Information Theoretic Approaches for Security and Privacy

By

WENWEN TU

B.E. (University of Science and Technology of China, Hefei, China) 2013

DISSERTATION

Submitted in partial satisfaction of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

Electrical and Computer Engineering

in the

OFFICE OF GRADUATE STUDIES

of the

UNIVERSITY OF CALIFORNIA

DAVIS

Approved:

Assoc. Lifeng Lai, Chair

Prof. Shuguang Cui

Prof. Bernard C. Levy

Committee in Charge

2018

Wenwen Tu
Sept. 2018
Electrical and Computer Engineering

Abstract

Information Theoretic Approaches for Security and Privacy

Information theoretic security and privacy is an emerging field in information theory that aims to secure future generations of communication systems by exploiting physical layer properties of communication channels or sources. The notion "information theoretic" means that the security and privacy of the system does not depend on the computational power of the adversary, i.e., it cannot be compromised even when the adversary has an unlimited computational power. In this dissertation, we examine several information theoretic security and privacy issues, including *Simulatability condition, Secret key sharing, Message authentication* and *Function computation*.

Utilizing a common secret key for communication is a basic approach to protect secrecy and privacy. In the first part of this dissertation, we investigate the problem of checking *simulatability condition*, a fundamental concept in studying key generation in the presence of an active adversary. This condition determines whether there exist communication protocols so that the legitimate parties are able to share secret keys in certain important scenarios. In this problem, we provide an efficient algorithm to check whether the simulatability condition holds or not. Furthermore, we provide an efficient algorithm for finding the attack strategy that the adversary can use to attack the key generation process. We also show that simulatability condition is not sensitive on the knowledge about the adversary's observations.

We then investigate the problem of simultaneously generating multiple keys in a joint source-channel model in Chapter 3. In this problem, we first study a special case where Eve has no side information and provide a full characterization on the secret-key capacity region.

The obtained result shows that there exists a trade-off between individual secret-key rates. Then we generalize the result into the general case where Eve has side information, and fully characterize the corresponding secret-key capacity region as well.

In Chapter 4, we consider the problem of keyless message authentication over noisy channels. We study how to exploit the channel properties to guarantee that the receiver is able to determine the authenticity of received messages. We characterize both the authentication exponent (the speed at which the optimal successful attack probability can be driven to zero) and the authenticated capacity (the largest message rate at which the optimal successful attack probability can be made arbitrarily small).

The goal of secure function computation is to design methods for communication parties to compute a function over their inputs while keeping those inputs private. We investigate both secrecy and privacy issues in the problem of function computation. We allow distortion in the computed function and study the relationship of the message rates, the rate distortion, the private information leakage of the transmitters' sources to the receiver, and the secrecy of those sources at the eavesdropper. We fully characterize the achievable region of these parameters in a special case. We further provide both inner and outer bounds for the general case. These inner and outer bounds are tight for certain scenarios.

Acknowledgement

I would like to say thanks to many people, without whose supports this dissertation along with the work invested to it would have not been possible.

First of all, I would like to express my sincere gratitude to my research advisor Dr. Lifeng Lai, for his guidance and encouragement through my career as a Ph.D. student these years. I appreciate it that he took me into the research area of information theory, and shared me his valuable insights in analyzing and solving meaningful problems. I am also grateful to him for the time he has spent in suggesting me potential research directions, correcting my writing style as well as writing papers together with me. I learnt a lot from him, not only because of his talent in supervising students but also his charming personality. It is a marvelous pleasure to work under his supervision.

I am indebted to Prof. Bernard C. Levy, Prof. Shuguang "Robert" Cui and Prof. Khaled Abdel-Ghaffar, for the time they spent in evaluating this dissertation and the final exit seminar. I am also thankful to Prof. Zhi Ding and Dr. Yingbin Liang, who served on my Ph.D. qualifying exam committee. It is both my honor and my pleasure to share my research work with them all.

I want to thank all my friends and colleagues in the last five years, especially Dr. Jun Geng and Dr. Ain-ul-Aisha who spent lots of time, together with me, in study, chatting and discussing interesting problems in the lab. In addition, I want to acknowledge all faculty and staff in the department of Electrical and Computer Engineering for their efforts in providing the students a pleasant atmosphere so that I could focus on study and self improvement.

Last but not least, I would like to express my appreciation to my family for their emotional support of my decision of pursuing a Ph.D. degree. Especially, I want to say thanks to my wife, Wenwen Zhao, who has the same footprint with me pursuing a Ph.D. degree here. Without their unconditional love and support, I cannot imagine how my life of the last five years would have been.

The work involved in this dissertation was supported in part by the National Science Foundation under Grants CCF-1760889, CCF-1665073, ECCS-1408114 and ECCS-1660140, and the National Science Foundation CAREER Award under Grant CCF-1318980.

Contents

List of Figures

Chapter 1

Introduction

Security and privacy are two of the most important issues in communications. Security issues arising in communication networks include, but not limited to, *confidentiality, authentication* and *privacy*: 1) Confidentiality is a property that information is kept confidential from unauthorized parties; 2) Authentication guarantees that the legitimate recipients have the ability to identify the transmitter of the received information; and 3) Privacy is a practice to help individuals selectively express themselves and keep their inputs private.

There have been many existing studies on security and privacy issues from a variety of perspectives [5, 12, 29, 71, 102]. The adversaries can be divided into two classes: *eavesdroppers* (or passive attackers) and *active attackers*. An eavesdropper is a listener, who does not interfere with the legitimate communication while an active attacker could not only listen, but also intercept, modify and even falsify signals to interfere with the legitimate communication. Information theoretic security and privacy is an emerging field in information theory that aims to secure future generations of communication systems by exploiting physical layer properties of communication channels or sources. The notion of "information theoretic" means that the security does not depend on the computational power of the adversary, i.e., it cannot be compromised even when the adversary has an unlimited computational power.

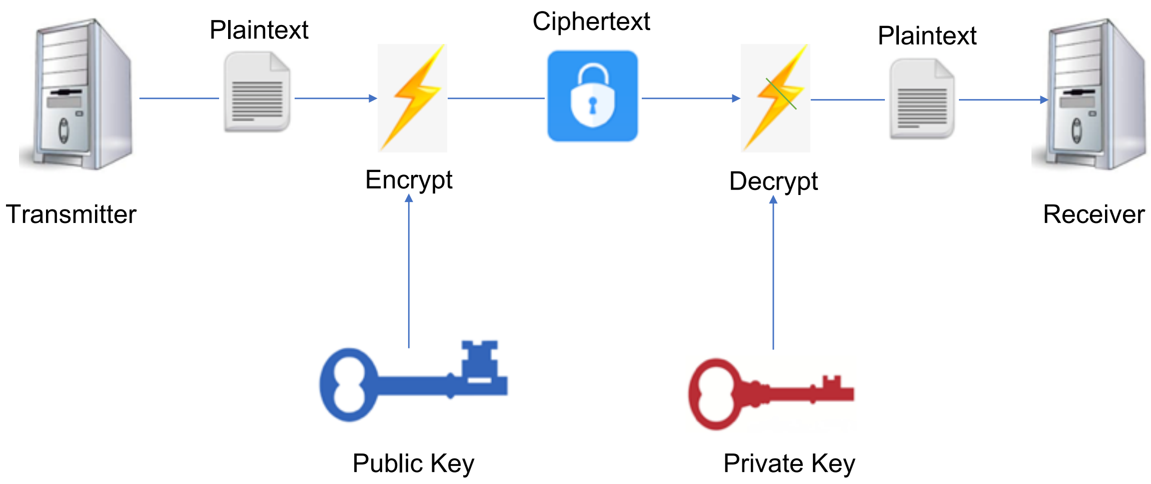


Figure 1.1: Public-key cryptosystem.

1.1 Computational Security vs Information Theoretic Security

There are two popular security notions: computational security and information theoretic security. Roughly speaking, the computational security is based on the assumptions that the adversary is computationally limited and certain mathematical problems are difficult to solve within given time, while the information theoretic security makes no such assumptions. In cryptography, a cryptosystem is said to be computationally secure or conditionally secure, if the cost and the time to break the cipher exceeds the value and the useful lifetime of the encrypted information. A cryptosystem is said to be information theoretically secure or unconditionally secure if the generated ciphertext does not leak any information about the corresponding plaintext even when the adversary has unlimited computational power. Thus, such cryptosystems are typically considered to be cryptanalytically unbreakable.

As illustrated in Fig.1.1, an example of the computational security cryptosystem is *public-key* encryption system, which is also referred as *asymmetric key* cryptosystem since the encryption and decryption use different keys [76]. The well known public-key cryptosystem, *RSA*, is a classic computational security system. The RSA algorithm consists of four stages:

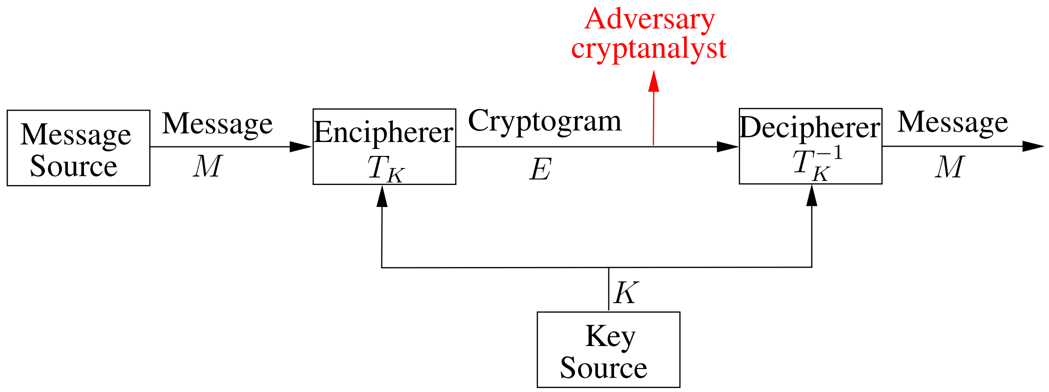


Figure 1.2: Shannon's cryptosystem.

key generation, key distribution, encryption and decryption. In the key generation stage, the RSA receiver randomly chooses two large prime numbers, based on which it creates one public key and one private key. Then the public key is released to the public including the transmitter during the key distribution stage. After receiving the public key, the transmitter uses it to encrypt the transmitted information and sends it to the receiver. Finally, the receiver decrypts the received message using its private key. It has been proved that, using the private key, the message decrypted from the ciphertext encrypted with the public key is the same with the original message. The secrecy of the transmitted message in the RSA cryptosystem relies on the computational hardness assumptions of two mathematical problems: the RSA problem and the problem of factoring large numbers [1, 13, 76, 108]. That is, given the public key generated in the key generation stage, it is practically difficult to determine the corresponding private key, and given the ciphertext, it is also difficult to infer the encrypted message with only public key. Similarly, there exists a variety of cryptographic hardness assumptions that are widely used in various computational security systems. However, one common challenge is that the hardness of these underlying problems is unproven. In addition, the security of the computationally secure system is compromised once the adversary has sufficiently large computational power. Thus, many researchers seek to create certain systems that are unconditionally secure.

The information theoretic approaches for security and privacy open new directions in achieving unconditionally secure communication systems. Shannon initiated the information theoretic analysis of security for secret-key communication system. In his classic model of the communication system as illustrated in Fig.1.2, the source would like to confidentially transmit a message M to the decipherer over a public noiseless channel, to which the adversary has full access [81]. The encipherer and the decipherer are assumed to have access to a key source (i.e., they pre-share a secret key K) that is unknown to the adversary). As the adversary will receive an identical copy of the ciphertext transmitted over the channel, the message source encrypts M with K into ciphertext $E := T_K M$, where T_K denotes the K-th transformation of encryption, and transmits it over the channel. On the other end of the channel, the decipherer will use K to decrypt the received ciphertext E into the message via doing the reverse transformation: $M = T_K^{-1} E$. A cipher system is considered to be *perfectly secure* if the ciphertext E contains no information of the plaintext message M, i.e., $I(M; E) = 0$, where $I(\cdot; \cdot)$ denotes the mutual information of its arguments. Shannon showed that perfect secrecy can be achieved only if the length of the secret key is larger than or equal to the length of the plaintext, i.e., $H(K) \geq H(M)$, where $H(\cdot)$ denotes the entropy of its argument. A well known information theoretically secure scheme is the one-time pad scheme, which requires one-time use of the pre-shared key [37]. Besides the fact that it can be made perfectly secure, the secret key cryptosystem is also computationally efficient. However, to achieve perfect secrecy, the requirement on secret key is extremely high, as every time when we need to send a distinct message we need a new key.

From the discussion above, both computational security and information theoretic security have advantages and disadvantages. Computational security based systems are practically useful and have been widely adopted, but their security is based on unproved assumptions. Systems based on information theoretic security, on the other hand, can offer provable security, but they have stringent requirements. The fact that many challenges remain makes the information theoretic approaches not practically useful yet, e.g., how to enable communication parties to share high rate of secret keys. In this dissertation, we focus on designing information theoretically secure schemes:

- *Secret key sharing:* from the discussion above, we see that the secret key plays a significant role in protecting the confidentiality of the transmitted information. We will first design efficient algorithms to check *simulatability condition*, a condition that determines whether it is possible to generate secret keys when the attacker is active. Then, we will exploit our understanding in secret key sharing to study scenarios where multiply secret keys are required to be generated in the presence of an eavesdropper.

- *Keyless message authentication:* authentication is an important security primitive, which guarantees that the receiver can determine whether a message is truly from the claimed transmitter or it has been modified or even falsified by other users. We will design schemes to achieve this property without any pre-shared key.

- *Secure function computation:* the goal of secure function computation is to design protocols for communication parties to compute a function of their inputs and keep those inputs private. We investigate privacy issue in the secure function computation problem. In this problem, we will take both the secrecy and the privacy issues into consideration, and characterize the relationship of the message rates, the rate distortion, the private information leakage of the transmitters' sources to the receiver, and the secrecy of those sources at the eavesdropper.

In the following, we briefly introduce the problem setups that we will discuss in the following chapters, and review existing related results.

1.2 Introduction to Secret Key Sharing

As discussed above, enabling communication parties to share a common secret key is fundamental in cryptography. There are two main classes of existing key generation models: source models and channel models [2,3,9,15,17,19–21,33,47,55,59,60,69,86,104,105,109].

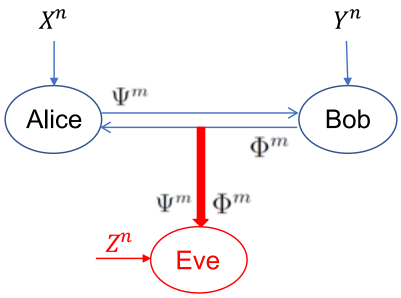


Figure 1.3: Basic setup in source.

Under the source model, the legitimate users have access to correlated random sources, from which they aim to generate secret keys by exchanging messages over a public noiseless channel [3, 19, 20, 55]. Under the channel model, the legitimate users typically have no correlated randomness in advance, but they can utilize the channel properties to obtain correlated sequences, from which the users can establish a secret key [21, 47, 69].

1.2.1 Key Generation under Source Model

As illustrated in Fig.1.3, in the basic setup of key generation via public discussion under the source model [3, 55], two legitimate users Alice and Bob, along with an eavesdropper Eve, have access to one component of three correlated sequences (X^n, Y^n, Z^n) respectively, which are i.i.d. generated according to a given joint PMF P_{XYZ}:

$$P_{X^nY^nZ^n}(x^n, y^n, z^n) = \prod_{i=1}^{n} P_{XYZ}(x_i, y_i, z_i).$$

Alice and Bob are connected via a public noiseless channel, to which Eve has full access. In order to agree on a common secret key, Alice and Bob are allowed to communicate with each other using the public noiseless channel. In particular, at the beginning of public discussion, Alice and Bob can generate two local randomnesses F_1 and F_2, which are independent of (X^n, Y^n, Z^n). Then, for each round use of the public channel, Alice transmits a message Ψ_i as a deterministic function of (F_1, X^n, Φ^{i-1}), and Bob transmits a message Φ_i as a deterministic function of $(F_2, Y^n, \Psi^{i-1}), i = 1, 2, \cdots$. In the end, after m rounds of public discussion, Alice and Bob can compute the key value by $K \triangleq K(F_1, X^n, \Psi^m)$ and $L \triangleq L(F_2, Y^n, \Phi^m)$, respectively.

Definition 1.1. A key rate R is said to be achievable if $\forall \epsilon > 0$, there exists a key generation protocol when n is sufficiently large, such that

$$\Pr\{K \neq L\} \leq \epsilon, \tag{1.1}$$

$$\frac{1}{n} I(K; Z^n, \Phi^m, \Psi^m) \leq \epsilon, \tag{1.2}$$

$$\frac{1}{n} H(K) \geq \frac{1}{n} \log |\mathcal{K}| - \epsilon, \tag{1.3}$$

$$\frac{1}{n} H(K) \geq R - \epsilon., \tag{1.4}$$

where $\mathcal{K}$ is the alphabet of K. We further define the maximal value of R as the corresponding key capacity C.

Here, (1.1) requires that the keys generated by Alice and Bob should be the same with high probability; (1.2) measures the information Eve has about the generated key and it should be negligible; (1.3) implies that the generated key should be uniformly distributed over the key value alphabet; and (1.4) measures the rate of the generated key.

Characterizing the key capacity in the basic setup is still an open problem. For the simplified case where $Z = \emptyset$, we have the following result.

Theorem 1.1 ([3,55])**.** If $Z = \emptyset$, the secret-key capacity is

$$C = I(X; Y). \tag{1.5}$$

To achieve a key with rate defined in (1.5), we can apply the Slepian-Wolf coding [16] to let Alice send partial information of X^n at the rate of $H(X|Y)$ ($H(\cdot|\cdot)$ denotes the conditional entropy of its arguments), to Bob via the public channel such that Bob can decode X^n correctly with high probability. And the unreleased information of rate $H(X) - H(X|Y) = I(X; Y)$ can be transformed as the final key. In particular, Alice will randomly and independently assign each typical X^n sequence into $2^{nH(X|Y)}$ bins using a uniform distribution, with each bin having around $2^{nI(X;Y)}$ X^n sequences. Upon observing a sequence X^n, Alice transmits the index of the bin in which X^n is, to the public channel. Then, with the observed Y^n as well as the received bin index, Bob can recover X^n correctly with high probability. Both Alice and Bob will set the sub-bin index within the bin of X^n as the key value. It can be shown that Eve has negligible information about the generated key, as the sub-bin index and bin index can be shown to be nearly independent. Thus, the generated key is secure from Eve.

For the general case when $Z \neq \emptyset$, active investigation is still undergoing. A well known lower bound and upper bound are listed as follows.

Theorem 1.2 ([3]). Given P_{XYZ}, the secret-key capacity C of X and Y with respect to Z is lower bounded by

$$C \geq \max_{V \to U \to X \to (Y,Z)} I(U;Y|V) - I(U;Z|V), \tag{1.6}$$

in which V and U are two auxiliary random variables and V. Furthermore, the secret-key capacity is upper bounded by

$$C \leq I(X;Y|Z). \tag{1.7}$$

Here, $I(\cdot;\cdot|\cdot)$ denotes the conditional mutual information; $V \to U \to X \to (Y,Z)$ means that (V,U,X,Y,Z) form a Markov chain in that order, and other similar relationships throughout the dissertation are defined in a similar manner. To achieve the lower bound defined in (1.6), we can i.i.d. generate $2^{nI(X;V)}$ sequences V^n, and for each generated V^n, i.i.d. generate $2^{nI(X;U|V)}$ sequences U^n according to $P_{U|V}$. Then we randomly and independently assign each sequence U^n that is generated by V^n into $2^{n(I(U;X|V)-I(U;Y|V))}$ bins, within each bin, uniformly assign each U^n into $2^{nI(U;Z|V)}$ sub-bins, and set the index within each sub-bin as the key value. Within each bin, there are around $2^{n(I(U;Y|V)-I(U;Z|V))}$ U^n sequences. Then, upon observing X^n, Alice finds a sequence V^n which is jointly typical with X^n, then Alice finds a U^n among those U^n sequences generated by V^n, which is jointly typical with

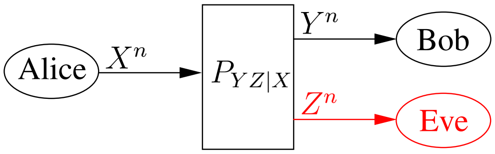


Figure 1.4: Wiretap channel.

(V^n, X^n). Finally, Alice sends V^n along with the bin index of U^n to Bob. Thus, the total information Alice needs to send is $I(U;X) - I(U;Y)$. With the received messages along with the observed sequence Y^n, Bob can correctly recovers (U^n, V^n) with high probability. Besides, with high probability, there exists at least one U^n within each sub-bin, which is jointly typical with (V^n, Z^n), thus there is no preference for Eve to decide which sub-bin U^n lies in. Thus, we can show the generated key is secure from Eve. For more details, one may refer to [3].

1.2.2 Key Generation under Channel Model

The basic key generation problem under the channel model is considered in [17, 113]. As illustrated in Fig.1.4, in the wiretap channel introduced by [113], two terminals Alice and Bob would like to share a secret key that is secure from the eavesdropper Eve. Alice is connected to Bob and Eve via noisy channels. Different from the source model, Alice, Bob and Eve observe no correlated sequences in advance. Instead, Alice is allowed to transmit a sequence X^n into the channel, and Bob and Eve will receive two output sequences Y^n and Z^n according to $\prod_{i=1}^{n} P_{YZ|X}(y_i z_i|x_i)$, respectively. Other than the sequence X^n transmitted through the wiretap channel, no further public discussion between Alice and Bob is allowed. After transmitting X^n, Alice and Bob can compute the key value, via functions $K \triangleq K(X^n)$ and $L \triangleq L(Y^n)$, respectively.

Definition 1.2. A key rate R is said to be achievable if $\forall \epsilon > 0$, there exists a key generation protocol when n is sufficiently large, such that

$$\Pr\{K \neq L\} \leq \epsilon, \tag{1.8}$$

$$\frac{1}{n}I(K;Z^n) \leq \epsilon, \tag{1.9}$$

$$\frac{1}{n}H(K) \geq \frac{1}{n}\log|\mathcal{K}| - \epsilon, \tag{1.10}$$

$$\frac{1}{n}H(K) \geq R - \epsilon., \tag{1.11}$$

where $\mathcal{K}$ is the alphabet of K. In addition, the secrecy capacity C is defined as the maximal value of R.

We have the following result on C.

Theorem 1.3 ([17])**.** Given channel $P_{YZ|X}$, the secrecy capacity is given by

$$C = \max_{P_{SX}} I(S;Y) - I(S;Z). \tag{1.12}$$

The random variable S in Theorem 1.3 is subject to the Markov chain $S \rightarrow X \rightarrow (Y,Z)$. To achieve the key rate defined by the right-hand side of (1.12), we randomly and independently generate $2^{nI(S;Y)}$ sequences S^n according to $\prod_{i=1}^{n} P_S(s_i)$, and assign each S^n into $2^{n(I(S;Y)-I(S;Z))}$ bins, using a uniform distribution. And we set the bin indices as the key value alphabet. Then, Alice randomly selects a sequence S^n and transmits it to Bob via the channel $P_{X|S}P_{YZ|X}$. After receiving the channel output sequence Y^n, Bob is able to recover the transmitted sequence S^n. On the other side, since there are $2^{nI(S;Z)}$ sequences S^n on average in each bin, there are at least one sequence in each bin that is of the same statistical property with S^n from Eve's perspective, thus it has no preference for it to decide in which bin S^n is. Thus, the generated key is secure from Z^n.

1.3 Introduction to Message Authentication

In this section, we briefly introduce the message authentication problem. Message authentication is a fundamental concept in cryptography in the presence of an active attacker. It has been investigated intensively from different perspectives [32, 36, 41, 45, 49, 58, 61–63,

$83, 84, 103, 110$]. Most of existing works on authentication rely on a pre-shared secret (in the form of a shared key or shared randomness) between the transmitter and the legitimate receiver. The receiver uses this pre-shared secret to determine whether the received message is authentic or not. Under this shared key assumption, the authentication problem has been studied under both noiseless and noisy channel models.

