17])**.** *An $(\mathcal{X}, \mathcal{G}, \delta)$-Algebraic Manipulation Detection code ($(\mathcal{X}, \mathcal{G}, \delta)$-AMD code) has two algorithms* (AMDenc *and* AMDdec)*. Encoding,* $\mathsf{AMDenc} : \mathcal{X} \to \mathcal{G}$*, is probabilistic and maps an element of a set $\mathcal{X}$ to an element of an additive group $\mathcal{G}$. Decoding,* $\mathsf{AMDdec} : \mathcal{G} \to \mathcal{X} \cup \{\perp\}$*, is deterministic and for any $x \in \mathcal{X}$, we have* $\mathsf{AMDdec}(\mathsf{AMDenc}(x)) = x$*. Security of AMD codes is defined by requiring,*

$$\mathsf{Pr}[\mathsf{AMDdec}(\mathsf{AMDenc}(x) + \Delta) \notin \{x, \perp\}] \leq \delta, \tag{4.3}$$

for all $x \in \mathcal{X}, \Delta \in \mathcal{G}$.

An AMD code is *systematic* if the encoding has the form $\mathsf{AMDenc} : \mathcal{X} \to \mathcal{X} \times \mathcal{G}_1 \times \mathcal{G}_2$, mapping x to $(x, r, t = f(x, r))$, for some function f, and $r \leftarrow \mathcal{G}_1$. The decoding function results in $\mathsf{AMDdec}(x, r, t) = x$, if and only if $t = f(x, r)$, and $\perp$ otherwise.

We use the systematic AMD code in [17] over an extension field. Let ϕ be a bijection between vectors $\mathbf{v}$ of length N over $\mathbb{F}_q$, and elements of $\mathbb{F}_{q^N}$, and let d be an integer such that $d + 2$ is not divisible by q. Define the function $\mathsf{AMDenc} : \mathbb{F}_{q^N}^d \to \mathbb{F}_{q^N}^d \times \mathbb{F}_{q^N} \times \mathbb{F}_{q^N}$ as, $\mathsf{AMDenc}(x) = (x, r, f(x, r))$ where,

$$f(x, r) = \phi^{-1}\left(\phi(r)^{d+2} + \sum_{i=1}^{d} \phi(x_i)\phi(r)^i\right) \mod q^N.$$

Lemma 16. *For the AMD code above, the success chance of an adversary in tampering with a stored codeword (x, r, t), and constructing a new codeword $(x', r', t') = (x' = x + \Delta x, r' = r + \Delta r, t' = t + \Delta t)$ that satisfies $t' = f(x', r')$, is no more than $\frac{d+1}{q^N}$.*

The Lemma follows from Theorem 2 in [17], when the underlying field is $\mathbb{F}_{q^N}$.

4.3 Model and Definitions

We consider the following scenario. Alice wants to a send messages $m \in \mathcal{M}$, securely and reliably to Bob, over a communication channel that is partially controlled by an adversary, Eve.

Let Σ denote the channel alphabet, and $\mathcal{C}$ be a code, $\mathcal{C} \subset \Sigma^N$. We assume Σ is an additive group with "+" and "−" denoting group addition and its inverse operation, respectively. For a vector $x \in \Sigma^N$, we use $\mathsf{SUPP}(x) \subset [N]$ to denote the set of indexes i, where x_i is non-zero.

Alice will use the encoding algorithm to generate a codeword c for a message m. The adversary interacts with the codeword as described below, as a result of which Bob will receive a word $y \neq c$. Bob uses the decoding algorithm to recover the message.

4.3.1 Adversarial Wiretap: Channel and Code

Let $[N] = \{1, \cdots, N\}$, and let $S_r = \{i_1, \cdots, i_{\rho_r N}\} \subseteq [N]$ and $S_w = \{j_1, \cdots, j_{\rho_w N}\} \subseteq [N]$ be two subsets of $[N]$.

Definition 25. *A* (ρ_r, ρ_w)-Adversarial Wiretap channel (or a (ρ_r, ρ_w)-AWTP channel)*, is an adversarially corrupted communication channel between Alice and Bob, such that it is (partially) controlled by an adversary Eve with two types of abilities: Read and Write. For a codeword of length* N*, Eve can do the following.*

- **Read** *(*Eavesdrop*): Eve selects a subset* $S_r \subseteq [N]$ *of size at most* $\rho_r N$ *and reads the components of the sent codeword* c *with index in* S_r*. Eve's view of the communication (codeword) is given by,* $\mathsf{View}_{\mathcal{A}}(c) = \{c_{i_1}, \cdots, c_{i_{\rho_r N}}\}$.
- **Write** *(*Jam, Modify*): Eve chooses a subset* $S_w \subseteq [N]$ *of size at most* $\rho_w N$ *to "write to", and adds an error vector* e *with* $\mathsf{SUPP}(\mathsf{e}) \subseteq S_w$*, to* c*. Here addition is over* Σ *and*

component-wise. The corrupted components of c are $\{y_{j_1}, \cdots, y_{j_{\rho_w N}}\}$ and $y_{j_\ell} = c_{j_\ell} + e_{j_\ell}$. The error e can be generated according to the Eve's best strategy for making Bob's decoder to output in error.

We assume the adversary is *adaptive* and can select components of the sent codeword for reading and writing one by one, at each step using its information about the codeword at that time.

Let $S = S_r \cup S_w$ denote the set of codeword components that the adversary either reads, or writes to. Let $|S| = \rho N$. We have $\rho \leq \rho_r + \rho_w$.

An AWTP channel is called *restricted* if, $S_r = S_w = \rho N$, where $\rho = \rho_r = \rho_w$ is a constant. A restricted ρ-AWTP channel is a special type of AWTP channel where the adversary is limited to select $S_r = S_w$.

Definition 26. *An* $(\mathcal{M}, N, \Sigma, \epsilon, \delta)$ Adversarial Wiretap Code *(or (ϵ, δ)-AWTP code for short) for a (ρ_r, ρ_w)-AWTP channel, consists of a pair of algorithms: a randomized encoding algorithm* $\mathsf{AWTPenc} : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$ *from the message space $\mathcal{M}$ to a code $\mathcal{C} \subset \Sigma^N$, and a deterministic decoding algorithm* $\mathsf{AWTPdec} : \Sigma^N \to \mathcal{M}$ *from the set of N-tuples over Σ to the message space. The code guarantees the following two properties:*

- **Secrecy:** *For a pair of messages $m_1, m_2 \in \mathcal{M}$, the statistical distance between the adversary's views, for any choice of the randomness $r_{\mathcal{A}}$ by the adversary, is bounded by ϵ. That is,*

$$\mathsf{Adv}^{\mathsf{ds}}(\mathsf{AWTPenc}, \mathsf{View}_{\mathcal{A}}) \stackrel{\triangle}{=} \max_{m_0, m_1} \mathbf{SD}(\mathsf{View}_{\mathcal{A}}(\mathsf{AWTPenc}(m_1), r_{\mathcal{A}}), \mathsf{View}_{\mathcal{A}}(\mathsf{AWTPenc}(m_2), r_{\mathcal{A}})) \leq \epsilon.$$

- **Reliability:** *For* any *message m that is encoded to c by the encoder and corrupted to $y = c + e$ by the (ρ_r, ρ_w)-AWTP channel, the probability that the receiver outputs the correct message m is at least $1 - \delta$. That is,*

$$\mathsf{Pr}(M_{\mathcal{S}} \neq M_{\mathcal{R}}) \leq \delta,$$

where the probability is over the randomness of the communicants and the adversary. Without loss of generality, we assume $\delta < 1/2$.

In above definition, decoder always outputs a message, and with a probability at least $1-\delta$ the output message is the correct one. A decoder provides *strong reliability* if it only output correct messages, or $\perp$.

The AWTP code is *perfectly secure* if $\epsilon = 0$.

For $1 \geq \epsilon > 0$, an *ϵ-secure AWTP code family* $\mathbb{C}^\epsilon$, is a family $\{\mathcal{C}^N\}_{N\in\mathbb{N}}$ of codes indexed by $N \in \mathbb{N}$, where $\mathcal{C}^N$ is an $(\mathcal{M}, N, \Sigma, \epsilon, \delta)$-AWTP code for a (ρ_r, ρ_w)-AWTP channel. When $\epsilon = 0$, the family is called a *perfectly secure AWTP code family.*

The rate of a code $R(\mathcal{C})$, achievable rate of a code family $\mathbb{C}^\epsilon$, and ϵ-secrecy capacity of a (ρ_r, ρ_w)-AWTP channel, have been defined in Section 4.1.

4.4 Bound on the Rate of (ϵ, δ)-AWTP Codes

We derive an upper bound on the rate of AWTP codes, and use it to find the secrecy capacity of AWTP channels.

The bound is derived by considering an adversary that uses a special strategy given below, and requiring that the AWTP code provide security against the adversary. Since the strategy can be used against any AWTP code over the (ρ_r, ρ_w)-AWTP channel, it follows that the bound holds for all AWTP codes over the channel.

The adversary strategy is probabilistic strategy and is described below.

1. Eve chooses uniform distribution on the message space.

2. Eve selects two pairs of read and write subsets, $\{S_r^i, S_w^i\}, i = 1, 2$, satisfying $S_r^1 \cap S_w^2 = \emptyset$ and $S_r^2 \cap S_w^1 = \emptyset$. The set sizes satisfy, $|S_r^i| \leq \rho_r N$, $|S_w^i| \leq \rho_w N$, and $|S_r^i \cup S_w^i| \leq \rho N$, $i = 1, 2$, and $0 \leq \rho \leq 1$. This can be done by selecting S_r^1 and S_w^1 such that $|S_r^1 \cup S_w^1| \leq \rho N$, and selecting S_w^2 such that $S_r^1 \cap S_w^2 = \emptyset$, and finally selecting S_r^2 such

that $S_r^2 \cap S_w^1 = \emptyset$ and $|S_r^2 \cup S_w^2| \leq \rho N$. The adversary then uses a uniform distribution (over S_w^i) $\mathsf{Pr}(S_r^1, S_w^1) = \mathsf{Pr}(S_r^2, S_w^2) = \frac{1}{2}$, to selects one of the two pairs.

3. Eve uses the chosen read and write pair $\{S_r^i, S_w^i\}$, (i) to read the $\rho_r N$ components of the codeword corresponding to the subset S_r^i, (ii) chooses an error vector $e \in \Sigma^{\rho_w N}$ with $\mathsf{SUPP}(e) \in S_w^i$, randomly with uniform distribution, and adds it component-wise to the codeword.

Note that in the above adversary's strategy, selection of $\{S_r^i, S_w^i\}, i = 1, 2$ and e are independent of the codeword c.

Let C_i denote the random variable associated with the i^{th} component of a codeword in the (ϵ, δ)-AWTP code, and let $C_{S_r^i}$ and $C_{S_w^i}$ denote the components of a codeword on the sets S_r^i, S_w^i, $i = 1, 2$, respectively. Let A be the random variable corresponding to the index of the reading and writing set pair that the adversary chooses. We have $A = 1$ for $\{S_r^1, S_w^1\}$, and $A = 2$ for $\{S_r^2, S_w^2\}$. We use $\overline{A}$ to denote a variable whose values are $\overline{A} = 2$ if $A = 1$, and $\overline{A} = 1$ if $A = 2$. Let V be random variable (vector variable) defined as $V = C_{S_r^{\overline{A}}}$, and Y denote the word that Bob receives.

In the following we prove the following theorem.

Theorem 11. *The secrecy capacity of an ϵ-AWTP code family over (ρ_r, ρ_w)-AWTP channel is upper bounded by,*

$$\mathsf{C}^{\epsilon} \leq 1 - \rho_r - \rho_w + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon}).$$

The proof has the following steps. We first prove two Lemmas 17 and Lemma 18, that rely on the secrecy and reliability guarantees of the code. The Lemmas are used to derive an upper-bound on the rate of an (ϵ, δ)-AWTP code (Lemma 19), followed by an upper-bound on the achievable rate of a code family, and finally on the secrecy capacity of the channel.

Lemma 17. *An (ϵ, δ)-AWTP code for a (ρ_r, ρ_w)-AWTP channel satisfies,*

$$\mathsf{I}(M; V) \leq 2\epsilon\rho_r N \log \frac{|\Sigma|}{\epsilon}.$$

Proof is in Section 4.7.1.

Lemma 18. *An (ϵ, δ)-AWTP code for a (ρ_r, ρ_w)-AWTP channel, satisfies,*

$$\mathsf{H}(M|Y, A) \leq \mathsf{H}(\delta) + \delta N \log |\Sigma|.$$

Proof. From Fano's inequality (Theorem 2.10.1, Page 38, [16]) on decoding error probability δ, we have,

$$\mathsf{H}(M|Y) \leq \mathsf{H}(\delta) + \delta N \log |\Sigma|.$$

So we have,

$$\mathsf{H}(M|Y, A) \leq \mathsf{H}(M|Y) \leq \mathsf{H}(\delta) + \delta N \log |\Sigma|.$$

□

Lemma 19. *The upper bound on the rate of an (ϵ, δ) AWTP code $\mathcal{C}^N$ for a (ρ_r, ρ_w) AWTP channel is,*

$$R(\mathcal{C}^N) \leq 1 - \rho_r - \rho_w + 2\mathsf{H}(\delta) + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon}).$$

Proof is in Section 4.7.2.

The following is the proof of Theorem 11.

Proof. (Theorem 11) Proof is by contradiction. Suppose there is an ϵ-AWTP code family $\mathbb{C}^\epsilon$ with achievable rate $R(\mathbb{C}^\epsilon) = 1 - \rho_r - \rho_w + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon}) + \hat{\xi}$, for some small constant $0 < \hat{\xi} < \frac{1}{2}$.

For any $0 < \hat{\xi}'$ with $\mathsf{H}(\hat{\xi}') \leq \frac{\hat{\xi}}{4}$, there is an N_0 such that for any $N > N_0$, we have $\delta_N < \hat{\xi}'$ and,

$$\begin{aligned}
&R(\mathcal{C}^N) \geq R(\mathbb{C}^\epsilon) - \hat{\xi}' \\
&= 1 - \rho_r - \rho_w + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon}) + \hat{\xi} - \hat{\xi}' \\
&\overset{(1)}{\geq} 1 - \rho_r - \rho_w + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon}) + 2\mathsf{H}(\delta) + \frac{\hat{\xi}}{2} - \hat{\xi}' \\
&\overset{(2)}{>} 1 - \rho_r - \rho_w + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon}) + 2\mathsf{H}(\delta),
\end{aligned}$$

where (1) is from $2\mathsf{H}(\delta) \leq 2\mathsf{H}(\hat{\xi}') < \frac{\hat{\xi}}{2}$, and (2) is from $\hat{\xi}' < \mathsf{H}(\hat{\xi}') < \frac{\hat{\xi}}{2}$.

This contradicts the bound on $R(\mathcal{C}^N)$ in Lemma 19, and so

$$R(\mathbb{C}^\epsilon) \leq 1 - \rho_r - \rho_w + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon}).$$

□

For $\epsilon = 0$, we have the upper bound on the achievable rate of a perfectly secure AWTP code family.

Corollary 3. *The upper bound on the achievable rate of a perfectly secure AWTP code family for a (ρ_r, ρ_w)-AWTP channel is*

$$\mathsf{C}^0 \leq 1 - \rho_r - \rho_w.$$

4.4.1 Restricted AWTP channels

The above proof is general in the sense that the sets S_r and S_w can have nonempty intersection. Restricted AWTP channels limit the adversary to choose $S_r = S_w$ and $|S_r| = |S_w| = \rho N$. Using the above approach with the added restriction that the adversary chooses $S_r^i = S_w^i, i = 1, 2$, we can derive the following bounds on C^0 and C^ϵ. Note that the proof requires $\rho \leq 1/2$ as the two subset pairs must satisfy $S_r^1 \cap S_w^2$.

Corollary 4. *The perfect secrecy capacity of a* restricted ρ-AWTP channel *is bounded by,*

$$\mathsf{C}^0 \leq 1 - 2\rho.$$

The ϵ-secrecy capacity of a restricted ρ-AWTP channel is bounded by,

$$\mathsf{C}^\epsilon \leq 1 - 2\rho + 2\epsilon\rho(1 + \log_{|\Sigma|} \frac{1}{\epsilon}).$$

We note that a more direct proof of Theorem 11 can be obtained by using an adversary with a deterministic strategy in which $S_r \cap S_w = \emptyset$, and following the same proof strategy as used for Theorem 11. However such proof cannot be used for restricted AWTP channels

because this adversarial strategy is not applicable to restricted channels. The above proof with randomized adversarial strategy removes this restriction and allows us to apply the same proof method for restricted AWTP channels.

4.5 AWTP Code Construction

The intuition behind the construction was outlined in Section 4.1. The construction uses, (i) an AMD code, (ii) an FRS code, and (iii) a subspace evasive set. We show how to choose the parameters of these building blocks such that for any arbitrarily small $\xi > 0$, we have a code $\mathcal{C}^N$ with $R(\mathcal{C}^N) = 1 - \rho_r - \rho_w - \xi$. Let $\xi_1 = \xi/13$. Parameters of the code building blocks are given in terms of ξ_1.

1. We first choose the parameters of the FRS code. We have two considerations: the code must correct $\rho_w N$ errors, and the message of the FRS code must be an element of the subspace evasive set construction in Section 3.2.2. We set, (i) folding parameter $u = \xi_1^{-2}$, (ii) decoding parameter $v = \xi_1^{-1}$, (iii) the length $N \geq (1/\xi_1)^{D/\xi_1 \log\log 1/\xi_1}$, and (iv) the field size satisfying $q > uN$. Here D is a constant given in Claim 4.3 in [29].

   We will use linear algebraic decoding of [38] with decoding parameter v. This results in the decoder output list to be expressible as a subset of $\mathbb{F}_q$ generated as in Lemma 4.

2. For simplicity assume $uR(\mathcal{C}^N)$ is an integer. (The argument can be straightforwardly be extended to the case that this does not hold.) The AMD code will be the code in Section 4.2.1, and will have message space $\mathcal{X} = \mathbb{F}_q^{uR(\mathcal{C}^N)N}$, codeword space $\mathcal{G} = \mathbb{F}_q^{uR(\mathcal{C}^N)N+2N}$, and $\delta \leq \frac{uR(\mathcal{C}^N)+1}{q^N}$.

3. We will use the subspace evasive set construction in Theorem 3.2 [29] and outlined in Section 3.2.2. The construction is a $(v, v^{D \cdot v \cdot \log\log v})$- subspace evasive set $\mathcal{S}$, that is a subset of size q^{n_1} of $\mathbb{F}_q^n$. The parameters n and n_1 are chosen as shown below, following the approach in Section 3.2.2.

Let $w = v^2$ and $b = \lceil \frac{uR(\mathcal{C}^N)N+2N}{w-v} \rceil$. We choose $n_1 = (w-v)b$ and $n = wb$. Here n_1 is very close to $(uR(\mathcal{C}^N)+2)N$, the codeword length of the AMD code. Using $v = \xi_1^{-1}$ we have,

$$n_1 = \frac{w-v}{w}n = \frac{v^2-v}{v^2}n = (1-\frac{1}{v})n = (1-\xi_1)n.$$

Let γ be a primitive element of $\mathbb{F}_q$, and $\mathsf{AWTPenc}$ and $\mathsf{AWTPdec}$, denote the encoding and decoding algorithms of the code, respectively. The encoder and decoder algorithms for $\mathcal{C}^N$ are given in the follow.

AWTP Code

Encoding: Alice does the following:

1. Consider a message $\mathbf{m}$ of length $uR(\mathcal{C}^N)N$, as a vector $\mathbf{x} \in \mathbb{F}_{q^N}^{uR(\mathcal{C}^N)}$. Choose $\mathbf{r} \in \mathbb{F}_{q^N}$ randomly with uniform distribution, and use it to encode $\mathbf{x}$ using the AMD code construction in Section 4.2.1, $\mathsf{AMDenc}(\mathbf{x}) = (\mathbf{x}, \mathbf{r}, \mathbf{t})$. The AMD codeword has length $uR(\mathcal{C}^N)N + 2N$ over $\mathbb{F}_q$.

2. Extend the AMD codeword to length n_1 by appending zeros (in $\mathbb{F}_q$). Encode the resulting vector to an element $\mathbf{s} \in \mathcal{S}$, using the bijection mapping of the subspace evasive set,

$$\mathbf{s} = \mathsf{SE}(\mathbf{x}, \mathbf{r}, \mathbf{t}||0, \cdots, 0).$$

   Note that elements of $\mathcal{S}$ are from $\mathbb{F}_q^n$ and so, $\mathbf{s}$ has length n.

3. Append a randomly and uniformly selected vector $\mathbf{a} = (a_1 \cdots a_{u\rho_r N}) \in \mathbb{F}_q^{u\rho_r N}$ to $\mathbf{s}$ to form the vector that will be the message of the FRS code. Use $\mathbf{s}$ and $\mathbf{a}$ as the coefficients of the FRS codeword polynomial $f(x)$, over $\mathbb{F}_q$. That is $(f_0, \cdots, f_{k-1}) = (\mathbf{s}||\mathbf{a})$. We have $k = deg(f) + 1 = n + u\rho_r N$.

4. Use FRSenc to construct the FRS codeword $c = \mathsf{FRSenc}(f(X)) = (c_1, \cdots, c_N)$, with $c_i = (f(\gamma^{i(u-1)}), \cdots, f(\gamma^{iu-1})) \in \mathbb{F}_q^u$, for $i = 1, \cdots, N$.

Decoding: Bob does the following:

1. Let $y = c + e$, and $w_H(e) \leq \rho_w N$. Let, $y = (y_1, \cdots, y_N)$ and $y_i = (y_{i,1}, \cdots, y_{i,u})$ for $i = 1, \cdots, N$.

   Use the FRS (linear algebraic) decoding algorithm $\mathsf{FRSdec}(y)$ to output a matrix $\mathbf{M} \in \mathbb{F}_q^{k \times v}$, and a vector $\mathbf{z} \in \mathbb{F}_q^k$, such that the decoder output list is of the form, $\mathcal{L}_{\mathsf{FRS}} = \mathbf{M}\mathbf{b} + \mathbf{z}$. $\mathbf{M}$ has $k(= n + u\rho_r N)$ rows, and for each $\mathbf{b} \in \mathbb{F}_q^v$, gives a codeword in the output list.

2. Let $\mathcal{H}$ denote the vector space spanned by the first n equations. That is

$$\mathcal{H} = \mathbf{M}_{n \times v}\mathbf{b} + \mathbf{z}_n, \mathbf{b} \in \mathbb{F}_q^v,$$

   where $\mathbf{M}_{n \times v}$ is the first n rows of the submatrix of $\mathbf{M}$ and $\mathbf{z}_n$ is the first n elements of $\mathbf{z}$.

   The AWTP decoder calculates the intersection $\mathcal{S} \cap \mathcal{H}$ and outputs a list $\mathcal{L}$ of size at most $v^{D \cdot v \cdot \log\log v}$. Each codeword in the list is parsed and a potential AMD codeword $(\mathbf{x}_i, \mathbf{r}_i, \mathbf{t}_i)$ is formed. For each such codeword $(\mathbf{x}_i, \mathbf{r}_i, \mathbf{t}_i)$, the AMDdec checks if, $\mathbf{t}_i = f(\mathbf{x}_i, \mathbf{r}_i)$. If there is a *unique* valid AMD codeword in the list $\mathcal{L}$ of the FRS decoder, the AWTP decoder outputs the first uRN components of $\mathbf{x}$ as the correct message $\mathbf{m}$. Otherwise, Bob outputs $\perp$.

We prove secrecy and reliability of the above code, and derive the rate of the AWTP code family.