1.3.1 Message Authentication over Noiseless Channel

The authentication model over a noiseless channel was developed by Simmons [83]. In this model, the communication channel is assumed to be noiseless, and the transmitter Alice and the receiver Bob share a secret key K. In order to send a message M to Bob, instead of transmitting M directly, Alice transmits a codeword $E = f(M, K)$ into the channel with f being the encoding function used by Alice. Upon receiving a codeword $\hat{E}$ ($\hat{E} = E$ if there is no attack; Otherwise, $\hat{E}$ is determined by the adversary), Bob first needs to check whether $\hat{E}$ is sent by Alice or not, based on the pre-shared key K. In [83], two types of attacks are considered. The first one is *impersonation attack*, in which the adversary Eve sends the fake codeword before Alice transmits anything. The impersonation attack is successful if the fake codeword is accepted by Bob. The successful attack probability of this attack is denoted by P_I. The second one is *substitution attack*, in which Eve initiates an attack after she observes the codeword sent by Alice. In particular, Eve intercepts the codeword sent by Alice (hence Bob does not receive this codeword), and replaces the intercepted codeword with her own attack codeword. The substitution attack is successful if the codeword from Eve is accepted by Bob and decoded into a message different from the message intended by Alice. The successful attack probability of the substitution attack is denoted as P_S. [83] establishes lower bounds for P_I and P_S.

Theorem 1.4 ([83])**.**

$$P_I \geq 2^{-I(K;E)} \text{ and } P_S \geq 2^{-H(K|E)}.$$

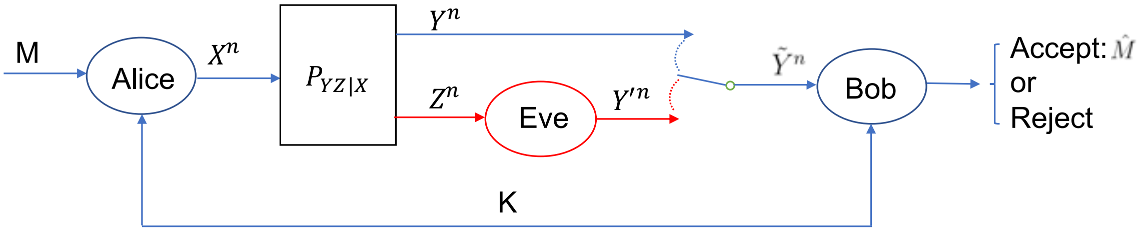


Figure 1.5: Message authentication over noisy channels.

It is clear that there exists a tradeoff between making P_I and P_S smaller. To make P_I smaller, E should contain more information about the shared key K, that is $I(K;E)$ should be larger. However, this makes the substitution attack easier (i.e., $H(K|E)$ becomes smaller), as E will be overheard by Eve perfectly over the noiseless channel.

1.3.2 Message Authentication over Noisy Channels

To overcome the tradeoff faced by the noiseless model in [83], as a natural extension, [45] extends Simmons's model to a noisy channel model. As illustrated in Fig.1.5, Alice connects to Bob via a wiretap channel $P_{YZ|X}$ in the presence of Eve, and the link between Eve and Bob is assumed to be noiseless. The wiretap channel is assumed to be discrete memoryless, i.e.,

$$P_{X^nY^n|Z^n}(x^n, y^n|z^n) = \prod_{i=1}^{n} P_{XY|Z}(x_i, y_i|z_i).$$

Eve can intercept the output Y^n from Alice and fake a sequence Y'^n to deceive Bob. More specifically, to transmit a message M to Bob, Alice encodes it along with a pre-shared key K, into a codeword X^n and send it into the wiretap channel. On the other side, after receiving the output sequence $\tilde{Y}^n$ (it can be from Alice or from Eve), Bob uses a decoder function to decode it into $(\hat{M}, \hat{K})$. Bob will accept $\hat{M}$ if $\hat{K} = K$; otherwise, he rejects it.

Both impersonation attack and substitution attack are considered in this model, and denote P_D to be the maxima of P_I and P_S. In the case when $\tilde{Y}^n = Y^n$, we require that the decoding error probability is arbitrarily small, i.e., for any $\epsilon > 0$, there exits a positive integer

n_0 such that for all $n \geq n_0$, we have

$$\text{Pr}\{\hat{M} \neq M | \tilde{Y}^n = Y^n\} \leq \epsilon.$$

Then, we have the following result.

Theorem 1.5 ([45])**.** Given wiretap channel $P_{YZ|X}$, if the secrecy capacity is nonzero, then there exists constants $c > 0$ and $\beta > 0$ so that

$$2^{-H(K)} \leq P_D \leq 2^{-H(K)} + c \cdot e^{-n\beta}$$

when n is sufficiently large.

Note that when n goes to infinity, $P_D = \max\{P_I, P_S\} = 2^{-H(K)}$. The lower bound is trivial, as Eve can randomly guess the value of K with a probability $2^{-H(K)}$. Once Eve knows the value of K, it can invoke any attack and this attack will be successful. Furthermore, [45] proposes a scheme such that we can achieve the upper bound. The main idea is that the noisy channel between Alice and Eve may prevent Eve from learning information about K contained in E. In this way, we can embed more information about K in E to make the impersonation attack more difficult, while not making the substitution attack easier as the noisy channel between Alice and Eve may prevent Eve from learning information about K.

1.4 Introduction to Function Computation

In this section, we briefly discuss the function computation problem. The goal of the function computation problem is to create communication protocols to enable communication parties to compute a function over their inputs [6, 8, 25, 43, 44, 68, 80, 97–99, 122]. The main process for function computation is to do public discussion first, so that the function computing parties are able to decode certain desired sequences, and then use the decoded sequences along with the sequence observed in local to compute the function value. One straightforward

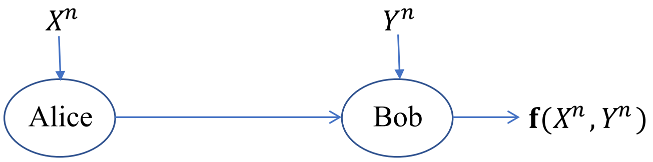


Figure 1.6: Basic function computation model.

scheme for function computation is to ask each information source to send enough information (for example, using schemes in distributed source coding [4, 112, 114, 116, 117]) so that the function computing parties can first recover all sources and then compute functions of interest using the recovered sources. However, as shown in many of existing works, full source recovery is not necessary in many scenarios [52–54, 70, 78, 79]. As the result, information transmitting parties can reduce their transmitted message rates while still enabling the function computing parties to compute functions of interest. This can significantly reduce the resource (in terms of energy, spectrum etc.) requirements and hence is very appealing for resource-constrained applications such as IoT where the goal of communication is decision making (hence requires function computing) but not full source recovery [50, 64, 106].

1.4.1 Basic Function Computation Model

As illustrated in Fig.1.6, in the basic function computation setup considered in [70], two terminals Alice and Bob observe two correlated sources X^n and Y^n, respectively. Bob would like to reliably compute the value of a given function $\mathbf{f}(X^n, Y^n)$, which is assumed to be component-wise, i.e., $\mathbf{f}(X^n, Y^n) := \{f(X_i, Y_i)\}_{i=1}^n$. The variables X and Y have a joint probability mass function P_{XY}, and the sequences X^n and Y^n are generated according to

$$\text{Pr}\{X^n, Y^n\} = \prod_{i=1}^{n} P_{XY}(X_i, Y_i).$$

Alice is allowed to transmit a message M, to Bob via a noiseless channel, and Bob needs to compute the function f solely based on (M, Y^n). [70] investigates what the minimal message rate is so that the function can be computed with a negligibly small error probability.

It provides an efficient method, by introducing conditional characteristic graph, to characterize the optimal message rate R. The characteristic graph G of X, Y and f is defined over the support set of X, and distinct vertices x, x' are connected if there is a Y such that $f(x, Y) = f(x', Y)$ with $P_X(x) \cdot P_X(x') > 0$. The graph G is said to be independent if no two vertices are connected to each other. Define $\Gamma(G)$ the collection of independent sets of G, then we have the following result.

Theorem 1.6 ([70])**.** The minimal message rate R, is given by

$$R = \min_{\substack{W \to X \to Y \\ X \in W \in \Gamma(G)}} I(W; X|Y). \tag{1.13}$$

Note that the realization value of W in (1.13) is a set of X. We use an example in [70] to illustrate the main idea of Theorem 1.6.

Example 1.1. *Assume $X, Y \in \{1, 2, 3\}$, and define*

$$P_{XY}(x, y) \triangleq \begin{cases} 1/6, & \textit{if } x \neq y; \\ 0, & \textit{if } x = y, \end{cases} \tag{1.14}$$

and

$$f(x, y) \triangleq \begin{cases} 1, & \textit{if } x > y; \\ 0, & \textit{if } x < y. \end{cases} \tag{1.15}$$

According to (1.14) *and* (1.15)*, G contains only one single edge $1 \leftrightarrow 3$. Thus, we can set the support set of W be $\{\{1, 2\}, \{2, 3\}\}$. Obviously, the value of $f(X, Y)$ is uniquely determined by (W, Y). Thus, after observing a sequence X^n, Alice only need to send a message to Bob so that Bob can recover W^n. By setting Pr$\{W = \{1, 2\}|X = 2\} =$ Pr$\{W = \{2, 3\}|X = 2\} = \frac{1}{2}$, we can easily calculate that the minimal rate of the message is $I(W; X|Y) = H(W|Y) - H(W|X, Y) = \frac{1}{3} + \frac{2}{3}h(\frac{1}{4}) - \frac{1}{3}$, where $h(p) \triangleq p \log_2 p + (1 - p) \log_2(1 - p)$.*

And this is the minimal message rate of all possible choices so that Bob is able to compute the value of $\mathtt{f}(X^n, Y^n)$.

1.4.2 Recent works on Function Computation

The basic model is further extended to more complex scenarios in many interesting recent papers [52–54, 78, 79]. In particular, [52] studies the problem of a two-terminal interactive distributed source coding for function computation at both terminals. In this model, these two terminals are allowed to exchange t (a finite nonnegative integer) coded messages, and each of them would like to compute a function within a certain distortion level respectively. [52] provides a single-letter characterization on the corresponding message rate region. Properties of the limit of the sum-rate-distortion function (i.e., the minimal value of the sum of message rates) when t goes to infinity are further investigated in [53]. Furthermore, [78] studies the message rate region of function computation in a different setup. This model consists of three terminals, two of them (transmitters) are allowed to send messages to the third terminal who needs to compute a function, but there is no interaction between the two transmitters. This model is further discussed in [79] by allowing an additional one-way discussion between the two transmitters. [80] further generalizes this model to a more sophisticated scenario that consists of more terminals over a rooted multi-level directed tree. In this scenario, each terminal is allowed to transmit a message to its parent terminal and the function is computed at the root. [80] provides both outer and inner bounds on the message rate region, which recover capacity regions of many function computing setups.

1.5 Introduction to Our Work

In this section, we briefly introduce the contributions of this dissertation.

- *Simulatability condition:* as discussed above, most of existing works on key generation assume that the adversary is an eavesdropper, while the work on an active attacker is limited. When the attacker is active, the key generation problem is much more challenging as the attacker can disrupt the key generation process. It is important to understand whether it is possible or not to generate keys when the attacker is active. In Chapter 2, we consider a model similar to the basic key generation setup as described in Section 1.2. The only difference is that the adversary Eve, in our model, is an active attacker. This problem is much more challenging as the attacker can arbitrarily modify the messages exchanged to disrupt the key generation process. We will discuss a fundamental concept named simulatability condition introduced by Maurer and Wolf [57,61–63]. This condition determines whether it is possible or not to generate a secret key when the attacker is active. However, until our work, it is unclear how to check this condition efficiently. In our work, we propose a polynomial complexity algorithm to check this important condition. We further investigate the sensitivity of this condition on the our knowledge about the attacker's observation model. Part of this work has been published in [89].

- *Multiple key generations:* we then investigate the problem of simultaneously generating multiple keys in a restricted communication structure in Chapter 3. One important assumption in the existing works is that the public discussion is directly available to *all* legitimate users. While it is important to assume that the public discussion is available to Eve (so that the generated key is secure in the worst case), there are some practical scenarios in which the public discussion is directly received only by a subset of the legitimate users. For example, in key generation over wireless networks [119], public discussion messages are transmitted over wireless channels. Hence, it is reasonable to assume that public discussion messages are directly received only by neighboring legitimate users. In the considered model, Alice is connected to Bob via a public noiseless channel, and Bob connects Carol and Eve via noisy channels. Alice and Bob would like to share individual secret keys with Carol, but there is no direct link between Alice and Carol. We study the relationship between individual secret-key rates, and provide a full characterization on the secret-key capacity region. The obtained results show that there exists a trade-off. Part of the work stated in this chapter has been published in [87, 88].

- *Message authentication:* as stated previously, most existing message authentication works focus on creating protocols using a pre-shared secret key while little attention has been paid to the keyless case. In Chapter 4, we discuss the keyless message authentication problem. In this model, there are two legitimate terminals, Alice and Bob, and an active attacker Eve. Alice would like to transmit a message to Bob. However, the output of the channel connecting Alice to Bob is under control of Eve: it can be intercepted and replaced by the output of the channel connecting Eve to Bob. Thus, after receiving an output sequence, Bob first needs to determine whether it is from Alice or not. If it is, then Bob will decode it into a corresponding message. Different from the models considered in [83] and [45], we assume that terminals Alice, Bob and Eve are connected by all noisy channels, and there is no pre-shared secret keys between Alice and Bob. Both impersonation and substitution attacks are considered in this chapter. By interpreting the message authentication as a hypothesis testing problem, we investigate the authentication exponent and the authenticated channel capacity of the noisy channel. We first show that the impersonation and the substitution attacks have the same performance in authentication exponent, which is in contrast to that in the pre-shared authentication problems, as the substitution attack is typically more powerful than the impersonation attack. Thus, the channel connecting Alice to Eve has no effect in increasing the successful attack probability and we only need to consider the impersonation attack. In the authentication exponent problem, we fully characterize the authentication exponent for the case where a zero-rate message is required to be transmitted to Bob, and we provide both an upper bound and a lower bound on the exponent in this case. These lower and upper bounds match when a certain convex condition regarding the channel statistics holds. In the authenticated capacity problem, we introduce simulatability condition to channel statistics. We establish an *all or nothing result*: we show that the authenticated channel capacity is the same as the classic channel capacity if simulatability condition is not satisfied, while the authenticated capacity will be zero if this condition holds. Furthermore, similar as the analysis in Chapter 2, we provide efficient algorithms to check this condition. We further show that our results are robust to modeling uncertainties about the eavesdropper's channels. The work investigated in this chapter has been published in [90, 93].

- *Secure function computation:* most of the existing works on function computation do not take both secrecy and privacy of the sources into consideration [52–54, 70, 78, 79]. In Chapter 5, we discuss the secure function computation problem with both secrecy and privacy constraints. In this model, Alice and Bob are connected to a fusion center via public noiseless channels in the presence of an eavesdropper Eve. These four terminals observe correlated sources and the fusion center is required to compute a function of legitimate input sequences. We allow a prefixed distortion level on the value of the computed function. To facilitate the computation, Alice and Bob need to send messages to the fusion center. Different from the existing setups in function computing, we assume that there are both *secrecy* and *privacy* constraints on the sources at Alice and Bob: we use equivocation of sources at Eve to measure the secrecy constraint and we introduce a quantity to precisely measure the privacy information leakage to the fusion center. Under this model, we study the relationship among message rates, private information leakage, equivocation and distortion. To facilitate understanding, we first consider a special scenario involving only one transmitter, i.e., the source observed by Bob is empty, and we provide a single-letter characterization on the corresponding parameter region. Then, we consider the more general case and provide both inner and outer bounds on the corresponding parameter region. These bounds do not match in general, but when a certain Markov chain condition holds, these bounds match, in which sense we fully characterize it. The work studied in this chapter has been published in [91, 92, 94].

Chapter 2

Simulatability Condition in Key Generation

Simulatability condition is a fundamental concept in studying key generation over a non-authenticated public channel, in which Eve is active and can intercept, modify and falsify messages exchanged over the non-authenticated public channel. Using this condition, Maurer and Wolf showed a remarkable "all or nothing" result: if simulatability condition does not hold, the key capacity over the non-authenticated public channel will be the same as that of the case with a passive Eve, while the key capacity over the non-authenticated channel will be zero if simulatability condition holds. However, several questions remain open so far: 1) For a given joint probability mass function (PMF), are there polynomial complexity algorithms for checking whether simulatability condition holds or not?; 2) If simulatability condition holds, are there efficient algorithms for finding the corresponding attack strategy? and 3) How sensitive is this condition on the knowledge about Eve's observations? In this chapter, we fully answer these open questions. In particular, for a given joint PMF, we construct a linear programming (LP) problem and show that simulatability condition holds *if and only if* the optimal value obtained from the constructed LP is zero. In addition, we construct another LP and show that the minimizer of the newly constructed LP is a valid attack strategy. Both LPs can be solved with a polynomial complexity. We further show that simulatability condition is not sensitive on the knowledge about Eve's observations.

2.1 Motivation

The problem of secret key generation via public discussion under both source and channel models has attracted significant research interests [2, 3, 10, 15, 19, 33, 39, 56, 61–63, 86, 104, 105, 109, 118, 119, 125]. Under the source model, it is common to assume that the public discussion will be overheard by Eve, and the public channel can either be authenticated or non-authenticated. An authenticated public channel implies that Eve is a passive listener [2, 3, 105]. On the other hand, a non-authenticated public channel implies that Eve is active and can intercept, modify or falsify any message exchanged through the public channel[48, 57, 73, 124]. Most of existing works focus on the passive Eve case, while the work on active Eve case is limited. However, the case of active Eve is more practical, and is more challenging.

Under the source model, users observe correlated sources generated from a certain joint probability mass function (PMF), and can discuss with each other via a noiseless public channel. Clearly, the secret key rate that can be generated using the non-authenticated public channel is no larger than that can be generated using the authenticated pulic channel. In [57, 61–63], Maurer and Wolf introduced a concept of simulatability condition (this condition will be defined precisely in the sequel) and established a remarkable "all or nothing" result. In particular, they showed that for the secret key generation via a non-authenticated public channel with two legitimate terminals in the presence of an active adversary: 1) if simulatability condition holds, the two legitimate terminals will not be able to establish a secret key, and hence the key capacity is 0; and 2) if simulatability condition does not hold, the two legitimate terminals can establish a secret key and furthermore the key capacity will be the same as that of the case when Eve is passive. Intuitively speaking, if simulatability condition holds, from its own source observations, Eve can generate fake messages that are indistinguishable from messages generated from legitimate users. On the other hand, if simulatability condition does not hold, the legitimate users will be able to detect modifications made by Eve.

It is clear that simulatability condition is a fundamental concept for the key generation via a non-authenticated public channel, and hence it is important to design efficient algorithms to check whether simulatability condition holds or not. Using ideas from mechanical models, [63] made significant progress in designing efficient algorithms. In particular, [63] proposed to represent PMFs as mass constellations in a coordinate, and showed that simulatability condition holds if and only if one mass constellation can be transformed into another mass constellation using a finite number of basic mass operations. Furthermore, [63] introduced another notion of one mass constellation being "more centered" than another constellation and designed a low-complexity algorithm to check this "more centered" condition. For some important special cases, which will be described precisely in Section 2.2, [63] showed that the "more centered" condition is necessary and sufficient for the mass constellation transformation problem (and hence is necessary and sufficient condition for simulatability condition for these special cases). However, in the general case, the "more centered" condition is a necessary but not sufficient condition for the mass constellation transformation problem. Hence, whether there exists efficient algorithms for the mass constellation transformation problem (and hence simulatability condition) in the general case is still an open question.

As the result, despite the significant progress, [63] left the following questions regarding simulatability condition for the general case as open questions:

(1) For a given joint PMF, are there efficient algorithms (polynomial complexity algorithms) for checking whether simulatability condition holds or not?

(2) If simulatability condition holds, are there efficient algorithms for finding the corresponding Eve's attack strategy?

(3) Suppose the PMF is not exactly known, how sensitive is the condition on the modeling uncertainty?

In this chapter, we fully answer these open questions.

To answer the first open question, we construct a linear programming (LP) problem and show that simulatability condition holds **if and only if** the optimal value obtained from this LP is zero. We establish our result in three main steps. We first show that, after some basic transformations, checking whether simulatability condition holds or not is equivalent to checking whether there exists a nonnegative solution to a specially constructed system of linear equations. We then use a basic result from linear algebra to show that whether there exists a nonnegative solution to the constructed system of linear equations is equivalent to whether there is a solution (not necessarily nonnegative) to a related system of inequalities or not. Finally, we use Farkas' lemma [77] to show that whether the system of inequalities has a solution or not is equivalent to whether the optimal value of a specially constructed LP is zero or not. Since there exists polynomial complexity algorithms for solving LP problems[11,28, 38], we thus find a polynomial complexity algorithm for checking simulatability condition for a general PMF.

To answer the second open question, we construct another LP and show that the minimizer of this LP is a valid attack strategy. The proposed approach is very flexible in the sense that one can simply modify the cost function of the constructed LP to obtain different attack strategies. Furthermore, the cost function can be modified to satisfy various design criteria. For example, a simple cost function can be constructed to minimize the amount of modifications Eve needs to perform during the attack. All these optimization problems with different cost functions can be solved with a polynomial complexity.

To answer the third open question, we show that if simulatability condition does not hold for a given PMF, then simulatability condition does not hold if the PMF related to Eve's observation is changed up to a certain threshold. We fully characterize this threshold.

2.2 Preliminaries and Problem Setup

Let $\mathcal{X} = \{1, \cdots, |\mathcal{X}|\}$, $\mathcal{Y} = \{1, \cdots, |\mathcal{Y}|\}$ and $\mathcal{Z} = \{1, \cdots, |\mathcal{Z}|\}$ be three finite sets. Consider three correlated random variables (X, Y, Z), taking values from $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, with joint PMF P_{XYZ}, simulatability condition is defined as follows.

Definition 2.1. ([57]) For a given P_{XYZ}, we say X is simulatable by Z with respect to Y, denoted by $\text{Sim}_Y(Z \rightarrow X)$, if there exists a conditional PMF $P_{\bar{X}|Z}$ such that $P_{Y\bar{X}} = P_{YX}$, with

$$P_{Y\bar{X}}(y, x) = \sum_{z \in \mathcal{Z}} P_{YZ}(y, z) \cdot P_{\bar{X}|Z}(x|z), \tag{2.1}$$

in which P_{YX} and P_{YZ} are the joint PMFs of (Y, X) and (Y, Z) under P_{XYZ} respectively.

One can also define $\text{Sim}_X(Z \rightarrow Y)$ in the same manner. This concept of simulatability, first defined in [57], is a fundamental concept in the problem of secret key generation over a non-authenticated public channel [61–63], in which two terminals Alice and Bob would like to establish a secret key in the presence of an adversary Eve. These three terminals observe sequences X^N, Y^N and Z^N generated according to

$$P_{X^N Y^N Z^N}(x^N, y^N, z^N) = \prod_{i=1}^{N} P_{XYZ}(x_i, y_i, z_i). \tag{2.2}$$

Alice and Bob can discuss with each other via a public **non-authenticated** noiseless channel, which means that Eve not only has full access to the channel but can also interrupt, modify and falsify messages exchanged over this public channel. The largest key rate that Alice and Bob[1] can generate with the presence of the active attacker is denoted as $S^*(X; Y||Z)$. Let $S(X; Y||Z)$ denote the largest key rate that Alice and Bob can generate when Eve is passive, i.e., when the public channel is authenticated. Clearly, $S(X; Y||Z) \geq S^*(X; Y||Z)$. Although a full characterization of $S(X; Y||Z)$ is unknown in general, [62] established the

[1] Please see [61–63] for precise definitions.

following remarkable “all or nothing” result:

Theorem 2.1. ([62]) If $\text{Sim}_Y(Z \to X)$ or $\text{Sim}_X(Z \to Y)$, then $S^*(X;Y||Z) = 0$. Otherwise, $S^*(X;Y||Z) = S(X;Y||Z)$.

This significant result implies that, if simulatability condition does not hold, one can generate a key with the same rate as if Eve were passive. On the other hand, if simulatability condition holds, the key rate will be zero. When $\text{Sim}_Y(Z \to X)$ and $\text{Sim}_X(Z \to Y)$ don’t hold, [62] introduces one protocol to modify any existing key generation scheme with passive Eve into a scheme against active Eve such that the generated key rate is almost the same as that generated when Eve is passive. This protocol contains three phases: The first phase is to generate a short key with each single message bit authenticated by a sequence of source observations. Then in the second phase, one can use the generated short key to authenticate messages with hash functions to generated a longer key. Finally, the protocol ends with transmitting a message of a block of realizations to verify the success of the last exchanged message. See [62] for more details. While on the other hand, if $\text{Sim}_Y(Z \to X)$ holds, then after observing Z^N, Eve can generate $\bar{X}^N$ by passing Z^N through a channel defined by $P_{\bar{X}|Z}$. Then $(\bar{X}^N, Y^N)$ has the same statistics as (X^N, Y^N). Hence by knowing only Y^N, Bob cannot distinguish $\bar{X}^N$ and X^N, and hence cannot distinguish Alice or Eve.

As mentioned in the introduction, [63] has made important progress in developing low-complexity algorithms for checking whether $\text{Sim}_Y(Z \to X)$ (or $\text{Sim}_X(Z \to Y)$) holds or not. In particular, [63] developed an efficient algorithm to check a related condition called “more centered” condition. When $|\mathcal{Y}| = 2$, that is when Y is a binary random variable, this “more centered” condition is shown to be necessary and sufficient for $\text{Sim}_Y(Z \to X)$. Hence, [63] has found an efficient algorithm to check $\text{Sim}_Y(Z \to X)$ for the special case of Y being binary (the algorithm is also effective in checking $\text{Sim}_X(Z \to Y)$ when X is binary). However, when Y is not binary, the “more centered” condition is only a necessary condition for $\text{Sim}_Y(Z \to X)$. Hence, the following questions remain open:

(1) For a general given P_{XYZ}, are there efficient algorithms (polynomial complexity algorithms) for checking whether $\text{Sim}_Y(Z \to X)$ (or $\text{Sim}_X(Z \to Y)$) holds or not?

(2) If $\text{Sim}_Y(Z \to X)$ (or $\text{Sim}_X(Z \to Y)$) holds, are there efficient algorithms for finding the corresponding $P_{\bar{X}|Z}$ (or $P_{\bar{Y}|Z}$)?

(3) Suppose P_{XYZ} is not precisely known, especially with regards to the random variable Z, how sensitive is SC with regards to this modeling uncertainty?

In this chapter, we solve these open questions.

Notation: Throughout this chapter, we use boldface uppercase letters to denote matrices, boldface lowercase letters to denote vectors. We also use $\mathbf{1}$, $\mathbf{0}$ and $\mathbf{I}$, unless stated otherwise, to denote all ones column vector, all zeros column vector and the identity matrix, respectively. In addition, we denote the vectorization of a matrix by $\text{Vec}(\cdot)$. Specifically, for an $m \times n$ matrix $\mathbf{A}$, $\text{Vec}(\mathbf{A})$ is an $mn \times 1$ column vector:

$$\text{Vec}(\mathbf{A}) = [a_{11}, \cdots, a_{m1}, \cdots, a_{1n}, \cdots, a_{mn}]^T, \tag{2.3}$$

in which $[\cdot]^T$ is the transpose of the matrix. And vice versa can be done by $\mathbf{A} = \text{Reshape}(\text{Vec}$ $(\mathbf{A}), [m, n])$. We use $\mathbf{A} \otimes \mathbf{B}$ to denote the Kronecker product of matrices $\mathbf{A}$ and $\mathbf{B}$. Specifically, assume $\mathbf{A}$ is an $m \times n$ matrix, then

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{bmatrix}. \tag{2.4}$$

All matrices and vectors in this chapter are real.

2.3 Main Results

In this chapter, we focus on $\text{Sim}_Y(Z \to X)$. The developed algorithm can be easily modified to check $\text{Sim}_X(Z \to Y)$. We rewrite (2.1) in the following matrix form

$$\mathbf{C} = \mathbf{A}\mathbf{Q}, \tag{2.5}$$

in which $\mathbf{C} = [c_{ij}]$ is a $|\mathcal{Y}| \times |\mathcal{X}|$ matrix with $c_{ij} = P_{YX}(i,j)$, $\mathbf{A} = [a_{ik}]$ is a $|\mathcal{Y}| \times |\mathcal{Z}|$ matrix with $a_{ik} = P_{YZ}(i,k)$, and $\mathbf{Q} = [q_{kj}]$ is a $|\mathcal{Z}| \times |\mathcal{X}|$ matrix with $q_{kj} = P_{\bar{X}|Z}(j|k)$ if such $P_{\bar{X}|Z}$ exists.

Checking whether $\text{Sim}_Y(Z \to X)$ holds or not is equivalent to checking whether there exists a transition matrix $\mathbf{Q}$ such that (2.5) holds. As $\mathbf{Q}$ is a transition matrix, its entries q_{kj}s must satisfy

$$q_{kj} \geq 0, \qquad \forall k \in [1:|\mathcal{Z}|], j \in [1:|\mathcal{X}|], \tag{2.6}$$

$$\sum_{j=1}^{|\mathcal{X}|} q_{kj} = 1, \qquad \forall k \in [1:|\mathcal{Z}|]. \tag{2.7}$$

We note that if q_{kj}s satisfy (2.6) and (2.7), they will automatically satisfy $q_{kj} \leq 1$. Hence, we don't need to state this requirement here.

If there exists at least one transition matrix $\mathbf{Q}$ satisfying (2.5), (2.6) and (2.7) simultaneously, we can conclude that simulatability condition $\text{Sim}_Y(Z \to X)$ holds.

(2.7) can be written in the matrix form

$$\mathbf{1}_{|\mathcal{Z}|\times 1} = \mathbf{Q}\mathbf{1}_{|\mathcal{X}|\times 1}, \tag{2.8}$$

Then, (2.5) and (2.8) can be written in the following compact form:

$$\begin{aligned}\begin{bmatrix}\text{Vec}(\mathbf{C}^T)\\ \mathbf{1}_{|\mathcal{Z}|\times 1}\end{bmatrix} &= \begin{bmatrix} a_{11}\mathbf{I} & a_{12}\mathbf{I} & \cdots & a_{1|\mathcal{Z}|}\mathbf{I}\\ \vdots & \vdots & \ddots & \vdots\\ a_{|\mathcal{Y}|1}\mathbf{I} & a_{|\mathcal{Y}|2}\mathbf{I} & \cdots & a_{|\mathcal{Y}||\mathcal{Z}|}\mathbf{I}\\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0}\\ \mathbf{0} & \mathbf{1} & \ddots & \vdots\\ \vdots & \ddots & \ddots & \vdots\\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{1}\end{bmatrix}\text{Vec}(\mathbf{Q}^T)\\ &= \begin{bmatrix}\mathbf{A}\otimes\mathbf{I}\\ \mathbf{I}_{|\mathcal{Z}|}\otimes\mathbf{1}\end{bmatrix}\text{Vec}(\mathbf{Q}^T), \qquad (2.9)\end{aligned}$$

in which the sizes for $\mathbf{I}$, $\mathbf{1}$ and $\mathbf{0}$ are $|\mathcal{X}|\times|\mathcal{X}|$, $1\times|\mathcal{X}|$ and $1\times|\mathcal{X}|$, respectively.

For notational convenience, we define

$$\mathbf{c} \triangleq \begin{bmatrix}\text{Vec}(\mathbf{C}^T)\\ \mathbf{1}_{|\mathcal{Z}|\times 1}\end{bmatrix}, \qquad (2.10)$$

$$\mathbb{A} \triangleq \begin{bmatrix}\mathbf{A}\otimes\mathbf{I}\\ \mathbf{I}_{|\mathcal{Z}|}\otimes\mathbf{1}\end{bmatrix}, \qquad (2.11)$$

$$\mathbf{q} \triangleq \text{Vec}(\mathbf{Q}^T). \qquad (2.12)$$

From (2.9), it is clear that $\mathbf{c}$ is an $m\times 1$ vector, $\mathbb{A}$ is an $m\times n$ matrix, and $\mathbf{q}$ is an $n\times 1$ vector, in which

$$m = |\mathcal{Y}||\mathcal{X}| + |\mathcal{Z}|, \qquad (2.13)$$

$$n = |\mathcal{Z}||\mathcal{X}|. \qquad (2.14)$$

With these notation and combining (2.9) with (2.6), the original problem of checking whether $\text{Sim}_Y(Z \rightarrow X)$ holds or not is equivalent to checking whether there exists **nonnegative** solutions $\mathbf{q}$ for the system

$$\mathbb{A}\mathbf{q} = \mathbf{c}. \tag{2.15}$$

In the following, we check whether there exists at least a nonnegative solution for the system defined by (2.15). There are two main steps: 1) whether the system is consistent or not; 2) if it is consistent, whether there exists a nonnegative solution or not. Checking the consistency of (2.15) is straightforward: a necessary and sufficient condition for a system of non-homogenous linear equations to be consistent is

$$\text{Rank}(\mathbb{A}) = \text{Rank}((\mathbb{A}|\mathbf{c})), \tag{2.16}$$

where $(\mathbb{A}|\mathbf{c})$ is the augmented matrix of $\mathbb{A}$. If (2.16) is not satisfied, it can be concluded that $\text{Sim}_Y(Z \rightarrow X)$ does not hold. If (2.16) is satisfied, we need to further check whether there exists a nonnegative solution to (2.15) or not.

To proceed further, we need the following definition of generalized inverse (g-inverse) of a matrix $\mathbf{G}$.

Definition 2.2. ([75]) For a given $m \times n$ real matrix $\mathbf{G}$, an $n \times m$ real matrix $\mathbf{G}^g$ is called a g-inverse of $\mathbf{G}$ if

$$\mathbf{G}\mathbf{G}^g\mathbf{G} = \mathbf{G}.$$

The g-inverse $\mathbf{G}^g$ is generally not unique (If $n = m$ and $\mathbf{G}$ is full rank, then $\mathbf{G}^g$ is unique and equal to the inverse matrix $\mathbf{G}^{-1}$). A particular choice of g-inverse is called the Moore-Penrose pseudoinverse $\mathbf{G}^+$, which can be computed using multiple different approaches. One approach is to use the singular value decomposition (SVD): by SVD, for a given $\mathbf{G}$ and its SVD decomposition

$$\mathbf{G} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T, \tag{2.17}$$

then, $\mathbf{G}^+$ can be obtained as

$$\mathbf{G}^+ = \mathbf{V}\mathbf{\Sigma}^+\mathbf{U}^T, \tag{2.18}$$

in which $\mathbf{\Sigma}^+$ is obtained by taking the reciprocal of each non-zero element on the diagonal of the diagonal matrix $\mathbf{\Sigma}$, leaving the zeros in place. One can easily check that the Moore-Penrose pseudoinverse $\mathbf{G}^+$ obtained by SVD satisfies the g-inverse matrix definition and hence is a valid g-inverse.

With the concept of g-inverse, we are ready to state our main result regarding the first open question.

Theorem 2.2. Let $\mathbb{A}^g$ be any given g-inverse of $\mathbb{A}$ (e.g., it can be chosen as the Moore-Penrose pseudoinverse $\mathbb{A}^+$), and h^* be obtained by the following LP

$$\begin{aligned} & h^* = \min_{\mathbf{t}}\{\mathbf{t}^T\mathbb{A}^g\mathbf{c}\}, && (2.19) \\ \text{s. t.} \quad & \mathbf{t} \succeq \mathbf{0}, \\ & (\mathbf{I} - \mathbb{A}^g\mathbb{A})^T\mathbf{t} = \mathbf{0}. \end{aligned}$$

Then $\mathrm{Sim}_Y(Z \to X)$ holds, **if and only if** $h^* = 0$ and (2.16) holds.

Proof. If (2.16) does not hold, then there is no solution to (2.15), and hence $\mathrm{Sim}_Y(Z \to X)$ does not hold.

In the remainder of the proof, we assume that (2.16) holds. If (2.16) holds, the general solution to (2.15) can be written in the following form (see, e.g., Theorem 2 a.(d) of [74])

$$\mathbf{q} = \mathbb{A}^g\mathbf{c} + (\mathbb{A}^g\mathbb{A} - \mathbf{I})\mathbf{p}, \tag{2.20}$$

in which $\mathbb{A}^g$ can be any given g-inverse of $\mathbb{A}$, and $\mathbf{p}$ is an arbitrary length-n vector.

As the result, the problem of whether there exists a nonnegative solution to (2.15) (i.e., $\mathbf{q} \succeq \mathbf{0}$) is equivalent to the problem of whether there exists a solution $\mathbf{p}$ for the following system defined by

$$(\mathbf{I} - \mathbb{A}^g\mathbb{A})\mathbf{p} \preceq \mathbb{A}^g\mathbf{c}. \tag{2.21}$$

To check whether the system defined by (2.21) has a solution, we use Farkas' lemma, a fundamental lemma in linear programming and related area in optimization. For completeness, we state the form of Farkas' lemma as follows.

Lemma 2.3. (Farkas' Lemma [77]) Let $\mathbf{B}$ be a matrix, and $\mathbf{b}$ be a vector, then the system specified by $\mathbf{B}\mathbf{p} \preceq \mathbf{b}$, has a solution $\mathbf{p}$, if and only if $\mathbf{t}^T\mathbf{b} \geq 0$ for each column vector $\mathbf{t} \succeq \mathbf{0}$ with $\mathbf{B}^T\mathbf{t} = \mathbf{0}$.

To use Farkas' lemma, we first write a LP related to the system defined in (2.21)

$$\begin{aligned} & h^* = \min_{\mathbf{t}}\{\mathbf{t}^T\mathbb{A}^g\mathbf{c}\}, \\ \text{s.t.} \quad & \mathbf{t} \succeq \mathbf{0}, \\ & (\mathbf{I} - \mathbb{A}^g\mathbb{A})^T\mathbf{t} = \mathbf{0}. \end{aligned}$$

The above LP is always feasible since $\mathbf{t} = \mathbf{0}$ is a vector that satisfies the constraints, which results in $\mathbf{t}^T\mathbb{A}^g\mathbf{c} = 0$. Hence the optimal value $h^* \leq 0$. Using Farkas' lemma, we have that (2.21) has a solution **if and if** $h^* = 0$. More specifically, if $h^* = 0$, then there exists at least a solution $\mathbf{p}$ for (2.21), which further implies that there is a nonnegative solution to (2.15), and hence $\text{Sim}_Y(Z \to X)$ holds. On the other hand, if $h^* < 0$, then there is no solution $\mathbf{p}$ for (2.21), which further implies that there is no nonnegative solution to (2.15), and hence $\text{Sim}_Y(Z \to X)$ does not hold. □

As mentioned above, if $\text{Rank}(\mathbb{A}) = m = n$ holds, then $\mathbb{A}^g = \mathbb{A}^{-1}$ is unique. For other cases, $\mathbb{A}^g$ might not be unique. One may wonder whether different choices of $\mathbb{A}^g$ will affect the result in Theorem 2.2 or not. The following proposition answers this question.

Proposition 2.1. Different choices of $\mathbb{A}^g$ will not affect the result on whether h^* equals 0 or not.

Proof. Let $\mathbb{A}_1^g$ and $\mathbb{A}_2^g$ be two different g-inverses of $\mathbb{A}$, and let h_1^* and h_2^* be the values obtained using $\mathbb{A}_1^g$ and $\mathbb{A}_2^g$ in (2.19) respectively. It suffices to show that if $h_1^* = 0$, then $h_2^* = 0$.

Assuming that $h_1^* = 0$, then there exists a vector $\mathbf{p}_1$ satisfying $(\mathbf{I} - \mathbb{A}_1^g\mathbb{A})\mathbf{p}_1 \preceq \mathbb{A}_1^g\mathbf{c}$, we will show that there exists a vector $\mathbf{p}_2$ satisfying $(\mathbf{I} - \mathbb{A}_2^g\mathbb{A})\mathbf{p}_2 \preceq \mathbb{A}_2^g\mathbf{c}$, which then implies $h_2^* = 0$.

First, we know that $\mathbb{A}_1^g\mathbf{c}$ and $\mathbb{A}_2^g\mathbf{c}$ are two solutions to the system $\mathbb{A}\mathbf{q} = \mathbf{c}$, which can be easily verified by setting $\mathbb{A}^g$ as $\mathbb{A}_1^g$ and $\mathbb{A}_2^g$ in (2.20) respectively and setting $\mathbf{p} = \mathbf{0}$. This implies that

$$\mathbb{A}(\mathbb{A}_2^g\mathbf{c} - \mathbb{A}_1^g\mathbf{c}) = \mathbf{0}, \tag{2.22}$$

and hence $\mathbb{A}_2^g\mathbf{c} - \mathbb{A}_1^g\mathbf{c}$ is a solution to the system $\mathbb{A}\mathbf{q} = \mathbf{0}$.

Second, we know that any solution to the system $\mathbb{A}\mathbf{q} = \mathbf{0}$ can be written in the form $(\mathbf{I} - \mathbb{A}^g\mathbb{A})\mathbf{p}$ [74]. As $\mathbb{A}_2^g\mathbf{c} - \mathbb{A}_1^g\mathbf{c}$ is a solution to system $\mathbb{A}\mathbf{q} = \mathbf{0}$, there must exist a $\mathbf{p}_0$ such that

$$(\mathbf{I} - \mathbb{A}_2^g\mathbb{A})\mathbf{p}_0 = \mathbb{A}_2^g\mathbf{c} - \mathbb{A}_1^g\mathbf{c}. \tag{2.23}$$

In addition, it is easy to check that $(\mathbf{I} - \mathbb{A}_1^g\mathbb{A})\mathbf{p}_1 + (\mathbf{I} - \mathbb{A}_2^g\mathbb{A})\mathbf{p}_0$ is also a solution to the system $\mathbb{A}\mathbf{q} = \mathbf{0}$. Thus, there exists a $\mathbf{p}_2$ such that

$$(\mathbf{I} - \mathbb{A}_2^g\mathbb{A})\mathbf{p}_2 = (\mathbf{I} - \mathbb{A}_1^g\mathbb{A})\mathbf{p}_1 + (\mathbf{I} - \mathbb{A}_2^g\mathbb{A})\mathbf{p}_0. \tag{2.24}$$

Plugging (2.23) into (2.24), we have

$$\begin{aligned}
(\mathbf{I} - \mathbb{A}_2^g\mathbb{A})\mathbf{p}_2 &= (\mathbf{I} - \mathbb{A}_1^g\mathbb{A})\mathbf{p}_1 + (\mathbf{I} - \mathbb{A}_2^g\mathbb{A})\mathbf{p}_0 \\
&= (\mathbf{I} - \mathbb{A}_1^g\mathbb{A})\mathbf{p}_1 + \mathbb{A}_2^g\mathbf{c} - \mathbb{A}_1^g\mathbf{c} \qquad (2.25) \\
&\preceq \mathbb{A}_2^g\mathbf{c}, \qquad (2.26)
\end{aligned}$$

in which the last inequality comes from the assumption that $(\mathbf{I} - \mathbb{A}_1^g\mathbb{A})\mathbf{p}_1 \preceq \mathbb{A}_1^g\mathbf{c}$. Hence, we have found a $\mathbf{p}_2$, such that $(\mathbf{I} - \mathbb{A}_2^g\mathbb{A})\mathbf{p}_2 \preceq \mathbb{A}_2^g\mathbf{c}$. This implies that $h_2^* = 0$.

□

Remark 2.4. The proposed algorithm for checking whether $\text{Sim}_Y(Z \to X)$ holds or not has a polynomial complexity. Among all operations required, computing the g-inverse and solving the LP defined by (2.19) require most computations. The complexity to obtain $\mathbb{A}^g$ is of order $O(n^3)$ [65]. Furthermore, there exists polynomial complexity algorithms to solve the LP defined by (2.19). For example, [28] provided an algorithm to solve LP using $O(n^3L)$ operations, where L is number of binary bits needed to store input data of the problem (one can refer to Chapter 8 in [11] for more details about the complexity of algorithms for solving LP). Hence, the total operations of our algorithm for checking $\text{Sim}_Y(Z \to X)$ is of order $O(n^3L)$. In addition, we note that we can terminate the LP algorithm earlier once the algorithm finds a $\mathbf{t}$ such that $\mathbf{t}\mathbb{A}^g\mathbf{c} < 0$, as this indicates that $h^* < 0$. This can potentially further reduce the computational complexity.

Thus, we can conclude that the proposed algorithm can check whether $\text{Sim}_Y(Z \to X)$ holds or not with a polynomial complexity. Algorithm 2.1 summarizes the main steps involved in our algorithm. In the following algorithm, we use Res $= 0$ to denote that $\text{Sim}_Y(Z \to X)$ does not hold and Res $= 1$ to denote that $\text{Sim}_Y(Z \to X)$ holds.

In the following, we provide our answer to the second open question, i.e., if $\text{Sim}_Y(Z \to X)$ holds, how to find $P_{\bar{X}|Z}$ efficiently.

Theorem 2.5. Let $\mathbf{e}$ be any $n \times 1$ vector with $\mathbf{e} \succ \mathbf{0}$, and $\mathbf{q}^*$ be the obtained from the

Algorithm 2.1 Checking $\text{Sim}_Y(Z \to X)$

```
Input: PMF $P_{XYZ}$;

Initiate:
    a. Calculate matrices $\mathbf{A}$ and $\mathbf{C}$;
    b. Construct $\mathbf{c}$ and $\mathbb{A}$ using (2.10) and (2.11) respectively;
    c. Set Res $= 0$;

if (Rank($\mathbb{A}$) $\neq$ Rank($\mathbb{A}|\mathbf{c}$)) then
    break;
else
    d. Find a $\mathbb{A}^g$, and calculate $\mathbb{A}^g\mathbf{c}$, $\mathbf{I} - \mathbb{A}^g\mathbb{A}$;
    e. Solve LP (2.19) and obtain $h^*$;
    if ($h^* == 0$) then
        Res $= 1$;
    else
        break;
    end if
end if

Output: Res.
```

following LP:

$$\begin{aligned} & \min_{\mathbf{q}} f(\mathbf{q}) = \mathbf{e}^T\mathbf{q}, \\ \text{s.t.} \quad & \mathbf{q} \succeq \mathbf{0}, \\ & \mathbb{A}\mathbf{q} = \mathbf{c}. \end{aligned} \tag{2.27}$$

If $\text{Sim}_Y(Z \to X)$ holds, then $\mathbf{Q}^* = \text{Reshape}(\mathbf{q}^*, [|\mathcal{X}|, |\mathcal{Z}|])^T$ is a valid choice for $P_{\bar{X}|Z}$.

Proof. By assumption, $\text{Sim}_Y(Z \to X)$ holds, which implies that the system defined by (2.15) is consistent and it has nonnegative solutions. Hence, the following LP is feasible

$$\begin{aligned} & \min_{\mathbf{q}} f(\mathbf{q}) = \mathbf{e}^T\mathbf{q}, \\ \text{s.t.} \quad & \mathbf{q} \succeq \mathbf{0}, \\ & \mathbb{A}\mathbf{q} = \mathbf{c}, \end{aligned} \tag{2.28}$$

where $\mathbf{e} \succ \mathbf{0}$. Hence, the minimizer $\mathbf{q}^*$ is nonnegative and satisfies $\mathbb{A}\mathbf{q}^* = \mathbf{c}$. We can then reshape $\mathbf{q}^*$ into matrix $\mathbf{Q}^*$ (see (2.12)). $\mathbf{Q}^*$ is a valid choice for $P_{\bar{X}|Z}$. □

Remark 2.6. Since finding a suitable $P_{\bar{X}|Z}$ using our approach is equivalent to solving a LP, the complexity is of polynomial order.