Lemma 20 (Secrecy)**.** *The AWTP code $\mathcal{C}^N$ above is perfectly secure for (ρ_r, ρ_w)-AWTP channels.*

Proof. It is sufficient to show that an AWTP codeword sent over a (ρ_r, ρ_w)-AWTP channel does not leak any information about the element of the subspace evasive set that the message is mapped to. The codeword polynomial is of degree $n + u\rho_r N - 1$ and so has $n + u\rho_r N$ unknown coefficients, $u\rho_r N$ of which are randomly chosen and the rest represent the element of subspace evasive set corresponding to m. The adversary sees $\rho_r N$ components of the FRS code, each an element of $\mathbb{F}_q^u$, resulting in $u\rho_r N$ linear equations over $\mathbb{F}_q$. The coefficient matrix of the equation set is a Vandermonde matrix and so the remaining n coefficients remain completely unknown (one solution for the equation set, for each element of $\mathbb{F}_q^n$) to the adversary.

$$\begin{bmatrix} 1 & \gamma^{(i_1-1)u} & \dots & \gamma^{(i_1-1)u(k-1)} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \gamma^{i_1 u-1} & \dots & \gamma^{(i_1 u-1)(k-1)} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \gamma^{(i_{\rho_r N}-1)u} & \dots & \gamma^{(i_{\rho_r N}-1)u(k-1)} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \gamma^{i_{\rho_r N} u-1} & \dots & \gamma^{(i_{\rho_r N} u-1)(k-1)} \end{bmatrix} \times \begin{bmatrix} \mathbf{s} \\ \mathbf{a} \end{bmatrix} = \begin{bmatrix} c_{i_1,1} \\ \vdots \\ c_{i_1,u} \\ \vdots \\ c_{i_{\rho_r N},1} \\ \vdots \\ c_{i_{\rho_r N},u} \end{bmatrix}. \tag{4.4}$$

Hence for an adversary observation $\mathsf{View}_{\mathcal{A}}(c) = \{c_{j_1}, \cdots, c_{j_{\rho_r N}}\}$,

$$\mathsf{H}(S|\mathsf{View}_{\mathcal{A}}) = \mathsf{H}(S),$$

where S is the element of the subspace evasive set which the message M is mapped to. □

The above FRS coding can be seen as a variant of coset coding in [66]. That is, consider the generator matrix of the FRS code as a $k \times N$ matrix B over $\mathbb{F}_q$ where $k = n + u\rho_r N$. The rows of B is partitioned into two sets: a set of $u\rho_r N$ rows that defines a code B', and a set of

n rows that define cosets of B' within the row span of B (each element of $\mathbb{F}_q^n$ corresponding to the element of SES is a coset leader). The final codeword is the sum of a coset leader and a random codeword of the code B'.

Lemma 21 (Reliability)**.** *i) For $N \geq v^2$, The AWTP code $\mathcal{C}^N$ described above provides reliability for a (ρ_r, ρ_w)-AWTP channel when,*

$$\rho_w < \frac{v}{v+1} - \frac{v}{v+1}\frac{\frac{v}{v-1}(uR(\mathcal{C}^N)+3)+u\rho_r}{u-v+1}. \tag{4.5}$$

ii) The decoding error probability of AWTPdec *is bounded by $\delta \leq \frac{v^{D'\cdot v\cdot \log\log v}}{q^N}$, where $D' = D+3$.*

The decoder always outputs the correct message, or outputs $\perp$.

Proof. i) FRS decoding algorithm FRSdec [38] requires,

$$N - \rho_w N > N\left(\frac{1}{v+1} + \frac{v}{v+1}\frac{uR_{\mathsf{FRS}}}{u-v+1}\right). \tag{4.6}$$

The dimension of the FRS code is bounded by,

$$\begin{aligned} k &= uR_{\mathsf{FRS}}N = u\rho_r N + n \\ &= u\rho_r N + w\left\lceil \frac{uR(\mathcal{C}^N)N + 2N}{w-v} \right\rceil \\ &\overset{(1)}{\leq} u\rho_r N + \frac{w}{w-v}(uR(\mathcal{C}^N)N + 3N), \end{aligned} \tag{4.7}$$

where (1) is from $N \geq v^2$.

Thus, we have, $uR_{\mathsf{FRS}} \leq u\rho_r + \frac{w}{w-v}(uR(\mathcal{C}^N)+3)$. Replacing R_{FRS} in the decoding condition of the FRS code (4.6) gives,

$$\rho_w < \frac{v}{v+1} - \frac{v}{v+1}\frac{\frac{v}{v-1}(uR(\mathcal{C}^N)+3)+u\rho_r}{u-v+1}.$$

ii) There is a decoding error if there are at least two codewords in the FRS decoder output list, that are AMD encodings of two messages $\mathbf{m}' \neq \mathbf{m}$. Note that the correct message is always in the decoder list. This is because the FRS decoder output contains all codewords

that are at distance at most $\rho_w N$ from the received word y. The message of the sent codeword is an element of subspace evasive set also. The first n components of the decoded vectors (ignoring the random components appended to the subspace evasive set element) defines an affine space of dimension n. By finding the intersection of this space and the subspace evasive set, we ensure that the correct message is always output by the decoding algorithm.

Next, we show that the probability that the message associated with any other codeword in the decoder list is a valid AMD codeword, is small. That is,

$$\begin{aligned}&\mathsf{Pr}([\mathsf{SE}(\mathbf{x}', \mathbf{r}', \mathbf{t}'||0, \cdots, 0) \in \mathcal{S} \cap \mathcal{H}] \wedge [\mathbf{t}' = f(\mathbf{x}', \mathbf{r}')]) \\ &\leq \frac{uR(\mathcal{C}^N) + 1}{q^N}.\end{aligned}$$

From Lemma 20, the adversary has no information about the encoded elements of the subspace evasive set $\mathbf{s}$, that encodes the AMD codeword $\mathsf{SE}(\mathbf{x}, \mathbf{r}, \mathbf{t}||0, \cdots, 0) = \mathbf{s}$. This means that the adversary's error, $(\Delta\mathbf{x}_i = \mathbf{x}' - \mathbf{x}, \Delta\mathbf{r}_i = \mathbf{r}' - \mathbf{r}, \Delta\mathbf{t}_i = \mathbf{t}' - \mathbf{t})$, is independent of $(\mathbf{x}, \mathbf{r}, \mathbf{t})$. According to Lemma 16, the probability that a tampered AMD codeword $(\mathbf{x}', \mathbf{r}', \mathbf{t}')$, passes the verification is no more than $\frac{uR(\mathcal{C}^N)+1}{q^N}$.

To show that the probability of decoding error is bounded as $\delta \leq \frac{v^{D' \cdot v \cdot \log\log v}}{q^N}$, we note that the list size is at most $|\mathcal{S} \cap \mathcal{H}| \leq v^{D \cdot v \cdot \log\log v}$, and $uR(\mathcal{C}^N) + 1 \leq u + 1 \leq v^3$. Using the union bound and letting $D' = D + 3$, the probability that some $(\mathbf{x}', \mathbf{r}', \mathbf{t}') \neq (\mathbf{x}, \mathbf{r}, \mathbf{t})$ in the decoded list passes the verification $\mathbf{t}' = f(\mathbf{x}', \mathbf{r}')$, is no more than $\frac{v^{D' \cdot v \log\log v}}{q^N}$.

So the probability that decoder outputs $\perp$ is no more than $\frac{v^{D' \cdot v \log\log v}}{q^N}$. □

Rate of AWTP code family

The achievable rate of the code family $\mathbb{C}^0 = \{\mathcal{C}^N\}_{N \in \mathbb{N}}$ is given by the following Lemma.

Lemma 22 (Achievable Rate of $\mathbb{C}^0$)**.** *The AWTP code family $\mathbb{C}^0 = \{\mathcal{C}^N\}_{N \in \mathbb{N}}$ achieves the rate $R(\mathbb{C}^0) = 1 - \rho_r - \rho_w$ for a (ρ_r, ρ_w)-AWTP channel.*

Proof. We show that for any small $0 < \xi < \frac{1}{2}$, by choosing $\xi_1 = \frac{\xi}{13}$, decoding parameters $v = 1/\xi_1$ and $u = 1/\xi_1^2$, and $N_0 > (1/\xi_1)^{D'/\xi_1 \log\log 1/\xi_1}$ where $D' = D + 3$, the rate of the code will be $R(\mathcal{C}^N) \geq \mathbb{C}^0 - \xi$.

We substitute the values in the RHS of (4.5) with the above chosen values,

$$\begin{aligned}
&\frac{v}{v+1} - \frac{v}{v+1}\frac{\frac{v}{v-1}(uR(\mathcal{C}^N)+3)+u\rho_r}{u-v+1} \\
&\quad = \frac{1}{\xi_1+1} - \frac{1}{\xi_1+1}\frac{\frac{1}{1-\xi_1}(R(\mathcal{C}^N)+3\xi_1^2)+\rho_r}{1-\xi_1+\xi_1^2} \\
&\quad = \frac{1}{\xi_1+1} - \frac{\frac{1}{1-\xi_1}(R(\mathcal{C}^N)+3\xi_1^2)+\rho_r}{1+\xi_1^3} && (4.8)\\
&\quad \geq 1-\xi_1-(\frac{1}{1-\xi_1}(R(\mathcal{C}^N)+3\xi_1^2)+\rho_r) && (4.9)\\
&\quad \geq 1-\xi_1-((1+2\xi_1)(R(\mathcal{C}^N)+3\xi_1)+\rho_r) && (4.10)\\
&\quad = 1-\xi_1-(R(\mathcal{C}^N)+11\xi_1+\rho_r) && (4.11)\\
&\quad = 1-R(\mathcal{C}^N)-\rho_r-12\xi_1.
\end{aligned}$$

Here, (4.9) is by multiplying the numerator and denominator of the first term on the RHS of (4.8) by $1-\xi_1$ and ignoring ξ_1^2, and also ignoring ξ_1^3 in the denominator of the second term on the RHS of (4.8); we have (4.10) by noting that for $\xi_1 \leq \frac{1}{2}$ we have $\frac{1}{1-\xi_1} \leq 1+2\xi_1$, and finally (4.11) is by replacing $2\xi R(\mathcal{C}^N)$ by 2ξ (because $R(\mathcal{C}^N) \leq 1$), and $6\xi^2$ with 6ξ (because $\xi \ll 1$).

Hence the decoding condition (4.5) of the AWTP code is satisfied for,

$$\rho_w = 1 - R(\mathcal{C}^N) - \rho_r - 12\xi_1, \tag{4.12}$$

and so, $R(\mathcal{C}^N) = 1-\rho_r-\rho_w-12\xi_1$.

Now since $\xi = 13\xi_1$, for any $N > N_0$, the rate of the AWTP code $\mathcal{C}^N$ is

$$\begin{aligned}
\frac{1}{N}\log_{|\Sigma|}|\mathcal{M}| = R(\mathcal{C}^N) &= 1-\rho_r-\rho_w-12\xi_1 \\
&> 1-\rho_r-\rho_w-\xi = \mathsf{C}^0-\xi.
\end{aligned}$$

Since the probability of decoding error is bounded by,

$$\delta \leq (1/\xi_1)^{D'/\xi_1 \log\log 1/\xi_1} q^{-N} \leq Nq^{-N} \leq \xi,$$

we conclude that the achievable rate of the AWTP code family $\mathbb{C}^0$, is $R(\mathbb{C}^0) = 1 - \rho_r - \rho_w$.

□

The computational complexity of encoding is $\mathcal{O}((N \log q)^2)$. The computational complexity of the FRS decoding algorithm is $\mathcal{O}((N \log q)^2)$, and that of subspace evasive set intersection algorithm is, $\mathsf{poly}((1/\xi)^{D/\xi \log\log 1/\xi})$. The AMD code verification costs $\mathcal{O}((N \log q)^2)$, and so the total complexity of the AWTP decoding is $\mathsf{poly}(N)$.

Theorem 12. *For any sufficiently small $\xi > 0$, there is a $(0, \delta)$-AWTP code $\mathcal{C}^N$ of length N for a (ρ_r, ρ_w)-AWTP channel, such that the information rate is $R(\mathcal{C}^N) = 1 - \rho_r - \rho_w - \xi$, the alphabet size is $|\Sigma| = \mathcal{O}(q^{1/\xi^2})$, and the decoding error is bounded by $\delta < q^{-\mathcal{O}(N)}$. The computational complexity of decoding is $\mathsf{poly}(N)$. The AWTP code family $\mathbb{C}^0 = \{\mathcal{C}^N\}_{N \in \mathbb{N}}$ achieves secrecy capacity $\mathsf{C}^0 = R(\mathbb{C}^0) = 1 - \rho_r - \rho_w$ of (ρ_r, ρ_w)-AWTP channels.*

4.6 AWTP Codes and SMT

AWTP codes are defined over an alphabet Σ and so all components of a codeword are elements of Σ. In SMT protocols however, the set of transmissions on each wire may be different.

Definition 27 (Symmetric SMT)**.** *An SMT protocol is called a* symmetric SMT protocol *if the protocol remains invariant under any permutation of the wires.*

Let $\mathcal{W}_j^i, j = 1 \cdots N, i = 1 \cdots r$, denote the set of possible transmissions on wire j in an r-round SMT protocol. For symmetric protocol, $\mathcal{W}_j^i = \mathcal{W}^i$ is independent of j. *All known constructions of threshold SMT protocols are symmetric.*

Theorem 13. *There is a one-to-one correspondence between an (ϵ, δ)-AWTP code $\mathcal{C}^N$ that provides security for a restricted ρ-AWTP channel, and a 1-round $(\epsilon_{\mathsf{SMT}}, \delta_{\mathsf{SMT}})$ symmetric SMT protocol for N wires with security against a (t, N) threshold adversary, where $t = \rho N$.*

An (ϵ, δ)-AWTP code can be used to construct a 1-round $(\epsilon_{\mathsf{SMT}}, \delta_{\mathsf{SMT}})$ symmetric SMT, where $\epsilon_{\mathsf{SMT}} = \epsilon$ and $\delta_{\mathsf{SMT}} = \delta$. The converse is also true.

Proof. Consider an (ϵ, δ)-AWTP code $\mathcal{C}^N$ for a restricted AWTP channel. By associating each component of the code with a distinct wire, one can construct a 1-round $(\epsilon_{\mathsf{SMT}}, \delta_{\mathsf{SMT}})$ symmetric SMT protocol for N wires. The protocol security is against a threshold (t, N) adversary with $t = \rho N$. The SMT encoding and decoding are obtained from the corresponding functions in the (ϵ, δ)-AWTP code; that is, $\mathsf{SMTenc}(m, r_{\mathcal{S}}) = \mathsf{AWTPenc}(m, r_{\mathcal{S}})$ and $\mathsf{SMTdec}(y) = \mathsf{AWTPdec}(y)$. To relate the security and reliability of the SMT protocol to those of the AWTP-code, we note the following:

1. Definition of privacy in both cases is in terms of the statistical distance of the adversary's view for any two messages chosen by the adversary (definitions 14 and 26).
2. Decoding error is both cases requires the decoder to output the correct message with probability at least $1 - \delta$.
3. The corruption of a codeword in a (ρ_r, ρ_w)-AWTP channel is by additive error, while in SMT the adversary can arbitrarily modify the $|S| = t$ corrupted wires. However in restricted ρ-AWTP channels $S = S_r = S_w, |S| = \rho N$ and so modifying the components $(c_{i_1}, \cdots c_{i_t})$ to $(c'_{i_1}, \cdots c'_{i_t})$ is t equivalent to calculating an error e with $\mathsf{SUPP}(e) = S$ and $(e_{i_1}, \cdots e_{i_t}) = ((c'_{i_1} - c_{i_1}), \cdots (c'_{i_t} - c_{i_t}))$, and adding it to the codeword. This means that for these channels additive error can be used to generate all possible adversarial tampering.

The theorem follows by constructing a restricted (ϵ, δ)-AWTP code with $S = S_r = S_w$, from a 1-round $(\epsilon_{\mathsf{SMT}}, \delta_{\mathsf{SMT}})$ symmetric SMT, using the same correspondence between the code components and the wires. We will have $\epsilon = \epsilon_{\mathsf{SMT}}$ and $\delta = \delta_{\mathsf{SMT}}$.

□

Corollary 5 below follows from the one-to-one correspondence established in Theorem 13.

Corollary 5. *Let $R(\mathcal{C}^N)$ be the rate of an (ϵ, δ)-AWTP code $\mathcal{C}^N$ for a restricted AWTP channel. The transmission rate of the associated 1-round (ϵ, δ) symmetric SMT is given by,* $\tau_R(\mathsf{SMT}) = \frac{N \log |\mathcal{V}|}{\log |\mathcal{M}|} = \frac{1}{R(\mathcal{C}^N)}$.

The upper bound on the secrecy rate (Lemma 4) of $(0, \delta)$-AWTP codes for restricted AWTP channels, gives a lower bound on the transmission rate of 1-round $(0, \delta)$ symmetric SMT protocols.

Theorem 14. *For a 1-round (ϵ, δ) symmetric SMT protocol, transmission rate is lower bounded by,*

$$\tau_R(\mathsf{SMT}) \geq \frac{N}{N - 2t + 2t\epsilon(1 + \log_{|\mathcal{V}|}(\frac{1}{\epsilon}))}.$$

For $\epsilon = 0$, the bound reduces to the known bound, $\tau_R(\mathsf{SMT}) \geq \frac{N}{N-2t}$ [67].

Proof. Using Theorem 4, for a 1-round (ϵ, δ) symmetric SMT over N wires with $t = \rho N$, there is a corresponding (ϵ, δ)-AWTP code for a restricted AWTP channel with $S = S_r = S_w$ whose information rate is upper bounded by,

$$R(\mathcal{C}^N) \leq 1 - 2\rho + 2\epsilon\rho(1 + \log_{|\Sigma|} \frac{1}{\epsilon}).$$

Since the transmission rate of an (ϵ, δ) symmetric SMT protocol is the inverse of the information rate of the corresponding (ϵ, δ)-AWTP code, we have,

$$\begin{aligned} \tau_R(\mathsf{SMT}) &= \frac{1}{R(\mathcal{C}^N)} \\ &\geq \frac{1}{1 - 2\rho + 2\epsilon\rho(1 + \log_{|\mathcal{V}|} \frac{1}{\epsilon})} \\ &= \frac{N}{N - 2t + 2t\epsilon(1 + \log_{|\mathcal{V}|} \frac{1}{\epsilon})}. \end{aligned}$$

□

Corollary 6. *For $N = 2t + 1$, we will have,*

$$\tau_R(\mathsf{SMT}) = \frac{1}{R(\mathcal{C}^N)} \geq \frac{2t+1}{1 + 2t\epsilon(1 + \log_{|\mathcal{V}|} \frac{1}{\epsilon})}.$$

This is the first and the only known lower bound on the transmission rate of (ϵ, δ) symmetric SMT protocols. Using a similar approach one can obtain an alternative proof for the known lower bound on the transmission rate of 1-round $(0, \delta)$ symmetric SMT protocols (Theorem 10, [67])

4.7 Proof of Chapter 4

4.7.1 Proof of Lemma 17

Proof. From the definition of ϵ-secrecy we have,

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{ds}}(\mathsf{AWTPenc}, \mathsf{View}_{\mathcal{A}}) \\
&= \frac{1}{2} \sum_{c_{S_r^1}} |\mathsf{Pr}(c_{S_r^1}|m) - \mathsf{Pr}(c_{S_r^1}|m')| \\
&+ \frac{1}{2} \sum_{c_{S_r^2}} |\mathsf{Pr}(c_{S_r^2}|m) - \mathsf{Pr}(c_{S_r^2}|m')| \\
&\leq \epsilon.
\end{aligned} \tag{4.13}$$

This implies that for any pair of messages, $m, m' \in \mathcal{M}$, we have,

$$\frac{1}{2} \sum_{c_{S_r^1}} |\mathsf{Pr}(c_{S_r^1}|m) - \mathsf{Pr}(c_{S_r^1}|m')| \leq \epsilon,$$

and so it follows that for any $m \in \mathcal{M}$,

$$\begin{aligned}
&\mathbf{SD}(C_{S_r^1}|M=m, C_{S_r^1}) \\
&= \frac{1}{2}\sum_{c_{S_r^1}} |\mathsf{Pr}(c_{S_r^1}|m) - \mathsf{Pr}(c_{S_r^1})| \\
&= \frac{1}{2}\sum_{c_{S_r^1}} |\mathsf{Pr}(c_{S_r^1}|m) - \sum_{m' \in \mathcal{M}} \mathsf{Pr}(c_{S_r^1}|m')\mathsf{Pr}(m')| \\
&= \frac{1}{2}\sum_{c_{S_r^1}} |\mathsf{Pr}(c_{S_r^1}|m) - \sum_{m' \in \mathcal{M}} \mathsf{Pr}(c_{S_r^1}|m')\mathsf{Pr}(m')| \\
&\leq \sum_{m' \in \mathcal{M}} \mathsf{Pr}(m')\frac{1}{2}\sum_{c_{S_r^1}} |\mathsf{Pr}(c_{S_r^1}|m) - \sum_{m' \in \mathcal{M}} \mathsf{Pr}(c_{S_r^1}|m')| \\
&\leq \sum_{m' \in \mathcal{M}} \mathsf{Pr}(m')\epsilon \\
&= \epsilon.
\end{aligned}$$

Using Theorem 17.3.3 (Page 664, [16]), for sufficiently small ϵ we have,

$$\begin{aligned}
&\mathsf{H}(C_{S_r^1}) - \mathsf{H}(C_{S_r^1}|M=m) \\
&\leq 2\mathbf{SD}(C_{S_r^1}, C_{S_r^1}|M=m)\log\frac{|\Sigma|^{\rho_r N}}{\mathbf{SD}(C_{S_r^1}, C_{S_r^1}|M=m)} \\
&\leq 2\epsilon\rho_r N \log\frac{|\Sigma|}{\epsilon}.
\end{aligned}$$

This implies,

$$\begin{aligned}
\mathsf{I}(M; C_{S_r^1}) &= \mathsf{I}(C_{S_r^1}; M) \\
&= \mathsf{H}(C_{S_r^1}) - \sum_{m \in \mathcal{M}} \mathsf{Pr}(m)\mathsf{H}(C_{S_r^1}|M=m) \\
&= \sum_{m \in \mathcal{M}} \mathsf{Pr}(m)(\mathsf{H}(C_{S_r^1}) - \mathsf{H}(C_{S_r^1}|M=m)) \\
&\leq \sum_{m \in \mathcal{M}} \mathsf{Pr}(m) 2\epsilon\rho_r N \log\frac{|\Sigma|}{\epsilon} \\
&\leq 2\epsilon\rho_r N \log\frac{|\Sigma|}{\epsilon}.
\end{aligned}$$

Similar we have,

$$\mathsf{I}(M; C_{S_r^2}) \leq 2\epsilon\rho_r N \log\frac{|\Sigma|}{\epsilon}.$$

It follows that,

$$\begin{aligned}
\mathsf{I}(M;V) &= \mathsf{H}(M) - \mathsf{H}(M|V) \\
&= \mathsf{H}(M) - \mathsf{Pr}(A=1)\mathsf{H}(M|C_{S_r^{\overline{A}}}) - \mathsf{Pr}(A=2)\mathsf{H}(M|C_{S_r^{\overline{A}}}) \\
&= \frac{1}{2}(\mathsf{H}(M) - \mathsf{H}(M|C_{S_r^2})) + \frac{1}{2}(\mathsf{H}(M) - \mathsf{H}(M|C_{S_r^1})) \\
&\leq 2\epsilon\rho_r N \log\frac{|\Sigma|}{\epsilon}.
\end{aligned}$$

□

4.7.2 Proof of Lemma 19

Proof. We have,

$$\begin{aligned}
\mathsf{H}(M) &= \mathsf{I}(M;Y,A) + \mathsf{H}(M|Y,A) - \mathsf{I}(M;V) + \mathsf{I}(M;V) \\
&\leq \mathsf{I}(M;Y,V,A) - \mathsf{I}(M;V) + \mathsf{H}(M|Y,A) + \mathsf{I}(M;V) \\
&\overset{(1)}{=} \mathsf{I}(M;Y,V,A) - \mathsf{I}(M;V,A) + \mathsf{H}(M|Y,A) + \mathsf{I}(M;V) \\
&\overset{(2)}{=} \mathsf{I}(M;Y|V,A) + \mathsf{H}(M|Y,A) + \mathsf{I}(M;V) \\
&= \mathsf{H}(Y|V,A) - \mathsf{H}(Y|M,V,A) + \mathsf{H}(M|Y,A) + \mathsf{I}(M;V) \\
&\overset{(3)}{\leq} \mathsf{H}(Y|V,A) - \mathsf{H}(Y|M,V,C,A) + \mathsf{H}(M|Y,A) + \mathsf{I}(M;V) \\
&\overset{(4)}{\leq} \mathsf{H}(Y|V,A) - \mathsf{H}(E|M,V,C,A) + \mathsf{H}(M|Y,A) + \mathsf{I}(M;V) \\
&\overset{(5)}{=} \mathsf{H}(Y|V,A) - \mathsf{H}(E|A) + \mathsf{H}(M|Y,A) + \mathsf{I}(M;V).
\end{aligned} \tag{4.14}$$

In above, (1) follows from the Markov chain $M \to C \to \{C_{S_r^1}, C_{S_r^2}\} \to C_{S_r^{\overline{A}}} = V \to \{S_r^{\overline{A}}, S_w^{\overline{A}}\} \to \overline{A} \to A$, which gives $\Pr(A=i, M=m|V=v) = \Pr(M=m|V=v)\Pr(A=i|V=v)$; (2) is from mutual information chain relation; (3) is from $\mathsf{H}(Y|M,V,C,A) \leq \mathsf{H}(Y|M,V,A)$; (4) is by noting that $E = Y - C$ (here "$-$" is the operation over Σ); and (5) is from $\mathsf{Pr}(E=e|M=m,V=v,C=c,A=i) = \mathsf{Pr}(E=e|A=i)$.

So we have,

$$\mathsf{H}(M) \leq \mathsf{H}(Y|V,A) - \mathsf{H}(E|A) + \mathsf{H}(M|Y,A) + \mathsf{I}(M;V).$$

We upper bound $\mathsf{H}(M)$ by bounding the four terms on the right hand side (RHS) of the above inequality.

First, we have the bound, $\mathsf{H}(Y|V,A) \leq (1-\rho_r)N\log|\Sigma|$. Let $Y_{[N]\setminus S_r^1}$ be the components of Y on the set $[N]\setminus S_r^1$. Since $S_r^1 \cap S_w^2 = \emptyset$, if the adversary selects $A=2$, the components of Y on the set S_r^1 will not have error and will be equal to the components of C on S_r^1. That is,

$$\mathsf{H}(Y_{S_r^1}|C_{S_r^1}, A=2) = 0. \tag{4.15}$$

Similarly, since $S_r^2 \cap S_w^1 = \emptyset$, we have,

$$\mathsf{H}(Y_{S_r^2}|C_{S_r^2}, A=1) = 0. \tag{4.16}$$

So we have,

$$\begin{aligned}
\mathsf{H}(Y|V,A) &= \mathsf{Pr}(A=1)\mathsf{H}(Y|C_{S_r^2}, A=1) + \mathsf{Pr}(A=2)\mathsf{H}(Y|C_{S_r^1}, A=2) \\
&= \frac{1}{2}\mathsf{H}(Y_{S_r^2}Y_{[N]\setminus S_r^2}|C_{S_r^2}, A=1) + \frac{1}{2}\mathsf{H}(Y_{S_r^1}Y_{[N]\setminus S_r^1}|C_{S_r^1}, A=2) \\
&= \frac{1}{2}(\mathsf{H}(Y_{S_r^2}|C_{S_r^2}, A=1) + \mathsf{H}(Y_{[N]\setminus S_r^2}|C_{S_r^2}, Y_{S_r^2}, A=1)) \\
&\quad + \frac{1}{2}(\mathsf{H}(Y_{S_r^1}|C_{S_r^1}, A=2) + \mathsf{H}(Y_{[N]\setminus S_r^1}|C_{S_r^1}, Y_{S_r^1}, A=2)) \\
&\leq \frac{1}{2}(\mathsf{H}(Y_{S_r^2}|C_{S_r^2}, A=1) + \mathsf{H}(Y_{[N]\setminus S_r^2})) + \frac{1}{2}(\mathsf{H}(Y_{S_r^1}|C_{S_r^1}, A=2) + \mathsf{H}(Y_{[N]\setminus S_r^1})) \\
&\overset{(1)}{\leq} \frac{1}{2}\log|Y_{[N]\setminus S_r^2}| + \frac{1}{2}\log|Y_{[N]\setminus S_r^1}| \\
&\leq (1-\rho_r)N\log|\Sigma|,
\end{aligned}$$

where (1) is from (4.15) and (4.16).

To bound the second item notice that for any choice of $A=i, i=1,2$ by the adversary, E is uniformly distributed and so,

$$\begin{aligned}
&\mathsf{H}(E|A) \\
&= \mathsf{Pr}(A=1)\mathsf{H}(E|A=1) + \mathsf{Pr}(A=2)\mathsf{H}(E|A=2) \\
&= \rho_w N\log|\Sigma|.
\end{aligned} \tag{4.17}$$

Moreover, from Lemmas 17 and 18, we have the bounds $\mathsf{H}(M|Y,A) \leq \mathsf{H}(\delta) + \delta N \log|\Sigma|$, and $\mathsf{H}(M) - \mathsf{H}(M|V) \leq 2\epsilon\rho_r N \log\frac{|\Sigma|}{\epsilon}$, respectively. So the upper bound on $\mathsf{H}(M)$ is,

$$\mathsf{H}(M) \leq (1-\rho_r-\rho_w)N\log|\Sigma| + \mathsf{H}(\delta) + \delta N\log|\Sigma| + 2\epsilon\rho_r N\log\frac{|\Sigma|}{\epsilon}. \tag{4.18}$$

For $0 < \delta < \frac{1}{2}$, we have $\delta < \mathsf{H}(\delta)$ and so,

$$\mathsf{H}(\delta) + \delta N\log|\Sigma| \leq 2\mathsf{H}(\delta)N\log|\Sigma|.$$

The upper bound on the rate is obtained by considering uniform distribution on $\mathcal{M}$ and using $\mathsf{H}(M) = \log|\mathcal{M}|$.

That is,

$$\begin{aligned} R(\mathcal{C}^N) &= \frac{\log|\mathcal{M}|}{N\log|\Sigma|} \\ &\leq 1-\rho_r-\rho_w + 2\epsilon\rho_r(1+\log_{|\Sigma|}\frac{1}{\epsilon}) + 2\mathsf{H}(\delta). \end{aligned}$$

□

Chapter 5

Adversarial Wiretap Channel with Public Discussion

5.1 Introduction

In Wyner's [89] model of secure communication and its generalization to broadcast scenario [18], Alice is connected to Bob and Eve through two noisy channels, referred to as the *main channel* and the *eavesdropper channel*, respectively. The goal is to send a message from Alice to Bob with perfect secrecy and reliability. Wyner's pioneering work showed that communication with (asymptotic) perfect secrecy and reliability is possible if the eavesdropper's channel is noisier than the main channel. Importantly, security is information theoretic and does not require a pre-shared secret key. Adversarial model of wiretap channel where the adversary is active, dates back to Ozarow and Wyner [66]. In their model instead of the noise corrupting the adversary's view of the transmissed codewprd, the adversary can select a fraction of the codeword that it would like to "see". More recently, wiretap channels where the active adevrsary also corrupts the communication have been considered [2, 12, 64, 85]. In these models the adversary can select its view (also, observation or eavedropping) of the communication and is also able to *partially jam* the channel by injecting noise in the main channel. In this section we consider a model of adversarial wiretap channel (AWTP channel) that is proposed in [85, 86]. In this model, the adversary adaptively chooses a fraction ρ_r of the coordinates of the sent codeword for eavesdropping, and a fraction ρ_w of the codeword to corrupt by adding an adversarial noise to the channel. The adversary's eavesdropings and corruptions are adaptive: for each action the adversary uses all its observations and corruptions up to that point, to make its next choice. The goal of the adversary is to break the security and/or reliability of communication.

Motivation

It was proved [85] that perfect secrecy and reliability for AWTP in 1-round communication is possible if and only if, $\rho_r + \rho_w < 1$. We consider a scenario where in addition to the AWTP channel, a public discussion channel denoted by PD, is available to the communicants. We call this model *AWTP with public discussion* (or $\mathsf{AWTP}_{\mathsf{PD}}$ for short). Our goal is to see if the use of this extra resource can make secure communication possible when $\rho_r + \rho_w > 1$ (for example $\rho_r = \rho_w = 0.9$).

Public discussion channels had been considered in wiretap and SMT models, both. In wiretap setting it was shown [61, 3] that a public discussion channel substantially expands the range of scenarios in which secure communication is possible. In particular secure communication becomes possible even if the eavesdroper channel is less noisy than the main channel. A similar result holds for SMT. Access to a public discussion channel in SMT was considered by Garay *et.al.* [34] who showed that secure message tranmission will be possible when $N \geq t + 1$ while without a PD, $N \geq 2t + 1$.

We allow communicants to interact over the PD but assume *communication over the AWTP channel is one-way* and from Alice to Bob. This restriction is to simplify our analysis and as we will show, will still allow us to construct protocols that are optimal. The assumption is also natural in settings where the sender node is more powerful such as a base station.

Our Results

1). Model and Definitions. We define a multi-round *message transmission protocol* over $\mathsf{AWTP}_{\mathsf{PD}}$. The protocol may leak information to the adversary and the decoder may output an incorrect message. We define secrecy as the statistical distance between the adversary's view of any two adversarially chosen messages, and reliability as the probability that the decoded message being different from the sent one, for any message.

An $\mathsf{AWTP}_{\mathsf{PD}}$ protocol in general, has multiple *message rounds* where in each message

round a *protocol message* is sent by Alice over AWTP channel or the PD channel, or by Bob over the PD channel, each message possibly of different length. In each invocation of the AWTP channel the adversary can choose a different read and write set. An (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol guarantees that the leaked information about the message is bounded by ϵ, and the probability of decoding an incorrect message is bounded by δ. The information *rate* R of a $\mathsf{AWTP_{PD}}$ protocol measures transmission efficiency of the protocol in terms of transmission over the AWTP channel and is the number of message (information) bits transmitted by the protocol, divided by the total number of transmitted bits over this channel. The secrecy capacity C^ϵ of an $\mathsf{AWTP_{PD}}$ channel is the maximum information rate that can be achieved by a $\mathsf{AWTP_{PD}}$ protocol family as the total number of bits communicated over the AWTP channel goes to infinity when the security loss is bounded by ϵ.

2). Bounds. We derive a tight upper bound on rate: we first derive a bound on $\mathsf{H}(M)$, and then use the bound to prove that the highest secrecy rate of an (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol is bounded by $\mathsf{C}^\epsilon \leq 1-\rho+2\epsilon\cdot(1+\log_{|\Sigma|}\frac{1}{\epsilon})+2\epsilon n$, where n is the total (bit) length of transmission over the PD channel, Σ is the alphabet of the AWTP channel, and $\rho = \frac{1}{N}|S_r \cup S_w|$ is the fraction of components of a codeword that are read or written to, by the adversary. For perfect secrecy capacity we have $\mathsf{C}^0 \leq 1-\rho$. When $S_r \cap S_w \neq \emptyset$, we have $\rho < \rho_r + \rho_w$, and perfectly secure communication *is* possible even if $\rho_r + \rho_w > 1$ (e.g. $\rho_r = \rho_w = 0.9$), as long as $\rho < 1$.

A second efficiency measure is the message round complexity RC of the protocol. We derive a tight lower bound on RC for any $\mathsf{AWTP_{PD}}$ protocol (one-way communication over AWTP) with positive rate, when $\rho_r + \rho_w > 1$. We show that a secure $\mathsf{AWTP_{PD}}$ protocol with $\rho_r + \rho_w > 1$ and $\rho < 1$, cannot have two message rounds and so $\mathsf{RC} \geq 3$.

3). Construction of $\mathsf{AWTP_{PD}}$ *protocol.* We construct a family of three message round $(0, \delta)$-$\mathsf{AWTP_{PD}}$ protocols for which the rate can be made arbitrarily close to the upper bound. That is, for any small $\xi > 0$, there is N_0, such that for all $N > N_0$, the rate of the $\mathsf{AWTP_{PD}}$

protocol family satisfies, $R(\Pi^N) \geq 1 - \rho - \xi$ and so the family achieves the capacity. The number of message rounds of the protocol is minimal and meets the lower bound on RC. The construction is as follows: in the first message round Alice sends to Bob over the AWTP channel a random sequence over Σ. In the second message round, Bob randomly chooses elements of a universal hash family to calculate the hash values of each of the received elements, and sends the hash values together with the randomness used when choosing the hash function, to Alice over the PD channel. In the third message round, Alice, encrypts the message using a key that is extracted from the random values that are correctly received by Bob and sends it over the PD channel to Bob, together with sufficient information that allows Bob to calculate the same key and recover the message.

4). Relation with SMT-PD. In *Secure Message Transmission with public discussion protocol (SMT-PD)* [34], Alice and Bob are connected by N node disjoint communication paths in a network, a subset of which can be controlled by a computationally unlimited adversary, and also an authenticated public discussion channel that can be read by everyone. The adversary chooses a subset of wires and corrupts them arbitrarily. In Section 4.6 we define (ϵ, δ)-SMT$^{[ows]}$-PD , a subset of SMT-PD protocols in which the wires are used by Alice only, and show our results for $\mathsf{AWTP_{PD}}$ including bounds on the rate and round complexity, and the construction of an optimal $\mathsf{AWTP_{PD}}$ protocol give a similar results for (ϵ, δ)-SMT$^{[ows]}$-PD.

Related Work

Maurer's [61] introduced PD channels first in the context of *key agreement* over wiretap channels; this was also independently considered in [3]. Since the PD channel is considered free, the established key can be used to send the message securely over this channel and so the communication cost of the message transmission will stay the same as that of the key establishment. Our construction also has two steps: a key establishment, followed by encrypting the message and sending it over the public discussion channel. This is also the approach in [34] (Protocol I) and [75].

5.2 Preliminary

5.2.1 Universal Hash Family

An (N, n, m)-hash family is a set $\mathcal{F}$ of N functions, $f : \mathcal{X} \to \mathcal{T}$, $f \in \mathcal{F}$, where $|\mathcal{X}| = n$ and $|\mathcal{T}| = m$. Without loss of generality, we assume $n \geq m$.

Definition 28. *[82] Suppose that the (N, n, m)-hash family $\mathcal{F}$ has range $\mathcal{T}$ which is an additive Abelian group. $\mathcal{F}$ is called ϵ-Δ universal, if for any two elements $x_1, x_2 \in \mathcal{X}, x_1 \neq x_2,$, and for any element $t \in \mathcal{T}$, there are at most ϵN functions $f \in \mathcal{F}$ such that $f(x_1) - f(x_2) = t$, were the operation is from the group.*

We will use a classic construction of $\frac{u}{q}$-universal hash family [82]. Let q be a prime and $u \leq q - 1$. Let the message be $\mathbf{x} = \{x_1, \cdots, x_u\} \in \mathbb{F}_q$. For $\alpha \in \mathbb{F}_q$, define the universal hash function hash_α by the rule,

$$t = \mathsf{hash}_\alpha(\mathbf{x}) = x_1\alpha + x_2\alpha^2 + \cdots + x_u\alpha^u \mod q. \tag{5.1}$$

Then $\{\mathsf{hash}_\alpha(\cdot) : \alpha \in \mathbb{F}_q\}$ is a $\frac{u}{q}$-Δ universal (q, q^u, q)-hash family.

5.2.2 Randomness Extractor

A randomness extractor is a function, which is applied to a weakly random entropy source (i.e., a non-uniform random variable), to obtain a uniformly distributed source.

Definition 29. *[27] A (seeded) (n, m, r, δ)-strong extractor is a function $\mathsf{Ext} : q^n \times q^d \to q^m$ such that for any source X with $\mathsf{H}_\infty(X) \geq r$, we have,*

$$\mathbf{SD}((\mathsf{Ext}(X, \mathsf{Seed}), \mathsf{Seed}), (U, \mathsf{Seed})) \leq \delta.$$

with the seed uniformly distributed over $\mathbb{F}_q^d$.

A function $\mathsf{Ext} : q^n \to q^m$ is a (seedless) (n, m, r, δ)-extractor if for any source X with $\mathsf{H}_\infty(X) \geq r$, the distribution $\mathsf{Ext}(X)$ satisfies $\mathbf{SD}(\mathsf{Ext}(X), U) \leq \delta$.

A seedless extractor can be constructed from Reed-Solomon (RS) codes [15]. The construction works only for a restricted class of sources, known as *symbol-fixing sources.*

Definition 30. *An (n, m) symbol-fixing source is a tuple of independent random variables $\mathbf{X} = (X_1, \cdots, X_n)$, defined over a set Ω, such that m of the variables take values uniformly and independently from Ω, and the rest have fixed values.*

We show a construction of a seedless $(n, m, m \log q, 0)$-extractor from RS-codes. Let $q \geq n + m$. Consider an (n, m) symbol-fixing source $\mathbf{X} = (X_1, \cdots, X_n) \in \mathbb{F}_q^n$ with $\mathsf{H}_\infty(X) \geq m \log q$. The extraction has two steps:

1. Construct a polynomial $f(x) \in \mathbb{F}_q[X]$ of degree $\leq n - 1$, such that $f(i) = x_i$ for $i = 0, \cdots, n - 1$.

2. Evaluate the polynomial at $i = \{n, \cdots, n + m - 1\}$. That is,

$$\mathsf{Ext}(\mathbf{x}) = (f(n), f(n + 1), \cdots, f(n + m - 1)).$$

5.3 $\mathsf{AWTP}_{\mathsf{PD}}$ Protocol

5.3.1 Channel Models

We consider two types of channels: AWTP channel and PD channel. A channel can be one-way or two-way.

Definition 31. *A* one-way channel *from Alice to Bob (Bob to Alice) is used to send messages from Alice to Bob (Bob to Alice). A* two-way channel *can be used in both directions, from Alice to Bob, or from Bob to Alice.*

Let $[N] = \{1, \cdots, N\}$, $S_r = \{i_1, \cdots, i_{\rho_r N}\} \subseteq [N]$ and $S_w = \{j_1, \cdots, j_{\rho_w N}\} \subseteq [N]$. Support of a vector $x = (x_1 \cdots x_N) \in \Sigma^N$, denoted by $\mathsf{SUPP}(x)$, is the set of positions where $x_i \neq 0$.

Definition 32. *A (ρ_r, ρ_w)-Adversarial Wiretap Channel ((ρ_r, ρ_w)-AWTP Channel) is an adversarial channel that it is (partially) controlled by an adversary Eve, with two capabilities: Reading and Writing. For a codeword of length N, Eve selects a subset $S^r \subseteq [N]$ of size $|S^r| = \rho_r N$ to read (eavesdrop), and selects a subset $S^w \subseteq [N]$ of size $|S^w| = \rho_w N$ to* write to *(corrupt). The writing is by adding to c an error vector e with $\mathsf{SUPP}(e) = S^w$, resulting in $c + e$ to be received. The adversary is adaptive and to select a component for reading and/or writing, it uses its knowledge of the codeword at the time. The subset $S = S^r \cup S^w$ of size $|S| = \rho N$, is the set of components of the codeword that the adversary reads or writes to.*

The AWTP channel is called a *restricted*-AWTP channel if $S_r = S_w = S$.

We assume the adversarial wiretap channel is one-way and can only be used by Alice.

Definition 33. *(Public Discussion Channel (PD Channel)) is an authenticated channel between Alice and Bob, that can be read by everyone including Eve.*

We assume the PD channel is two-way and can be used by Alice and Bob, both.

Hence in our $\mathsf{AWTP_{PD}}$ *setting Alice and Bob have access to a one-way AWTP channel and a two-way PD channel.* We consider protocols with multiple message rounds and assume in each message round a message is sent on one of the channels available to the communicants. In particular, in each message round Alice can use either the AWTP or the PD channel.

Definition 34. *The message round complexity RC_m of a protocol is the total number invocations of channels (AWTP and PD) by the two the communicants.*

5.3.2 $\mathsf{AWTP_{PD}}$ Protocol

Alice (sender) wants to send a message (information) $m \in \mathcal{M}$, securely and reliably to Bob (receiver), using a multi-round protocol over a $\mathsf{AWTP_{PD}}$ channel, called an $\mathsf{AWTP_{PD}}$ *protocol.*

The protocol consists of a sequence of message rounds. Each message round is in one of the following form: (i) Alice sends a message to Bob over AWTP channel, (ii) Alice sends

a message to Bob over PD channel, and (iii) Bob sends a message to Alice over the PD channel.

Let ℓ_c and ℓ_d denote the total number of invocations of the AWTP channel, and the PD channel, respectively, and assume $\ell = \ell_c + \ell_d$. Let r_A and r_B denote the randomness used by Alice and Bob, respectively.

The *protocol messages (also called codewords)* sent over the AWTP channel and the PD channel are denoted by c_i and d_i, respectively.

We use $c^i = \{c_1 \cdots c_i\}$ to denote the concatenation of protocol messages, transmitted over the AWTP channel after the i^{th} invocation of the AWTP channel. Similarly $d^i = \{d_1 \cdots d_i\}$ is the concatenation of protocol messages sent over PD, after the i^{th} invocation of this channel.

Let the protocol message alphabets of the AWTP and PD channels be Σ and $\mathbb{F}_2$, respectively. In the i^{th} invocation of the AWTP channel, Alice sends a codeword of length N_i. In the i^{th} invocation of the PD channel, Alice or Bob, sends a binary message of length n_i. The number of symbols sent over the AWTP channel is $N = \sum_{i=1}^{\ell_c} N_i$, and the number of bits transmitted over the PD, is $n = \sum_{i=1}^{\ell_d} n_i$.

Let the view of Alice and Bob when sending the i^{th} codeword be, v_A^i and v_B^i, respectively. The view of a participant consists of all the protocol messages that are received before sending the i^{th} codeword. When sending a message m, in the i^{th} invocation of the AWTP channel, Alice constructs a codeword c_i using her view, local randomness, and m,

$$c_i = \mathsf{AWTP}_{\mathsf{PD}}(m, r_A, i, v_A^i, \mathsf{AWTP}).$$

In each invocation of the PD channel, Alice (or Bob) generates the codeword d_i using their view, local randomness and m,

$$d_i = \mathsf{AWTP}_{\mathsf{PD}}(m, r_X, i, v_X^i, \mathsf{PD}),$$

where $X \in \{A, B\}$ if the protocol message constructed by Alice (Bob).

Definition 35 ((ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol)**.** *A secure* (ϵ, δ)-$\mathsf{AWTP_{PD}}$ *protocol satisfies the following two properties:*

1. *Secrecy: For any two messages* $m_1, m_2 \in \mathcal{M}$*, the statistical distance between Eve's views of the protocol, when the same random coins* $r_{\mathcal{A}}$ *are used by Eve, is bounded by* ϵ*,*

$$\max_{m_0, m_1} \mathbf{SD}(\mathsf{View}_{\mathcal{A}}(\mathsf{AWTP_{PD}}(m_1), r_{\mathcal{A}}), \mathsf{View}_{\mathcal{A}}(\mathsf{AWTP_{PD}}(m_2), r_{\mathcal{A}})) \leq \epsilon.$$

2. *Reliability: For any message* $M_{\mathcal{S}}$ *chosen by Alice, the probability that Bob outputs the message sent by Alice, is at least* $1 - \delta$*. That is,*

$$\mathsf{Pr}(M_{\mathcal{R}} \neq M_{\mathcal{S}}) \leq \delta.$$

Here probability is over the randomness of Alice and Bob and the adversary.

The $\mathsf{AWTP_{PD}}$ protocol provides *perfect secrecy* if $\epsilon = 0$. If adversary is passive, then Bob can always output the correct message $m_{\mathcal{S}}$ and $\mathsf{Pr}(M_{\mathcal{R}} = M_{\mathcal{S}}) = 1$. A *restricted* (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol is over a restricted $\mathsf{AWTP_{PD}}$ channel where $N_i = N_j$, $S_i = S_j = S$ for any $1 \leq i \leq j \leq \ell$. An $\mathsf{AWTP_{PD}}$ protocol is *optimal* if the message round complexity meets the minimum requirement of round complexity.

The efficiency measures of an (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol Π are, *(i) the information rate* $R(\Pi) = \frac{\log |\mathcal{M}|}{N \log |\Sigma|}$ *and, (ii) the message round complexity* $\mathsf{RC}(\Pi) = (r_{\mathsf{awtp}}, r_{\mathsf{pd}})$ *denoting the number of invocations of the AWTP and PD channels, respectively.*

Definition 36. *An* (ϵ, δ)-$\mathsf{AWTP_{PD}}$ *protocol family for a* (ρ_r, ρ_w)*-AWTP channel, is a family of protocols* $\mathbf{\Pi} = \{\Pi^N\}_{N \in \mathbb{N}}$*, where* $\Pi^N = (\epsilon, \delta)$-$\mathsf{AWTP_{PD}}$ *is an* $\mathsf{AWTP_{PD}}$ *protocol for the* (ρ_r, ρ_w)*-AWTP channel. A protocol family* $\mathbf{\Pi}$ *achieves* information rate $R(\mathbf{\Pi})$*, if for any* $\xi > 0$ *there exist* N_0 *such that for any* $N \geq N_0$*, there is* $\delta < \xi$ *and,*

$$\frac{\log |\mathcal{M}|}{N \log |\Sigma|} \geq R(\mathbf{\Pi}) - \xi.$$

The *ϵ-secrecy (perfect secrecy) capacity* C^{ϵ} *(*C^{0}*)* of a (ρ_r, ρ_w)-$\mathsf{AWTP_{PD}}$ channel is the largest achievable rate of all (ϵ, δ)-$\mathsf{AWTP_{PD}}$ ($(0, \delta)$-$\mathsf{AWTP_{PD}}$) protocol families for the channel.