Remark 2.7. For a given distribution P_{XYZ}, there may be more than one possible $P_{\bar{X}|Z}$ such that (2.1) holds. Different choices of **e** in (2.27) give different values for $P_{\bar{X}|Z}$.

Remark 2.8. The objective function $f(\mathbf{q})$ can be further modified to satisfy various design criteria of Eve. For example, let

$$\tilde{\mathbf{q}} = \text{Vec}(\tilde{\mathbf{Q}}[\tilde{q}_{kj}]^T)$$

with $\tilde{q}_{kj} = P_{X|Z}(k|j)$, then setting

$$f(\mathbf{q}) = ||\mathbf{q} - \tilde{\mathbf{q}}||_2^2$$

will minimize the amount of changes in the conditional PMF in the l_2 norm sense. This is a quadratic programming, which can still be solved efficiently.

2.4 Complexity Reduction

In Proposition 2.1, we show that different choices of $\mathbb{A}^g$ will not affect the result on whether h^* equals zero or not. However, different choices of $\mathbb{A}^g$ may affect the amount of computation needed. Primal-dual path-following method is one of the best methods for solving LP of the following form [11]:

$$\begin{aligned} &\min_{\mathbf{t}} \mathbf{t}^T\mathbf{b} \\ \text{s.t.} \quad &\mathbf{t} \succeq \mathbf{0}, \end{aligned}$$

$$\mathbf{Bt} = \mathbf{d},$$

in which $\mathbf{B}$ is a matrix of size $m \times n$. The complexity is related to the size of $\mathbf{B}$. In particular, in terms of m and n, the complexity is $O((nm^2 + n^{1.5}m)L)$ [66,67]. In LP (2.19) constructed in the proof of Theorem 2.2, $\mathbf{B} = (\mathbf{I} - \mathbb{A}^g\mathbb{A})^T$, which is an $n \times n$ matrix, and hence the complexity is $O(n^3L)$ as mentioned in Section 2.3.

In the following, we show that if we choose the g-inverse of $\mathbb{A}$ to be $\mathbb{A}^+$, the Moore-Penrose inverse, the problem size can be reduced by some further transformations. Let the SVD of $\mathbb{A}$ be $\mathbf{U\Sigma V}^T$. Then $\mathbb{A}^+ = \mathbf{V\Sigma}^+\mathbf{U}^T$. Suppose rank$(\mathbf{\Sigma}_{m\times n}) = r$ and set $s = n-r$.We have

$$\begin{aligned} \mathbb{A}^+\mathbb{A} &= \mathbf{V\Sigma}^+\mathbf{U}^T\mathbf{U\Sigma V}^T \\ &= \mathbf{V}\begin{bmatrix} \mathbf{I}_r & \mathbf{0}_{r\times s} \\ \mathbf{0}_{s\times r} & \mathbf{0}_{s\times s} \end{bmatrix}\mathbf{V}^T. \end{aligned} \qquad (2.29)$$

As discussed in the proof of Theorem 2.2, checking $\text{Sim}_Y(Z \to X)$ holds or not is equivalent to checking whether

$$(\mathbf{I} - \mathbb{A}^+\mathbb{A})\mathbf{p} \preceq \mathbb{A}^+\mathbf{c} \qquad (2.30)$$

has a solution or not. We now perform some transformations on (2.30). First we have

$$\begin{aligned} \mathbf{I} - \mathbb{A}^+\mathbb{A} = \mathbf{V}\begin{bmatrix} \mathbf{I}_r\, \mathbf{0}_{r\times s} \\ \mathbf{0}_{s\times r}\;\; \mathbf{I}_s \end{bmatrix}\mathbf{V}^T - \mathbf{V}\begin{bmatrix} \mathbf{I}_r\;\; \mathbf{0}_{r\times s} \\ \mathbf{0}_{s\times r}\mathbf{0}_{s\times s} \end{bmatrix}\mathbf{V}^T \\ = \mathbf{V}\begin{bmatrix} \mathbf{0}_{r\times r} & \mathbf{0}_{r\times s} \\ \mathbf{0}_{s\times r} & \mathbf{I}_s \end{bmatrix}\mathbf{V}^T. \end{aligned} \qquad (2.31)$$

Hence, (2.30) is equivalent to

$$\mathbf{V}\begin{bmatrix} \mathbf{0}_{r\times r} & \mathbf{0}_{r\times s} \\ \mathbf{0}_{s\times r} & \mathbf{I}_s \end{bmatrix}\mathbf{V}^T\mathbf{p} \preceq \mathbb{A}^+\mathbf{c}. \tag{2.32}$$

$\mathbf{V}$ can be split into four blocks as

$$\mathbf{V} = \begin{bmatrix} \mathbf{V}_{r\times r} & \mathbf{V}_{r\times s} \\ \mathbf{V}_{s\times r} & \mathbf{V}_{s\times s} \end{bmatrix}. \tag{2.33}$$

We use $\mathbf{w}$ to denote the $n \times 1$ column vector $\mathbf{V}^T\mathbf{p}$, i.e.,

$$\mathbf{w} = \mathbf{V}^T\mathbf{p}. \tag{2.34}$$

Note that $\mathbf{p} \leftrightarrow \mathbf{w}$ is a reversible bijection, since $\mathbf{V}^T$ is a full rank matrix.

Then (2.32) is equivalent to

$$\begin{bmatrix} \mathbf{0}_{r\times r} & \mathbf{V}_{r\times s} \\ \mathbf{0}_{s\times r} & \mathbf{V}_{s\times s} \end{bmatrix}\begin{bmatrix} \mathbf{w}_{r\times 1} \\ \mathbf{w}_{s\times 1} \end{bmatrix} \preceq \mathbb{A}^+\mathbf{c}, \tag{2.35}$$

which is equivalent to

$$\begin{bmatrix} \mathbf{V}_{r\times s} \\ \mathbf{V}_{s\times s} \end{bmatrix}\begin{bmatrix} \mathbf{w}_{s\times 1} \end{bmatrix} \preceq \mathbb{A}^+\mathbf{c}. \tag{2.36}$$

Hence, checking whether (2.30) has a solution or not is equivalent to checking whether (2.36) has a solution or not. To check whether (2.36) has a solution or not, we can construct a new LP for (2.36) in the same way as in the proof in Theorem 2.2. However, the size of the newly constructed LP will be smaller than that of (2.19) constructed in the proof of Theorem 2.2. The complexity for the newly constructed LP will be $O((ns^2 + n^{1.5}s)L)$. Since s is always less than or equal to n (sometimes, s can be much less than n, e.g. $s = O(\sqrt{n})$) and that L doesn't change, compared with the LP (2.19), the computational complexity for this new LP will be reduced.

2.5 Sentitivity Analysis

Simulatability condition $\text{Sim}_Y(Z \to X)$ requires the precise information about the joint PMFs P_{YX} and P_{YZ}. In practice, it's reasonable to assume that P_{YX} is precisely known. However, in certain scenarios, we may not know P_{YZ} perfectly, as Z is the random variable observed at the adversary. In this section, we investigate the sensitivity of simulatability condition $\text{Sim}_Y(Z \to X)$ with regards to the modeling uncertainty about P_{YZ}. The techniques can be applied to analyze $\text{Sim}_X(Z \to Y)$.

In particular, we assume that P_{YX} is perfectly known but P_{YZ} is known only to a certain precision. To be more precise, we assume that the true joint PMF of Bob and Eve is $P_{Y\tilde{Z}}$, but the legitimate users know only an estimate P_{YZ} to a certain precision in the following sense:

$$|\Delta a_{i,k}| \leq \delta, \quad \forall i \in [1 : |\mathcal{Y}|], k \in [1 : |\mathcal{Z}|], \tag{2.37}$$

in which

$$\Delta a_{i,k} \triangleq P_{Y\tilde{Z}}(i,k) - P_{YZ}(i,k). \tag{2.38}$$

As P_{YX} is perfectly known, which implies P_Y is perfectly known, we have

$$P_Y(i) = \sum_{k=1}^{|\mathcal{Z}|} P_{Y\tilde{Z}}(i,k) = \sum_{k=1}^{|\mathcal{Z}|} P_{YZ}(i,k). \tag{2.39}$$

Similar to (2.5), we use $\mathbf{A}$ to denote P_{YZ}, and $\tilde{\mathbf{A}} = \mathbf{A} + \Delta\mathbf{A}$ to denote $P_{Y\tilde{Z}}$. Using these notation, we can rewrite (2.37) and (2.39) as

$$|\Delta a_{ik}| \leq \delta, \quad \forall i = 1, \cdots, |\mathcal{Y}|, k = 1, \cdots, |\mathcal{Z}|, \tag{2.40}$$

$$\text{and} \quad \sum_{k=1}^{|\mathcal{Z}|} \Delta a_{ik} = 0, \quad \forall i = 1, \cdots, |\mathcal{Y}|. \tag{2.41}$$

Suppose $\text{Sim}_Y(Z \to X)$ does not hold with regards to P_{XYZ} (the perceived model by the legitimate users), we would like to know whether $\text{Sim}_Y(Z \to X)$ holds or not regarding $P_{XY\tilde{Z}}$ (the true underlying model).

From the discussion in Section 2.3, we know that checking $\text{Sim}_Y(Z \to X)$ is equivalent in checking whether there exists a $\mathbf{Q}$ satisfying (2.5), (2.6) and (2.7). In Section 2.3, to facilitate the analysis of the algorithm complexity, we convert these equations to an LP problem. In this section, to facilitate the sensitivity analysis, we construct another optimization problem:

$$\min_{\mathbf{q}} \quad ||\mathcal{A}\mathbf{q} - \mathfrak{c}||_1 \tag{2.42}$$

$$\text{s.t.} \quad \mathbf{q} \succeq \mathbf{0}, \tag{2.43}$$

$$[\mathbf{I}_{|\mathcal{Z}|} \otimes \mathbf{1}_{1\times|\mathcal{X}|}]\mathbf{q} = \mathbf{1}_{|\mathcal{Z}|}, \tag{2.44}$$

where $|| \cdot ||_1$ is the ℓ_1 norm, $\mathfrak{c} \triangleq \text{Vec}(\mathbf{C}^T)$, $\mathcal{A} \triangleq [\mathbf{A} \otimes \mathbf{I}_{|\mathcal{X}|}]$ and $\mathbf{q} \triangleq \text{Vec}(\mathbf{Q}^T)$. Here, (2.42) corresponds to (2.5), (2.43) corresponds to (2.6), and (2.44) corresponds to (2.7), respectively. It is clear that simulatability condition holds iff the optimal value for (2.42) equals 0.

Now, suppose $\text{Sim}_Y(Z \to X)$ does not hold with regards to P_{XYZ}, that is the optimal value of (2.42) is $\varepsilon_0 > 0$, we have the following theorem.

Theorem 2.9. Suppose $\text{Sim}_Y(Z \to X)$ does not hold with regards to P_{XYZ}, then for any $\delta < \frac{\varepsilon_0}{|\mathcal{Y}||\mathcal{Z}|}$, $\text{Sim}_Y(Z \to X)$ does not hold with regards to $P_{XY\tilde{Z}}$ neither .

Proof. To prove simulatability condition doesn't hold for $P_{XY\tilde{Z}}$ is equivalent to show the optimal value for the following convex optimization problem is lager than 0. We have

$$\begin{aligned} &\min_{\mathbf{q}} \;\; ||\tilde{\mathcal{A}}\mathbf{q} - \mathfrak{c}||_1 \\ \text{s.t.} \quad &\mathbf{q} \succeq \mathbf{0}, \\ &[\mathbf{I}_{|\mathcal{Z}|} \otimes \mathbf{1}_{1\times|\mathcal{X}|}]\mathbf{q} = \mathbf{1}_{|\mathcal{Z}|}, \end{aligned} \tag{2.45}$$

in which $\tilde{\mathcal{A}} \triangleq [\tilde{\mathbf{A}} \otimes \mathbf{I}]$. We have

$$\begin{aligned} \min_{\mathbf{q}} ||\tilde{\mathcal{A}}\mathbf{q} - \mathfrak{c}||_1 &= \min_{\mathbf{q}} ||[(\mathbf{A} + \Delta\mathbf{A}) \otimes \mathbf{I}]\mathbf{q} - \mathfrak{c}||_1 \\ &= \min_{\mathbf{q}} ||\mathcal{A}\mathbf{q} + \Delta\mathcal{A}\mathbf{q} - \mathfrak{c}||_1 \\ &\geq \min_{\mathbf{q}} \{||\mathcal{A}\mathbf{q} - \mathfrak{c}||_1 - ||\Delta\mathcal{A}\mathbf{q}||_1\} \\ &\geq \min_{\mathbf{q}} ||\mathcal{A}\mathbf{q} - \mathfrak{c}||_1 - \max_{\mathbf{q}} ||\Delta\mathcal{A}\mathbf{q}||_1 \\ &= \min_{\mathbf{q}} ||\mathcal{A}\mathbf{q} - \mathfrak{c}||_1 - \max_{\mathbf{Q}} ||\text{Vec}(\Delta\mathbf{A}\mathbf{Q})||_1 \\ &\overset{(a)}{\geq} \varepsilon_0 - |\mathcal{Y}||\mathcal{Z}|\delta \\ &> 0, \end{aligned}$$

if $\delta < \frac{\varepsilon_0}{|\mathcal{Y}||\mathcal{Z}|}$. In the above derivation, step (a) holds, because the summation of each row of $\mathbf{Q}$ equals to 1. This completes the proof. □

The bound obtained in Theorem 2.9 is sharp. In particular, there are examples in which once $\delta = \frac{\varepsilon_0}{|\mathcal{Y}||\mathcal{Z}|}$, we can find $P_{XY\tilde{Z}}$ such that simulatability condition holds although the condition does not hold for P_{XYZ}. In the following, we give such an example.

Assume

$$\mathbf{A} = \begin{bmatrix} 1/4 & 1/4 \\ 1/4 & 1/4 \end{bmatrix}, \; \mathbf{C} = \begin{bmatrix} 1/3 & 1/6 \\ 1/6 & 1/3 \end{bmatrix}. \tag{2.46}$$

Then, by setting $\mathbf{Q} = \begin{bmatrix} \lambda_1 & 1-\lambda_1 \\ \lambda_2 & 1-\lambda_2 \end{bmatrix}$, we have

$$\begin{aligned}
\varepsilon_0 &:= \min_{\mathbf{q}} ||\mathcal{A}\mathbf{q} - \mathfrak{c}||_1 && (2.47)\\
&= \min_{\mathbf{Q}} ||\text{Vec}(\mathbf{AQ} - \mathbf{C})||_1 && (2.48)\\
&= \min_{\lambda_1,\lambda_2} \left|\left|\text{Vec}\left(\begin{bmatrix} \frac{\lambda_1+\lambda_2}{4} - \frac{1}{3} & \frac{1}{3} - \frac{\lambda_1+\lambda_2}{4} \\ \frac{\lambda_1+\lambda_2}{4} - \frac{1}{6} & \frac{1}{6} - \frac{\lambda_1+\lambda_2}{4} \end{bmatrix}\right)\right|\right|_1 && (2.49)\\
&= 2\min_{\lambda_1,\lambda_2}\left\{\left|\frac{\lambda_1+\lambda_2}{4} - \frac{1}{3}\right| + \left|\frac{\lambda_1+\lambda_2}{4} - \frac{1}{6}\right|\right\} && (2.50)\\
&= 2\cdot\left|\frac{1}{3} - \frac{1}{6}\right| && (2.51)\\
&= 1/3, && (2.52)
\end{aligned}$$

which implies that $\text{Sim}_Y(Z \to X)$ does not hold for the given P_{XYZ}.

Now if

$$\delta = \frac{\varepsilon_0}{|\mathcal{Y}||\mathcal{Z}|} = \frac{1}{2\cdot 2}\varepsilon_0 = \frac{1}{12},$$

then $\tilde{\mathbf{A}}$ can be

$$\begin{aligned}
\tilde{\mathbf{A}} &= \begin{bmatrix} 1/4 + 1/12 & 1/4 - 1/12 \\ 1/4 - 1/12 & 1/4 + 1/12 \end{bmatrix} && (2.53)\\
&= \begin{bmatrix} 1/3 & 1/6 \\ 1/6 & 1/3 \end{bmatrix}. && (2.54)
\end{aligned}$$

This is exactly the same as $\mathbf{C}$, which obviously indicates that simulatability condition holds for the perturbed PMF $P_{XY\tilde{Z}}$.

2.6 Numerical Examples

In this section, we provide several examples to illustrate the proposed algorithm. We also use some of the examples used in [63] to compare our proposed algorithm with the method in [63].

Example 1: Let P_{XYZ} with ranges $\mathcal{X} = \{x_1, x_2\}$, $\mathcal{Y} = \{y_1, y_2\}$ and $\mathcal{Z} = \{z_1, z_2, z_3\}$ be:

$$\begin{aligned}
&P_{XYZ}(x_1, y_1, z_1) = 6/100,\\
&P_{XYZ}(x_2, y_1, z_1) = 4/100,\\
&P_{XYZ}(x_1, y_1, z_2) = 9/100,\\
&P_{XYZ}(x_2, y_1, z_2) = 6/100,\\
&P_{XYZ}(x_1, y_1, z_3) = 15/100,\\
&P_{XYZ}(x_2, y_1, z_3) = 10/100,\\
&P_{XYZ}(x_1, y_2, z_1) = 36/100,\\
&P_{XYZ}(x_2, y_2, z_1) = 4/100,\\
&P_{XYZ}(x_1, y_2, z_2) = 9/100,\\
&P_{XYZ}(x_2, y_2, z_2) = 1/100,\\
&P_{XYZ}(x_1, y_2, z_3) = 0,\\
&P_{XYZ}(x_2, y_2, z_3) = 0.
\end{aligned}$$

To use our algorithm, we have the following steps:

Step 1: Compute P_{YZ} and P_{YX}, and write them in the matrix form $\mathbf{A}$ and $\mathbf{C}$:

$$\mathbf{A} = \begin{bmatrix} 0.1 & 0.15 & 0.25 \\ 0.4 & 0.1 & 0 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 0.3 & 0.2 \\ 0.45 & 0.05 \end{bmatrix}. \tag{2.55}$$

Step 2: Construct $\mathbb{A}$ and **c** using (2.10) and (2.11) respectively:

$$\mathbb{A} = \begin{bmatrix} 0.1 & 0 & 0.15 & 0 & 0.25 & 0 \\ 0 & 0.1 & 0 & 0.15 & 0 & 0.25 \\ 0.4 & 0 & 0.1 & 0 & 0 & 0 \\ 0 & 0.4 & 0 & 0.1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \tag{2.56}$$

$$\mathbf{c} = [0.3, 0.2, 0.45, 0.05, 1, 1, 1]^T. \tag{2.57}$$

Step 3: Check the ranks of $\mathbb{A}$ and $(\mathbb{A}|\mathbf{c})$:

We get

$$\text{Rank}(\mathbb{A}) = \text{Rank}((\mathbb{A}|\mathbf{c})) = 5. \tag{2.58}$$

Step 4: Choose the g-inverse to be the Moore-Penrose pseudoinverse $\mathbb{A}^+$ and calculate $\mathbb{A}^+\mathbf{c}$ and $\mathbf{I} - \mathbb{A}^+\mathbb{A}$:

$$\mathbb{A}^+\mathbf{c} = \begin{bmatrix} 0.9762 \\ 0.0238 \\ 0.5952 \\ 0.4048 \\ 0.4524 \\ 0.5476 \end{bmatrix}, \tag{2.59}$$

$$\mathbf{I} - \mathbb{A}^{+}\mathbb{A} = \begin{bmatrix} 0.0238 & -0.0238 & -0.0952 & 0.0952 & 0.0476 & -0.0476 \\ -0.0238 & 0.0238 & 0.0952 & -0.0952 & -0.0476 & 0.0476 \\ -0.0952 & 0.0952 & 0.3810 & -0.3810 & -0.1905 & 0.1905 \\ 0.0952 & -0.0952 & -0.3810 & 0.3810 & 0.1905 & -0.1905 \\ 0.0476 & -0.0476 & -0.1905 & -0.1905 & 0.0952 & -0.0952 \\ -0.0476 & 0.0476 & 0.1905 & -0.1905 & -0.0952 & 0.0952 \end{bmatrix}. \tag{2.60}$$

Step 5: Solve LP (2.19). Using the above data, we obtain $h^* = 0$, which implies that $\text{Sim}_Y(Z \to X)$ holds.

Step 6: Obtain a possible $P_{\bar{X}|Z}$. We construct the LP defined in (2.27) with $\mathbf{e} = [2, 2, 2, 1, 1, 1]^T$, and get

$$\mathbf{q}^* = [1, 0, 1/2, 1/2, 1/2, 1/2]^T.$$

Thus the simulatability channel is

$$P_{\bar{X}|Z} = \begin{bmatrix} 1 & 0 \\ 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}, \tag{2.61}$$

which is consistent with the result obtained from the criterion proposed in [63]. If we set $\mathbf{e} = [1, 1, 1, 1, 1, 1]^T$, we get

$$\mathbf{q}^* = [0.9762, 0.0238, 0.5952, 0.4048, 0.4524, 0.5476]^T,$$

which implies that another valid choice is

$$P_{\bar{X}|Z} = \begin{bmatrix} 0.9762 & 0.0238 \\ 0.5962 & 0.4048 \\ 0.4524 & 0.5476 \end{bmatrix}. \tag{2.62}$$

Example 2: In this example, we consider a case in which Y is not binary. To represent the joint PMF concisely, we follow the same approach in [63] and use

$$M_{UV} = (P_U(u), (P_{V|U=u}(v_1), \cdots, P_{V|U=u}(v_{|\mathcal{V}|-1})))_{u \in \mathcal{U}}$$

to represent the joint PMF P_{UV}. For this example, we set

$$\begin{aligned} M_{ZY} &= (0.3,(0,0)),(0.3,(0.5,0)), \\ &\quad (0.3,(0.25,\sqrt{3}/4)),(0.1,(0.25,\sqrt{3}/12)), \\ M_{XY} &= (0.3,(0.25,0)),(0.3,(0.375,\sqrt{3}/8)), \\ &\quad (0.3,(0.125,\sqrt{3}/8))(0.05,(0.24,\sqrt{3}/12)) \\ &\quad (0.05,(0.26,\sqrt{3}/12)). \end{aligned} \tag{2.63}$$

In step 1, we write P_{YZ} and P_{YX} in the matrix form $\mathbf{A}$ and $\mathbf{C}$:

$$\mathbf{A} = \begin{bmatrix} 0 & 0.1500 & 0.0750 & 0.0250 \\ 0 & 0 & 0.1299 & 0.0144 \\ 0.3000 & 0.1500 & 0.0951 & 0.0606 \end{bmatrix},$$

$$\mathbf{C} = \begin{bmatrix} 0.0750 & 0.1125 & 0.0375 & 0.0120 & 0.0130 \\ 0 & 0.0650 & 0.0650 & 0.0072 & 0.0072 \\ 0.2250 & 0.1225 & 0.1975 & 0.0308 & 0.0298 \end{bmatrix}.$$

To make the presentation concise, we do not list the values of $\mathbb{A}$, $\mathbf{c}$ and following steps in details. Steps $2, 3, 4$ are similar to those in Example 1. But in Step 5, we obtain that $h^* < 0$, which indicates that $\text{Sim}_Y(Z \to X)$ does not hold. This result is also consistent with the conclusion in [63], which is obtained by an analysis that exploits the special mass constellation structure of the data. We note that the mechanical model based "more centered" criterion in [63] does not work for this example, as Y is not binary anymore, although the mass constellation representation of PMFs can still be used to exploit the special structure that this set of data has.

Next, we provide an example for which the mass constellation presentation does not work while our algorithm can easily obtain the answers.

Example 3: In this example, we consider X, Y, Z with larger dimensions, in particular, we set $|\mathcal{X}| = 4$, $|\mathcal{Y}| = 4$, and $|\mathcal{Z}| = 6$. Again to represent the joint PMF concisely, we use the same method as that used in Example 2 to represent P_{XYZ}. For this example, we randomly set

$$\begin{aligned}
M_{ZY} = \ & (0.1604,(0.1966,0.1054,0.4198)),(0.1654,(0.1230,0.4709,0.3355)),\\
& (0.1613,(0.0350,0.6219,0.0823)),(0.1504,(0.4585,0.2504,0.2343)),\\
& (0.1207,(0.2443,0.4704,0.0701)),(0.2419,(0.2979,0.1151,0.4601));\\
M_{XY} = \ & (0.2603,(0.1784,0.3822,0.2056)),(0.2181,(0.1538,0.4409,0.2255)),\\
& (0.2356,(0.2129,0.2684,0.3913)),(0.2861,(0.3422,0.2044,0.3363)).
\end{aligned}$$

We denote the above PMF with following two matrices

$$\mathbf{A} = \begin{bmatrix} 0.0315 & 0.0203 & 0.0056 & 0.0690 & 0.0295 & 0.0720 \\ 0.0169 & 0.0779 & 0.1003 & 0.0377 & 0.0568 & 0.0278 \\ 0.0673 & 0.0555 & 0.0133 & 0.0352 & 0.0085 & 0.1113 \\ 0.0446 & 0.0117 & 0.0421 & 0.0085 & 0.0260 & 0.0307 \end{bmatrix},$$

$$\mathbf{C} = \begin{bmatrix} 0.0464 & 0.0335 & 0.0502 & 0.0979 \\ 0.0995 & 0.0962 & 0.0632 & 0.0585 \\ 0.0535 & 0.0492 & 0.0922 & 0.0962 \\ 0.0609 & 0.0392 & 0.0300 & 0.0335 \end{bmatrix}. \tag{2.64}$$

Following the same steps as those in Example 1, we obtain that $h^* = 0$, which means $\text{Sim}_Y(Z \to X)$ holds. Furthermore, by setting $\mathbf{e} = \mathbf{1}_{24\times 1}$ in (2.27), we obtain one possible

$P_{\bar{X}|Z}$, denoted by matrix $\mathbf{Q}^*$:

$$\mathbf{Q}^* = \begin{bmatrix} 0.4979 & 0.1504 & 0.2038 & 0.1479 \\ 0.0148 & 0.3751 & 0.5618 & 0.0483 \\ 0.5210 & 0.4391 & 0.0254 & 0.0144 \\ 0.1302 & 0.0917 & 0.0301 & 0.7481 \\ 0.5638 & 0.2674 & 0.0161 & 0.1527 \\ 0.0261 & 0.0622 & 0.4110 & 0.5006 \end{bmatrix}. \tag{2.65}$$

One can easily check that $\mathbf{AQ}^* = \mathbf{C}$ holds. We note that, because of the lack of special data structure and the high dimensions, it is difficult to use the mass constellation structure of [63] to check whether $\mathrm{Sim}_Y(Z \to X)$ holds or not in this example.

Example 4: In this example, we consider the following PMF P_{XY}:

$$P_{XY}(x, y) = \begin{cases} \frac{1-\alpha}{2}, & \text{if } x = y; \\ \frac{\alpha}{2}, & \text{if } x \neq y, \end{cases}$$

and Z is generated by $[X, Y]$ via an erasure channel with erasure probability $1 - \gamma$, i.e., $Z = (X, Y)$ with a probability γ and $Z = \phi$ with probability $1 - \gamma$. It was shown in [63] that $\mathrm{sim}_Y(Z \to X)$ and $\mathrm{sim}_X(Z \to Y)$ hold if and only if $\gamma \geq 1 - 2\alpha$. In the following, we use our algorithm to verify the obtained result.

As above, in step 1, we compute P_{YZ} and write P_{YZ} and P_{YX} in matrix form $\mathbf{A}$ and $\mathbf{C}$:

$$\mathbf{A} = \begin{bmatrix} \frac{(1-\alpha)\gamma}{2} & \frac{\alpha\gamma}{2} & 0 & 0 & \frac{1-\gamma}{2} \\ 0 & 0 & \frac{\alpha\gamma}{2} & \frac{(1-\alpha)\gamma}{2} & \frac{1-\gamma}{2} \end{bmatrix}, \mathbf{C} = \begin{bmatrix} \frac{1-\alpha}{2} & \frac{\alpha}{2} \\ \frac{\alpha}{2} & \frac{1-\alpha}{2} \end{bmatrix}. \tag{2.66}$$

In step 2, we calculate matrices $\mathbb{A}$ and $\mathbf{c}$:

$$\mathbb{A} = \begin{bmatrix} \frac{(1-\alpha)\gamma}{2} & 0 & \frac{\alpha\gamma}{2} & 0 & 0 & 0 & 0 & 0 & \frac{1-\gamma}{2} & 0 \\ 0 & \frac{(1-\alpha)\gamma}{2} & 0 & \frac{\alpha\gamma}{2} & 0 & 0 & 0 & 0 & 0 & \frac{1-\gamma}{2} \\ 0 & 0 & 0 & 0 & \frac{\alpha\gamma}{2} & 0 & \frac{(1-\alpha)\gamma}{2} & 0 & \frac{1-\gamma}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{\alpha\gamma}{2} & 0 & \frac{(1-\alpha)\gamma}{2} & 0 & \frac{1-\gamma}{2} \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$\mathbf{c} = [1-\alpha, \alpha, \alpha, 1-\alpha, 1, 1, 1, 1, 1]^T.$$

The following steps are similar to those in Examples 1 and 2. Using our algorithm, we can find that, for any given values α and γ, as long as $\gamma \geq 1 - 2\alpha$, $h^* = 0$, and simulatability condition holds. We can also obtain a possible simulatability channel $P_{\bar{X}|Z}$ that Eve may use, following the same steps as in Example 1. On the other side, if $\gamma < 1 - 2\alpha$, we obtained $h^* < 0$, and hence simulatability condition does not hold.

From the above examples, we can see our proposed algorithm works for general given P_{XYZ}, and it's more powerful than the algorithm proposed in [63].

2.7 Concluding Remarks

In this chapter, we have studied an fundamental concept simulatability condition in the presence of an active attacker. We have proposed an efficient algorithm to check simulatability condition, an important condition in the problems of secret key generation using a non-authenticated public channel. We have also proposed a simple and flexible method to calculate a possible simulatability channel if simulatability condition holds. The proposed algorithms have polynomial complexities. We have shown that simulatability condition is not sensitive to modelling uncertainty. Finally, we have proposed an approach to further reduce the computational complexity, and used several numerical example to illustrate the efficiency of our propose algorithm.

Chapter 3

Generation of Multiple Keys

In this chapter, the problem of simultaneously generating multiple keys over a cascade of a noiseless channel and a wiretap channel is considered. The problem consists of three legitimate parties (i.e., Alice, Bob, and Carol), where Alice and Bob wish to agree with Carol on independent secret keys. Alice and Bob are connected via a noiseless channel, and Bob is connected with Carol via a wiretap channel, while there is no direct connection between Alice and Carol. To Alice and Carol, Bob acts as a relay. Under this model, we first provide a full characterization of the secret-key capacity region for the case when Eve has no side information. The result shows that there exists a trade-off between the individual secret-key rates. Then we generalize the obtained result into the case when Eve has side information, and fully characterize the corresponding secret-key capacity region.

3.1 Motivation

To gain some understanding of scenarios with limited direct access to the public discussion by certain legitimate users, we consider an extension of the joint source-channel model of [40]. In our model, there are three legitimate users: Alice, Bob, and Carol. Alice and Bob are connected by a noiseless public channel (Eve can observe this noiseless channel), and Bob is connected with Carol via a noisy channel (Eve can also eavesdrop on this channel).

However, Alice has no direct connection with Carol and therefore Carol does not have direct access to the public discussion messages sent by Alice. This network setting captures many relevant scenarios such as the scenario where Alice is a server who connects with the base station Bob over an optical fiber, which can be viewed as noiseless, and Carol is a wireless user. Furthermore, we assume that Alice and Carol have access to correlated random sources.

Under this network topology, we consider the problem of simultaneously generating two secret keys: One between Alice and Carol, and one between Bob and Carol. The problem of simultaneously generating multiple keys is well motivated in applications in which multiple keys are needed for different communication sessions [46, 118, 120, 121, 123]. In our setup, we require that the key generated by Alice and Carol is secure from Bob and Eve, while the key generated by Bob and Carol is secure from Alice and Eve. We first consider a case where Eve has no side information, and fully characterize the secret-key capacity region. Then, we generalize the considered model to the case when Eve has side information, and obtain a full characterization of the corresponding capacity region as well. It turns out that if we only care about the key between Alice and Carol, the considered model can be simplified to the source model with one-way limited-rate public discussion as studied in [19], and we show that our result recovers the result in [19]. On the other hand, if we only care about the key between Bob and Carol, the model can be viewed as a wiretap channel [17] and our result recovers that of the wiretap channel. Furthermore, there is a trade-off between the two cases so that Alice and Bob cannot attain their maximal secret-key rates simultaneously.

In addition to the work mentioned above, our work is related to recent papers on simultaneously generating multiple keys in networks consisting of trusted and untrusted parties [46, 118, 120, 121, 123]. The main differences between our model and models in these papers are: 1) we consider a joint source-channel model; and 2) we assume that the public discussion is not directly available to all users.

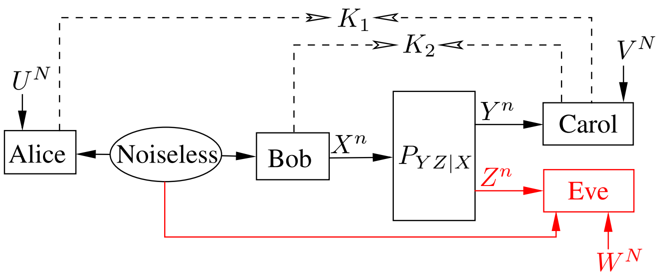


Figure 3.1: System model.

3.2 System Model and Problem Statement

As illustrated in Fig. 3.1, we consider a scenario in which Alice and Carol wish to agree on a secret key K_1 taking values from $\mathcal{K}_1$, while Bob wishes to agree with Carol on a secret key K_2 taking values from $\mathcal{K}_2$. Under this model, K_1 is required to be kept confidential from Bob and Eve, while K_2 is required to be kept confidential from Alice and Eve.

Unlike Bob who can communicate with Carol over a noisy channel eavesdropped by Eve, Alice has no direct connection with Carol and therefore she needs assistance from Bob. The link between Bob and Carol is modeled as a wiretap channel $(\mathcal{X}, P_{YZ|X}, \mathcal{Y}, \mathcal{Z})$, where $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ denote finite channel input and output alphabets. Thus, X^n, a sequence encoded by Bob, is the input of the wiretap channel while Y^n and Z^n are the corresponding outputs, where n is the sequence length. Alice and Bob can communicate through a noiseless link. However, any message exchanged over this noiseless link will also be perfectly overheard by Eve.

Alice, Carol and Eve are assumed to have access to three correlated random sequences U^N, V^N and W^N, $N \in I\!N$, which are generated i.i.d. according to P_{UVW}. And U, V and W take values from the finite alphabets $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{W}$, respectively. Here and hereafter, N is the length of the source sequences, which can be different from n.

Definition 3.1. An (N, n) key-agreement protocol for the joint source-channel model is as follows.

- **Step** 0**).** Alice generates a random variable (RV) F_0, and Bob generates another RV

F_0'. F_0 and F_0' are mutually independent, and are independent with all other RVs in the model.

- **Step** 1**).** Alice and Bob exchange messages f_1 and f_1', where $f_1 \triangleq f_1(F_0, U^N)$ and $f_1' \triangleq f_1'(F_0')$, over the noiseless channel.

- **Step** i**).** Alice and Bob exchange messages $f_i(F_0, U^N, \mathbf{f}'^{i-1})$ and $f_i'(F_0', \mathbf{f}^{i-1})$, in which $\mathbf{f}^{i-1} \triangleq (f_1, \cdots, f_{i-1})$ and $\mathbf{f}'^{i-1}$ is defined in a similar manner.

- **Step** k**).** (After Alice and Bob finish their discussion) Denote $\mathbf{F} \triangleq (\mathbf{f}^{k-1}, \mathbf{f}'^{k-1})$. Bob generates another independent RV F_b and transmits $X^n(\mathbf{F}, F_b)$ into the wiretap channel.

- **Final step).** Alice computes a key via a function $K_1 \triangleq K_1(U^N, \mathbf{F}, F_0)$; Bob computes a key via a function $K_2 \triangleq K_2(\mathbf{F}, F_0', F_b)$; Carol computes two keys via functions $K_1' \triangleq K_1'(Y^n, V^N), K_2' \triangleq K_2'(Y^n, V^N)$.

Here, the use of RVs F_0 and F_0' enables the messages exchanged over the public noiseless channel to be random functions of U^N, while F_b ensures that Bob can use stochastic coding to generate his own key with Carol.

Definition 3.2. A secret-key rate pair (R_1, R_2) is said to be achievable if $\forall \epsilon > 0$ there exists an $n(\epsilon) \in I\!N$ and a sequence of (N, n) codes such that $\forall n \geq n(\epsilon)$, we have

$$\Pr\{K_i \neq K_i'\} \leq \epsilon, \quad i = 1, 2, \tag{3.1}$$

$$\frac{1}{n} I(K_1; \mathbf{F}, F_0', F_b) \leq \epsilon, \tag{3.2}$$

$$\frac{1}{n} I(K_2; \mathbf{F}, F_0, U^N) \leq \epsilon, \tag{3.3}$$

$$\frac{1}{n} I(K_1, K_2; \mathbf{F}, Z^n, W^N) \leq \epsilon, \tag{3.4}$$

$$\frac{1}{n} H(K_i) \geq \frac{1}{n} \log |\mathcal{K}_i| - \epsilon, \quad i = 1, 2, \tag{3.5}$$

$$\frac{1}{n} H(K_1) \geq R_1 - \epsilon, \ \frac{1}{n} H(K_2) \geq R_2 - \epsilon. \tag{3.6}$$

Here, (3.1) indicates that the keys generated at the key generating parties should be the same with high probability, (3.2) means that K_1 is required to be secure from Bob, (3.3) means that K_2 should be secure from Alice, (3.4) implies that (K_1, K_2) should be jointly secure from Eve, (3.5) indicates that the generated keys should be nearly uniformly distributed, and (3.6) indicates that R_1 and R_2 are the key rates of K_1 and K_2, respectively.

Definition 3.3. The secret-key capacity region $\mathcal{C}$ is defined as:

$$\mathcal{C} \triangleq \big\{(R_1, R_2) \in \mathbb{R}_+^2 \,|\, (R_1, R_2) \text{ is achievable}\big\}.$$

Furthermore, we use C_1 to denote the maximal value of R_1 (i.e., the key capacity of K_1), C_2 to denote the maximal value of R_2 (i.e., the key capacity of K_2) and C_{sum} to denote the maximal value of $R_1 + R_2$ (i.e., the sum capacity of (K_1, K_2)).

3.3 Main Results

In this section, to facilitate the presentation and understanding of our scheme, we first consider the special case when Eve has no side information, i.e., the case where $\mathcal{W} = \emptyset$, and denote the corresponding secret-key capacity region by $\mathcal{C}_0$. For this case, we fully characterize $\mathcal{C}_0$. Then, we extend the obtained result to the general model with side information at Eve.

3.3.1 Capacity Region with No Side Information at Eve

For auxiliary RVs S_1, S_2 and T_2 satisfying Markov chain conditions $S_1 \to U \to V$ and $T_2 \to S_2 \to X \to (Y, Z)$, define

$$\begin{aligned} \mathcal{R}(P_{S_1|U}, P_{T_2S_2}P_{X|S_2}) \triangleq \{(R_1, R_2) : R_1 \leq \frac{1}{\beta} I(S_1; V), \\ R_2 \leq \big[I(S_2; Y|T_2) - I(S_2; Z|T_2)\big]^+, \end{aligned} \qquad (3.7)$$

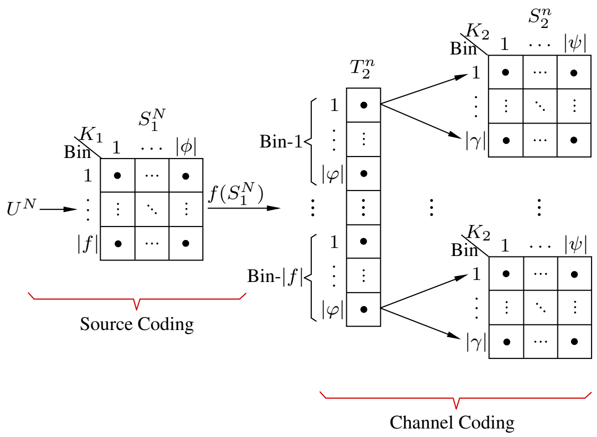


Figure 3.2: Codebook construction: S_1^N sequences are generated i.i.d. according to P_{S_1}; T_2^n sequences are generated i.i.d. according to P_{T_2} and for each T_2^n, generate certain S_2^n sequences according to $P_{S_2|T_2}$.

$$\text{s.t.} \quad I(S_1;U) - I(S_1;V) \leq \beta I(T_2;Y).\} \tag{3.8}$$

Here, $[x]^+ \triangleq \max\{0, x\}$ and $\beta = n/N$. To make the problem nontrivial, β is assumed to be a positive constant. Furthermore, the notation $S_1 \to U \to V$ means that RVs (S_1, U, V) form a Markov chain in that order, and other similar relationships throughout the chapter are defined in a similar manner.

We have the following result.

Theorem 3.1. The secret-key capacity region for the case with no side information at Eve is

$$\mathcal{C}_0 = \bigcup_{P_{S_1|U}, P_{T_2 S_2} P_{X|S_2}} \mathcal{R}(P_{S_1|U}, P_{T_2 S_2} P_{X|S_2}). \tag{3.9}$$

Proof. The proof contains two parts: converse and achievability. In the converse proof presented in Appendix A.1.1, we show that $\mathcal{C}_0$ defined by (3.9) is an outer bound. In the achievability part, we show that for any given $(P_{S_1|U} P_{UV}, P_{T_2 S_2} P_{X|S_2})$, rate pair (R_1, R_2) with

$$R_1 = \frac{1}{\beta} I(S_1;V) - \epsilon, R_2 = \left[I(S_2;Y|T_2) - I(S_2;Z|T_2)\right]^+ - \epsilon$$

$$\text{s.t.}\quad I(S_1;U) - I(S_1;V) \leq \beta I(T_2;Y), \tag{3.10}$$

is achievable, and hence the region specified in (3.9) is achievable. A detailed proof of the achievability part is provided in Appendix A.1.2. Here, we provide a high level idea of how the achievability scheme works. As illustrated in Fig. 3.2, the codebook construction is a combination of source coding techniques and channel coding techniques. We first generate S_1^N sequences according to P_{S_1}. Then, we generate T_2^n sequences according to P_{T_2} and for each generated sequence T_2^n, we generate S_2^n sequences according to $P_{S_2|T_2}$. From Alice and Carol's perspective, the noisy channel $P_{Y|X}$ acts as a noiseless channel with rate $I(T_2;Y)$. This guarantees that, if messages sent by Alice have a rate less than $I(T_2;Y)$, they can be correctly decoded with high probability by Carol using Y^n. As a result, the key generation model between Alice, Carol and Eve can be viewed as a source model (with no side information at Eve) using one way public discussion with rate constraint, and the rate $\frac{1}{\beta}I(S_1;V) - \epsilon$ is achievable using techniques for this model. In particular, to generate K_1, we generate $2^{N(I(S_1;U)+\epsilon)}$ sequences S_1^N , and randomly assign them into $2^{N(I(S_1;U)-I(S_1;V)+2\epsilon)}$ bins (we choose the number of bins to guarantee that its rate is less than $I(T_2;Y)$). Alice then sends the bin index to Carol through Bob. With this bin index along with its source observation V^N, Carol will be able to decode S_1^N. We will obtain a key at the rate of $\frac{1}{\beta}I(S_1;V) - \epsilon$ by setting the sub-bin index of the decoded S_1^N as the key value of K_1. At Bob's side, Bob chooses T_2^n to convey the received message to Carol, while using S_2^n generated by the selected T_2^n to generate his own key with Carol: We generate $2^{n(I(T_2;Y)-\epsilon)}$ sequences T_2^n. For each T_2^n we generate $2^{n(I(S_2;Y|T_2)-\epsilon)}$ sequences S_2^n and randomly assign them into $2^{n(I(S_2;Y|T_2)-I(S_2;Z|T_2)-2\epsilon)}$ bins. We set the bin index of S_2^n as the key value of K_2. □

Note that the role of T_2^n is to convey the message received from Alice, i.e., the bin index of S_1^N, to Carol. Since Eve has access to the public channel between Alice and Bob, it is not necessary to keep T_2^n secure from Eve. That's why we have only one term $\beta I(T_2;Y)$ on the right-side of (3.8).

3.3.2 Capacity Region with Side Information at Eve

In this subsection, we show that the result of Section 3.3.1 can be generalized to the case when Eve has access to side information, i.e. $\mathcal{W} \neq \emptyset$. Under this model, we fully characterize the corresponding secret-key capacity region as well.

For auxiliary RVs S_1, S_2, T_1 and T_2 satisfying Markov chain conditions $T_1 \to S_1 \to U \to (V,W)$ and $T_2 \to S_2 \to X \to (Y,Z)$, we define

$$\begin{aligned}\mathcal{R}(P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2}) \triangleq \{(R_1,R_2) : R_1 \leq \frac{1}{\beta}\big[I(S_1;V|T_1) - I(S_1;W|T_1)\big]^+,& \\ R_2 \leq \big[I(S_2;Y|T_2) - I(S_2;Z|T_2)\big]^+,& \quad (3.11) \\ \text{s.t.} \quad I(S_1;U) - I(S_1;V) \leq \beta I(T_2;Y).\}& \quad (3.12)\end{aligned}$$

Then, we have the following result.

Theorem 3.2. In the joint source-channel model with side information at Eve, the secret-key capacity region is

$$\mathcal{C} = \bigcup_{P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2}} \mathcal{R}(P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2}). \quad (3.13)$$

Proof. Similar to the proof of Theorem 3.1, this proof also contains two parts: converse and achievability. The converse proof is provided in Appendix A.3.

In the following, for the achievability, we outline the encoding/decoding and key generation process while omitting detailed analyses of key rates, error and information leakage as these follow similar lines as those in the proof of Theorem 3.1.

It suffices to show that the pair (R_1, R_2) with

$$R_1 = \frac{1}{\beta} I(S_1;V|T_1) - I(S_1;W|T_1) - \epsilon, \quad (3.14)$$

$$R_2 = I(S_2;Y|T_2) - I(S_2;Z|T_2) - \epsilon, \quad (3.15)$$

$$\text{s.t.} \quad I(S_1;U) - I(S_1;V) < \beta I(T_2;Y), \quad (3.16)$$

is achievable.

Given $(P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2})$, without loss of generality, we assume $I(S_1;V|T_1) - I(S_1;W|T_1) > 0$ and $I(S_2;Y|T_2) - I(S_2;Z|T_2) > 0$.

Codebook Construction:

$\mathcal{C}_A$ *at Alice*. Given P_{T_1}, randomly and independently generate $2^{NR_{10}}$ sequences T_1^N according to $\prod_{i=1}^{N} P_{T_1}(T_{1i})$, and assign each T_1^N uniformly at random into $2^{NR_{11}}$ bins indexed by $f_1(T_1^N)$ with $f_1 \in [1:2^{NR_{11}}]$. We denote the corresponding bin by $\mathcal{B}_0(f_1)$.

For each T_1^N, randomly and independently generate $2^{NR_{12}}$ sequences S_1^N according to $\prod_{i=1}^{N} P_{S_1|T_1}(S_{1i}|T_{1i})$. Assign each S_1^N uniformly at random into $2^{NR_{13}}$ bins indexed by $f_2(S_1^N)$ with $f_2 \in [1:2^{NR_{13}}]$. We denote the corresponding bin by $\mathcal{B}_1(f_2)$. Within each bin $\mathcal{B}_1(f_2)$, assign each S_1^N uniformly at random into $2^{NR_{14}}$ sub-bins indexed by $\phi(S_1^N)$ with $\phi \in [1:2^{NR_{14}}]$.