Note that we effectively assume communication over PD is free and consider communication cost of the AWTP only.

5.4 Bounds on (ϵ, δ)-$\mathsf{AWTP_{PD}}$ Protocols

We derive two bounds for (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocols: an upper bound on the rate, and a lower bound on the minimum number of message rounds required for such protocols.

5.4.1 Upper Bound on Rate

Theorem 15. *The rate of an* (ϵ, δ)-$\mathsf{AWTP_{PD}}$ *protocol is bounded by,*

$$\mathsf{C}^{\epsilon} \leq 1 - \rho + 2\epsilon \cdot (1 + \log_{|\Sigma|} \frac{1}{\epsilon}) + 2\epsilon n.$$

In the following proof we assume $\rho_r + \rho_w = 1$, and $|S_i^r \cup S_i^w| = \rho N < N$ for $i = 1, \cdots, \ell_c$. The proof can be extended to $\rho_r + \rho_w > 1$ and $|S_i^r \cup S_i^w| = \rho N < N$ also. The proof outline is as follows. We define an adversary Adv_1 and prove an upper bound on the rate of any protocol over the $\mathsf{AWTP_{PD}}$ channel assuming this adversary. This gives an upper bound on the rate of the $\mathsf{AWTP_{PD}}$ protocol against any general adversary.

The proof has three steps.

First (Step1), we define a weak adversary that before the start of the protocol chooses, (i) the reading and writing sets of all invocations of the AWTP channel, and (ii) the random errors of appropriate weight for each AWTP channel invocation. For this adversary, we prove two lemmas (Lemmas 5.2 and 24) related to the entropy of the transmitted message. Second (Step 2), we use the lemmas to derive a bound on $\frac{\log |\mathcal{M}|}{N \log |\Sigma|}$. Finally (Step 3) we prove the bound on the channel capacity.

Notations. Let the codeword length in the i^{th} invocation of the AWTP channel be N_i, and $[N] = \bigcup_{i=1}^{\ell_c}[N_i]$. Let S_i^r and S_i^w denote the read and write sets of the adversary in the i^{th} invocation of the AWTP channel with $|S_i^r| = \rho_r N_i$ and $|S_i^w| = \rho_w N_i$, and denote $S^{i,r} = \{S_1^r, \cdots, S_i^r\}$ and $S^{i,w} = \{S_1^w, \cdots, S_i^w\}$.

Let $S_i^a = S_i^r \backslash S_i^w$ be the set of read only, $S_i^b = S_i^r \cap S_i^w$ the set of read and write, $S_i^c = S_i^w \backslash S_i^r$ the set of write only, and $S_i^d = [N_i] \backslash (S_i^r \cup S_i^w)$ the set of neither read nor write components, in the i^{th} invocation of the AWTP channel. Finally, $S^{\ell_c,a} = \cup_{i=1}^{\ell_c} S_i^a$, $S^{\ell_c,b} = \cup_{i=1}^{\ell_c} S_i^b$, $S^{\ell_c,c} = \cup_{i=1}^{\ell_c} S_i^c$, and $S^{\ell_c,d} = \cup_{i=1}^{\ell_c} S_i^d$.

Let c_i and d_i be the codewords transmitted over the AWTP channel and PD channel in the i^{th} invocations of the two channels, respectively; $c_{i,j}$ and $d_{i,j}$ denote the j^{th} components of codeword c_i and d_i, respectively; c^i and d^i denote concatenations of all codewords sent in all invocations up to, and including, the i^{th} invocations of the AWTP and the PD channels, respectively. We use capital letters to refer to the random variables associated with, c_i, d_i, $c_{i,j}$, $d_{i,j}, c^i$ and d^i, as $C_i, D_i, C_{i,j}, D_{i,j}, C^i$ and D^i, respectively. Let $C^{\ell_c,r}$ and $C^{\ell_c,w}$ be the random variables of the protocol messages on the sets $S^{\ell_c,r}$ and $S^{\ell_c,w}$, and $C^{\ell_c,a}$, $C^{\ell_c,b}$, $C^{\ell_c,c}$, $C^{\ell_c,d}$ be the random variables corresponding to the sets, $S^{\ell_c,a}, S^{\ell_c,b}, S^{\ell_c,c}, S^{\ell_c,d}$, respectively.

Proof. The proof has three steps:

Step 1.

We define an adversary Adv_1 that works as follows:

1. Selects the reading and writing sets $S^{\ell_c,r}$ and $S^{\ell_c,w}$, of all AWTP channel invocations, before the start of the protocol.
2. For each invocation, chooses a random error vector e_i of appropriate weight; that is, chooses e_i, with $\mathsf{SUPP}(e_i) \in S_i^w$ randomly with uniform distribution; we have $\mathsf{Pr}(e_i) = \frac{1}{|\Sigma|^{\rho_w N_i}}$.

3. During the protocol execution, uses the error vectors to corrupt the AWTP messages, reads the transmission on $S^{\ell_c,r}$ and over PD channel.

We give two lemmas that follow from ϵ-secrecy and δ-reliability of the (ϵ,δ)-$\mathsf{AWTP_{PD}}$ protocol against Adv_1. Let V_E denote the random variable of the adversary view at the end of the protocol.

Lemma 23. *For an (ϵ,δ)-$\mathsf{AWTP_{PD}}$ protocol, the following holds:*

$$\mathsf{I}(M;V_E) \leq 2\epsilon N \cdot \log(\frac{|\Sigma|}{\epsilon}) + 2\epsilon n.$$

Proof is in Section 5.7.1.

Since Adv_1 selects the reading sets $S^{\ell_c,r}$ before the start of the protocol, we have, $V_E = \{C^{\ell_c,r}, D^{\ell_d}\}$, and so, we have,

$$\mathsf{I}(M;C^{\ell_c,r}D^{\ell_d}) \leq 2\epsilon N \cdot \log(\frac{|\Sigma|}{\epsilon}) + 2\epsilon n. \tag{5.2}$$

Lemma 24. *For an (ϵ,δ)-$\mathsf{AWTP_{PD}}$ protocol, the following holds assuming Adv_1 adversary,*

$$\mathsf{H}(M|C^{\ell_c,a}C^{\ell_c,d}D^{\ell_d}) \leq \mathsf{H}(\delta) + \delta \log |\mathcal{M}|.$$

Proof is in Section 5.7.2.

Lemma 5.2 and Lemma 24 are used to prove an upper bound on the rate of an (ϵ,δ)-$\mathsf{AWTP_{PD}}$ protocol, assuming adversary Adv_1.

Step 2. We prove the upper bound,

$$\frac{\log|\mathcal{M}|}{N\log|\Sigma|} \leq 1-\rho+2\epsilon\cdot(1+\log_{|\Sigma|}\frac{1}{\epsilon}) + 2\epsilon n + 2\mathsf{H}(\delta) + \delta n.$$

Here, N is the total number of symbols sent over AWTP channel, and n is the number of bits sent over the PD channel. Let $\mathcal{C}^{\ell_c}$ and $\mathcal{D}^{\ell_d}$ denote the set of possible protocol messages over the AWTP channel and the PD channel, respectively. We have,

$$\mathsf{H}(M) = \mathsf{I}(M;C^{\ell_c,r}D^{\ell_d}) + \mathsf{H}(M|C^{\ell_c,r}D^{\ell_d}). \tag{5.3}$$

From Lemma 5.2, the first term can be upper bound as,

$$\mathsf{I}(M; C^{\ell_c,r} D^{\ell_d}) \leq 2\epsilon \cdot N \log(\frac{|\Sigma|}{\epsilon}) + 2\epsilon n. \tag{5.4}$$

The upper bound on the second item $\mathsf{H}(M|C^{\ell_c,r} D^{\ell_d})$ is,

$$\begin{aligned}
&\mathsf{H}(M|C^{\ell_c,r}, D^{\ell_d}) \\
&= \mathsf{H}(M|C^{\ell_c,a}, C^{\ell_c,b}, D^{\ell_d}) \\
&= \mathsf{H}(M, C^{\ell_c,b}|C^{\ell_c,a}, D^{\ell_d}) - \mathsf{H}(C^{\ell_c,b}|C^{\ell_c,a}, D^{\ell_d}) \\
&= \mathsf{H}(M|C^{\ell_c,a}, D^{\ell_d}) + \mathsf{H}(C^{\ell_c,b}|M, C^{\ell_c,a}, D^{\ell_d}) - \mathsf{H}(C^{\ell_c,b}|C^{\ell_c,a}, D^{\ell_d}) \\
&= \mathsf{H}(M, C^{\ell_c,d}|C^{\ell_c,a}, D^{\ell_d}) - \mathsf{H}(C^{\ell_c,d}|M, C^{\ell_c,a}, D^{\ell_d}) + \mathsf{H}(C^{\ell_c,b}|M, C^{\ell_c,a}, D^{\ell_d}) - \mathsf{H}(C^{\ell_c,b}|C^{\ell_c,a}, D^{\ell_d}) \\
&= \mathsf{H}(M|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) + \mathsf{H}(C^{\ell_c,d}|C^{\ell_c,a}, D^{\ell_d}) \\
&\quad - \mathsf{H}(C^{\ell_c,d}|M, C^{\ell_c,a}, D^{\ell_d}) \\
&\quad + \mathsf{H}(C^{\ell_c,b}|M, C^{\ell_c,a}, D^{\ell_d}) - \mathsf{H}(C^{\ell_c,b}|C^{\ell_c,a}, D^{\ell_d}) \\
&\overset{(1)}{\leq} \mathsf{H}(M|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) + \mathsf{H}(C^{\ell_c,d}|C^{\ell_c,a}, D^{\ell_d}) - \mathsf{H}(C^{\ell_c,d}|M, C^{\ell_c,a}, D^{\ell_d}) \\
&\overset{(2)}{\leq} \mathsf{H}(M|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) + \mathsf{H}(C^{\ell_c,d}).
\end{aligned} \tag{5.5}$$

Inequality (1) is from, $\mathsf{H}(C^{\ell_c,b}|M, C^{\ell_c,a}, D^{\ell_d}) \leq \mathsf{H}(C^{\ell_c,b}|C^{\ell_c,a}, D^{\ell_d})$. Inequality (2) follows from, $\mathsf{H}(C^{\ell_c,d}|C^{\ell_c,a}, D^{\ell_d}) \leq \mathsf{H}(C^{\ell_c,d})$ and $\mathsf{H}(C^{\ell_c,d}|M, C^{\ell_c,a}, D^{\ell_d}) \geq 0$.

From $\mathsf{H}(C^{\ell_c,d}) \leq \log|\mathcal{C}^{\ell_c,d}| \leq N(1-\rho)\log|\Sigma|$, we have,

$$\mathsf{H}(C^{\ell_c,d}) \leq N(1-\rho)\log|\Sigma|. \tag{5.6}$$

Using Lemma 24, we have,

$$\mathsf{H}(M|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \leq \delta \log|\mathcal{M}| + \mathsf{H}(\delta). \tag{5.7}$$

From (5.5), (5.6), (5.7), we have,

$$\mathsf{H}(M|C^{\ell_c,r}, D^{\ell_d}) \leq N(1-\rho)\log|\Sigma| + \delta\log|\mathcal{M}| + \mathsf{H}(\delta). \tag{5.8}$$

We also have,

$$\log|\mathcal{M}| \overset{(1)}{\leq} \log|\mathcal{C}^{\ell_c}\mathcal{D}^{\ell_d}| \overset{(2)}{\leq} N\log|\Sigma| + n. \tag{5.9}$$

where $\mathcal{C}^{\ell_c}\mathcal{D}^{\ell_d}$ are possible (error free) transcripts of the protocol generated by the protocol encoders (at Alice and Bob), (1) is because decoding without adversarial error recovers the message and so the number of possible encoding transcripts is $\geq |\mathcal{M}|$, and (2) is because of the set of corrupted transcripts is larger than uncorrupted ones.

Using (5.8) and (5.9), we have,

$$\mathsf{H}(M|C^{\ell_c,r}, D^{\ell_d}) \leq N(1-\rho)\log|\Sigma| + \delta(N\log|\Sigma| + n) + \mathsf{H}(\delta). \tag{5.10}$$

Using (5.3), (5.4), and (5.10), gives the upper bound on $\mathsf{H}(M)$,

$$\mathsf{H}(M) \leq N(1-\rho)\log|\Sigma| + 2\epsilon\cdot N\log(\frac{|\Sigma|}{\epsilon}) + 2\epsilon n + \delta N\log|\Sigma| + \delta n + \mathsf{H}(\delta).$$

The above inequality must hold for any distribution on $\mathcal{M}$, and in particular for a uniform distribution with $\mathsf{H}(M) = \log|\mathcal{M}|$. Using $\delta \leq \mathsf{H}(\delta)$ for $0 \leq \delta \leq 1/2$, we have,

$$\frac{\log|\mathcal{M}|}{N\log|\Sigma|} \leq 1 - \rho + 2\epsilon\cdot(1 + \log_{|\Sigma|}\frac{1}{\epsilon}) + 2\epsilon n + 2\mathsf{H}(\delta) + \delta n.$$

Step 3. We show that ϵ-secrecy capacity of a (ρ_r, ρ_w)-$\mathsf{AWTP}_{\mathsf{PD}}$ is bounded by,

$$\mathsf{C}^{\epsilon} \leq 1 - \rho + 2\epsilon\cdot(1 + \log_{|\Sigma|}\frac{1}{\epsilon}) + 2\epsilon n.$$

Proof is by contradiction.

Let $\mathsf{C}^{\epsilon} = 1-\rho+2\epsilon\cdot(1+\log_{|\Sigma|}\frac{1}{\epsilon})+2\epsilon n+\hat{\xi}$, for some small constant $\hat{\xi} > 0$. From Definition 36, for any $0 < \hat{\xi}' \leq \min(\frac{\hat{\xi}}{5n}, \mathsf{H}^{-1}(\frac{\hat{\xi}}{5}))$, there is N_0, such that for any $N > N_0$, we have $\delta < \hat{\xi}'$ and,

$$\begin{aligned}
\frac{\log|\mathcal{M}|}{N\log|\Sigma|} &\geq \mathsf{C}^{\epsilon} - \hat{\xi}' \\
&= 1 - \rho + 2\epsilon\cdot(1 + \log_{|\Sigma|}\frac{1}{\epsilon}) + 2\epsilon n + 2\mathsf{H}(\delta) + \delta n + \hat{\xi} - \hat{\xi}' - 2\mathsf{H}(\delta) - \delta n \\
&\geq 1 - \rho + 2\epsilon\cdot(1 + \log_{|\Sigma|}\frac{1}{\epsilon}) + 2\epsilon n + 2\mathsf{H}(\delta) + \delta n + \hat{\xi}' \\
&> \frac{\log|\mathcal{M}|}{N\log|\Sigma|}.
\end{aligned}$$

This contradicts the bound on $\frac{\log|\mathcal{M}|}{N\log|\Sigma|}$, and so,

$$\mathsf{C}^{\epsilon} \leq 1-\rho+2\epsilon\cdot(1+\log_{|\Sigma|}\frac{1}{\epsilon})+2\epsilon n.$$

□

Corollary 7. *The perfect secrecy capacity of a* (ρ_r,ρ_w)-$\mathsf{AWTP_{PD}}$ *channel is bounded as,*

$$\mathsf{C}^0 \leq 1-\rho.$$

5.4.2 Lower Bound on Message Round Complexity

An efficient construction of a $(0,\delta)$-AWTP code (one message round) with rate $\mathsf{R}=1-\rho_r-\rho_w$ is given in [86] (Section 4.5), implying that secure transmission over AWTP channels with one message round protocols is possible if, $\rho_r+\rho_w<1$. In Section 5.4.1, we proved that for $\mathsf{AWTP_{PD}}$ channels, $\mathsf{C}^0 \leq 1-\rho$ and so secure communication with $\rho_r+\rho_w>1$ may be possible, as long as $\rho<1$.

Theorem 16. *Perfectly secure communication over* $\mathsf{AWTP_{PD}}$ *channel requires,*
(i) one message round protocol, if $\rho_r+\rho_w<1$.
(ii) a protocol with at least three message rounds, if $\rho_r+\rho_w\geq 1$. *That is,*

$$\mathsf{RC}\begin{cases}\geq 1 & \text{if } \rho_r+\rho_w<1;\\ \geq 3 & \text{if } \rho_r+\rho_w\geq 1.\end{cases}$$

We use the same notations as in Section 5.4.1.

Proof. We only need to prove (ii). The protocol must have at least two message rounds and so can have one of the following forms. Note that to achieve privacy, at least one message round of AWTP channel is needed.

1. Rnd 1: Alice $\overset{\mathsf{AWTP}}{\longrightarrow}$ Bob; Rnd 2: Alice $\overset{\mathsf{PD}}{\longrightarrow}$ Bob.
2. Rnd 1: Alice $\overset{\mathsf{AWTP}}{\longrightarrow}$ Bob; Rnd 2: Alice $\overset{\mathsf{AWTP}}{\longrightarrow}$ Bob.

3. Rnd 1: Alice $\stackrel{\mathsf{AWTP}}{\longrightarrow}$ Bob; Rnd 2: Bob $\stackrel{\mathsf{PD}}{\longrightarrow}$ Alice.

4. Rnd 1: Alice $\stackrel{\mathsf{PD}}{\longrightarrow}$ Bob; Rnd 2: Alice $\stackrel{\mathsf{AWTP}}{\longrightarrow}$ Bob.

5. Rnd 1: Bob $\stackrel{\mathsf{PD}}{\longrightarrow}$ Alice; Rnd 2: Alice $\stackrel{\mathsf{AWTP}}{\longrightarrow}$ Bob.

The third, fourth and fifth forms are not possible: in all these cases Bob's decoder will have the vector received through a one round AWTP channel and so the protocol cannot have rate higher than $1 - \rho_r - \rho_w$.

We show that it is impossible to have first and second forms of $\mathsf{AWTP}_{\mathsf{PD}}$ protocol.

Lemma 25. *In an* $(0, \delta)$-$\mathsf{AWTP}_{\mathsf{PD}}$ *protocol of the forms (1) or (2) above, if* $\rho_r + \rho_w \geq 1$*, then,*

$$2\mathsf{H}(\delta) \geq 1 - \frac{1}{|\mathcal{M}|}.$$

Proof is in Section 5.7.3.

Since all forms of two rounds $\mathsf{AWTP}_{\mathsf{PD}}$ protocol is impossible, it implies the message round complexity of $\mathsf{AWTP}_{\mathsf{PD}}$ protocol is at least three.

□

5.5 An optimal $(0, \delta)$-$\mathsf{AWTP}_{\mathsf{PD}}$ Protocol

We show the construction of $\mathsf{AWTP}_{\mathsf{PD}}$ protocol. The rate of the protocol meets the upper bound. The protocol has three message rounds and so meets the minimum message round complexity. The construction is inspired by Shi *et al.* [75].

Let the AWTP channel have alphabet $\Sigma = \mathbb{F}_q^u$ where $q > 2uN^2$, and the message be $\mathbf{m} = \{m_1, \cdots, m_\ell\} \in \mathcal{M}$, where $m_i \in \mathbb{F}_q$. Let N denote the transmission length over the AWTP channel. Our construction uses the $\frac{u}{q}$-Δ universal (q, q^{u-1}, q)-hash family and the seedless $(uN, \ell, \ell \log q, 0)$-extractor.

$\mathsf{AWTP}_{\mathsf{PD}}$ Protocol

- Rnd 1: Alice $\stackrel{\mathsf{AWTP}}{\longrightarrow}$ Bob. For $i \in N$:

  Alice randomly chooses a vector $\mathbf{r}_i = \{r_{i,1}, \cdots, r_{i,u-1}\} \in \mathbb{F}_q^{u-1}$, and $\beta_i \in \mathbb{F}_q$. Alice sends $c = (c_1, \cdots, c_N) \in \mathbb{F}_q^u$ with $c_i = \{\mathbf{r}_i, \beta_i\}$ to Bob, over the AWTP channel.

  Bob receives $y = (y_1, \cdots, y_N)$, where $y_i = \{\mathbf{r}'_i, \beta'_i\}$.

- Rnd 2: Bob $\stackrel{\mathsf{PD}}{\longrightarrow}$ Alice.

  Bob generates random keys, $(\alpha_1, \cdots, \alpha_N)$, $\alpha_i \in \mathbb{F}_q$, for the hash family, and generates $\mathbf{t} = (t_1, \cdots, t_N)$ where, $t_i = \mathsf{hash}_{\alpha_i}(\mathbf{r}'_i) + \beta'_i \mod q$. Bob maps $d_1 = \{\alpha_1, \cdots, \alpha_N, t_1, \cdots, t_N\}$ to a binary vector over $\mathbb{F}_2$, and sends d_1 to Alice, over the PD channel. Alice receives d_1.

- Rnd 3: Alice $\stackrel{\mathsf{PD}}{\longrightarrow}$ Bob.

  - Alice checks,

    $$\mathsf{hash}_{\alpha_i}(\mathbf{r}_i) + \beta_i \stackrel{?}{=} t_i \mod q,\ i = 1 \cdots N$$

    and constructs a binary vector $\mathbf{v} = (v_1, \cdots, v_N)$, where with $v_i = 1$ if $\mathsf{hash}_{\alpha_i}(\mathbf{r}_i) + \beta_i = t_i \mod q$, and $v_i = 0$, otherwise.

  - Let, $v_{i_1} \cdots = v_{i_s} = 1$. Alice does the following.

    –concatenates all $\mathbf{r}_{i_j}$ for which $v_{i_j} = 1$, and obtains $(\mathbf{r}_{i_1} || \cdots || \mathbf{r}_{i_s})$ over $\mathbb{F}_q$.

    –uses the extractor on this string, and obtains a uniformly random string, $\mathbf{k} = \mathsf{Ext}(\mathbf{r}_{i_1} || \cdots || \mathbf{r}_{i_s})$.

  - Alice encrypts the message $\mathbf{m}$ and obtains $\mathbf{c} = \{c_1, \cdots, c_\ell\}$, where $c_i = k_i + m_i \mod q$ for $i = 1, \cdots, \ell$. Alice maps $d_2 = \{\mathbf{c}, \mathbf{v}\}$ (over $\mathbb{F}_q$) into a binary vector and sends it to Bob over the PD channel.

    Bob receives d_2.

- Bob decodes $\mathsf{Dec}(y_1, d_1, d_2)$ as follows.

– Constructs the vector $(\mathbf{r}'_{i_1}||\cdots||\mathbf{r}'_{i_s})$ with $\mathbf{r}'_{i_j} \in \mathbb{F}_q$, for all $v_{i_j} = 1$ in $\mathbf{v}$. He uses the extractor to obtain, $\mathbf{k}' = \mathsf{Ext}(\mathbf{r}'_{i_1}||\cdots||\mathbf{r}'_{i_s})$.

– Recovers the message $\mathbf{m}'$ with $m'_i = c_i - k'_i \mod q$ for $i = 1, \cdots, \ell$.

Secrecy and Reliability

Lemma 26. *The* $\mathsf{AWTP}_{\mathsf{PD}}$ *protocol above, provides perfect secrecy if* $\ell \leq (u-1)(1-\rho)N$.

Proof. First, assume the adversary reads the last $\rho_r N$ components of c, and the first $(1-\rho)N$ components is the set of components that is neither read, nor written to, by the adversary. Let $v'_{\mathcal{A}} = \{\mathbf{r}_{(1-\rho_r)N+1} \cdots \mathbf{r}_N, \beta_{(1-\rho_r)N+1} \cdots \beta_N, \alpha_1 \cdots \alpha_N, t_1 \cdots t_N, v_0 \cdots v_N\}$ denote the view of the adversary, except for $\mathbf{c}$.

If $\ell \leq (u-1)(1-\rho)N$, the vector of random variables, $(\mathbf{r}_{i_1}||\cdots||\mathbf{r}_{i_s})$, corresponds to a symbol-fixing source. The components that the adversary do not read are uniformly distributed and are independent from the adversary's view $v'_{\mathcal{A}}$, and the components that the adversary reads are determined and fixed. So the randomness $\mathbf{k}$ that is generated from the extractor, is uniformly distributed and is independent of the adversarial view. That is,

$$\mathsf{Pr}(\mathbf{k}|v'_{\mathcal{A}}) = \mathsf{Pr}(\mathbf{k}). \tag{5.11}$$

Second, since Alice selects the message $\mathbf{m} \in \mathcal{M}$ independent from $\mathbf{k}$ and $v'_{\mathcal{A}}$, we have $\mathsf{Pr}(\mathbf{m}|\mathbf{k}, v'_{\mathcal{A}}) = \mathsf{Pr}(\mathbf{m})$. For any message $\mathbf{m} \in \mathcal{M}$, we have,

$$\mathsf{Pr}(\mathbf{m}) \leq \mathsf{Pr}(\mathbf{m}|v'_{\mathcal{A}}) \leq \mathsf{Pr}(\mathbf{m}|\mathbf{k}, v'_{\mathcal{A}}) = \mathsf{Pr}(\mathbf{m}).$$

This implies,

$$\mathsf{Pr}(\mathbf{m}) = \mathsf{Pr}(\mathbf{m}|v'_{\mathcal{A}}) = \mathsf{Pr}(\mathbf{m}|\mathbf{k}, v'_{\mathcal{A}}). \tag{5.12}$$

and so we have,

$$\begin{aligned}\mathsf{Pr}(\mathbf{k}|\mathbf{m}, v'_{\mathcal{A}}) &= \frac{\mathsf{Pr}(\mathbf{k}, \mathbf{m}, v'_{\mathcal{A}})}{\mathsf{Pr}(\mathbf{m}, v'_{\mathcal{A}})} \\ &= \frac{\mathsf{Pr}(\mathbf{m}|\mathbf{k}, v'_{\mathcal{A}})\mathsf{Pr}(\mathbf{k}, v'_{\mathcal{A}})}{\mathsf{Pr}(\mathbf{m}|v'_{E})\mathsf{Pr}(v'_{\mathcal{A}})} \\ &= \mathsf{Pr}(\mathbf{k}|v'_{\mathcal{A}}).\end{aligned} \tag{5.13}$$

Third, the adversarial view for any $\mathbf{m} \in \mathcal{M}$ is $v_{\mathcal{A}} = \{\mathbf{c}, v'_{\mathcal{A}}\}$, and so,

$$\begin{aligned}\mathsf{Pr}(v_{\mathcal{A}}|\mathbf{m}) &= \mathsf{Pr}(\mathbf{c}, v'_{\mathcal{A}}|\mathbf{m}) \\ &= \mathsf{Pr}(\mathbf{c}|\mathbf{m}, v'_{\mathcal{A}})\mathsf{Pr}(v'_{\mathcal{A}}|\mathbf{m}) \\ &\overset{(1)}{=} \mathsf{Pr}(\mathbf{k}|\mathbf{m}, v'_{\mathcal{A}})\mathsf{Pr}(v'_{\mathcal{A}}) \\ &\overset{(2)}{=} \mathsf{Pr}(\mathbf{k})\mathsf{Pr}(v'_{\mathcal{A}}).\end{aligned}$$

where, (1) is from $c_i = k_i + m_i \mod q$ for $i = 1 \cdots \ell$, and (2) is from (5.11) and (5.13).

This means the statistical distance between adversarial views of any two messages $\mathbf{m}_1, \mathbf{m}_2 \in \mathcal{M}$, is zero and the $\mathsf{AWTP}_{\mathsf{PD}}$ protocol is perfectly secure. That is,

$$\mathbf{SD}(\mathsf{View}_{\mathcal{A}}|\mathbf{m}_1, \mathsf{View}_{\mathcal{A}}|\mathbf{m}_2) = \sum_{v_{\mathcal{A}} \in \mathsf{View}_{\mathcal{A}}} |\mathsf{Pr}(v_{\mathcal{A}}|\mathbf{m}_1) - \mathsf{Pr}(v_{\mathcal{A}}|\mathbf{m}_2)| = 0.$$

□

Lemma 27. *The probability of decoding error in the* $\mathsf{AWTP}_{\mathsf{PD}}$ *protocol is* $\delta \leq \frac{uN}{q}$.

Proof. First, we show the probability that vector $(\mathbf{r}_{i_1}, \cdots, \mathbf{r}_{i_s}) \neq (\mathbf{r}'_{i_1}, \cdots, \mathbf{r}'_{i_s})$ is no more than $\frac{uN}{q}$. This is from,

$$\begin{aligned}&\mathsf{Pr}((\mathbf{r}_{i_1}, \cdots, \mathbf{r}_{i_s}) \neq (\mathbf{r}'_{i_1}, \cdots, \mathbf{r}'_{i_s})) \\ &\leq \sum_{i=1}^{N} \mathsf{Pr}(\mathbf{r}_i \neq \mathbf{r}'_i) \\ &= \sum_{i=1}^{N} \mathsf{Pr}(\mathbf{r}_i \neq \mathbf{r}'_i, v_i = 1) \\ &\leq \sum_{i=1}^{N} \mathsf{Pr}(\mathbf{r}_i \neq \mathbf{r}'_i, [\mathsf{hash}_{\alpha_i}(\mathbf{r}_i) - \mathsf{hash}_{\alpha_i}(\mathbf{r}'_i)] = [\beta'_i - \beta_i]) \\ &\leq \frac{uN}{q}\end{aligned} \tag{5.14}$$

Second, for the two random vectors $\mathbf{k} = \mathsf{Ext}(\mathbf{r}_{i_1}, \cdots, \mathbf{r}_{i_s})$ and $\mathbf{k}' = \mathsf{Ext}(\mathbf{r}'_{i_1}, \cdots, \mathbf{r}'_{i_s})$, we have,

$$\mathsf{Pr}(\mathbf{k} \neq \mathbf{k}') \leq \mathsf{Pr}((\mathbf{r}_{i_1}, \cdots, \mathbf{r}_{i_s}) \neq (\mathbf{r}'_{i_1}, \cdots, \mathbf{r}'_{i_s})). \tag{5.15}$$

Third, Bob correctly receives $d_2 = \{\mathbf{c}, \mathbf{v}\}$ sent by Alice and so, $m_i + k_i = m'_i + k'_i \mod q$ for $i = 1 \cdots \ell$. That is, the probability that the message $\mathbf{m} \neq \mathbf{m}'$, is the same as the probability $\mathbf{k} \neq \mathbf{k}'$. That is,

$$\mathsf{Pr}(\mathbf{m} \neq \mathbf{m}') = \mathsf{Pr}(\mathbf{k} \neq \mathbf{k}'). \tag{5.16}$$

From (5.14) (5.15) (5.16), there is $\mathsf{Pr}(\mathbf{m} \neq \mathbf{m}') = \mathsf{Pr}(\mathbf{k} \neq \mathbf{k}') \leq \frac{uN}{q}$. □

Rate of $\mathsf{AWTP}_{\mathsf{PD}}$ Protocol

Lemma 28. *The rate of the $\mathsf{AWTP}_{\mathsf{PD}}$ protocol family is $R(\mathbf{\Pi}) = 1 - \rho$.*

Proof. For a small $\xi > 0$, let the parameters of $\mathsf{AWTP}_{\mathsf{PD}}$ protocol be chosen as $u = \frac{1}{\xi}$, $q > 2uN^2$, $\ell = (u-1)(1-\rho)N$, $N_0 \geq \frac{1}{\xi}$ and $\Sigma = \mathbb{F}_q^u$. For uniform message distribution, we have $\log|\mathcal{M}| = \ell \log q$, and so for any $N > N_0$, the rate of $\mathsf{AWTP}_{\mathsf{PD}}$ protocol family is given by,

$$R(\Pi^N) = \frac{\log|\mathcal{M}|}{N \log|\Sigma|} = \frac{(u-1)(1-\rho)N \log q}{uN \log q} = (1-\xi)(1-\rho) \geq 1 - \rho - \xi.$$

The probability of decoding error is bounded by,

$$\delta \leq \frac{uN}{q} \leq \frac{1}{2N} \leq \frac{\xi}{2} \leq \xi.$$

It implies the rate of $\mathsf{AWTP}_{\mathsf{PD}}$ protocol family is $R(\mathbf{\Pi}) = 1 - \rho$. □

Theorem 17. *For any small $\xi > 0$, the protocol above is a $(0, \delta)$-$\mathsf{AWTP}_{\mathsf{PD}}$ protocol with rate $\mathsf{R}(\Pi^N) = 1 - \rho - \xi$. The transmission alphabet over the AWTP channel is of size $|\Sigma| = q^{\frac{1}{\xi}}$, and the decoding error is $\delta < \xi$. The rate of the protocol approaches $\mathsf{R} = 1 - \rho$ as, $N \to \infty$. The protocol has RC=3 and the decoder computation is $\mathcal{O}((N \log q)^2)$.*

5.6 $\mathsf{AWTP}_{\mathsf{PD}}$ Protocol and SMT-PD

AWTP codes are defined over an alphabet Σ and all components of a codeword are elements of Σ. In SMT protocols however, the set of transmissions over different wires may be different.

Definition 37 (Symmetric SMT)**.** *An SMT protocol is called a* symmetric *if the protocol remains invariant under any permutation of the wires.*

Let $\mathcal{W}_j^i, j = 1 \cdots N, i = 1 \cdots r$, denote the set of possible transmissions on wire j in an r-round SMT protocol. For a symmetric protocol, $\mathcal{W}_j^i = \mathcal{W}^i$ is independent of j. *All known constructions of threshold SMT protocols are symmetric.*

Definition 38. *A* one-way symmetric secure message transmission with public discussion ((ϵ, δ)-SMT$^{[ows]}$-PD) protocol *is an SMT-PD protocol in which transmission over wires is in one direction (from Alice to Bob, or Bob to Alice). The protocol is invariant under any permutation of the wires. The N wires and the PD channel, can be invoked simultaneously.*

We consider protocols where Alice wants to send a message to Bob and so AWTP channel is used by Alice.

Theorem 18. *There is a one-to-one correspondence between restricted (ϵ, δ)-$\mathsf{AWTP}_{\mathsf{PD}}$ protocols and (ϵ, δ)-SMT$^{[ows]}$-PD protocols. The following results on the latter protocols, follow from the results on the former in Section 5.4.*

1. *The lower bound on the transmission rate of a (ϵ, δ)-SMT$^{[ows]}$-PD protocol is,*

$$\mathsf{TR} \geq \frac{N}{N - t + \epsilon' + 2\mathsf{H}(\delta)N + \delta nN}. \tag{5.17}$$

where $\epsilon' = 2N\epsilon(1 + \log_{|\mathcal{W}|} \frac{1}{\epsilon}) + 2\epsilon nN$.

For protocols with perfect secrecy ($\epsilon = 0$) we have,

$$\mathsf{TR} \geq \frac{N}{N - t + 2\mathsf{H}(\delta)N + \delta nN}. \tag{5.18}$$

2. The lower bound on the round complexity of (ϵ, δ)-SMT$^{[ow]}$-PD protocol is three.

The one-to-one correspondence follows from definitions of the protocols and their security. The lower bound on transmission rate follows by noting that the transmission rate of a (ϵ, δ)-SMT$^{[ows]}$-PD protocol is the inverse of the rate of the corresponding $\mathsf{AWTP_{PD}}$ protocol, and so the upper bound on the rate of $\mathsf{AWTP_{PD}}$ protocols implies a lower bound on the transmission rate of (ϵ, δ)-SMT$^{[ows]}$-PD protocols. The lower bound on the round complexity follows from the bound on the corresponding $\mathsf{AWTP_{PD}}$ protocols. Details are given in Appendix 5.7.4.

Construction

A (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol gives a restricted-(ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol with $\rho = \rho_r = \rho_w$. This latter, using the protocol conversion in Theorem 18, gives an (ϵ, δ)-SMT$^{[ows]}$-PD protocol. In Section 5.5 we gave the construction of a $(0, \delta)$-$\mathsf{AWTP_{PD}}$ protocol with minimum number of rounds, and rate approaching the capacity of the (ρ_r, ρ_w)-AWTP channel. This leads to the following.

Lemma 29. *There is a three round (ϵ, δ)-SMT$^{[ows]}$-PD protocol, with transmission rate, $\mathcal{O}(\frac{N}{N-t})$, and decoding computational complexity equal to, $\mathcal{O}((N \log q)^2)$.*

Comparison with known results

The SMT-PD protocols were first considered in [34]. It was shown that secure protocols exist for $N \geq t + 1$, and the following lower bound on the transmission rate of the protocols were derived.

$$\mathsf{TR} \geq \frac{N \cdot (-\log(\frac{1}{|\mathcal{M}|} + 2\epsilon) - \mathsf{H}(\sqrt{\delta}) - 2m\sqrt{\delta})}{(N-t)m}. \tag{5.19}$$

where, $m = \log |\mathcal{M}|$. The bound also gives a lower bound on the transmission rate of (ϵ, δ)-SMT$^{[ows]}$-PD protocols as these protocols are a subset of SMT-PD protocols. The two bounds, (5.17) and (5.19), are not directly comparable. For example, for $\epsilon = 0$ and $\delta > 0$, (5.19) will be a tighter bound. For $\delta \approx 0$ and $\epsilon = \frac{a}{|\mathcal{M}|}$ however, (5.17) could be higher (for

example $|\mathcal{M}| = 2^N$ and $\epsilon = \frac{1}{|\mathcal{M}|}$). For perfectly secure SMT-PD protocols, (5.19) is a tighter bound.

The lower bound on the round complexity of $\mathsf{AWTP_{PD}}$ protocols cannot be directly used for (ϵ, δ)-SMT$^{[ows]}$-PD because in the latter Alice can use her two channels simultaneously. In [75], it was shown that the minimum round complexity of general SMT-PD protocols is three. Since (ϵ, δ)-SMT$^{[ows]}$-PD satisfying the rate bound are a subset of SMT-PD satisfying the rate bound, the minimum RC of the latter is lower bounded by the minimum RC of the former. The rate-optimal (ϵ, δ)-SMT$^{[ows]}$-PD protocol from Section 5.5 has three rounds and so it achieves the lower bound on the $\mathsf{RC}$of (ϵ, δ)-SMT$^{[ows]}$-PD protocols.

5.7 Proof of Chapter 5

5.7.1 Proof of Lemma 23

Proof. The proof is similar to Theorem 4.9 [6] and uses Pinsker's Lemma:

Lemma 30. *Let P, Q be probability distributions. Let $\mathbf{SD}(P, Q) \leq \epsilon$. Then*

$$\mathsf{H}(P) - \mathsf{H}(Q) \leq 2\epsilon \cdot \log(\frac{|P \cup Q|}{\epsilon}).$$

Let the random variable of the adversarial view, V_E, be over the set V_E. According to the definition of ϵ-secrecy (Definition 35), for any pair of message $m_1, m_2 \in \mathcal{M}$, the statistical distance between the distribution of V_E when Alice sends m_1, and the distribution of V_E when Alice sends m_2, is no more than ϵ. That is,

$$\begin{aligned}\epsilon &\geq \max_{m_1,m_2} \mathbf{SD}(V_E|M = m_1, V_E|M = m_2) \\ &\geq \max_{m_1,m_2} \sum_{v \in \mathcal{V}_E} |\mathsf{Pr}(v|m_1) - \mathsf{Pr}(v|m_2)|.\end{aligned}$$

Assuming distribution $\Pr(m)$ on $\mathcal{M}$, this implies,

$$\begin{aligned}
&\mathbf{SD}(V_E, V_E|M=m) \\
&= \frac{1}{2}\sum_{v\in\mathcal{V}_E} |\mathsf{Pr}(v|m) - \mathsf{Pr}(v)| \\
&= \frac{1}{2}\sum_{v\in\mathcal{V}_E} |\mathsf{Pr}(v|m) - \sum_{m'} \mathsf{Pr}(v|m')\mathsf{Pr}(m')| \\
&= \frac{1}{2}\sum_{v\in\mathcal{V}_E} |\sum_{m'} \mathsf{Pr}(m')(\mathsf{Pr}(v|m) - \mathsf{Pr}(v|m'))| \\
&\leq \frac{1}{2}\sum_{v\in\mathcal{V}_E}\sum_{m'} \mathsf{Pr}(m')|\mathsf{Pr}(v|m) - \mathsf{Pr}(v|m')| \\
&= \sum_{m'} \mathsf{Pr}(m')\frac{1}{2}\sum_{v\in\mathcal{V}_E} |\mathsf{Pr}(v|m) - \mathsf{Pr}(v|m')| \\
&\leq \sum_{m'} \mathsf{Pr}(m') \max_{m_1,m_2} \mathbf{SD}(V_E|M=m_1, V_E|M=m_2) \\
&\leq \epsilon.
\end{aligned} \tag{5.20}$$

From Pinsker Lemma and Eq. (5.20), we have,

$$\mathsf{H}(V_E) - \mathsf{H}(V_E|M=m) \leq 2\epsilon \cdot \log(\frac{|\mathcal{V}_E|}{\epsilon}).$$

From $|\mathcal{V}_E| \leq 2^n \times |\Sigma|^N$, it implies,

$$\mathsf{H}(V_E) - \mathsf{H}(V_E|M=m) \leq 2\epsilon \cdot \log(\frac{|\Sigma|^N}{\epsilon}) + 2\epsilon n.$$

So the difference between $\mathsf{H}(M)$ and $\mathsf{H}(M|V_E)$ is

$$\begin{aligned}
\mathsf{H}(M) - \mathsf{H}(M|V_E) &= \mathsf{H}(V_E) - \mathsf{H}(V_E|M) \\
&= \mathsf{H}(V_E) - \sum_{m\in\mathcal{M}} \mathsf{Pr}(m)\mathsf{H}(V_E|m) \\
&= \sum_{m\in\mathcal{M}} \mathsf{Pr}(m)(\mathsf{H}(V_E) - \mathsf{H}(V_E|m)) \\
&\leq 2\epsilon N \cdot \log(\frac{|\Sigma|}{\epsilon}) + 2\epsilon n.
\end{aligned} \tag{5.21}$$

□

5.7.2 Proof of Lemma 24

Proof. Let $\delta' = \mathsf{H}(\delta) + \delta \log |\mathcal{M}|$. The proof has two steps.

1. We show that $\mathsf{H}(M|C^{\ell_c,a}, Y^{\ell_c,w}, C^{\ell_c,d}, D^{\ell_d}) \leq \delta'$.

   Let $\delta = \Pr(M_{\mathcal{R}} \neq M_{\mathcal{S}})$. From Fano's inequality,

   $$\mathsf{H}(\delta) + \delta \log |\mathcal{M}| \geq \mathsf{H}(M_{\mathcal{S}}|M_{\mathcal{R}}) \geq \mathsf{H}(M_{\mathcal{S}}|Y^{\ell_c}, D^{\ell_d}).$$

   Here $\{y^{\ell_c}, d^{\ell_d}\}$, is the received vectors of Bob. Since $y^{\ell_c} = \{c^{\ell_c,a}, y^{\ell_c,w}, c^{\ell_c,d}\}$, we have,

   $$\mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}, Y^{\ell_c,w}, C^{\ell_c,d}, D^{\ell_d}) \leq \mathsf{H}(M_{\mathcal{S}}|M_{\mathcal{R}}) \leq \delta'. \tag{5.22}$$

2. We show that

   $$\mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \leq \delta' + \mathsf{I}(Y^{\ell_c,w}; C^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}).$$

   Writing the conditional entropy in two ways, we have,

   $$\begin{aligned}
   &\mathsf{H}(M_{\mathcal{S}}, Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \\
   &= \mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}Y^{\ell_c,w}, C^{\ell_c,d}, D^{\ell_d}) + \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \\
   &= \mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) + \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}, M_{\mathcal{S}}).
   \end{aligned}$$

   and so,

   $$\begin{aligned}
   &\mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \\
   &= \mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}Y^{\ell_c,w}, C^{\ell_c,d}, D^{\ell_d}) + \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \\
   &\quad - \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}, M_{\mathcal{S}}).
   \end{aligned} \tag{5.23}$$

   Because of the Markov chain $M_{\mathcal{S}} \to C^{\ell_c}D^{\ell_d}(= C^{\ell_c,a}C^{\ell_c,w}C^{\ell_c,d}D^{\ell_d}) \to C^{\ell_c,w}$, we have,

   $$\mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}, M_{\mathcal{S}}) \geq \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,w}, C^{\ell_c,d}, D^{\ell_d}). \tag{5.24}$$

From (5.22) (5.23) and (5.24), we have,

$$\begin{aligned}
&\mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \\
&= \mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}, Y^{\ell_c,w}, C^{\ell_c,d}D^{\ell_d}) + \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \\
&\quad - \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}, M_{\mathcal{S}}) \qquad (5.25) \\
&\leq \delta' + \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) - \mathsf{H}(Y^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,w}, C^{\ell,d}, D^{\ell_d}) \\
&\leq \delta' + \mathsf{I}(Y^{\ell_c,w}; C^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}).
\end{aligned}$$

Note that $Y^{\ell_c,w} = C^{\ell_c,w} + E^{\ell_c,w}$ where $E^{\ell_c,w}$ is a uniformly distributed variable, and so,

$$\mathsf{I}(Y^{\ell_c,w}; C^{\ell_c,w}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) = 0. \qquad (5.26)$$

This means that,

$$\mathsf{H}(M_{\mathcal{S}}|C^{\ell_c,a}, C^{\ell_c,d}, D^{\ell_d}) \leq \delta'.$$

□

5.7.3 Proof of Lemma 25

Proof. We only show that it is impossible to have a two message round $(0, \delta)$-$\mathsf{AWTP}_{\mathsf{PD}}$ protocol of form with rate higher than $1 - \rho_r - \rho_w$:

1. Rnd 1: Alice $\stackrel{\mathsf{AWTP}}{\longrightarrow}$ Bob
2. Rnd 2: Alice $\stackrel{\mathsf{PD}}{\longrightarrow}$ Bob

The impossible result to have a two message round $(0, \delta)$-$\mathsf{AWTP}_{\mathsf{PD}}$ protocol of form: Rnd 1, Alice $\stackrel{\mathsf{AWTP}}{\longrightarrow}$ Bob; Rnd 2, Alice $\stackrel{\mathsf{AWTP}}{\longrightarrow}$ Bob, with rate higher than $1 - \rho_r - \rho_w$, can be proved similarly.

We only consider the case that $\rho_r = 1 - \rho_w$. The case that $\rho_r > 1 - \rho_w$ can be proved similarly.

We consider a pair of adversaries, $\{\mathsf{Adv}_2, \hat{\mathsf{Adv}}_2\}$, both with the following properties:

1. Adversary selects the reading and writing sets before the start of the $\mathsf{AWTP}_{\mathsf{PD}}$ protocol.
2. Adversary also chooses the error e^w randomly and uniformly from $\Sigma^{\rho_w N}$. That is $\mathsf{Pr}(e^w) = \frac{1}{|\Sigma^{\rho_w N}|}$.

Adversary Adv_2 uses the read and write sets, $S^r = \{S^a, S^b\}$ and $S^w = \{S^b, S^c\}$.

Because of $\rho_r = 1 - \rho_w$, we have $[N] = S^a S^b S^c S^d$ and $|S^b| = |S^d|$

Adversary $\hat{\mathsf{Adv}}_2$ uses the read and write sets, $\hat{S}^r = \{S^a, S^d\}$, and $\hat{S}^w = \{S^c, S^d\}$.

We have the following:

- Since the reading and writing capabilities of adversary Adv_2 is same as the adversary Adv_1 in Section 5.4, using Lemma 24 we have,

$$\mathsf{H}(M|C^a, C^d, D) \leq \mathsf{H}(\delta) + \delta(\mathsf{H}(M) - 1). \tag{5.27}$$

- Since the reading capability of $\hat{\mathsf{Adv}}_2$ is the same as Adv_1 in Section 5.4, from Lemma 5.2, we have,

$$\mathsf{I}(M; C^a, C^d, D) = 0. \tag{5.28}$$

- From (5.27) (5.28), we obtain,

$$\mathsf{H}(\delta) + \delta\mathsf{H}(M) \geq \mathsf{H}(M|C^{\ell,a}, C^{\ell,d}, D^\ell) \geq \mathsf{H}(M),$$

and so,

$$\frac{\mathsf{H}(\delta)}{1-\delta} \geq \mathsf{H}(M).$$

Since $0 \leq \delta < \frac{1}{2}$ and the message is uniformly distributed, we have,

$$1 - 2\mathsf{H}(\delta) \leq 2^{-2\mathsf{H}(\delta)} \leq 2^{-\mathsf{H}(M)} = \frac{1}{|\mathcal{M}|},$$

and, $2\mathsf{H}(\delta) \geq 1 - \frac{1}{|\mathcal{M}|}$.