$\mathcal{C}_B$ *at Bob*. Given P_{T_2}, randomly and independently generate $2^{nR_{20}}$ sequences T_2^n according to $\prod_{i=1}^{n} P_{T_2}(T_{2i})$, indexed by (f_1, f_2, φ). For each $T_2^n(f_1, f_2, \varphi)$, randomly and independently generate $2^{nR_{21}}$ sequences S_2^n according to $\prod_{i=1}^{n} P_{S_2|T_2}(S_{2i}|T_{2i})$, and assign each S_2^n uniformly at random into $2^{nR_{22}}$ bins indexed by $\psi(S_2^n)$ with $\psi \in [1:2^{nR_{22}}]$. Here, we set

$$\begin{aligned}
&R_{10} = I(T_1;U) + \epsilon, \quad R_{11} = I(T_1;U) - I(T_1;V) + 2\epsilon,\\
&R_{12} = I(S_1;U|T_1) + \epsilon, \quad R_{13} = I(S_1;U|T_1) - I(S_1;V|T_1) + 2\epsilon,\\
&R_{14} = I(S_1;V|T_1) - I(S_1;W|T_1) - 2\epsilon, \quad R_{20} = I(T_2;Y) - \epsilon,\\
&R_{21} = I(S_2;Y|T_2) - \epsilon, \quad R_{22} = I(S_2;Y|T_2) - I(S_2;Z|T_2) - 2\epsilon.
\end{aligned}$$

Encoding: With the observed sequence U^N, Alice looks into $\mathcal{C}_A$, in order to find a T_1^N that is jointly typical with U^N according to P_{T_1U}. If there are more than one such sequence, she randomly selects one (suppose $T_1^N = t_1^N$ is selected); If Alice can't find it, she declares an error. Then, Alice looks into the set of S_1^N sequences generated by T_1^N, in order to find one S_1^N that is jointly typical with (T_1^N, U^N) according to $P_{T_1S_1U}$. If there are more than one such sequence, she randomly selects one (suppose $S_1^N = s_1^N$ is selected); If there exists no such sequence, she declares an error. Finally, Alice sends $(f_1(T_1^N), f_2(S_1^N))$ to Bob.

Upon receiving (f_1, f_2), Bob first randomly generates a value for φ and selects a sequence $T_2^n(f_1, f_2), \varphi)$ in $\mathcal{C}_B$. Then Bob randomly selects one $S_2^n = s_2^n$ from those S_2^n sequences that are generated by $T_2^n(f_1, f_2), \varphi)$, and transmits it to Carol via the channel $P_{X|S_2}P_{YZ|X}$.

Decoding: Upon receiving Y^n, Carol first tries to decode $(\hat{T}_2^n, \hat{S}_2^n)$ using the same method as described in the proof of Theorem 3.1.

After decoding $\hat{T}_2^n$ Carol will obtain corresponding values for (f_1, f_2). Then Carol refers to $\mathcal{C}_A$, looking for a unique $\hat{T}_1^N$ in $\mathcal{B}_0(f_1)$ that is jointly typical with V^N. If Carol cannot find at least one such sequence, she randomly selects one $\hat{T}_1^N$. Then, Carol turns to those S_1^N sequences that are generated by $\hat{T}_1^N$, in order to find a unique sequence $\hat{S}_1^N$ that is jointly typical with $(\hat{T}_1^N, V^N)$ according to $P_{T_1S_1V}$. If Carol does not find such sequence, she selects one at random.

Key Generation: Alice sets $K_1 = \phi(S_1^N)$; Bob sets $K_2 = \psi(S_2^n)$; Carol sets $\hat{K}_1 = \phi(\hat{S}_1^N)$ and $\hat{K}_2 = \psi(\hat{S}_2^n)$.

Finally, following similar arguments as those in the proof of Theorem 3.1, we can conclude that there exists at least one scheme such that (R_1, R_2) specified in (3.14) and (3.15) are achievable, and hence $\mathcal{R}(P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2})$ is achievable. □

3.3.3 Discussion

In this part, we discuss the implications of the results developed in this chapter. Except stated otherwise, we focus on the case with no side information at Eve, since the case with side information at Eve follows in a similar manner.

According to Theorem 3.1, the following rate is achievable for K_1:

$$\begin{aligned} & R_1 \leq \frac{1}{\beta} I(S_1;V), \\ \text{s.t.} \quad & I(S_1;U) - I(S_1;V) \leq \beta I(T_2;Y). \end{aligned} \tag{3.17}$$

Due to the Markov chain condition $T_2 \to X \to Y$, we have that (3.17) is contained in the set

$$\begin{aligned} \{ & R_1 \in I\!R_+ : R_1 \leq \frac{1}{\beta} I(S_1;V), \\ & \text{s.t.} \quad I(S_1;U) - I(S_1;V) \leq \beta I(X;Y)\}, \end{aligned} \tag{3.18}$$

which is achievable by setting $T_2 = X$. Hence, we can conclude via maximizing (3.18) that the secret-key capacity of K_1 for the case with no side information at Eve is

$$\begin{aligned} & C_1 = \max_{S_1 - U - V} \frac{1}{\beta} I(S_1;V), \\ \text{s.t.} \quad & I(S_1;U) - I(S_1;V) \leq \max_{P_X} \beta I(X;Y). \end{aligned} \tag{3.19}$$

Equation (3.19) shows that if one cares only about the key K_1, the channel between Alice and Carol can be viewed as a noiseless channel with rate constraint $R = \max_{P_X} \beta I(X;Y)$ and our problem is equivalent to the problem of generating a single key with one-way public discussion subject to a rate constraint as studied in [19, Sec. II. Case 6]. Our result is consistent with [19, Thm. 2.4].

Remark 3.3. Following a similar reasoning, we can also conclude that the secret-key capacity of K_1 for the case with side information at Eve is

$$\begin{aligned} & C_1 = \max_{T_1 - S_1 - U - (V,W)} \frac{1}{\beta} \big[I(S_1;V|T_1) - I(S_1;W|T_1) \big], \\ \text{s.t.} \quad & I(S_1;U) - I(S_1;V) \leq \max_{P_X} \beta I(X;Y). \end{aligned} \tag{3.20}$$

We would like to emphasize that, in general, the secret-key capacity with side information at Eve under multiple rounds of public discussion is still unknown [3]. The reason why we are able to characterize the key capacity of K_1 in our model is that, even though we allow multiple rounds of discussion over the public noiseless channel, the public discussion is between Alice and Bob, not between Alice and Carol. In our model, Carol is connected to this noiseless channel via a wiretap channel, which is a one-way link. Since Bob observes no randomness correlated with (U, V, W), compared with the case of one-way discussion between Alice and Bob, the multiple rounds of discussion between Alice and Bob do not increase the key rate between Alice and Carol. Thus, the link between Alice and Carol can be viewed as a one-way channel with rate constraint.

Furthermore, we have that the secret-key capacity of K_2 for the case with no side information at Eve is

$$C_2 = \max_{P_{S_2X}} \{I(S_2; Y) - I(S_2; Z)\}, \tag{3.21}$$

which can simply be derived from Theorem 3.1:

$$\begin{aligned} C_2 &= \max_{P_{T_2S}P_{X|S_2}} \{I(S_2; Y|T_2) - I(S_2; Z|T_2)\} \\ &= \max_{P_{T_2S_2}P_{X|S_2}} \sum_{t_2} P_{T_2}(t_2) \big[I(S_2; Y|T_2 = t_2) - I(S_2; Z|T_2 = t_2)\big] \\ &\overset{(a)}{\leq} \max_{P_{T_2S_2}P_{X|S_2}} \max_{t_2} \big[I(S_2; Y|T_2 = t_2) - I(S_2; Z|T_2 = t_2)\big] \\ &= \max_{P_{S_2X}} \{I(S_2; Y) - I(S_2; Z)\}, \end{aligned} \tag{3.22}$$

in which the equality in (a) can be obtained by setting T_2 to be some constant.

Equation (3.21) shows that if one cares only about K_2, the key capacity is the same as the capacity of a discrete memoryless wiretap channel. This implies that the correlated sources (U^N, V^N) do not help in increasing R_2, as we require K_2 to be secure from Alice.

Finally, from Theorem 3.1 we can easily obtain that the sum capacity of (K_1, K_2) for the

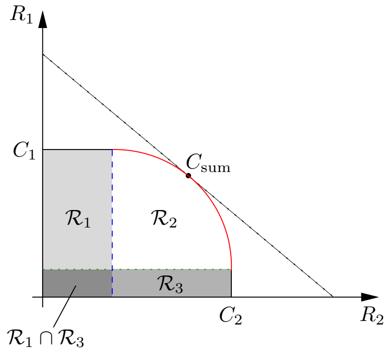


Figure 3.3: Secret-key capacity region $\mathcal{C} \triangleq \mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3$.

case with no side information at Eve is

$$
\begin{aligned}
C_{\text{sum}} = \max_{\substack{S_1 - U - V \\ T_2 - S_2 - X - (Y,Z)}} &\{I(S_2;Y|T_2) - I(S_2;Z|T_2) + \frac{1}{\beta} I(S_1;V)\}, \\
\text{s.t.} \quad & I(S_1;U) - I(S_1;V) \leq \beta I(T_2;Y). \qquad (3.23)
\end{aligned}
$$

The plot of $\mathcal{C}_0$ is shown in Fig. 3.3, where $\mathcal{C}_0 = \mathcal{R}_1 \bigcup \mathcal{R}_2 \bigcup \mathcal{R}_3$. $\mathcal{R}_1$ is the region where there exists a $P_{T_2^*}$ such that $\beta I(T_2^*;Y) \geq H(U|V) = \max\{I(S_1;U) - I(S_1;V)\}$ ($\mathcal{R}_1$ vanishes if $H(U|V) \geq \max_{P_X} \beta I(X;Y)$). One does not need to sacrifice R_1 in order to obtain a larger R_2 at least when $R_2 \leq \max_{P_{S_2|T_2^*} P_{S_2|X}} \{I(S_2;Y|T_2^*) - I(S_2;Z|T_2^*)\}$. $\mathcal{R}_3$ is the region obtained when $P_{T_2} = \arg\max_{P_{T_2}} \max_{P_{S_2|T_2} P_{X|S_2}} \{I(S_2;Y|T_2) - I(S_2;Z|T_2)\}$ and $I(S_1;U) - I(S_1;V) \leq \beta I(T_2;Y)$ ($\mathcal{R}_3$ vanishes if T_2 is a constant). And in $\mathcal{R}_3$, one doesn't need to sacrifice R_2 in order to obtain a larger R_1. Obviously, in $\mathcal{R}_2$, there exists a tradeoff between R_1 and R_2, and C_{sum} is obtained in this region.

Note that our model is related to the setup in [40], especially when one cares only about C_{sum}. The major difference is that we consider an achievable rate region while [40] equivalently focuses only on the sum capacity. In addition, in our model Alice and Bob are connected by a noiseless channel while the setup in [40] can be viewed this situation in which Alice and Bob are combined into one terminal. Furthermore, we require that K_1 is concealed from Bob and K_2 is concealed from Alice while these requirements do not exist in [40].

3.4 Concluding Remarks

In this chapter, we have introduced the problem of simultaneously generating multiple secret keys under a cascade model of a noiseless channel and a wiretap channel, using joint correlated sources and channels, to gain some understanding of key generation models with limited access to the public discussion channel. We have fully characterized the secret-key capacity region of the corresponding generated keys under the case when Eve has no side information, and generalized the result to the more general case when Eve has side information.

Chapter 4

Keyless Authentication

In this chapter, we consider the problem of keyless message authentication over noisy channels in the presence of an active adversary. Different from the existing models, in our model, the legitimate users do not have any pre-shared key for authentication. Instead, we use the noisy channel connecting the legitimate users for authentication. The main idea is to utilize the noisy channel connecting the legitimate users to generate an output at the receiver that is difficult for the adversary to replicate through its noisy channel, to distinguish a legitimate message from a fake message. By interpreting the message authentication as a hypothesis testing problem, we investigate the authentication exponent and the authenticated channel capacity of the noisy channel. In the authentication exponent problem, for a given message rate, we investigate the speed at which the optimal successful attack probability can be driven to zero. We fully characterize the authentication exponent for the zero-rate message case and provide both an upper bound and a lower bound on the exponent for the non-zero message rate case. In the authenticated capacity problem, we study the largest data transmission rate under which the attacker's optimal successful attack probability can still be made arbitrarily small. We establish an all or nothing result. In particular, we show that the authenticated channel capacity is the same as the classic channel capacity if a simulatability condition is not satisfied, while the authenticated capacity will be zero if this condition is satisfied. We also provide efficient algorithms to check this condition. We further show that our results are robust to modeling uncertainties about the eavesdropper's channels.

4.1 Motivation

From the previous discussion, using secret keys is an straightforward method to protect security in communication networks. However, there exist many scenarios in which certain concerned security issues can be achieved [35, 42]. In this chapter, we consider the authentication issue in security. We study a similar model as that in [30]: Alice, Bob and Eve are all connected with one another by noisy channels. Here we assume that Alice and Bob *do not share any secret key*. We will mainly rely on the channel $W(Y|X)$ connecting Alice and Bob for authentication. In particular, for any input PMF P_X generated by Alice, we produce an output distribution at Bob $P_Y = W(Y|X)P_X$. The main idea is to properly choose P_X so that the produced P_Y is difficult (precise meaning will be made clear in the sequel) for Eve to replicate through her noisy channel to Bob. In this way, after receiving a sequence Y^n, Bob can perform a hypothesis testing to check whether this sequence is generated from P_Y or not, which in return provides Bob evidences of whether the message is authentic or not. However, this hypothesis testing problem is more challenging than the classic hypothesis testing problems [72], in which each element of Y^n is typically assumed to be independently and identically generated from a certain PMF under each hypothesis. In our case, each element is not necessarily independent nor identically distributed. More importantly, the distribution under the alternative hypothesis, in which there is an attack, is totally controlled by the attacker (via the selection of the attack sequence) and can be arbitrary. Despite this challenge, we study and solve two closely related questions using this problem formulation.

In the first question, we focus on characterizing the optimal authentication exponent. In particular, for a given message rate, we investigate how to design the system so that the successful attack probability under Eve's optimal attack strategy is as small as possible.

The speed at which the successful attack probability goes to zero is called the authentication exponent. We derive an upper bound as well as a lower bound on the authentication exponent. We show that the upper bound and lower bound match in the zero-rate case. In the nonzero-rate scenario, we also identify some cases in which the upper and lower bound match. Hence the optimal authentication exponent is fully characterized in these cases.

In the second question, we focus on characterizing the authenticated capacity. In particular, we study what the largest data transmission rate is such that we can still design schemes to make Eve's successful attack probability arbitrarily small. We call such largest rate as the authenticated capacity. Compared with the classic definition of channel capacity, the authenticated capacity has an additional requirement that the decoded messages are guaranteed to come from the legitimate transmitter. We show an "all or nothing" result on the authenticated capacity. In particular, we show that if a "simulatability condition" is satisfied, the authenticated capacity is zero. On the other hand, if this condition is not satisfied, the authenticated capacity is the same as the classic notion of capacity. We also design efficient algorithms to check simulatability condition for any given channels. We further extend our study to the authenticated secrecy capacity and show a similar "all or nothing" result.

We would like to mention that the case without any shared key is also briefly discussed in [30]. In addition, Our work is related to recent papers on authentication exploiting the channel intrinsic randomness as well as the properties of channel reciprocality [34, 95, 107, 111, 115]. These papers also studied the authentication problem without using any pre-shared key, and proposed various novel authentication schemes to exploit the different channel statistics associated with different channels for authentication. Compared with these interesting papers, we characterize the fundamental limits of such systems by providing a more detailed and refined analysis.

Notation: We use X^n, Y^n and Z^n to denote the sequences generated or observed at Alice, Bob and Eve, respectively. Matrix $W(Y|X)$ is reserved as the channel statistics from Alice to Bob. $U(F|X)$ and $V(Y|Z)$ are defined in a similar manner. Furthermore, for any given

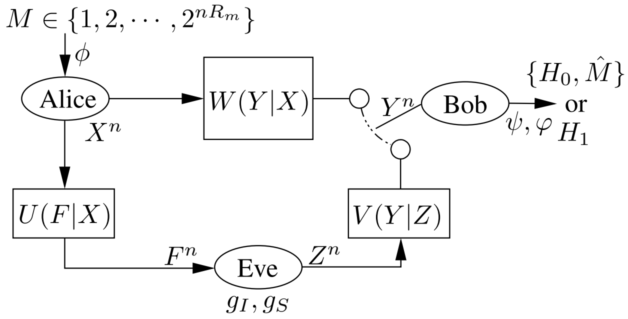


Figure 4.1: System model.

sequence $X^n \in \mathcal{X}^n$, the relative frequencies $\left(\frac{n_1}{n}, \cdots, \frac{n_{|\mathcal{X}|}}{n}\right)$ where $n_i, \forall i \in \mathcal{X}$ is the total number of indices $j \in [1:n]$ at which $X_j = i$, is called the type of X^n and is denoted by tp(X^n). We use P or Q to denote the PMF of a certain random variable, $\mathcal{T}_Y$ to denote the set of types of all sequences Y^n, and $\mathcal{T}_Y^n(P_Y)$ to denote the set of sequences Y^n with tp$(Y^n) = P_Y$. In addition, we denote $Q^n(A) \triangleq$ Pr$\{Y^n : Y^n \in A | Y \overset{iid}{\backsim} Q\}$, in which $Y \overset{iid}{\backsim} Q$ means that each component of Y^n is independently and identically distributed (i.i.d.) according to Q. Here, if $A = \mathcal{T}_Y^n(P_Y)$, we write it as $Q^n(P_Y)$ in short.

4.2 Preliminaries and Problem Setup

The model considered here is illustrated in Fig.4.1. Two terminals, Alice and Bob, would like to communicate with each other in the presence of an active adversary Eve. Alice and Bob do not share any secret key. Let $\mathcal{X} =: \{1, \cdots, |\mathcal{X}|\}$, $\mathcal{Y} =: \{1, \cdots, |\mathcal{Y}|\}$, $\mathcal{Z} =: \{1, \cdots, |\mathcal{Z}|\}$, and $\mathcal{F} =: \{1, \cdots, |\mathcal{F}|\}$ be four finite discrete sets, which represent the input alphabet set of Alice, the output alphabet set of Bob, the input alphabet set and the output alphabet set of Eve, respectively. These three users are connected with one another by three *noisy discrete memoryless channels* $W(Y|X)$, $U(F|X)$ and $V(Y|Z)$, which connect Alice and Bob, Alice and Eve, as well as Eve and Bob respectively. Here, $W(Y|X)$ is an $|\mathcal{Y}| \times |\mathcal{X}|$ matrix, with each column i, denoted by $W(Y|i)$, representing the output distribution at Bob when the input $X = i$. Other channel matrices are defined in a similar manner.

In this part, we assume that $W(Y|X)$ is perfectly known. As will be clear in the sequel, most of our schemes are universal with respect to Eve's channels $U(F|X)$ and $V(Y|Z)$. More specifically, with the exception of a particular scheme in Section 4.5, most of our schemes do not depend on any knowledge about $U(F|X)$ and $V(Y|Z)$. Furthermore, we will show that the particular scheme in Section 4.5 is robust against the uncertainty of the knowledge of $V(Y|Z)$. Hence, even for that particular scheme, we do not need perfect knowledge of $V(Y|Z)$.

Alice would like to send a message $M \in [1 : |M|]$ to Bob. She will use an encoder ϕ to convert M to a certain codeword X^n and transmit it via the channel $W(Y|X)$. However, Eve is an active attacker, and is assumed to be able to intercept the transmission of X^n such that Bob does not receive Y^n from the channel $W(Y|X)$ if Eve initiates the attack. This is a typical assumption in the authentication literature [32,36,41,45,49,58,61–63,83,84,103,110] and represents the worst case scenario from legitimate users' perspective. Furthermore, Eve can falsify messages and send them to Bob via the channel $V(Y|Z)$, based on her optimal strategy, to cheat Bob (details of the attacks considered will be made precisely in the sequel). Thus, after observing a sequence Y^n, Bob first needs to check the identity of Y^n: whether it is transmitted from Alice or faked by Eve. In particular, Bob will use a tester ψ to determine which of the following hypothesis is true:

$$H_0 : Y^n \text{ comes from Alice, no attack occurs,} \tag{4.1}$$

$$H_1 : Y^n \text{ comes from Eve, an attack occurs.} \tag{4.2}$$

If Bob determines that H_0 is true, he will then use a decoder φ to decode Y^n and obtain a decoded message $\hat{M} = \varphi(Y^n)$.

In summary, the system consists of the following components:

$$\text{Encoder } \phi : M \to X^n, \tag{4.3}$$

$$\text{Tester } \psi : Y^n \rightarrow H_0 \text{ or } H_1, \tag{4.4}$$

$$\text{Decoder } \varphi \text{ (if Bob determines } H_0) : Y^n \rightarrow \hat{M}. \tag{4.5}$$

For a given ψ, the acceptance region is defined by

$$\mathscr{A}_n = \{y^n \in \mathcal{Y}^n : \psi(y^n) = H_0\}.$$

Following the existing works on authentication [32, 41, 45, 58, 61–63, 83, 84], two types of attacks are considered:

- *Impersonation attack* g_I: This attack occurs before Alice sends anything. In particular, Eve uses an attack strategy g_I to select a sequence Z^n and sends it into the channel $V(Y|Z)$ to cheat Bob. We use PV(Z^n) to denote the output at Bob when Eve sends Z^n. The impersonation attack is said to be successful if Bob decides H_0. We use P_I to denote the success probability of the impersonation attack, i.e., $P_I = \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n)$.

- *Substitution attack* g_S: This attack occurs after Alice sends a codeword $X^n = \phi(M)$. In this attack, Eve intercepts the communication between Alice and Bob such that Bob receives no sequence from the channel $W(Y|X)$. Then Eve sends a sequence $Z^n = g_S(F^n)$ to Bob via the channel $V(Y|Z)$ based on the observations F^n obtained from the channel $U(F|X)$ connecting Alice and Eve. The attack is successful if Bob decides H_0 and the decoded message is different from the message sent by Alice. We use P_S to denote the success probability of the substitution attack, i.e., $P_S = \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n \text{ and } \hat{M} \neq M)$.

The goal of the attacker is to design the attack strategies g_I and g_S to maximize its successful attack probability

$$P_{SA} \triangleq \max\{P_I, P_S\}. \tag{4.6}$$

If there is no attack (i.e., when H_0 is true), two classes of errors could occur at Bob. The first class is the false rejection error, in which Bob falsely determines that an attack has occurred. This error probability is denoted by Pr$(H_1|H_0)$. The second class is that Bob correctly determines that there is no attack but incorrectly decodes the message. This error probability can be written as Pr$\{\hat{M} \neq M, H_0|H_0\}$.

Definition 4.1. A protocol (ϕ, ψ, φ) is called (ϵ, σ)-robust, if

$$\max_{M} \left\{ \text{Pr}\{\hat{M} \neq M, H_0|H_0\} + \text{Pr}(H_1|H_0) \right\} \leq \epsilon, \tag{4.7}$$

$$\max_{g_I, g_S} P_{SA} \leq \sigma. \tag{4.8}$$

Furthermore, R_m is said to be achievable using an (ϵ, σ)-robust protocol, if

$$\frac{1}{n} \log |M| \geq R_m - \epsilon. \tag{4.9}$$

Here, (4.7) implies that, if there is no attack, the maximum error probability over all messages is required to be smaller than ϵ. At the same time, (4.8) implies that, if there is an attack, the success probability of Eve's optimal attack strategy is less than σ. In other words, if there is an attack, Bob should detect the presence of the attack with a probability larger than $1 - \sigma$. With these definitions, two related problems are considered in this chapter:

- *Authentication Exponent:* for given R_m and ϵ, how fast can we make P_{SA} go to zero?
- *Authenticated Capacity:* what is the largest message rate R_m that a robust protocol can achieve?

4.2.1 Authentication Exponent

Define

$$\beta_n(R_m, \epsilon) = \min_{\phi, \psi, \varphi} \max_{g_I, g_S} P_{SA},$$

where ϕ, ψ and φ range over all possible functions satisfying (4.7) and (4.9). Furthermore, we define

$$\theta(R_m, \epsilon) = \liminf_{n \to \infty} -\frac{1}{n} \log \beta_n(R_m, \epsilon). \tag{4.10}$$

Here, $\theta(R_m, \epsilon)$ is the exponent (rate) at which the successful attack probability goes to zero as the block-length n increases.

Similarly, we can define

$$\beta_I(R_m, \epsilon) = \min_{\phi,\psi,\varphi} \max_{g_I} P_I, \tag{4.11}$$

$$\theta_I(R_m, \epsilon) = \liminf_{n \to \infty} -\frac{1}{n} \log \beta_I(R_m, \epsilon), \tag{4.12}$$

for the impersonation attack, and

$$\beta_S(R_m, \epsilon) = \min_{\phi,\psi,\varphi} \max_{g_S} P_S, \tag{4.13}$$

$$\theta_S(R_m, \epsilon) = \liminf_{n \to \infty} -\frac{1}{n} \log \beta_S(R_m, \epsilon), \tag{4.14}$$

for the substitution attack.

In this problem, our goal is to characterize $\theta(R_m, \epsilon)$.

4.2.2 Authenticated (Secrecy) Capacity

In the authenticated capacity problem, we would like to characterize the authenticated capacity of the channel $W(Y|X)$:

$$C^* = \sup_{\phi,\psi,\varphi} R_m,$$

in which the $\sup$ is taken over all ϕ, ψ, φ that satisfy (4.7) and (4.8) for arbitrarily small ϵ, σ. Compared with the classic definition of channel capacity C, the authenticated capacity has an additional requirement that the decoded messages are guaranteed to come from the legitimate transmitter. Clearly, we have $C^* \leq C$.

In addition, we would also like to characterize the authenticated secrecy capacity C_S^*, which is defined as the largest achievable rate such that (4.7) and (4.8) are satisfied and

$$\frac{1}{n} I(M; F^n) \leq \epsilon.$$

Again, compared with the classic definition of secrecy capacity C_S [113], our definition of authenticated secrecy capacity has the additional requirement that the accepted messages are guaranteed to come from the legitimate transmitter. Hence, we also have $C_S^* \leq C_S$.

4.3 Impersonation Attack vs Substitution Attack

In this section, we first analyze the relationship between the success probabilities of the impersonation attack and the substitution attack. This analysis illustrates that we can focus only on the impersonation attack, which can greatly simplify the presentation.

Theorem 4.1. If $|M| > 1$, we have

$$\theta(R_m, \epsilon) = \theta_I(R_m, \epsilon) = \theta_S(R_m, \epsilon). \tag{4.15}$$

Proof. We first prove the second equality. For the substitution attack, suppose a sequence X^n is transmitted by Alice, and Eve observes a corresponding sequence F^n, then we have

$$\begin{aligned}
\beta_S(R_m, \epsilon) &= \min_{\phi,\psi,\varphi} \max_{g_S(F^n)} P_S \\
&= \min_{\phi,\psi,\varphi} \max_{g_S(F^n)} \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n, \hat{M} \neq M) \\
&\leq \min_{\phi,\psi,\varphi} \max_{g_S(F^n)} \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&\leq \min_{\phi,\psi,\varphi} \max_{g_S(X^n)} \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n)
\end{aligned}$$

$$
\begin{aligned}
&\le \min_{\phi,\psi,\varphi} \max_{X^n} \max_{g_S(X^n)} \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&\overset{(a)}{\le} \min_{\phi,\psi,\varphi} \max_{g_I} P_I \\
&= \beta_I(R_m, \epsilon).
\end{aligned} \tag{4.16}
$$

Here, step (a) can be justified as follows. First, we note that the difference between the impersonation attack and the substitution attack lies in whether or not Eve observes the sequence F^n from the channel $U(F|X)$ before selecting the optimal attack sequence Z^n. Based on this observation, then for any given ϕ, ψ, φ and substitution attack strategy, we can construct a corresponding impersonation attack strategy as follows. Eve assumes that a codeword $\tilde{X}^n$ was transmitted by Alice and then generates $\tilde{F}^n$ using $U(F|X)$. With this $\tilde{F}^n$, Eve then makes the corresponding substitution attack. As Alice does not share a key with Bob in our model, Eve can generate $\tilde{X}^n$ in the same manner as Alice generates X^n (in the model with key considered in the existing work, Eve cannot do this as she does not know the key value shared by Alice and Bob), $\tilde{F}^n$ will have the same statistics as F^n. Since this is a particular impersonation attack strategy, we have

$$
\max_{\tilde{X}^n} \max_{g_S(\tilde{X}^n)} \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n) \le \max_{g_I} \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n),
$$

which indicates

$$
\begin{aligned}
\min_{\phi,\psi,\varphi} \max_{X^n} \max_{g_S(X^n)} \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n) &\le \min_{\phi,\psi,\varphi} \max_{g_I} \text{Pr}(\text{PV}(Z^n) \in \mathscr{A}_n) \\
&= \min_{\phi,\psi,\varphi} \max_{g_I} P_I.
\end{aligned}
$$

Thus, we have

$$
\theta_S(R_m, \epsilon) \ge \theta_I(R_m, \epsilon). \tag{4.17}
$$

Now, we show the other direction. The following is a valid substitution attack strategy:

Given ϕ, ψ and φ, no matter what F^n Eve observes from $U(F|X)$, she simply ignores F^n, and uses the corresponding optimal impersonation attack strategy to pick the attack sequence Z^n. We use P_S^* to denote the success probability of this particular substitution attack strategy, and we have

$$P_S^* = \left(1 - \frac{1}{|M|}\right) \max_{g_I} P_I,$$

with given ϕ, ψ and φ. Thus,

$$\begin{aligned}
\beta_S(R_m, \epsilon) &= \min_{\phi,\psi,\varphi} \max_{g_S} P_S \\
&\geq \min_{\phi,\psi,\varphi} P_S^* \\
&= \left(1 - \frac{1}{|M|}\right) \min_{\phi,\psi,\varphi} \max_{g_I} P_I \\
&= \left(1 - \frac{1}{|M|}\right) \beta_I(R_m, \epsilon), \qquad (4.18)
\end{aligned}$$

which implies

$$\theta_S(R_m, \epsilon) \leq \theta_I(R_m, \epsilon). \qquad (4.19)$$

Combining (4.17) with (4.19), we have

$$\theta_S(R_m, \epsilon) = \theta_I(R_m, \epsilon).$$

To show the first equality of (4.15), we have

$$\begin{aligned}
\beta_n(R_m, \epsilon) &= \min_{\phi,\psi,\varphi} \max_{g_I, g_S} P_{SA} \\
&= \min_{\phi,\psi,\varphi} \max_{g_I, g_S} \max\{P_I, P_S\} \\
&= \min_{\phi,\psi,\varphi} \max\{\max_{g_I, g_S} P_I, \max_{g_I, g_S} P_S\}
\end{aligned}$$

$$
\begin{aligned}
&= \min_{\phi,\psi,\varphi} \max\{\max_{g_I} P_I, \max_{g_S} P_S\} \\
&\overset{(a)}{=} \min_{\phi,\psi,\varphi} \max_{g_I} P_I \\
&= \beta_I(R_m, \epsilon),
\end{aligned}
$$

where step (a) is true due to (4.16). Thus,

$$\theta(R_m, \epsilon) = \theta_I(R_m, \epsilon).$$

□

Remark 4.2. This result shows that we can focus on analyzing the successful attack probability as well as its exponent based on the impersonation attack, as $\theta(R_m, \epsilon) = \theta_I(R_m, \epsilon) = \theta_S(R_m, \epsilon)$ and

$$|\beta_I(R_m, \epsilon) - \beta_S(R_m, \epsilon)| \leq \frac{1}{|M|}\beta_I(R_m, \epsilon), \tag{4.20}$$

which is true due to (4.16) and (4.18). The difference in (4.20) is a relatively small number, which has no influence on the authentication exponent analyzed in Section 4.4 even when $|M|$ is finite. In addition, this difference will not affect the capacity result analyzed in Section 4.5, since in that case $\beta_I(R_m, \epsilon)$ is an arbitrarily small value.

Remark 4.3. Here, we would like to compare this result with the result in the classic authentication setup [83], in which there exists a tradeoff between P_I and P_S as mentioned in the introduction: $P_I \geq 2^{-I(K;E)}$, $P_S \geq 2^{-H(K|E)}$. As discussed above, in the classic authentication setup, the authentication is based on the pre-shared key information. In the case with a shared key, the codeword E sent by Alice will contain information of K, which will be useful for Eve to carry out the substitution attack. In fact, the information about K contained in E is the main reason for the existence of a tradeoff between P_I and P_S in the classic setup. If E contains more information about K, the impersonation attack will be more difficult ($P_I \downarrow$) but the substitution attack will be easier ($P_S \uparrow$). Similarly, if E contains less information about K, $P_I \uparrow$ while $P_S \downarrow$. In our setup, there is no shared key, hence the codeword X^n sent by Alice does not carry any identification information and Eve can simply generate it by herself. In particular, when Alice sends nothing (thus the corresponding attack is an impersonation attack), Eve can construct an impersonation attack strategy by assuming a sequence $\tilde{X}^n$ was sent by Alice and using the corresponding substitution attack toward this $\tilde{X}^n$.

We note that, when $M = 1$, there is no substitution attack as there is no any other message for the attacker to substitute with. In this case, $\beta_S(R_m, \epsilon) = 0$ and the corresponding $\theta_S(R_m, \epsilon)$ is not defined while $\beta_I(R_m, \epsilon)$ can still be positive with well defined $\theta_I(R_m, \epsilon)$. This case will be analyzed in Theorem 4.4 below. Furthermore, we can easily conclude that $\theta(R_m, \epsilon) = \theta_I(R_m, \epsilon)$ still holds.

4.4 Authentication Exponent

In this section, for a given R_m and ϵ, we focus on characterizing the authentication exponent $\theta(R_m, \epsilon)$. We will first focus on the zero-rate case, in which $R_m = 0$, and then focus on the positive rate case.

4.4.1 Authentication of Zero-Rate Messages

To illustrate the main proof ideas, we first study the case of authentication for zero-rate messages: $|M|$ is finite, or infinite but

$$R_m = \frac{1}{n} \log |M| \to 0,$$

as $n \to \infty$. As discussed in Remark 4.2, it is sufficient to characterize $\theta_I(0, \epsilon)$.

Before deriving $\theta_I(0, \epsilon)$, we first analyze a special case: the case of single message, i.e.,

$|M| = 1$. In the single message case, the decoding step φ is not needed, hence the term Pr$\{\hat{M} \neq M, H_0|H_0\}$ vanishes and (4.11) becomes

$$\beta_I(0_1, \epsilon) = \min_{\phi,\psi} \max_{g_I} P_I,$$

with 0_1 denoting the fact that $|M| = 1$. We also use $\theta_I(0_1, \epsilon)$ to denote the corresponding exponent.

We have the following three elements:

- From Alice's perspective, it needs to design ϕ. In this case, it is equivalent to deciding which X^n to use as the codeword.

- From Bob's perspective, it needs to design ψ for the following hypothesis testing problem:

  $$H_0 : Y^n \sim PW(X^n),$$
  $$H_1 : Y^n \sim PV(Z^n),$$

  in which PW(X^n) denote the output at Bob when Alice sends X^n. However, it is more challenging than the classic hypothesis testing problem [72], in which $Y_i, i = 1, \cdots, n$ are typically assumed to be independently and identically generated from a certain PMF under each hypothesis. In our case, Y_i is not necessarily independent nor identically distributed for different i. More importantly, the distribution under H_1 is totally controlled by the attacker (via the selection of the attack sequence Z^n) and can be arbitrary.

- From Eve's perspective, its goal is to design g_I and the corresponding attack sequence Z^n to maximize the error probability.

Taking the above three elements into consideration, we have the following result.

Theorem 4.4.

$$\theta_I(0_1, \epsilon) = \max_{i \in \mathcal{X}} \min_{P_{Z,i} \in \mathcal{P}_{\mathcal{Z}}} D(P_{Y,i}||Q_{Y,i}), \tag{4.21}$$

in which

$$P_{Y,i} = W(Y|i), \tag{4.22}$$

$$Q_{Y,i} = \sum_{j \in \mathcal{Z}} V(Y|j) P_{Z,i}(j), \tag{4.23}$$

$P_{Z,i}$ is some distribution of Z for each $i \in \mathcal{X}$, and $D(\cdot||\cdot)$ is the Kullback-Leibler (KL) distance between its arguments.

Proof. Please see Appendix B.1. □

Remark 4.5. According to Theorem 2.7.2 of [16], $D(P_{Y,i}||Q_{Y,i})$ is convex in the pair ($P_{Y,i}$, $Q_{Y,i}$). Thus, for a fixed $P_{Y,i}$, we know that $D(P_{Y,i}||Q_{Y,i})$ is convex in $Q_{Y,i}$. In addition, $Q_{Y,i}$ is linear in $P_{Z,i}$ according to (4.23), we can conclude that $D(P_{Y,i}||Q_{Y,i})$ is convex in $P_{Z,i}$ (See Chapter 2 in [14]). Hence, $\min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i})$ with constraints (4.22) and (4.23) is a convex optimization problem, which can be solved efficiently.

Having obtained $\theta_I(0_1, \epsilon)$ of the single message case, we can easily generalize it to the case of multiple messages with zero-rate.

Theorem 4.6.

$$\theta_I(0, \epsilon) = \max_{i \in \mathcal{X}} \min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}),$$

where $P_{Y,i}$ and $Q_{Y,i}$ are defined by (4.22) and (4.23).

Proof. First, we show

$$\theta_I(0, \epsilon) \leq \theta_I(0_1, \epsilon) = \max_{i \in \mathcal{X}} \min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}).$$

For the multiple messages case, we again require $\Pr(H_1|H_0) \leq \epsilon$. Meanwhile,

$$\Pr(H_1|H_0) = \sum_{i=1}^{|M|} P(M=i)\Pr(H_1|H_0, M=i).$$

As the result, there must exist at least one $m \in [1:|M|]$, such that $\Pr(H_1|H_0, M=m) \leq \epsilon$. If we focus on the message $M = m$, it has the same requirements as the single message case. Thus, we can conclude that

$$\theta_I(0,\epsilon) \leq \max_{i\in\mathcal{X}} \min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}).$$

In the following, we show that we can construct a scheme to achieve $\max\limits_{i\in\mathcal{X}} \min\limits_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i})$. Let $k = \arg\max\limits_{i\in\mathcal{X}}\{\min\limits_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i})\}$. Since $\frac{1}{n}\log|M| \overset{n\to\infty}{\longrightarrow} 0$, there exist arbitrary small numbers $\{\epsilon_i\}_{i\in\mathcal{X}\backslash\{k\}}$, when n is sufficiently large, such that $2^{nI(X^*;Y)} > |M|$, where the distribution of X^* is given by

$$P_X^* \triangleq [\epsilon_1, \cdots, \epsilon_{k-1}, 1-\epsilon_0, \epsilon_{k+1}, \cdots, \epsilon_{|\mathcal{X}|}]^T, \epsilon_0 = \sum_{i\neq k} \epsilon_i. \tag{4.24}$$

Now, we use P_X^* defined above to do channel coding as that in [16, Chapter 7]: Generate $|M|$ sequences as codewords, and set the acceptance region be $\mathscr{A}_n := T_\epsilon^n(Y)$, in which the typical set is defined with respect to $P_Y = \sum\limits_{i\in\mathcal{X}} P_X^*(i)W(Y|i)$. Thus, we can easily verify that (4.7) is satisfied. Following similar steps as the derivation of (B.12) (details about this step are provided in Appendix B.4), we have

$$\begin{aligned}
2^{-n\theta_I(0,\epsilon)} &\leq 2^{-n(\min\limits_{P_Z} D(P_Y||Q_Y)-\epsilon')} \qquad (4.25)\\
&\triangleq 2^{-n(D(P_Y||Q_Y^*)-\epsilon')}\\
&\overset{(a)}{\leq} 2^{-n(D(P_{Y,k}||Q_Y^*)-\delta(\epsilon'))}\\
&\leq 2^{-n(\min\limits_{P_Z} D(P_{Y,k}||Q_Y)-\delta(\epsilon'))}\\
&= 2^{-n(\min\limits_{P_{Z,k}} D(P_{Y,k}||Q_{Y,k})-\delta(\epsilon'))}
\end{aligned}$$

$$= 2^{-n(\max_{i\in\mathcal{X}} \min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}) - \delta(\epsilon'))},$$

where $Q_Y = \sum_{j\in\mathcal{Z}} P_Z(j)V(Y|j)$, $Q_Y^* = \arg\min_{Q_Y} D(P_Y||Q_Y)$, and (a) is true due to Lemma B.2 in Appendix B.3, since $D(P_Y||P_{Y,k}) \leq \delta(\epsilon_0)$ because of (4.24). Thus, we have

$$\theta_I(0,\epsilon) \geq \max_{i\in\mathcal{X}} \min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}) - \delta(\epsilon').$$

Hence, we conclude that

$$\theta_I(0,\epsilon) = \max_{i\in\mathcal{X}} \min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}).$$

This completes the proof. □

4.4.2 Authentication of Nonzero-Rate Messages

In this subsection, we deal with the case with $R_m > 0$, which is a much more complicated scenario compared to the single message case. We first provide an upper bound and a lower bound on the exponent of the successful attack probability. We then provide conditions under which the upper and lower bounds match with each other.

Theorem 4.7. Let $P_Y = \sum_{i\in\mathcal{X}} P_X(i)W(Y|i)$ and $Q_Y = \sum_{j\in\mathcal{Z}} P_Z(j)V(Y|j)$, we have

$$\theta_I(R_m,\epsilon) \leq \min_{P_Z} \max_{P_X\in\mathcal{P}_R} D(P_Y||Q_Y), \tag{4.26}$$

$$\theta_I(R_m,\epsilon) \geq \max_{P_X\in\mathcal{P}_R} \min_{P_Z} D(P_Y||Q_Y), \tag{4.27}$$

in which

$$\mathcal{P}_R := \{P_X \in \mathcal{P}_X : I(X;Y) \geq R_m\}.$$

Proof. Please see Appendix B.2 □

In general, (4.26) and (4.27) do not match with each other. However, there do exist scenarios where these two bounds match and hence the authentication exponent is fully characterized for these scenarios.

Corollary 4.8. Let $f(P_X) \triangleq \min_{P_Z} D(P_Y||Q_Y)$, if $f(P_X) + I(X;Y)$ is convex with respect to $P_X \in \mathcal{P}_R$, then (4.26) and (4.27) match.

Proof. First, from (B.27) and (B.29), we know that the upper bound (4.26) can be equivalently written as

$$\theta_I(R_m, \epsilon) \leq \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m] \tag{4.28}$$

In the following, we will show that if $f(P_X) + I(X;Y)$ is convex with respect to $P_X \in \mathcal{P}_R$, then the lower bound in (4.27) can be equivalently written as

$$\theta_I(R_m, \epsilon) \geq \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m], \tag{4.29}$$

which implies that the upper bound (4.26) matches with the lower bound (4.27).

Hence, to show this corollary, we only need to show (4.29). Towards that end, let

$$\begin{aligned} \hat{P}_X &= \arg\max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m], \\ \tilde{P}_X &= \arg\max_{P_X \in \mathcal{P}_R} f(P_X). \end{aligned} \tag{4.30}$$

Since $D(P_Y||Q_Y)$ is convex in (P_Y, Q_Y), and (P_Y, Q_Y) are affine functions of (P_X, P_Z), then $D(P_Y||Q_Y)$ is convex in (P_X, P_Z). Thus, according to [14], $f(P_X)$ is convex in P_X. Since $I(X;Y)$ is concave in P_X, then depending on $W(Y|X)$ and $V(Y|Z)$, the summation $f(P_X) + I(X;Y)$ can be convex, concave or neither. For the case when $f(P_X) + I(X;Y)$ is convex in $P_X \in \mathcal{P}_R$, then the optimal value of $\max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m]$ is obtained on the boundary[96], that is $I(\hat{X};Y) = R_m$. Thus, we have

$$\begin{aligned} f(\hat{P}_X) &= f(\hat{P}_X) + I(\hat{X};Y) - R_m \\ &= \max_{P_X \in \mathcal{P}_R} [f(P_X) + I(X;Y) - R_m] \\ &\geq \max_{P_X \in \mathcal{P}_R} f(P_X) \\ &= f(\tilde{P}_X). \end{aligned}$$

On the other hand, according to the definition of $\tilde{P}_X$ as in (4.30), we have

$$f(\hat{P}_X) \leq \max_{P_X \in \mathcal{P}_R} f(P_X) = f(\tilde{P}_X).$$

Hence, it follows that

$$f(\hat{P}_X) = f(\tilde{P}_X).$$

Finally, if $f(P_X) + I(X;Y)$ is convex in $P_X \in \mathcal{P}_R$, the optimal value of the optimization problem (4.29) is same as

$$\max_{P_X \in \mathcal{P}_R} f(P_X),$$

which is (4.27). This finishes the proof. □

In the following, we provide an example for which the upper bound and lower bound match.

Example 1: Let

$$W(Y|X) = \begin{bmatrix} 1/3 & 1/4 \\ 2/3 & 3/4 \end{bmatrix}, V(Y|Z) = \begin{bmatrix} 2/5 & 2/3 \\ 3/5 & 1/3 \end{bmatrix},$$

and set $P_X = [\lambda_1, 1-\lambda_1]^T,\ P_Z = [\lambda_2, 1-\lambda_2]^T$, $\lambda_1, \lambda_2 \in [0:1]$. Then, we have

$$\begin{aligned} P_Y = W(Y|X)P_X &= \left[\frac{1}{4} + \frac{1}{12}\lambda_1, \frac{3}{4} - \frac{1}{12}\lambda_1\right]^T, \\ Q_Y = V(Y|Z)P_Z &= \left[\frac{2}{3} - \frac{4}{15}\lambda_2, \frac{1}{3} + \frac{4}{15}\lambda_2\right]^T. \end{aligned}$$

Define $\lambda_0 = \frac{1}{4} + \frac{1}{12}\lambda_1$, then

$$D(P_Y||Q_Y) = \lambda_0 \log \frac{\lambda_0}{\frac{2}{3} - \frac{4}{15}\lambda_2} + (1-\lambda_0)\log \frac{1-\lambda_0}{\frac{1}{3} + \frac{4}{15}\lambda_2}.$$

Following simple calculations, we have

$$\frac{\partial D(P_Y||Q_Y)}{\partial \lambda_2} = \frac{4}{15(\frac{2}{3} - \frac{4}{15}\lambda_2)\left(\frac{1}{3} + \frac{4}{15}\lambda_2\right)\ln 2}\left(\frac{4}{15}\lambda_2 + \lambda_0 - \frac{2}{3}\right).$$

Since $\lambda_0 \in [\frac{1}{4} : \frac{1}{3}]$, we have

$$\frac{\partial D(P_Y||Q_Y)}{\partial \lambda_2} < 0,\ \forall \lambda_0 \in \left[\frac{1}{4} : \frac{1}{3}\right], \lambda_2 \in [0:1].$$

Thus, for any given P_Y, $D(P_Y||Q_Y)$ is a decreasing function of λ_2. Hence,

$$\lambda_2^* = \arg\min_{\lambda_2} D(P_Y||Q_Y) = 1,\ \forall \lambda_0 \in \left[\frac{1}{4} : \frac{1}{3}\right],$$

which is equivalent to

$$Q_Y^* = \arg\min_{Q_Y} D(P_Y||Q_Y) = \left[\frac{2}{5}, \frac{3}{5}\right]^T,\ \forall P_X \in \mathcal{P}_X. \tag{4.31}$$

Hence,

$$f(P_X) + I(X;Y) = D(P_Y||Q_Y^*) + I(X;Y)$$

$$
\begin{aligned}
&= \sum_y P_Y \log \frac{P_Y}{Q_Y^*} + H(Y) - H(Y|X)\\
&= \sum_y P_Y \log \frac{P_Y}{Q_Y^*} - \sum_y P_Y \log P_Y - \sum_{i\in\mathcal{X}} P_X(i)H(Y|i)\\
&= \sum_y P_Y \log \frac{1}{Q_Y^*} - \sum_{i\in\mathcal{X}} P_X(i)H(Y|i).
\end{aligned}
$$

As $H(Y|X=i)$ are constants for either $i=1$ or $i=2$ and P_Y is an affine function of P_X, from the equation above, we have that $f(P_X)+I(X;Y)$ is linear (and hence convex) in P_X. Hence, for this example, we can conclude that

$$\max_{P_X\in\mathcal{P}_R}\min_{P_Z} D(P_Y||Q_Y) = \min_{P_Z}\max_{P_X\in\mathcal{P}_R} D(P_Y||Q_Y),$$

and hence the authentication exponent is fully characterized.