□

5.7.4 Proof of Lemma 18

Proof. First, we show that there is a one-to-one correspondence between (ϵ, δ)-SMT$^{[ows]}$-PD protocols and restricted (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocols, in the sense that given one of the former, a corresponding one in the latter can be constructed, and vice versa.

1. Consider a (ϵ, δ)-SMT$^{[ows]}$-PD protocol, with a fixed public numbering of wires. Recall that in each round of the (ϵ, δ)-SMT$^{[ows]}$-PD protocol, both the wires and the PD can be invoked by Alice, while in our $\mathsf{AWTP_{PD}}$ model, only one type channel is invoked by Alice in each round. In both models Bob can invoke the PD in each round. We can convert the protocol messages in round i of a (ϵ, δ)-SMT$^{[ows]}$-PD protocol to the protocol messages of round j and $j+1$, of a $\mathsf{AWTP_{PD}}$ protocol. In round i, transmissions over wire 1 to N, defines a codeword of length N in the i^{th} round j of the AWTP. The transmission over the PD directly defines the transmission over the PD in $\mathsf{AWTP_{PD}}$, in the $j+1$ round. Each round of the transmission over PD, when invoked by Bob in the (ϵ, δ)-SMT$^{[ows]}$-PD , defines a transmission over the PD for the a(ϵ, δ)-SMT$^{[ows]}$-PD protocol. The above transformation gives a $\mathsf{AWTP_{PD}}$ from a (ϵ, δ)-SMT$^{[ows]}$-PD . Similarly, a $\mathsf{AWTP_{PD}}$ protocol defines an (ϵ, δ)-SMT$^{[ows]}$-PD protocol.
   So a restricted (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol can be constructed from (ϵ, δ)-SMT$^{[ows]}$-PD protocol. Similarly, a (ϵ, δ)-SMT$^{[ows]}$-PD protocol can also be constructed from restricted (ϵ, δ)-$\mathsf{AWTP_{PD}}$ protocol.

2. $\mathsf{AWTP_{PD}}$ and (ϵ, δ)-SMT$^{[ows]}$-PD definitions of secrecy and reliability are the same. Definition of ϵ-secrecy in both primitives requires statistical distance of the adversary's view for two messages chosen by the adversary (Compare definition 14 and definition 35), to be bounded by ϵ. For δ-reliability, both primitives require the probability of outputting the correct message to be at least $1-\delta$, and the probability of outputting the wrong message to be at most δ.

Next, we show the lower bound of transmission rate for Using Theorem 18, for a (ϵ, δ)-SMT$^{[ows]}$-PD over N wires and $t = \rho N$, there is a corresponding restricted (ϵ, δ)-$\mathsf{AWTP}_{\mathsf{PD}}$ protocol whose rate is upper bounded by,

$$R \leq 1 - \rho + 2\epsilon(1 + \log_{|\Sigma|} \frac{1}{\epsilon}) + 2\epsilon n.$$

Since the transmission rate of a 1-(ϵ, δ)-SMT protocol is the inverse of the rate of the corresponding restricted (ϵ, δ)-$\mathsf{AWTP}_{\mathsf{PD}}$ protocol, we have

$$\begin{aligned}
\mathsf{TR} &= \frac{1}{R} \\
&\geq \frac{1}{1 - 2\rho + 2\epsilon(1 + \log_{|\mathcal{W}|} \frac{1}{\epsilon}) + 2\epsilon n} \\
&= \frac{N}{N - 2t + 2N\epsilon(1 + \log_{|\mathcal{W}|} \frac{1}{\epsilon}) + 2\epsilon n N}.
\end{aligned}$$

Last, we show the lower bound on round for (ϵ, δ)-SMT$^{[ows]}$-PD protocol. Since (ϵ, δ)-SMT$^{[ows]}$-PD protocol is a special case of (ϵ, δ)-SMT-PD protocol, and it was shown that the lower bound on round complexity for (ϵ, δ)-SMT-PD protocol is at least three, the lower bound of (ϵ, δ)-SMT$^{[ows]}$-PD protocol is also three.

□

Chapter 6

Secure Message Transmission and Reliable Message Transmission

6.1 Introduction

In a SMT system a sender is connected to a receiver through N wires, t of which are controlled by the adversary. The goal of the system is to provide *privacy* and *reliability* for transmitted messages. SMT protocols can have one or more *rounds* and their communication efficiency is measured by the number of rounds and *transmission rate* which is the total number of communicated bits per one message bit. Protocols whose transmission rate asymptotically matches the lower bound on the transmission rate for a given number of round, are called *optimal*. The initial motivation for this model was to establish secure links between nodes in a distributed setting (*e.g.,* multi-party computation [7, 14, 70]), where many node pairs are connected by communication paths, rather than direct links. In recent years however, the protocols, and in particular 1-round protocols, have found other applications including key agreement and key strengthening in wireless sensor networks [13, 87, 88].

In SMT systems with perfect privacy and reliability, referred to as *Perfectly Secure Message Transmission* (PSMT), the adversary does not learn anything about the message, and the sent message is always correctly received by the receiver. It has been shown [28] that 1-round PSMT is possible if and only if $N = 3t + 1$. That is, only when less than one third of wires are corrupted.

To increase the number of corrupted wires that can be tolerated by the protocol, one may resort to more rounds, or allow less than perfect reliability. It was shown [33, 47] that 2-round optimal PSMT is possible for $N = 2t + 1$. It is also possible to construct optimal

1-round protocols for $N = 2t + 1$ if the probability of receiving an incorrect message is allowed to be δ (instead of zero for perfect case): a $(0, \delta)$-SMT provides perfect privacy and bounds probability of error in receiving the message by δ. $(0, \delta)$-SMT is particularly attractive because of the statefulness of multi-round protocols and the challenges (including security) associated with using them in practice. Protocols providing no privacy and almost perfect reliability are called δ-reliable message transmisison (δ-RMT, for short).

In this section we consider 1-round $(0, \delta)$-SMT protocols and 1-round δ-RMT protocols.

Motivation

For $N = 3t + 1$, there is a simple and elegant construction of 1-round PSMT using Reed-Solomon (RS) code that uses the traditional efficient method of unique decoding for these codes [31] to recover the message. In this construction the dimension of the code is $t + 1$ and is determined by t, the number of corrupted wires. The minimum distance of the code is $d = 2t + 1$ allowing t (adversarial) errors to be corrected.

For less connectivity however, a natural question is: if this construction can be extended to the case that $2t + 1 \leq N \leq 3t$. That is to use RS codes (or any other error correcting code) to construct 1-round $(0, \delta)$-SMT protocols. Note that for $N < 3t + 1$, an RS code will have dimension $k = t + 1$ (the code dimension must be kept the same because of perfect privacy) and so the minimum distance is reduced to $t + 1 \leq d \leq 2t$ which makes unique decoding of t errors impossible.

All known 1-round δ-RMT and (0, δ)-SMT protocols use elaborate combinations of secret sharing (including secret sharing with cheater detection) and authentication systems, together with elaborate verification algorithms to decode the message. A disadvantage of these clever constructions is the difficulty of verifying their correctness. In [1] it was shown that the proofs of security of the 1-round (0, δ)-SMT protocol in [81] were not correct and thus the protocol was not secure. An immediate question is: if it is possible to base the construction of optimal 1-round $(0, \delta)$-SMT protocols on error correcting codes and provide

a systematic approach to the construction of SMT protocols.

Our Work

1). Constructing 1-round δ-RMT from RS codes. Firstly we construct a 1-round δ-RMT using the private code approach in [**?**]. This effectively reduces the construction of a δ-RMT to the construction of a list decodable code and a multireceiver MAC. We show that an instantiations of this construction using FRS code and our multireceiver MAC, results in an optimal 1-round δ-RMT protocol with the smallest δ among all known optimal protocols.

2). Constructing 1-round $(0, \delta)$-SMT from RS codes. The construction of 1-round PSMT for $N = 3t + 1$ [31] encodes a message $m \in \mathbb{F}_q$, together with $k - 1$ random elements of $\mathbb{F}_q$, $(m, r_1, \cdots, r_{k-1})$, as a codeword of a (k, n) RS code. For lower connectivity however, the construction does not work because the dimension of the code, that is determined by the privacy requirement, must be $t + 1$. Noting that the minimum distance of the RS code is $d = n - k + 1$, for $2t + 1 \leq N \leq 3t$, the minimum distance of the code will be $t + 1 \leq d \leq 2t$, which is below the unique decoding capability of the RS code. One can, however, use *list decoding* to correct errors beyond unique error correcting radius of the code. In a list decodable code the decoder outputs the list of all codewords that are at (relative) distance ρ from the received word. By introducing sufficient structure in the encoded message, the receiver would be able to detect the correct message (with a high probability) among the decoded list.

A similar approach is used [**?**] in the construction of *private codes*. Private codes were proposed by Langberg [50] with the goal of providing reliable communication over adversarially corrupted channels. It is well known [32] that concatenated codes achieve Shannon capacity against *random errors*. However, constructing codes that achieve $1 - R$ in adversarial error is an open problem. In private codes Alice and and Bob share a *secret key* which is unknown to the adversary and this allows them to communicate reliably at rates approaching Shannon's capacity.

The explicit construction of private codes in [**?**] uses message authentication codes to identify the sent codeword in the decoded list of a *list decodable code.* In SMT however there is no explicit shared secret key between the transmitter and the receiver. However there are private wires (wires that are not controlled by the adversary) that may be used to send key information from sender to the receiver.

Using this approach, the two major challenges that must be addressed are: (i) for $N = 2t + 1$, correcting t adversarial errors with minimum distance $d = t + 1$ requires explicit codes that achieve *list decoding capacity*, and (ii) efficient detection of the correct messages in the decoded list requires an authentication mechanism that uses private wires in SMT (instead of shared secret keys). Note that for code length $N = 2t + 1$ and code dimension $k = t+1$, we have $R = k/N = \frac{t+1}{2t+1}$ and the percentage of errors that needs to be corrected is $\rho = \frac{t}{2t+1} = 1 - R$. This means that using an error correcting code for SMT with $N = 2t+1$, requires the code to reach list decoding capacity.

Our construction works as follows: the message is first appended with sufficient redundancy (to guarantee privacy), and authentication information (MAC values to allow detection of the message in the decoded list), and then encoded using a Folded Reed-Solomon (FRS) code with well chosen parameters. FRS codes [39, 38] are explicit codes that achieve list decoding capacity and have efficient decoding algorithm. On each wire, one component of the code together with some key information for the MAC, is sent. The receiver uses the decoding of the FRS-code to recover the list of code vectors that are at distance at most t (in FRS code) from the received vector, and then uses the keys (possibly tampered) that are received on the wires to identify the correct message. The final SMT decoding algorithm either outputs the correct message, or outputs $\perp$. That is, it never outputs an incorrect message.

The optimal rate for the SMT is obtained by designing an authentication mechanism that is inspired by *multireceiver message authentication codes* (multireceiver MAC) introduced in

[23], and applying authentication to the information symbols only. The authentication mechanism is a new multireceiver MAC that effectively reduces the authentication information symbols that need to be sent, resulting in optimal transmission rate.

We prove perfect privacy of the construction and obtain δ, the success chance of the adversary in resulting the protocol to output $\perp$. The transmission rate of the protocol is $O(N)$ and so the protocol is optimal. The decoding however will not be polynomial because although the list decoding algorithm is efficient, the output list will be exponential (in N) and so checking the elements of the list will take exponential time.

We extend this construction ($N = 2t + 1$) to higher connectivities of the form $N = (2 + c)t, c > \frac{1}{t}$. Here the decoding parameters can be chosen such that the decoding list is polynomial (in N). The result is an optimal 1-round $(0, \delta)$-SMT that has efficient (polynomial time) decoding.

An important property is both protocols also have the lowest δ compared to all known optimal 1-round (0, δ)-SMT protocols, that only output correct messages, or $\perp$.

We also present two constructions. We give new constructions for MAC and multireceiver MACs with optimal and near optimal (different by a factor of 2) protection.

Related Work.

Patra *et al.* designed an efficient and optimal 1-round δ-RMT protocol [67]. There are two optimal and efficient 1-round (0, δ)-SMT protocols for $N = 2t + 1$ [67, 83]. On the other hand, for $N = (2 + c)t, c > \frac{1}{t}$, there are two optimal and efficient 1-round (0, δ)-SMT protocols [83, 72].

6.2 Preliminary

6.2.1 Multireceiver message authentication codes

Multireceiver authentication codes [23] allow a sender to send a message to a group of receivers such that each receiver can individually verify the message, using his individual shared key k_i with the sender. The sender is honest but receivers can be corrupted and attempt to forge a message to be acceptable by an uncorrupted receiver. In a (k, N) multireceiver message authentication system, there are N receivers and at most $k-1$ receivers can be corrupted.

Definition 39. *A one-time (k, n)-multireceiver authentication code (multireceiver MAC) with key $(\mathbf{r}_s, \mathbf{r}_1, \cdots, \mathbf{r}_n)$ with n receivers, and collusion size $k-1$, is δ-secure if the best success chance of any colluding set of receivers with access to a message, tag pair, $(\mathbf{m}, t = \mathsf{MAC}(\mathbf{m}, \mathbf{r}_s))$ in forging a different message, tag pair $(\mathbf{m}', t')$, where $\mathbf{m} \neq \mathbf{m}'$, and $\mathsf{Ver}((\mathbf{m}', t'), \mathbf{r}_i) = 1$, is at most δ, and probability is over all unknown keys.*

In the following we give two new constructions for multireceiver MACs that are used in the SMT constructions in Section 6.4 for 1-round (0, δ)-SMT with $N = 2t+1$, and in Section 6.5 for 1-round (0, δ)-SMT with $N = (2+c)t$. Construction I can be seen as a generalization of the construction in [23], when the sender sends a block of d messages. Construction II is built on a new MAC.

Multireceiver MAC I

Let $\mathbf{m} = (m_1, \cdots, m_d)$, where $m_i \in \mathbb{F}_q^{v'}, i = 1, \cdots, d$, be the message block.

- *Key distribution:* A trusted initializer does the following: (i) randomly generates $d+1$ polynomials $P_1(z), P_2(z), \cdots, P_{d+1}(z)$, each of degree at most $k-1$, over $\mathbb{F}_q^{v'}$; chooses N random distinct elements $z_1, z_2, \cdots, z_N$, where $z_i \in \mathbb{F}_q^{v'}, i = 1, \cdots, N$; makes $z_1, z_2, \cdots, z_N$

public and privately sends $\mathbf{r}_i = (P_1(z_i), P_2(z_i), \cdots, P_{d+1}(z_i))$ to each receiver i, for $1 \leq i \leq N$ and to the sender.

- *Constructing authenticated messages:* The sender computes the authentication tag as:

$$A(z) = P_1(z)m_1 + P_2(z)m_2 + \cdots + P_d(z)m_d + P_{d+1}(z).$$

and broadcasts the message and tag pair, $(m_1, m_2, \cdots, m_d, A(z))$.

- *Verification:* Receiver i accepts $(m_1, m_2, \cdots, m_d, A(z))$ if and only if $A(z_i) = P_1(z_i)m_1 + P_2(z_i)m_2 + \cdots + P_d(z_i)m_d + P_{d+1}(z_i) \mod q^{v'}$.

The above scheme is a multireceiver MAC in which each key can be used to authenticate a block of up to d messages. The size of tag is k and only depends on the collusion size, rather than the total number of receivers.

The following Lemma is proved in Section 6.6.2.

Lemma 31. *The best success chance of colluders, given a message and tag pair* $(\mathbf{m}, t)$*, in forging* $(\mathbf{m}', t')$ *where* $\mathbf{m}' \neq \mathbf{m}$ *and* $\mathsf{Ver}((\mathbf{m}', t'), \mathbf{r}_i) = 1$*, is at most* $q^{-v'}$*, where* $q^{v'}$ *is the size of the underlying finite field. Here* i *is an uncorrupted receiver.*

Multireceiver MAC II

The multireceiver MAC is built on a new one-time MAC. The MAC uses message block of size $\binom{t+2}{2}$ and has forgery probability bounded by $\frac{2}{q^{v'}}$. The multireceiver MAC can be constructed by using polynomials for key elements. We skip the description of the underlying MAC, and only present the multireceiver MAC.

Using the same notations and key distribution stage, as Construction I, we define:

$$\mathsf{MAC}(m, r) = m_1P_1(z_i) + \cdots + m_tP_t(z_i) + m_{t+1}P_1(z_i)^2 + \cdots + m_{2t}P_t(z_i)^2 + m_{2t+1}P_1(z_i)P_2(z_i)$$
$$+ \cdots + m_{\binom{t+2}{2}-1}P_{t-1}(z_i)P_t(z_i) + P_{t+1}(z_i) = A(z_i).$$

$P_1(z), P_2(z), \cdots, P_{t+1}(z)$ have degree t and the MAC function is over $\mathbb{F}_q^{v'}$. The MAC function is taking all products of at most two polynomials from the set. $\{P_1(z_i), P_2(z_i), \cdots, P_t(z_i)\}$.

Therefore there are total $\binom{t+2}{2} - 1$ coefficients over $\mathbb{F}_q^{v'}$. Finally $P_{t+1}(z_i)$ is used to mask the result.

Lemma 32. *The best success chance of colluders, given a message and tag pair* $(\mathbf{m}, t)$*, in forging* $(\mathbf{m}', t')$ *where* $\mathbf{m}' \neq \mathbf{m}$ *and* $\mathsf{Ver}((\mathbf{m}', t'), \mathbf{r}_i) = 1$*, is at most* $2q^{-v'}$*, where* $q^{v'}$ *is the size of the underlying finite field. Here* i *is an uncorrupted receiver.*

The proof outline is provided in Section 6.6.3.

6.3 One-round δ-RMT for $N \geq 2t + 1$

We give a general construction of 1-round δ-RMT using a list decodable code and a multi-receiver MAC. The sender (i) generates the key information for a multireceiver MAC and assigns the receiver key $\mathbf{r}_i$ to wire W_i, (ii) calculates the tag value and append it to the message, and encode the message and tag pair using the list decodable code. The sender sends the i^{th} component of the code together with the key $\mathbf{r}_i$, on the wire W_i. The receiver, parses the received word, decodes a list of codewords that are at distance at most t from the corrupted codeword, and use the appended MAC to the message, and the keys that are sent on each wire, to identify the sent message.

We give a general construction of 1-round δ-RMT using a list decodable code (FRS code) and a multi-receiver MAC.

1. FRS Code: We use u-Folded Reed Solomon Code with length N over $\mathbb{F}_q$ with interpolation parameter v.

2. Multi-receiver MAC: We use $(t + 1, N)$ multireceiver MAC II in Section 6.2.1.

The sender (i) select message vector $\mathbf{m} = (m_0, \cdots, m_{\binom{t+2}{2}v'-1})$ over $\mathbb{F}_q$ with $v' = \left\lfloor \frac{u(1-3\sigma)}{t+1} \right\rfloor$. The message vector can be mapped into $\mathbf{x} = (x_0, \cdots, x_{(\binom{t+2}{2}-1)})$ over $\mathbb{F}_q^{v'}$. (ii) generates the key information for a multireceiver MAC and assigns the receiver key $\mathbf{r}_i$ to wire W_i, (iii)

calculates the tag value and append it to the message, and encode the message and tag pair using the list decodable code. The sender sends the i^{th} component of the code together with the key $\mathbf{r}_i$, on the wire W_i. The receiver, parses the received word, decodes a list of codewords that are at distance at most t from the corrupted codeword, and use the appended MAC to the message, and the keys that are sent on each wire, to identify the sent message.

The details of this construction is given in follow:

RMT scheme for $N = 2t + 1$

Alice does the following:

1. $\mathcal{S}$ generates $t+1$ polynomials as key $\mathbf{r}_s = (P_1(z), \cdots, P_{t+1}(z))$, over $\mathbb{F}_q^{v'}$, each of degree t, randomly and makes $\{z_1, z_2, \cdots, z_N\}, z_i \in \mathbb{F}_q^{v'}$ public. $\mathcal{S}$ generates MAC code $(\mathbf{x}, A(z))$ in follow,

$$\begin{aligned} A(z) =&\mathsf{MAC}(\mathbf{x}, \mathbf{r}_s) = x_1 P_1(z_i) + \cdots + x_t P_t(z_i) + x_{t+1} P_1(z_i)^2 + \cdots + x_{2t} P_t(z_i)^2 \\ &+ x_{2t+1} P_1(z_i) P_2(z_i) + \cdots + x_{\binom{t+2}{2}-1} P_{t-1}(z_i) P_t(z_i) + P_{t+1}(z_i) \mod q^{v'}. \end{aligned}$$

2. For each wire W_i, $\mathcal{S}$ generates the key $\mathbf{r}_i$ for authentication,

$$\mathbf{r}_i = (P_1(z_i), P_2(z_i), \cdots, P_{t+1}(z_i)), \text{ for } i = 1, \cdots, N$$

   The tag can be obtained as follow,

$$\begin{aligned} A(z_i) =&\mathsf{MAC}(\mathbf{x}, \mathbf{r}_i) = x_1 P_1(z_i) + \cdots + x_t P_t(z_i) + x_{t+1} P_1(z_i)^2 + \cdots + x_{2t} P_t(z_i)^2 \\ &+ x_{2t+1} P_1(z_i) P_2(z_i) + \cdots + x_{\binom{t+2}{2}-1} P_{t-1}(z_i) P_t(z_i) + P_{t+1}(z_i) \mod q^{v'}. \end{aligned}$$

3. The message block of FRS code is composed of the information part and the MAC part. The structure of message is, $(\mathbf{x}, A(z))$. The dimension of FRS code is $(\binom{t+2}{2} - 1)v' + tv' + v'$.

4. $\mathcal{S}$ encodes the message to codeword c according to FRS encoding algorithm in section 3.2.1 by choosing the parameter v, u, q which makes the receiver's decoding capability up to t. Each channel j transmits a vector $(f(\gamma^{ju}), f(\gamma^{ju+1}), \cdots, f(\gamma^{ju+u-1}))$ and $\mathbf{r}_j$.

Bob does the following:

1. $\mathcal{R}$ receives from wire i the vector $(Y_{i,1}, Y_{i,2}, \cdots, Y_{i,u}, \hat{\mathbf{r}}_i)$ from channel i, where $\hat{\mathbf{r}}_i$ is the corrupted $\mathbf{r}_i$ and $Y_{i,j} \in \mathbb{F}_q, j = 1, \cdots, u$ from the i^{th} component of the FRS code.

2. $\mathcal{R}$ applies FRS list decoding to the received codeword introduced in Section 3.2.1 to the received vector Y with adversarial errors and decode a list of messages including the correct one.

3. $\mathcal{R}$ verifies the authentication vector $(\mathsf{MAC}(\mathbf{x}, \mathbf{r}_1) = A(z_1), \mathsf{MAC}(\mathbf{x}, \mathbf{r}_2) = A(z_2), \cdots, \mathsf{MAC}(\mathbf{x}, \mathbf{r}_N) = A(z_N))$.

4. If there is a unique message such that at least $t+1$ equations hold, $\mathcal{R}$ outputs the message $(m_0, m_1, \cdots, m_{(\binom{t+2}{2}-1)v'-1})$ which is the secret $\mathcal{S}$ sent. Otherwise output $\perp$.

Theorem 19. *In the above construction $\delta \leq \frac{t+1}{q^{v'-v+1}}$ and the transmission rate is optimal.*

Proof. First we need to prove that the received codeword are decodable. According to the linear interpolation decoding algorithm, the decoding condition are satisfied if we choose parameter $v = (N/\sigma) - 1$, $u = v^3$ and $v' = \left\lfloor \frac{u(1-3\sigma)}{t+1} \right\rfloor$. We also assume that $t \geq 2$ and the case of $t = 1$ can be proved similarly.

$$
\begin{aligned}
t+1 &\overset{(1)}{>} \sigma + \frac{t+2}{2} + 1 - 3\sigma \\
&\overset{(2)}{\geq} \sigma + \frac{t+2}{2} + \frac{(t+1)v'}{u} \\
&\overset{(3)}{\geq} \sigma + \frac{(\binom{t+2}{2} - 1)v' + (t+1)v'}{u} \\
&\overset{(4)}{\geq} N\frac{1}{v+1} + \frac{(\binom{t+2}{2} - 1)v' + (t+1)v'}{u} \\
&\overset{(5)}{\geq} N\frac{1}{v+1} + \frac{uRN}{u} \\
&\overset{(6)}{\geq} N\frac{1}{v+1} + N\frac{v}{v+1}\frac{uR}{u-v+1} \\
&\overset{(7)}{\geq} N(\frac{1}{v+1} + \frac{v}{v+1}\frac{uR}{u-v+1}).
\end{aligned}
\tag{6.1}
$$

Here (1) is from $t \geq 2$ and $\sigma > 0$. (2) is from $v' \leq \frac{u(1-3\sigma)}{t+1}$, and it implies $1-3\sigma \geq \frac{(t+1)v'}{u}$. (3) is from $v' \leq \frac{u(1-3\sigma)}{t+1}$. Since $\sigma > 0$, it implies $\frac{(t+1)v'}{u} < 1$, and so there is $\frac{t+2}{2} \geq \frac{t+2}{2}(t+1)\frac{v'}{u} \geq \frac{\binom{t+2}{2}-1)v'}{u}$. (4) is from $v = \frac{N}{\sigma} - 1$. (5) is from $uRN = \binom{t+2}{2}v' \leq (\binom{t+2}{2} - 1)v' + (t+1)v'$. (6) is from $u \geq v^3$, and implies $\frac{1}{u} \geq \frac{v}{(v+1)(u-v+1)}$.

Next we prove the reliability of RMT. We use the multireceiver MAC II (Section 3.2.1). From lemma 32, the probability that another message $\mathbf{m}' \neq \mathbf{m}$ pass the authentication is less than $2/q^{v'}$. The size of messages that are list decoded is less than q^{v-1}. Therefore the probability that any of other message pass at least one uncorrupted wire authentication is at most $\frac{2}{q^{v'-v+1}}$. Because there are totally $t+1$ uncorrupted wires, the reliability is at least $1 - \frac{2(t+1)}{q^{v'-v+1}}$.

Finally the transmission rate is optimal,

$$
\frac{uN + (v't + v')N}{(\binom{t+2}{2} - 1)v'} = \mathcal{O}(1).
$$

The computational time is exponential since the list size is q^v, and each must be verified. Since $v = \mathcal{O}(N)$, the computational complexity of decoding algorithm is $\mathcal{O}(q^N)$ which is not efficient.

□

Comparison with Related Work

Our protocol has the lowest δ and the optimal 1-round δ-RMT protocol of [67]. Their δ is $\frac{N^2(N-1)}{q}$ (with field size $q \geq \frac{N^2(N-1)}{\delta}$), whereas our δ is $\frac{t+1}{q}$ (with field size $q > Nu$).

Table 6.1: Comparison with 1-round δ-RMT protocols for $N = 2t + 1$

RMT Scheme	**Comp.**	$\mathbb{F} = q$	δ	**Optimality**	**Outputs Incorrect Message**
Patra *et al.* [67]	*Poly.*	$\geq \frac{N^2(N-1)}{\delta}$	$\leq \frac{N^2(N-1)}{q}$	Yes	No
This Work	*Exp.*	$\geq Nu$	$\leq \frac{t+1}{q}$	Yes	No

Table 6.1 compares our protocol with 1-round δ-RMT protocols that have the property that the output is either the correct message or $\perp$. For simplicity of comparison we have used $v' = v$, resulting in $\delta = \frac{t+1}{q}$.

6.4 One-round $(0, \delta)$-SMT for $N \geq 2t + 1$

To construct an SMT from the RMT above, we need to ensure that the view of the adversary does not leak any information about the message $\mathbf{m}$, chosen by the sender.

We give an explicit construction for a 1-round $(0, \delta)$-SMT protocol, first for the minimum connectivity ($N = 2t+1$), and then extend it to higher connectivities. The construction uses the instantiation of the 1-round δ-RMT construction above given in Section 6.3 and adds sufficient randomness in the encoding stage, to guarantee perfect privacy. The resulting protocol will have optimal transmission rate, and provides the highest reliability compared to all other known 1-round (0, δ)-SMT protocol in the literature.

The 1-round $(0, \delta)$-SMT Protocol for $N = 2t + 1$ is constructed from FRS code and multireceiver MAC.

1. Multireceiver MAC: We use the Multireceiver MAC I in Section 6.2.1 over $\mathbb{F}_q^{v'}$.

2. FRS Code: We use Folded Reed-Solomon code with length N, with interpolation parameter v.

We use FRS code over $\mathbb{F}_q$. The message block consists of three parts: (i) information part $\mathbf{m} = (m_0, m_1, \cdots, m_{\sigma u-1}), m_i \in \mathbb{F}_q$. The message vector can be mapped into $\mathbf{x} = (x_1, \cdots, x_d), x_i \in \mathbb{F}_q^{v'}$, with $d = \lceil \frac{\sigma u}{v'} \rceil$. (ii) ut random elements $(a_1, a_2, \cdots, a_{ut})$, $a_i \in \mathbb{F}_q$ that are used to ensure privacy; (iii) tags $\mathsf{MAC}(\mathbf{x}, \mathbf{r}_s)$, calculated using the multireceiver MAC. That is the message block of FRS code is given in following:

$$\{m_0, m_1, \cdots, m_{\sigma u-1}, a_1, a_2, \cdots, a_{ut}, \mathsf{MAC}(\mathbf{x}, \mathbf{r}_s)\}.$$

The ut random elements appended to the information block will ensure perfect privacy. The total length of the message block to be encoded by the FRS code is $ut + \sigma u + v'(t+1)$. Here $\sigma < 1$ is a constant to be determined later.

The codeword of the FRS code that will be constructed for this message block, will have N components, each an element of $\mathbb{F}_q^u$. The adversary's view will contain t components, of the FRS code.

SMT Protocol for $N = 2t + 1$

Alice does the following:

1. $\mathcal{S}$ randomly generates the secret key from $d+1$ polynomials $\mathbf{r}_s = (P_1(z), \cdots, P_{d+1}(z))$. Each polynomial is over $\mathbb{F}_q^{v'}$ with degree at most t. $\mathcal{S}$ randomly chooses $\{z_1, \cdots, z_N\}, z_i \in \mathbb{F}_q^{v'}$, and makes them public. For each wire W_i, $\mathcal{S}$ generates the verification key $\mathbf{r}_i$ as follow,

$$\mathbf{r}_i = (P_1(z_i), P_2(z_i), \cdots, P_{d+1}(z_i)), \text{ for } i = 1, \cdots, N.$$

2. $\mathcal{S}$ generates the multireceiver MAC code $(\mathbf{m}, A(z))$. The tag polynomial $A(z)$ of multireceiver MAC code is constructed as follow,

$$A(z) = \mathsf{MAC}(\mathbf{x}, \mathbf{r}_s) = P_1(z)x_1 + P_2(z)x_2 + \cdots + P_{d+1}(z)x_d.$$

3. $\mathcal{S}$ generates a randomness vector $\mathbf{a} = (a_1, \cdots, a_{ut})$. The message block of FRS code is $(\mathbf{x}, \mathbf{a}, A(z))$, and is composed of the information part, the random part and the tag part. The dimension of FRS code is $ut + \sigma u + tv' + v'$.

4. $\mathcal{S}$ encodes the message block into codeword using the FRS encoding algorithm in Section 3.2.1. Each wire j transmits a vector $(f(\gamma^{ju}), \cdots, f(\gamma^{ju+u-1}))$ and $\mathbf{r}_j$.

Bob does the fullowing:

1. The receiver receives from wire i the vector $(Y_i = (Y_{i,1}, Y_{i,2}, \cdots, Y_{i,u}), \hat{\mathbf{r}}_i)$. Here $\hat{\mathbf{r}}_i$ is the (possibly) corrupted $\mathbf{r}_i$, and $Y_{i,j} \in \mathbb{F}_q, j = 1, \cdots, u$ form the i^{th} component of the FRS code.

2. The receiver applies FRS list decoding introduced in Section 3.2.1 to the received vector $Y = (Y_1, \cdots, Y_N)$, and output a decoding list $\mathcal{L}$. Each element in decoding list is in the form $(\mathbf{x}, \mathbf{a}, A(z)) \in \mathcal{L}$.

3. For each message $\mathbf{x}$ in the list $\mathcal{L}$, the receiver checks the valid of authentication code,

$$\mathsf{MAC}(\mathbf{x}, \mathbf{r}_1) \stackrel{?}{=} A(z_1), \mathsf{MAC}(\mathbf{x}, \mathbf{r}_2) \stackrel{?}{=} A(z_2), \cdots, \mathsf{MAC}(\mathbf{x}, \mathbf{r}_N) \stackrel{?}{=} A(z_N).$$

   If the equalities hold in at least $t+1$, the message is considered acceptable. If there is unique message acceptable, $\mathcal{R}$ outputs the message $\mathbf{m}$. The decoder outputs $\perp$ if more than one acceptable message is found.

Theorem 20. *The SMT protocol described above is a* $(0, \delta)$*-SMT for* $N = 2t + 1$*, with* $\delta \leq \frac{t+1}{q^{v'-v+1}}$*. The transmission rate is* $\mathcal{O}(\frac{N}{N-t})$*. The computational time is exponential in* N*.*

First we show the perfect secrecy of SMT protocol.

Lemma 33. *The SMT protocol is perfectly secure.*

Proof. The adversary knows t positions of the FRS codeword which is t blocks, each of u components of the underlying RS code. The dimension of the FRS code (and RS code) is $ut + \sigma u + tv' + v'$. This leaves $\sigma u + tv' + v'$ elements (coefficients of the polynomial that is associated with the underlying RS codeword), that are independent from the adversary's view. We note that only σu elements forms the information block $\mathbf{m}$ and the remaining part is the verification information.

This gives in total $\mathbb{F}_q^{\sigma u}$ possible codewords for correct messages and so the adversary will be fully uncertain about the information block $\mathbf{m}$. □

Second we show the reliability of SMT protocol.

Lemma 34. *The probability of decoding error of SMT protocol is no more than* $\delta \leq \frac{t+1}{q^{v'-v+1}}$*.*

Proof. First we show the decoding condition of FRS code is satisfied.

We must choose the folding parameter u and v, and the finite field size q, to ensure that decoding succeeds of decoding to find a list of all codewords receiver decodes a list of codewords which is that are within radius ut from the received corrupted transcript (t errors in the FRS code). Since the FRS code will have length $N = 2t + 1$ and dimension $k = ut + \sigma u + tv' + v'$, according to the decoding condition of FRS code (Lemma 4), it implies,

$$t + 1 \geq N(\frac{1}{v+1} + \frac{v}{v+1}\frac{uR}{u-v+1}).$$

We set the parameter $v = (N/\sigma) - 1$, $u \geq v^3$, and $v' = \left\lfloor \frac{u(1-3\sigma)}{t+1} \right\rfloor$, where σ is small constant ($\sigma \leq 1/4$). It implies,

$$\begin{aligned} t+1 &\overset{(1)}{>} 2\sigma + t + 1 - 3\sigma \\ &\overset{(2)}{\geq} \sigma + \frac{ut + \sigma u + (t+1)v'}{u} \\ &\overset{(3)}{\geq} N\frac{1}{v+1} + \frac{ut + \sigma u + (t+1)v'}{u} \\ &\overset{(4)}{\geq} N\frac{1}{v+1} + \frac{v}{v+1}\frac{ut + \sigma u + (t+1)v'}{u - v + 1} \\ &\overset{(5)}{\geq} N\frac{1}{v+1} + \frac{v}{v+1}\frac{k}{u - v + 1} \\ &\overset{(6)}{\geq} N(\frac{1}{v+1} + \frac{v}{v+1}\frac{uR}{u - v + 1}). \end{aligned} \tag{6.2}$$

In the above, (1) is from $\sigma > 0$, (2) is from $v' \leq \frac{u(1-3\sigma)}{t+1}$, and implies $1 - 3\sigma \geq \frac{(t+1)v'}{u}$. (3) is from $v = (N/\sigma) - 1$. (4) is from $u \geq v^3$, and so $\frac{v}{(v+1)(u-v+1)} \leq \frac{1}{u}$. (5) is by replacing $ut + \sigma u + (t+1)v$ by k. (6) is by replacing R with k/N.

The adversary controls t lines and so t positions (u components each) of FRS code are changed. Without loss of generality assume the first t wires are corrupted by the adversary and so the last $t+1$ wires are private.

To break the reliability of the protocol the adversary needs to be able to change the values sent over the corrupted wires, such that the list of codewords resulting from the list decoding step, contain not only the correct message but also another codeword that encodes a message $\mathbf{m}'$ for which at least $t+1$ verification equations are satisfied. This will result in more than one message passing the verification test of the protocol and so, the protocol outputs $\perp$.

Note that the adversary controls the verification keys of the t corrupted wires. We assume a powerful adversary (it is unclear how this adversary can be constructed) that can change the t wires such that the verification tests of those t wires are successfully passed for a message $\mathbf{x}' = \mathbf{m}'$. Since the adversary does not know the verification keys of wires

$t+1, t+2, \cdots N$, the best success chance in forging one of these values is,

$$\begin{aligned}&\Pr[\mathsf{MAC}(\mathbf{x}', \mathbf{r}_{t+1}) = A'(z_{t+1}) \vee \cdots \vee \mathsf{MAC}(\mathbf{x}', \mathbf{r}_{2t+1}) = A'(z_{2t+1})] \\ &\leq \Pr[\mathsf{MAC}(\mathbf{x}', \mathbf{r}_{t+1}) = A'(z_{t+1})] + \cdots + \Pr[\mathsf{MAC}(\mathbf{x}', \mathbf{r}_{2t+1}) = A'(z_{2t+1})] = \frac{t+1}{q^{v'}}.\end{aligned} \tag{6.3}$$

The size of the decoded list is at most q^{v-1}. The probability that any other $\mathbf{x}'$ which is different from the correct one $\mathbf{m}$ passing through the authentication is $\frac{(t+1)}{q^{v'}} \times q^{v-1}$. □

Last we show the efficiency of SMT protocol.

Transmission rate: The transmission rate is $\frac{uN+(v'd+v')N}{\sigma u} = \mathcal{O}(N)$ and it is optimal for 1-round (0, δ)-SMT.

Computation complexity: The list size is at most q^{v-1} and each must be verified. Since $v = \mathcal{O}(N)$, so the complexity of decoding algorithm is $\mathcal{O}(q^v)$ which is not efficient.

Comparison with Related Work.

Table 6.2 compares the protocol with 1-round (0, δ)-SMT protocols that have the property that the output is either the correct message or $\perp$. For simplicity of comparison we have used $v' = v$, resulting in $\delta = \frac{t+1}{q}$.

Table 6.2: Comparison with 1-round $(0, \delta)$-SMT Protocols for $N = 2t + 1$

SMT	**Comp.**	$\mathbb{F}_q = q$	δ	**Optimality**	**Outputs Incorrect Message**
Kurosawa *et al.* [48]	*Exp.*	$\geq \binom{N}{t+1} - \binom{N-t}{t+1} - 1$	$\leq \frac{\binom{N}{t+1}-\binom{N-t}{t+1}}{q+1}$	Yes	No
Srinathan *et al.* [80]	*Poly.*	$\geq 2N^3$	$\leq \frac{N^3}{q}$	Yes	No
Desmedt *et al.* [22]	*Poly.*	$\geq t(t+1)$	$\leq \frac{t(t+1)}{q}$	No	No
Tuhin *et al.* [83]	*Poly.*	$\geq t(t+1)$	$\leq \frac{t(t+1)}{q}$	Yes	No
This Work	*Exp.*	$\geq Nu$	$\leq \frac{t+1}{q}$	Yes	No

6.5 One round $(0, \delta)$-SMT for $N = 2t + ct$

The construction in Section 6.4 is for minimum connectivity and is not computationally efficient. One question is if increasing connectivity can result in efficient computation for decoding.

We consider the case that $N = 2t + ct, c > \frac{1}{t}$.We use the same approach of using FRS code and a multireceiver MAC, but use Construction II of multireceiver MAC with parameters that allow the SMT construction to have optimal rate and efficient computation. The structure of the message is $(m_0, m_1, \cdots, m_{(\binom{t+2}{2}-1)v-1}, a_1, a_2, \cdots, a_{ut}, \mathsf{MAC}(\mathbf{x}, \mathbf{r}))$. The information block $\mathbf{m} = (m_0, m_1, \cdots, m_{(\binom{t+2}{2}-1)v-1})$ is mapped into $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \cdots, \mathbf{x}_{\binom{t+2}{2}-1})$.

The multireceiver MAC is as follows:

$$\begin{aligned} A(z_i) = \mathsf{MAC}(\mathbf{x}, r) =& \mathbf{x}_0 + \mathbf{x}_1 P_1(z_i) + \cdots + \mathbf{x}_t P_t(z_i) + \mathbf{x}_{t+1} P_1(z_i)^2 + \cdots \\ &+ \mathbf{x}_{2t} P_t(z_i)^2 + \mathbf{x}_{2t+1} P_1(z_i) P_2(z_i) + \cdots + \mathbf{x}_{\binom{t+2}{2}-1} P_{t-1}(z_i) P_t(z_i) + P_{t+1}(z_i). \end{aligned}$$

The degree of $P_1(z), P_2(z), \cdots, P_{t+1}(z)$ is t and the MAC function is over $\mathbb{F}_q^v$, where v is the parameter of FRS code (instead of $\mathbb{F}_q^{v'}$ for $N = 2t + 1$).

We need to choose parameter that makes the receiver decode up to t errors, where t is the errors. The number of correct wires $t + ct$ is

$$t + ct \;\; > \;\; N(\frac{1}{v+1} + \frac{v}{v+1}\frac{uR}{u-v+1}). \tag{6.4}$$

We assume that $u = c_0 t$ and show that a constant value for $v = v_0$ and $t \gg v_0$, the value of c that allows successful decoding should satisfy $c > \frac{v_0}{c_0} + \frac{1}{v_0}$. The details are in Appendix 6.6.1. Table 6.5 below gives example values for v_0 and c, and the size of the resulting list.

The complete protocol is given in the next Section.

SMT Protocol for $N = (2 + c)t, c > \frac{1}{t}$.

Table 6.3: Values of c for different values of v_0

v_0	list size	c
$v_0 = 1$	q^0	$c \approx \frac{1}{c_0} + 1$
$v_0 = 2$	q	$c \approx \frac{2}{c_0} + 1/2$
$v_0 = 3$	q^2	$c \approx \frac{3}{c_0} + 1/3$

Alice does the following:

1. The sender randomly generates $t+1$ polynomials $P_1(z), \cdots, P_{t+1}(z)$ over $\mathbb{F}_q$ of degree at most t, randomly chooses $(z_1, z_2, \cdots, z_N), z_i \in \mathbb{F}_q$ and make them public. Then for each wire W_i, the sender generate the key $\mathbf{r}_i$ given by,

$$\mathbf{r}_i = (P_1(z_i), P_2(z_i), \cdots, P_{t+1}(z_i)), i = 1, \cdots, N.$$

The tag which is composed by the coefficient of polynomial, can be obtained by computing

$$\begin{aligned} A(z) =& \mathbf{x}_1 P_1(z) + \cdots + \mathbf{x}_t P_t(z) + \mathbf{x}_{t+1} P_1(z)^2 + \cdots \\ &+ \mathbf{x}_{2t} P_t(z)^2 + \mathbf{x}_{2t+1} P_1(z) P_2(z) + \cdots + \mathbf{x}_{\binom{t+2}{2}-1} P_{t-1}(z) P_t(z) + P_{t+1}(z). \end{aligned}$$

2. The message $(m_0, m_1, \cdots, m_{(\binom{t+2}{2}-1)v_0-1}, a_1, a_2, \cdots, a_{ut}, A(z))$ is composed of the information part, random part and MAC part, where $(m_0, m_1, \cdots, m_{(\binom{t+2}{2}-1)v_0-1})$ is the secret message and $(a_1, a_2, \cdots, a_{ut})$ are random values. The dimension of FRS code is $ut + (\binom{t+2}{2} - 1)v_0 + tv_0 + v_0$. The parameters v_0, u, q make the receiver's decoding capability up to t errors (for FRS code).

3. The sender encodes the message to a codeword c using the FRS encoding algorithm. Each wire j transmits a vector $(f(\gamma^{ju}), f(\gamma^{ju+1}), \cdots, f(\gamma^{ju+u-1}), r_j)$ for $1 \leq j \leq 2t + ct$.

Bob does the following:

1. The receiver receives the vector $(\mathbf{r}_i, Y_{i,1}, Y_{i,2}, \cdots, Y_{i,u})$ from wire i.

2. The receiver applies FRS list decoding in Section 3.2.1 to the received vector Y and decode a list of messages. *The list will always include the correct message.*

3. The receiver constructs the authentication vector $(\mathsf{MAC}(\mathbf{x}, \mathbf{r}_1) \stackrel{?}{=} A(z_1), \mathsf{MAC}(\mathbf{x}, \mathbf{r}_2) \stackrel{?}{=} A(z_2), \cdots, \mathsf{MAC}(\mathbf{x}, \mathbf{r}_N) \stackrel{?}{=} A(z_N))$ to decide whether the decoded message acceptable. A message is acceptable if there are at least $t+1$ MAC function passing the verification. The decoder outputs $\perp$ if more than one acceptable message is found. Otherwise, it outputs the message $(m_0, m_1, \cdots, m_{(\binom{t+2}{2}-1)v_0})$ from the first $(\binom{t+2}{2}-1)v_0$ positions of the decoded message.

Theorem 21. *The protocol above is a 1-round (0, δ)-SMT for $N = (2+c)t$ with optimal transmission rate, and polynomial time decoding. The value of δ is given by $\frac{2(t+1)}{q}$ and is the smallest among all known protocols with the same connectivity.*

Proof. Perfect Privacy:

The adversary knows ut positions of codeword, while the dimension of FRS code is $ut + \binom{t+2}{2}v_0 + (t+1)v_0$. Therefore the first ut elements are unknown to adversary and independent with the randomness sent in each wire. There are totally $\mathbb{F}_q^{\binom{t+2}{2}v_0}$ possible codewords that he can not make sure which one corresponds to the correct message. So he has no information for the value $(m_0, m_1, \cdots, m_{\binom{t+2}{2}v_0-1})$ which is independent with the randomness sent in each wires.

δ-Reliability:

The correct message $\mathbf{m}$ passes through the authentication is passed though at least $t+ct$ of the authentication test. Any other messages $\mathbf{m}'$ in the list decoding which are different from the correct one are failed to be checked with probability at most $\frac{2(t+ct)}{q^{v_0}}$. So the reliability

of 1-round SMT for $N = 2t + ct, c > 1/t$ using list decoding is at most $1 - \frac{2(t+ct)}{q}$.

Transmission rate:

The total number of elements that are transmitted is $uN + (2t + ct)(t + 1)v_0$. The transmission rate is $\frac{(2t+ct)c_0t+(2t+ct)(t+1)v_0}{\binom{t+2}{2}v_0}$ which is $\mathcal{O}(1)$. Therefore our 1-round $(0, \delta)$-SMT for $N = 2t + ct$ is optimal.

Computation Complexity:

The decoding of FRS code needs $\mathcal{O}((Nu \log q)^2)$ computation. The authentication needs $\mathcal{O}(q^{v_0})$ computation. Therefore the total time is $\mathcal{O}(q^{v_0})$ which is efficient.

□

Comparison with Related Work

There has been two other optimal (in transmission rate) and efficient (in computation) 1-round (0, δ)-SMT protocols for higher connectivity ($N = (2 + c)t, c > \frac{1}{t}$) [72, 83]. But our protocol using list decoding of FRS codes and multi-receiver MAC has better reliability than both of them. The comparison with related work is outlined in Table 6.5.

Table 6.4: Comparison with 1-round $(0, \delta)$-SMT protocols for $N = 2t + 1$

Author	**Comp.**	δ	**Optimality**	**Outputs Incorrect Message**
Safavi-Naini *et al.* [72]	*Poly.*	$\leq \frac{Nt(t+1)}{q}$	Yes	Yes
Tuhin *et al.* [83]	*Poly.*	$\leq \frac{t(t+1)}{q}$	Yes	No
This Work	*Poly.*	$\leq \frac{2(t+1)}{q}$	Yes	No

6.6 Proof of Chapter 6

6.6.1 Details of 1-round (0, δ)-SMT for $N = (2 + c)t$

$$\begin{aligned} \frac{v}{v+1}ct &> \frac{t-tv}{v+1} + \frac{v}{v+1}\frac{c_0t^2 + \binom{t+2}{2}v + (t+1)v}{c_0t - v + 1} \\ c &> \frac{1}{v} - 1 + \frac{c_0t^2 + \binom{t+2}{2}v + (t+1)v}{c_0t^2 - vt + t}. \end{aligned} \tag{6.5}$$

If we choose constant value $v = v_0$ and $t \gg v_0$, the value c that promise the receiver can apply FRS code to the list decoded messages is

$$c > \frac{v_0}{c_0} + \frac{1}{v_0}.$$

6.6.2 Proof of Lemma 31

Proof. Consider the case that there are $k-1$ receivers who want to cheat an honest receiver i. Colluders want to forge a message and tag pair, $m' = (m'_1, m'_2, \cdots, m'_d, A'(z))$ where $(m'_1, m'_2, \cdots, m'_d) \neq (m_1, m_2, \cdots, m_d)$. The colluders know their $k-1$ keys, but do not know the secret key of user i, given by $P_1(z_i), P_2(z_i), \cdots, P_d(z_i), P_{d+1}(z_i)$. The known message and tag pair is given by,

$$A(z_i) = P_1(z_i)m_1 + P_2(z_i)m_2 + \cdots + P_d(z_i)m_d + P_{d+1}(z_i) \mod q^{v'}.$$

Since the forgery $m', A'(z)$, must pass the receiver i verification, it should satisfy the equation:

$$A'(z_i) = P_1(z_i)m'_1 + P_2(z_i)m'_2 + \cdots + P_d(z_i)m'_d + P_{d+1}(z_i) \mod q^{v'}.$$

It means the secret authentication key of receiver i satisfies,

$$\Delta A(z_i) = P_1(z_i)\Delta m_1 + P_2(z_i)\Delta m_2 + \cdots + P_d(z_i)\Delta m_d \mod q^{v'}.$$

So, there are $q^{v'(d-1)}$ choices for receiver i's secret key $P_1(z_i), P_2(z_i), \cdots, P_d(z_i)$. On the other hand, $P_1(z_i), P_2(z_i), \cdots, P_d(z_i)$ are totally random in adversary's view because she sees at most $k-1$ points of the polynomials $P_1(z_j), P_2(z_j), \cdots, P_d(z_j)$ where j is a corrupted receiver, and the values $P_1(z_i), P_2(z_i), \cdots, P_d(z_i)$ are blinded by $P_{d+1}(z_i)$. Therefore the probability that $P_1(z_i), P_2(z_i), \cdots, P_d(z_i)$ satisfy the above equation is $1/q^{v'}$. This means that the probability that the colluders success chance in constructing another message and tag pair $m', A'(x)$ that passes the honest receiver authentication is less than $1/q^{v'}$.

□

6.6.3 Proof of Lemma 32

Proof. For any message $m', A'(z)$ the chance of passing through the honest receiver's authentication is to satisfy:

$$\begin{aligned}\mathsf{MAC}(m', r) = {} & m'_1 P_1(z_i) + \cdots + m'_t P_t(z_i) + m'_{t+1} P_1(z_i)^2 + \cdots + m'_{2t} P_t(z_i)^2 + m'_{2t+1} P_1(z_i) P_2(z_i) \\ & + \cdots + m'_{\binom{t+2}{2}-1} P_{t-1}(z_i) P_t(z_i) + P_{t+1}(z_i) = A'(z_i).\end{aligned}$$

which means the vector $P_1(z_i), P_2(z_i), \cdots, P_t(z_i)$ satisfying

$$\begin{aligned}& \Delta m_1 P_1(z_i) + \cdots + \Delta m_t P_t(z_i) + \Delta m_{t+1} P_1(z_i)^2 + \cdots + \Delta m_{2t} P_t(z_i)^2 + \Delta m_{2t+1} P_1(z_i) P_2(z_i) \\ & + \cdots + \Delta m_{\binom{t+2}{2}-1} P_{t-1}(z_i) P_t(z_i) = \Delta A(z_i).\end{aligned}$$

There are totally $2q^{v'(t-1)}$ of $(P_1(z_i), P_2(z_i), \cdots, P_t(z_i))$ satisfying the polynomial. Because the number of random values for $(P_1(z_i), P_2(z_i), \cdots, P_t(z_i))$ is $q^{tv'}$, the adversary's success probability is at most $2/q^{v'}$.

□

Chapter 7

Conclusion

Secure and reliable communication over adversarial channel is a growing area in information security. In this dissertation, we considered four secure communication models: *limited view adversary channel, adversarial wiretap channel, adversarial wiretap channel with public discussion*, and *Secure Message Transmission*. We studied these models and proposed protocols to achieve secure communication in the models. We summarize our result and propose future research directions.

7.1 Limited View Adversarial Channel

We formalized the model of limited view adversary, and proposed the definition of LV codes to provide reliable communication. We defined the capacity as the highest rate that is achievable over a limited view adversary channel. We gave an upper bound on the rate of LV code families. We gave two efficient constructions of LV code families. The first LV-code construction achieves the bound with reading and writing parameter $S_r = S_w$. The second LV-code construction achieves the bound with equality when $\rho_r < 1 - \rho_w$ and so is capacity achieving.

LV codes provide a coding theoretic framework for the study of 1-round symmetric δ-RMT. The construction of RMT protocol obtained from the LV code in this dissertation has the lowest δ, and provides security for the case that $S_r \neq S_w$.

Open questions

- Construction of LV code families with $\rho_r > 1 - \rho_w$ and small designed δ, for example $\delta < 1/2$, is an open question. A list decodable code corrects errors up to $1 - \rho_w$ where ρ_w

is the fraction of errors and assuming the adversary can see the whole codeword ($\rho_r = 1$) before constructing the error vector. We showed that unique decoding for this fraction error is possible if the read fraction ρ_r is bounded. Finding the relationship between the list size and ρ_r is an open question.

- Our current LV code assumes that the message transmission is one-way from the sender to the receiver. Extending this work to include interaction and also other resources such as extra channels, or allowing interaction are future works.

7.2 Adversarial Wiretap Channel

We proposed a model for active adversaries in wiretap channels, derived secrecy capacity and gave an explicit construction for a family of capacity achieving codes. The model is a natural extension of Wyner wiretap models when the adversary is active and can use its view of the communication channel to introduce adversarial noise in the main channel. In our model, the adversary's read capability (choosing the codeword components that will be seen) is the same as wiretap II model. However unlike wiretap II in which communication over the main channel is noiseless, we allow this channel to be corrupted by the adversary's additive noise. The number of components affected by the noise is a constant fraction of the codeword length. We allow the adversary's eavesdropped information to be used to construct the adversarial noise. Previous work on active adversaries (See Section 4.1) consider an eavesdropper whose view of communication is not available to the jammer adversary that corrupts the communication.

AWTP model provides a framework for studying SMT which so far had been studied independent from wiretap model. The fruitfulness of this relation is demonstrated by deriving a new lower bound on the transmission rate of 1-round (ϵ, δ) symmetric SMT protocols.

Open questions

- The AWTP channel only assumes secure message transmission in one-way. More general settings such as allowing interaction between the sender and the receiver will be interesting directions for future work.

- Key agreement problem has been considered over wiretap channel with passive eavesdropping adversary [62]. But in reality, the adversary can implement active attacks to the channel of key agreement protocol. So another important direction for future work is the study of key agreement problem over adversarial wiretap channel model.

- We showed the upper bound on the rate of adversarial wiretap channels. This bound is for any alphabet size, and for small alphabets such as $\mathbb{F}_2$ may not be tight. Proving upper bounds on the rate of an adversarial wiretap channel with constant size alphabets and in particular binary alphabets, remains a challenging open problem. Our adversarial wiretap code is constructed over large alphabets. Constructing of capacity achieving codes for constant size alphabets and in particular binary alphabets, remain a challenging open problem.

- Extending the model to network setting, where each node is connected to a number of nodes and a message passes through a number of intermediate nodes to reach the destination remains an interesting open question.

7.3 Adversarial Wiretap Channel with Public Discussion

We motivated and introduced $\mathsf{AWTP}_{\mathsf{PD}}$ protocol, where Alice and Bob, in addition to the AWTP channel, have access to a public discussion channel and showed that with this new resource, secure communication is possible even when $\rho_r + \rho_w \geq 1$ as long as $\rho < 1$. We

derived an upper bound on the information rate, and a lower bound on the number of message rounds of protocols that provide ϵ-secrecy and δ-reliability, and constructed an optimal protocol family that achieve both these bounds. We showed the relationship between $\mathsf{AWTP_{PD}}$ protocol and (ϵ, δ)-SMT$^{[ows]}$-PD protocols in which wires are used by Alice only, and gave the construction of an optimal (ϵ, δ)-SMT$^{[ows]}$-PD protocol with minimum number of message rounds. A three-round protocol SMT-PD (two-way wires) with the same rate had been constructed in [75]. Our construction shows that assuming one-way communication over wires does not affect the number of message rounds of the optimal protocols.

Open questions

- $\mathsf{AWTP_{PD}}$ protocols remove the restriction of $\rho_r + \rho_w \leq 1$ and allow secure communication when $\rho_r + \rho_w \geq 1$ as long as $|S_r \cup S_w| < N$. In our model although we allow interaction, but the AWTP channel is one-way. An interesting open question is to obtain rate and lower bounds for round complexity for the case that interaction over the AWTP channel is possible.

- Our current $\mathsf{AWTP_{PD}}$ protocol is considered over interactive public discussion channel. This needs authenticated public discussion channel from sender to receiver, and vice versa. An open question is to construct $\mathsf{AWTP_{PD}}$ protocols over one-way AWTP channel with one-way PD channel only.

7.4 Secure Message Transmission

In Chapter 6 we show that 1-round δ-RMT and $(0, \delta)$-SMT can be constructed from list decodable code and MAC. The approach is particularly interesting because, (i) it is general and applicable to any connectivity including $N = 2t + k$, where k is a constant, (ii) relies on well-studied mathematical objects (list decodable codes and MACs) and so allow a wide range of instantiations, and direct translation of advances in those areas into better con-

structions for 1-round δ-RMT and $(0, \delta)$-SMT, and finally (iii) resulting in proofs of security and reliability to be straightforward.

Open questions

- Instantiation of this general approach, using FRS codes and our proposed multireceiver MACs result in constructions that have optimal transmission rates and the smallest δ, when $N = 2t + 1$ and $N = (2 + c)t$. For $N = 2t + 1$ however, the protocols are not computationally efficient, and we leave construction of protocols that achieve the same performance with efficient decoding, as an interesting open problem.

- $(0, \delta)$-SMT protocol has perfect security and δ decoding error probability. The SMT protocol with lower δ decoding error probability will make receiver high reliability to recover the correct message. Another open question is how to design $(0, \delta)$-SMT protocol with lower decoding error probability.

- The lower bound of decoding error for $(0, \delta)$-SMT has been considered by Kurosawa *et al.* [48]. But there is a gap between the $(0, \delta)$-SMT protocol with lowest decoding error (Table 6.2) and the lower bound on decoding error (Corollary 2 [48]). Finding a better lower bound for $(0, \delta)$-SMT protocol remains a challenging open question.

Bibliography

[1] S. Agarwal, R. Cramer, and R. de Haan. Asymptotically optimal two-round perfectly secure message transmission. In C. Dwork, editor, *Advances in Cryptology - CRYPTO 2006 - 26th Annual Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 394–408. Springer, 2006.

[2] V. Aggarwal, L. Lai, A. R. Calderbank, and H. V. Poor. Wiretap channel type II with an active eavesdropper. In *IEEE International Symposium on Information Theory, ISIT 2009, June 28 - July 3, 2009, Seoul, Korea, Proceedings*, pages 1944–1948. IEEE, 2009.

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

[4] R. Ahlswede and Z. Ffir. Elimination of correlation in random codes for arbitrarily varying channels. *Geb*, 44:159–175, 1978.

[5] A. R. S. W. M. Andrew Thangaraj, Souvik Dihidar and J. M. Merolla. Applications of ldpc codes to the wiretap channel. *IEEE Transactions on Information Theory*, 53(8):2933–2945, 2007.

[6] M. Bellare, S. Tessaro, and A. Vardy. Semantic security for the wiretap channel. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 294–311. Springer, 2012.

[7] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In J. Simon,

editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 1–10. ACM, 1988.

[8] J. Bierbrauer, T. Johansson, G. Kabatianskii, and B. Smeets. On families of hash functions via geometric codes and concatenation. In Y. Desmedt, editor, *Advances in Cryptology - CRYPTO 1994 - 14nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 21-25, 1994. Proceedings*, volume 839, pages 331–342. Springer, 1994.

[9] M. Bloch and J. Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, November 2011.

[10] M. B. Bloch and J. N. Laneman. Information-spectrum methods for information-theoretic security. In *Information Theory and Applications Workshop, 2009*, pages 23–28. IEEE, Feb 2009.

[11] M. R. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6):2515–2534, 2008.

[12] H. Boche and R. F. Schaefer. Capacity results and super-activation for wiretap channels with active wiretappers. *IEEE Transactions on Information Forensics and Security*, 8(9):1482–1496, 2013.

[13] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 197–213. IEEE, 2003.

[14] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 11–19. ACM, 1988.

[15] M. Cheraghchi, F. Didier, and A. Shokrollahi. Invertible extractors and wiretap protocols. *IEEE Transactions on Information Theory*, 58(2):1254–1274, 2012.

[16] T. M. Cover and J. A. Thomas. *Elements of information theory (2. ed.)*. Wiley, 2006.

[17] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In N. P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 471–488. Springer, 2008.

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

[19] I. Csiszár and P. Narayan. The capacity of the arbitrarily varying channel revisited: Positivity, constraints. *IEEE Transactions on Information Theory*, 34(2):181–193, 1988.

[20] L. Czap, V. M. Prabhakaran, C. Fragouli, and S. N. Diggavi. Secret message capacity of erasure broadcast channels with feedback. In *Information Theory Workshop*, pages 65–69. IEEE, 2011.

[21] L. B. David Blackwell and A. J. Thomasian. The capacities of the certain of certain channel classes under random coding. 31(3):558–567, 1960.

[22] Y. Desmedt, S. Erotokritou, and R. Safavi-Naini. Simple and communication complexity efficient almost secure and perfectly secure message transmission schemes. In D. J. Bernstein and T. Lange, editors, *Progress in Cryptology - AFRICACRYPT 2010, Third International Conference on Cryptology in Africa, Stellenbosch, South Africa, May 3-6, 2010. Proceedings*, volume 6055 of *Lecture Notes in Computer Science*, pages 166–183. Springer, 2010.

[23] Y. Desmedt, Y. Frankel, and M. Yung. Multi-receiver/multi-sender network security: Efficient authenticated multicast/feedback. In *INFOCOM*, volume 3, pages 2045–2054. IEEE, 1992.

[24] B. K. Dey, S. Jaggi, and M. Langberg. Codes against online adversaries. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 1169–1176. IEEE, 2009.

[25] Y. Ding, P. Gopalan, and R. Lipton. Error correction against computationally bounded adversaries. *Theory of Computing Systems*, 2006.

[26] Y. Dodis, J. Katz, L. Reyzin, and A. Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. In C. Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 232–250. Springer, 2006.

[27] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM journal on computing*, 38(1):97–139, 2008.

[28] D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *J. ACM*, 40(1):17–47, 1993.

[29] Z. Dvir and S. Lovett. Subspace evasive sets. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC, pages 351–358, New York, NY, USA, 2012. ACM.

[30] P. Elias. Error-correcting codes for list decoding. *Information Theory, IEEE Transactions on*, 37(1):5–12, 1991.

[31] M. Fitzi, M. Franklin, J. Garay, and S. H. Vardhan. Towards optimal and efficient perfectly secure message transmission. In *Theory of Cryptography*, pages 311–322. Springer, 2007.

[32] G. D. Forney and G. D. Forney. *Concatenated codes*, volume 11. MIT Press, Cambridge, Massachusetts, 1966.

[33] M. K. Franklin and R. N. Wright. Secure communication in minimal connectivity models. *J. Cryptology*, 13(1):9–30, 2000.

[34] J. Garay, C. Givens, and R. Ostrovsky. Secure message transmission with small public discussion. In *Advances in Cryptology–EUROCRYPT 2010*, pages 177–196. Springer, 2010.

[35] J. Garay and R. Ostrovsky. Almost-everywhere secure computation. In *Advances in Cryptology–EUROCRYPT 2008*, pages 307–323. Springer, 2008.

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

[37] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984.

[38] V. Guruswami. Linear-algebraic list decoding of folded reed-solomon codes. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, June 8-10, 2011*, pages 77–85. IEEE, 2011.

[39] V. Guruswami and A. Rudra. Explicit capacity-achieving list-decodable codes. In J. M. Kleinberg, editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 1–10. ACM, 2006.

[40] V. Guruswami and A. Smith. Codes for computationally simple channels: Explicit constructions with optimal rate. In *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*, pages 723–732. IEEE, 2010.

[41] R. W. Hamming. Error detecting and error correcting codes. *Bell System Technical Journal*, 29(2):147–160, 1950.

[42] M. Hayashi and R. Matsumoto. Construction of wiretap codes from ordinary channel codes. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2538–2542. IEEE, 2010.

[43] E. Hof and S. Shamai. Secrecy-achieving polar-coding for binary-input memoryless symmetric wire-tap channels. *arXiv preprint arXiv:1005.2759*, 2010.

[44] H. B. Igor Bjelaković and J. Sommerfeld. Capacity results for arbitrarily varying wiretap channels. In *Information Theory, Combinatorics, and Search Theory*, pages 123–144. Springer, 2013.

[45] B. Kanukurthi and L. Reyzin. Key agreement from close secrets over unsecured channels. In A. Joux, editor, *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*, pages 206–223. Springer, 2009.

[46] J. Katz and Y. Lindell. *Introduction to modern cryptography.* CRC Press, 2014.

[47] K. Kurosawa and K. Suzuki. Truly efficient 2-round perfectly secure message transmission scheme. In *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, pages 324–340. Springer, 2008.

[48] K. Kurosawa and K. Suzuki. Almost secure (1-round, n-channel) message transmission scheme. *IEICE Transactions*, 92-A(1):105–112, 2009.

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

[50] M. Langberg. Private codes or succinct random codes that are (almost) perfect. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '04, pages 325–334, Washington, DC, USA, 2004. IEEE.

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

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

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

[54] A. Lapidoth and P. Narayan. Reliable communication under channel uncertainty. *IEEE Transactions on Information Theory*, 44(6):2148–2177, 1998.

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

[56] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Information theoretic security. *Found. Trends Commun. Inf. Theory*, 5(4):355–580, 2009.

[57] R. J. Lipton. A new approach to information theory. In *STACS 94*, pages 699–708. Springer, 1994.

[58] T. Liu and S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Transactions on Information Theory*, 55(6):2547–2553, 2009.

[59] 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.

[60] Y. M. Martin Dietzfelbinger, Joseph Gil and N. Pippenger. Polynomial hash functions are reliable. In *Automata, Languages and Programming*, pages 235–246. Springer, 1992.

[61] U. M. Maurer. Protocols for secret key agreement by public discussion based on common information. In E. F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 461–470. Springer, 1992.

[62] U. M. Maurer and S. Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, pages 351–368, 2000.

[63] U. M. 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.

[64] E. MolavianJazi, M. Bloch, and J. N. Laneman. Arbitrary jamming can preclude secure communication. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 1069–1075. IEEE, 2009.

[65] M. Naor, G. Segev, and A. Smith. Tight bounds for unconditional authentication protocols in the manual channel and shared key models. In *Advances in Cryptology*

- *CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, pages 214–231. Springer, 2006.

[66] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. In *Advances in Cryptology: Proceedings of EUROCRYPT 84, A Workshop on the Theory and Application of of Cryptographic Techniques, Paris, France, April 9-11, 1984, Proceedings*, pages 33–50, 1984.

[67] A. Patra, A. Choudhury, C. P. Rangan, and K. Srinathan. Unconditionally reliable and secure message transmission in undirected synchronous networks: possibility, feasibility and optimality. *IJACT*, 2(2):159–197, 2010.

[68] C. Peikert. *Cryptographic error correction*. PhD thesis, Massachusetts Institute of Technology, 2006.

[69] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun. Investigation of signal and message manipulations on the wireless channel. In *Computer Security - ESORICS 2011 - 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14, 2011. Proceedings*, pages 40–59, 2011.

[70] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In D. S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA*, pages 73–85. ACM, 1989.

[71] R. Renner and S. Wolf. The exact price for unconditionally secure asymmetric cryptography. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 109–125. Springer, 2004.

[72] R. Safavi-Naini, M. A. Tuhin, and H. Shi. Optimal message transmission protocols with flexible parameters. In B. S. N. Cheung, L. C. K. Hui, R. S. Sandhu, and D. S. Wong, editors, *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011, Hong Kong, China, March 22-24, 2011*, pages 453–458. ACM, 2011.

[73] R. Safavi-Naini and P. Wang. Codes for limited view adversarial channels. In *Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*, pages 266–270. IEEE, 2013.

[74] C. E. Shannon. A mathematical theory of communication. *Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[75] H. Shi, S. Jiang, R. Safavi-Naini, and M. A. Tuhin. On optimal secure message transmission by public discussion. *IEEE Transactions on Information Theory*, 57(1):572–585, 2011.

[76] M. S. Silvio Micali, Chris Peikert and D. Wilson. Optimal error correction against computationally bounded noise. In *Theory of Cryptography*, pages 1–16. Springer, 2005.

[77] G. J. Simmons. Authentication theory/coding theory. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 411–431. Springer, 1984.

[78] A. Smith. Scrambling adversarial errors using few random bits, optimal information reconciliation, and better private codes. In *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '07, pages 395–404, Philadelphia, PA, USA, 2007. SIAM.

[79] K. Srinathan. *Secure distributed communication.* PhD thesis, PhD Thesis, IIT Madras, 2006.

[80] K. Srinathan, A. Choudhary, A. Patra, and C. P. Rangan. Efficient single phase unconditionally secure message transmission with optimum communication complexity. In R. A. Bazzi and B. Patt-Shamir, editors, *Proceedings of the Twenty-Seventh Annual ACM Symposium on Principles of Distributed Computing, PODC 2008, Toronto, Canada, August 18-21, 2008*, page 457. ACM, 2008.

[81] K. Srinathan, A. Narayanan, and C. P. Rangan. Optimal perfectly secure message transmission. In M. K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 545–561. Springer, 2004.

[82] D. Stinson. On the connections between universal hashing, combinatorial designs and error-correcting codes. *Congressus Numerantium*, pages 7–28, 1996.

[83] M. A. Tuhin and R. Safavi-Naini. Optimal one round almost perfectly secure message transmission (short paper). In G. Danezis, editor, *Financial Cryptography and Data Security - 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28 - March 4, 2011, Revised Selected Papers*, volume 7035 of *Lecture Notes in Computer Science*, pages 173–181. Springer, 2011.

[84] P. Wang and R. Safavi-Naini. A model for adversarial wiretap channel. *arXiv preprint arXiv:1312.6457*, 2013.

[85] P. Wang and R. Safavi-Naini. Adversarial wiretap channel with public discussion. CoRR abs/1403.5598, 2014.

[86] P. Wang and R. Safavi-Naini. An efficient code for adversarial wiretap channel. In *In*

Proceedings of the 2014 IEEE Information Theory Workshop, Hobart, Australia, Nov 2-5,, pages 40–44. IEEE, 2014.

[87] Y. Wang. Robust key establishment in sensor networks. *SIGMOD Record*, 33(1):14–19, 2004.

[88] J. Wu and D. R. Stinson. Three improved algorithms for multipath key establishment in sensor networks using protocols for secure message transmission. *IEEE Transactions on Dependable and Secure Computing*, 8(6):929–937, 2011.

[89] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal, The*, 54(8):1355–1387, Oct 1975.

[90] V. Zyablov and M. Pinsker. List cascade decoding. *Problems of Information Transmission*, 17(4):29–34, 1981.