4.5 Authenticated (Secrecy) Capacity

In this section, we focus on characterizing the authenticated capacity C^* and the authenticated secrecy capacity C_S^*, defined in Section 4.2.2.

4.5.1 Simulatability Condition and Authenticated (Secrecy) Capacity

We first introduce a concept named *simulatability condition* that plays an important role in our study. Simulatability condition was first defined under the source model in [63] for the study of key generation under unauthenticated public channel problems. Here, we extend the definition to the channel model. We note that [30] also introduced a similar concept for the channel model. We will show that our definition will lead to the definition given in [30].

Definition 4.2. For given channels $W(Y|X)$ (the channel connecting Alice and Bob) and $V(Y|Z)$ (the channel connecting Eve and Bob), if for each $P_X\in\mathcal{P}_{\mathcal{X}}$, there exists some

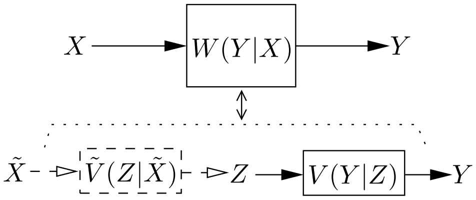


Figure 4.2: Construct a virtual channel $\tilde{X} \to Y$ that has the same statistics as $X \to Y$.

$P_Z \in \mathcal{P}_\mathcal{Z}$ such that

$$\sum_{j\in\mathcal{Z}} V(Y|j) \cdot P_Z(j) = \sum_{i\in\mathcal{X}} W(Y|i) \cdot P_X(i), \tag{4.32}$$

then, we say that the (channel) simulatability condition holds.

Remark 4.9. Simulatability condition here means that no matter what P_X Alice uses, Eve can always find a P_Z, such that the received sequences Y^n at Bob from both channels have the same distribution.

We have the following lemmas regarding simulatability condition.

Lemma 4.10. Given channels $W(Y|X)$ and $V(Y|Z)$, if simulatability condition holds, then Eve can construct a virtual channel $\tilde{V}(Z|\tilde{X})$, such that

$$V(Y|Z)\tilde{V}(Z|\tilde{X}) = W(Y|X). \tag{4.33}$$

Proof. The proof is given in Appendix B.8. □

As shown in Fig.4.2, Lemma 4.10 means that if simulatability condition holds, by concatenating $\tilde{V}(Z|\tilde{X})$ to $V(Y|Z)$, Eve can construct a channel from $\tilde{X}$ to Y that has the same statistics as the legitimate channel from X to Y. The definition of simulatability condition in [30] has the same interpretation as shown in Fig.4.2.

Using Lemma 4.10, we can greatly simplify simulatability condition as shown in the following lemma.

Lemma 4.11. Given $W(Y|X)$ and $V(Y|Z)$, simulatability condition holds if and only if $\forall i \in \mathcal{X}$, $\exists P_{Z,i} \in \mathcal{P}_{\mathcal{Z}}$, s.t.

$$V(Y|Z)P_{Z,i} = W(Y|i). \tag{4.34}$$

Proof. The proof is given in Appendix B.8. □

This lemma plays a key role in the proof of our main result on the authenticated capacity. It also facilitates us in the design of efficient algorithms for checking whether simulatability condition holds or not for any given $W(Y|X)$ and $V(Y|Z)$. The design of efficient algorithms will be discussed in Section 4.5.2.

Now, we state our result on C^* as follows.

Theorem 4.12. *Under the channel model when Eve is active, if the simulatability condition holds, $C^* = 0$; Otherwise, $C^* = C$.*

Suppose $P_X^\star = \arg\max_{P_X} I(X;Y)$ (the corresponding $P_Y \triangleq P_Y^\star$), then $C = I(X^\star;Y)$. If simulatability condition does not hold and $\min_{P_Z} D(P_Y^\star||Q_Y) > 0$, the result $C^* = C = I(X^\star;Y)$ is obvious, as we can fix $P_X = P_X^\star$ and use the same scheme as that in the achievability in Section 4.4.2. Using this scheme, the successful attack probability is upper bounded as

$$\beta_n(Z_0^n) \leq 2^{-n(\min\limits_{P_Z} D(P_Y^\star||Q_Y)-\varepsilon)} \leq \epsilon.$$

However, If simulatability condition doesn't hold but $\min_{P_Z} D(P_Y^\star||Q_Y) = 0$, the above scheme does not work. In the following, we present a scheme such that, as long as simulatability condition doesn't hold, we can guarantee that Alice can reliably transmit a message to Bob at a rate larger than $C - \epsilon$, meanwhile Bob can detect the attack by Eve with a probability larger than $1 - \sigma$.

Proof of Theorem 4.12. The case when simulatability condition holds is trivial: As shown in Lemma 4.10, if simulatability condition holds, Eve can concatenate a virtual channel $\tilde{V}(Z|\tilde{X})$ to the channel $V(Y|Z)$ such that the concatenated channel from $\tilde{X}$ to Y has the same statistics as the legitimate channel from X to Y. Now, for any legitimate users' strategy ϕ, ψ, φ that satisfy (4.7), Eve can always generate the same codebook as Alice's codebook. When Eve conducts an impersonation attack, she only needs to randomly pick a codeword from the codebook and sends it through the concatenated channel from $\tilde{X}$ to Y. Since this concatenated channel has the same statistics as that of the channel from X to Y, the successful attack probability equals the probability of that a message sent by Alice is accepted by Bob. As the latter probability is larger than $1-\epsilon$ due to (4.7), the successful attack probability will be larger than $1-\epsilon$. Thus, we have

$$C^* = 0.$$

For the case when simulatability condition does not hold, we show that there exists a scheme such that Alice can reliably transmit the message to Bob at a rate larger than $C-\epsilon$ when Eve does not attack, meanwhile Bob can detect the attack by Eve with a probability larger than $1-\sigma$.

According to Lemma 4.11, if simulatability condition doesn't hold, then there exists $i^* \in \mathcal{X}$ s.t.

$$V(Y|Z)P_Z \neq W(Y|i^*),\ \forall P_Z \in \mathcal{P}_Z. \tag{4.35}$$

To show that $C^* = C$, it suffices to show that for any $P_X \in \mathcal{P}_X$, $R = I(X;Y) - \epsilon$ is achievable.

Codebook generation: Fix P_X, i.i.d generate 2^{nR_m} sequences X^n according to the PMF P_X with $R_m = I(X;Y) - \epsilon_0$. We then construct a sequence $i^{*\sqrt{n}}$, that is to repeat i^* for $\sqrt{n}$ times and append $i^{*\sqrt{n}}$ to each generated X^n. We denote the new $n+\sqrt{n}$ length sequence

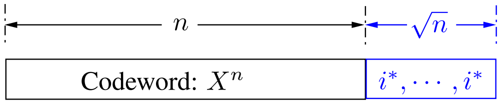


Figure 4.3: Codeword $\hat{X}^{n+\sqrt{n}}$.

as $\hat{X}^{n+\sqrt{n}}$. As will be clear in the sequel, $i^{*\sqrt{n}}$ will be used as an authenticator. We then set the sequences $\hat{X}^{n+\sqrt{n}}$ as the codewords, and each $\hat{X}^{n+\sqrt{n}}$ is assigned to one message. We use $\hat{X}^{n+\sqrt{n}}(M)$ to denote the M-th codeword. Fig.4.3 illustrates the codeword $\hat{X}^{n+\sqrt{n}}$.

Encoding: If Alice needs to send a message M to Bob, she transmits $\hat{X}^{n+\sqrt{n}}(M)$ into the channel.

Authentication: Upon receiving a sequence $Y^{n+\sqrt{n}}$, Bob first splits it into two parts: Y^n and $Y_{n+1}^{n+\sqrt{n}}$. Then he declares the signal to be from Alice if $Y_{n+1}^{n+\sqrt{n}}$ is P_{Y,i^*}-typical; Otherwise, he declares it to be from Eve and rejects it.

Decoding: If $Y^{n+\sqrt{n}}$ is authenticated to be from Alice, Bob tries to find a unique sequence $X^n(\hat{M})$ such that $(X^n(\hat{M}), Y^n)$ are jointly typical, and decodes the signal to $\hat{M}$. If there are more than one such sequence, he randomly picks one. If there is no such sequence, he declares an error.

Error analysis: Since the acceptance region is $\mathscr{A} = \mathcal{Y}^n \times T_\epsilon^{\sqrt{n}}(Y, i^*)$, and all X^n-jointly typical sequence Y^n is included in $\mathscr{A}$, thus we can easily obtain

$$\Pr\{\hat{M} \neq M, H_0 | H_0\} \leq \frac{\epsilon}{2},$$
$$\Pr\{H_1 | H_0\} \leq \frac{\epsilon}{2}.$$

Using the argument as in the proof of Theorem 7.7.1[16], we obtain that there exists at least one codebook such that (4.7) is satisfied.

Probability of successful attack: As discussed in Section 4.3 and (4.20) in particular, we only need to consider the impersonation attack. For this, we only need to focus on $Y_{n+1}^{n+\sqrt{n}}$. Since $Y_{n+1}^{n+\sqrt{n}}$ is i.i.d generated according to $P_{Y,i^*} = W(Y|i^*)$ when there is no attack, according to the achievability proof of Theorem 4.4, i.e. (B.12) to be precise, we have

$$P_I \leq 2^{-\sqrt{n}(D(P_{Y,i^*}||Q_{Y,i^*})-\epsilon_0)} \leq \sigma,$$

when n is sufficiently large.

Rate Per Channel Use:

$$\begin{aligned} R = \frac{nR_m}{n+\sqrt{n}} &= \frac{n}{n+\sqrt{n}}(I(X;Y)-\epsilon_0) \\ &= I(X;Y) - \frac{\sqrt{n}}{n+\sqrt{n}}I(X;Y) - \frac{n}{n+\sqrt{n}}\epsilon_0 \\ &\geq I(X;Y) - \epsilon, \end{aligned}$$

when n is large enough. □

Using the same idea of appending an $\sqrt{n}$ length sequence as the authentication sequence, we can easily obtain the following result regarding the authenticated secrecy capacity.

Corollary 4.13. Under the channel model when Eve is active, if simulatability condition holds, $C_S^* = 0$; Otherwise, $C_S^* = C_S$.

Proof. The proof follows similar steps as that of Theorem 4.12 and is omitted for brevity. □

Note that the role of simulatability condition in our setup is similar as that of symmetrizability condition for an arbitrarily varying channel (AVC) as defined in [18]. For an AVC, the state of the channel can be viewed as being controlled by an adversary. If the AVC is symmetrizable, there exists a state sequence which the adversary can use, such that the decoder cannot distinguish the true codeword from a false codeword no matter what scheme is applied. On the other hand, if the AVC is not symmetrizable, there exists a scheme such that no matter what state the channel is, the decoder can correctly decode the codeword of positive rate with high probability. In this respect, simulatability condition is weaker than symmetrizability condition since the simulatability condition only involves in two separate channels and the channel from the encoder to the decoder remains the same while for the AVC, the channel statistics from the encoder to the decoder is determined by the state sequence and it can be arbitrarily changed.

4.5.2 Algorithm

As shown above, simulatability condition plays an important role in our analysis. Hence, it is crucial to design efficient algorithms to check whether simulatability condition holds or not for any given $W(Y|X)$ and $V(Y|Z)$. From Lemma 4.11, we know that to check simulatability condition, we only need to check, for each $i \in \mathcal{X}$, whether there exists some $P_{Z,i} \in \mathcal{P}_{\mathcal{Z}}$ such that (4.34) holds.

It is easy to see that if there exists a $P_{Z,i} \in \mathcal{P}_{\mathcal{Z}}$ such that (4.34) holds, then the optimal value of the following optimization problem will be 0:

$$\begin{aligned} \min_{P_{Z,i}} \quad & ||V(Y|Z)P_{Z,i} - W(Y|i)||_1 \\ \text{s.t.} \quad & P_{Z,i} \succeq 0, \\ & \sum_{j \in \mathcal{Z}} P_{Z,i}(j) = 1, \end{aligned} \tag{4.36}$$

in which $|| \cdot ||_1$ is the ℓ_1 norm. At the same time, if the optimal value obtained from the optimization problem (4.36) is 0, the corresponding optimizer will satisfy (4.34). Hence, we conclude that (4.34) holds if and only if the optimal value obtained from (4.36) is 0. It is easy to check that (4.36) is a convex optimization problem, and hence can be solved efficiently. In fact, following similar steps as discussed in Chapter 3, the optimization problem (4.36) can be further simplified to be a linear programming problem.

Finally, using Lemma 4.11, we know that we only need to solve $|\mathcal{X}|$ convex optimization problems as (4.36) to check the simulatability condition (4.32).

4.5.3 Channel Uncertainty

It is important to note that, although our model involves Eve's channels $U(F|X)$ and $V(Y|Z)$, most of our schemes (with one exception to be discussed below) in both Section 4.4 and Section 4.5 are universal with respect to Eve's channels, in the sense that our schemes do not rely on the information on Eve's channels. However, in order to check simulatability condition, we need to know the exact channel state information of $V(Y|Z)$, which is impractical. Nonetheless, we show that simulatability condition here is not sensitive to modeling uncertainties, that is $V(Y|Z)$ does not need to be known perfectly.

Assume $W(Y|X)$ is perfectly known but $V(Y|Z)$ is known only to a certain precision. In particular, let the true channel between Eve and Bob to be $\hat{V}(Y|Z)$, but the legitimate users know only an estimate $V(Y|Z)$. Denote $\Delta V(Y|Z) = \hat{V}(Y|Z) - V(Y|Z)$, we assume $|\Delta V(Y|Z)|$ is bounded. In particular, we assume

$$|\Delta V(j|k)| \leq \delta, \ \forall j \in [1 : |\mathcal{Y}|], k \in [1 : |\mathcal{Z}|].$$

We clearly have

$$\sum_{j=1}^{|\mathcal{Y}|} \Delta V(j|k) = 0, \ \forall k \in [1 : |\mathcal{Z}|].$$

Suppose that based on $V(Y|Z)$, Alice and Bob determine that $W(Y|X)$ is not simulatable, i.e., there exists a i^* such that $W(Y|i^*)$ satisfies

$$V(Y|Z)P_Z \neq W(Y|i^*), \ \forall P_Z \in \mathcal{P}_Z. \tag{4.37}$$

As discussed in the proof of Theorem 4.12, Alice and Bob will use i^* to design the authenticator. This is the only part of our scheme that depends on Eve's channel. Let

$$\rho = \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1$$

$$\text{s.t.} \qquad P_{Z,i^*} \succeq 0, \; \sum_{j \in \mathcal{Z}} P_{Z,i^*}(j) = 1. \tag{4.38}$$

From (4.37), we know $\rho > 0$.

We have the following result.

Lemma 4.14. Suppose Eve can't simulate $W(Y|i^*)$ with regards to $V(Y|Z)$, then $\forall \delta < \frac{\rho}{|\mathcal{Y}|}$, Eve cannot simulate $W(Y|i^*)$ using $\hat{V}(Y|Z)$ neither.

Proof. The proof is shown in Appendix B.8. □

This result means that, although Alice and Bob only have an estimate of Eve's channel $V(Y|Z)$, the authenticator $i^{*,\sqrt{n}}$ designed based on the estimated channel still works for the true channel $\hat{V}(Y|Z)$ as long as the difference between these two channels measured by δ is less than $\rho/|\mathcal{Y}|$. Hence, our scheme is robust to the uncertainty in Eve's channel.

Here, we provide an example to illustrate this result.

Example 2: Let

$$V(Y|Z) = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}, W(Y|i^*) = \begin{bmatrix} 2/3 \\ 1/3 \end{bmatrix}.$$

Then, we have

$$\rho \triangleq \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1 = \min_{P_{Z,i^*}} \left|\left| \begin{bmatrix} \frac{1}{2} - \frac{2}{3} \\ \\ \frac{1}{2} - \frac{1}{3} \end{bmatrix} \right|\right|_1 = 1/3.$$

Now if

$$\delta < \frac{\rho}{|\mathcal{Y}|} = \frac{1}{2}\rho = \frac{1}{6}, \tag{4.39}$$

set $\hat{V}(Y|Z) = \begin{bmatrix} 1/2+\delta_1 & 1/2+\delta_2 \\ 1/2-\delta_1 & 1/2-\delta_2 \end{bmatrix}$, $|\delta_1| \leq \delta, |\delta_2| \leq \delta$ and $P_{Z,i^*} = \begin{bmatrix} \lambda_1 \\ 1-\lambda_1 \end{bmatrix}$, then we have

$$\hat{V}P_{Z,i^*} = \begin{bmatrix} 1/2+\delta_1\lambda_1+\delta_2(1-\lambda_1) \\ 1/2-\delta_1\lambda_1-\delta_2(1-\lambda_1) \end{bmatrix}.$$

Since the first entry $1/2+\delta_1\lambda_1+\delta_2(1-\lambda_1) < 1/2+1/6\lambda_1+1/6(1-\lambda_1) = 2/3$, we can conclude

$$\hat{V}P_{Z,i^*} \neq W(Y|i^*),\ \forall P_{Z,i^*} \in \mathcal{P}_Z.$$

Hence, Eve can't simulate $W(Y|i^*)$ for any perturbed channel $\hat{V}(Y|Z)$ with constraint (4.39).

4.6 Concluding Remarks

In this chapter, we have considered the problem of message authentication without any pre-shared key, in the presence of an active adversary over noisy channels. We have characterized the authentication exponent for the zero-rate case and provided both an upper bound and a lower bound on the exponent for the nonzero-rate case. We have shown an "all or nothing" result for the authenticated channel capacity, depending on a so called simulatability condition. We have further provided efficient algorithms to check simulatability condition. We have also shown that our schemes are robust to modeling uncertainties about Eve's channels.

Chapter 5

Secrecy and Privacy Issues in Function Computation

In this chapter, the problem of function computation with privacy constraints is considered. The considered model consists of three legitimate nodes (i.e., two transmitters Alice and Bob, and a fusion center which acts as the receiver), who observes correlated sources and connected by noiseless public channels, and an eavesdropper Eve, who has full access to the public channels and also has its own source observations. The fusion center would like to compute a function of the distributed sources to within a prefixed distortion level under a certain distortion metric. To facilitate the function computing, Alice and Bob will send messages to the fusion center. Different from the existing setups in function computing, we assume that there are *privacy* constraints on the sources at Alice and Bob. In particular, these terminals would like to enable the fusion center to compute the function but at same time do not want the fusion center to learn too much information about the source observations. We introduce a quantity to precisely measure the privacy information leakage to the fusion center. In addition to this privacy constraint, we also have *secrecy* constraint to Eve and use equivocation of sources to measure this. Under this model, we study the relationship among message rates, private information leakage, equivocation and distortion. We first consider the scenario involving only one transmitter, i.e., the source at Bob is empty, and fully single-letter characterize the corresponding regions. Then, we consider the more general case and provide both outer bounds and inner bounds on the corresponding regions.

5.1 Motivation

In this chapter, we consider privacy and secrecy issues arising in the function computing setup. In the considered model, two terminals, Alice and Bob, are connected to a fusion center, and they observe correlated source sequences X_1^n, X_2^n, Y^n respectively. The fusion center would like to compute a function of X_1^n, X_2^n, Y^n. To facilitate the function computing, Alice and Bob will send messages M_1 and M_2 respectively to the fusion center. Different from the setups in [52–54, 70], we assume that there are *privacy* constraints on the sources at Alice and Bob. In particular, these terminals would like to enable the fusion center to compute the function but at same time do not want the fusion center to learn too much information about the source observations. We use $I(X_1^n, X_2^n; M_1, M_2|Y^n)$ as our privacy measure. As this quantity is the same as $H(X_1^n, X_2^n|Y^n) - H(X_1^n, X_2^n|M_1, M_2, Y^n)$, hence this quantity measures additional information about the sources (X_1^n, X_2^n) that the fusion center learns from the transmitted messages. In addition to this privacy constraint, we also have *secrecy* constraint. In particular, there is an additional terminal Eve who observes Z^n, which is correlated with the source sequences, and the messages transmitted by Alice and Bob. We use equivocation of sources to measure the secrecy leakage to Eve.

For the function to be computed, we consider both lossless and lossy cases. In the lossless case, the fusion center is required to compute the function with a diminishingly small error probability. In the lossy case, we allow distortion in the computed function to within a certain distortion level measured by a given distortion metric. We would like to note that the lossless case in our model is not merely a special case of the lossy case when the distortion is zero. It will be clear in the sequel, the lossless case in our model has a more stringent constraint than setting distortion as zero in the lossy case. Thus, it deserves an independent study. We study the relationship of message rates, the private information leakage at the fusion center, the equivocation at Eve and the distortion.

To gain design insights, we first study an important special case where there is only one transmitter (by setting $X_2 = \emptyset$). This case recovers the basic the function computation problem [70] but with additional privacy and secrecy considerations. We fully characterize the regions of the involved parameters for both the lossless and lossy function computing cases. The results demonstrate that there exist tradeoffs among these parameters. For example, given the distortion level, the message rate and privacy leakage can be simultaneously optimized but the secrecy level of sources at Eve may not be simultaneously maximized. In addition, we show that, even though the lossless case has a more stringent constraint than that of lossy case with distortion being zero, the obtained result for the lossless case is equivalent to that of the special case of the lossy case.

Using the understanding from the single transmitter case, we then extend the study to the scenario with two transmitters. We first derive both an outer bound and an inner bound on the corresponding region for the lossless case. These outer and inner bounds have same form but with different range for the auxiliary random variables involved. The obtained results recover many existing results [16, 78]. The obtained results show that there exist tradeoffs among different parameters involved in the model. Furthermore, the techniques used in the lossless case are generalized into the lossy case. We also provide both outer and inner bounds on the corresponding region. Similar to the lossless case, the obtained outer and inner bounds have the same form but with different range for auxiliary random variables involved.

We now briefly review recent interesting works addressing secrecy issues in function computing, and discuss the difference between our work and these works. [97] considers a multi-terminal source model for secure computation. Under this model, each of these m terminals observes a component of correlated sources, and a subset of these terminals are required to compute a function via public discussion. Based on the result in [20], it characterizes the secure computability of the function, i.e., when the computed value of the function is secure from the adversary who has full access to the public discussion. The main difference between this work and our work is that [97] focuses on the secrecy of the computed function while we care about both the privacy of the sources at the fusion center and the secrecy at Eve. Furthermore, [97] allows nodes to conduct multiple rounds of interactive communications, while in our model only one way discussion is allowed. The extension of our model to the interesting scenario with multiple rounds of discussion is left for future work. The secure function computation problem is further studied in [26, 27, 98, 99]. Another line of related work is the class of secure multi-party computation (SMC) [7, 22, 51, 82] problems. In the paradigm of SMC, researchers focus on creating protocols for communication parties to jointly compute functions over distributed inputs while keeping the privacy of these inputs. Typically, these protocols involve in multiple rounds of discussion and they can work among untrusted communication parties. Most importantly, the privacy of most protocols mainly relies on the secrecy of the 1-out-n oblivious transfer schemes [24, 100], which is computational secure instead of information theoretic secure. In other words, this privacy is based on an assumption that the computational power in each party is finite. While in our work, we only allow one-way discussion from the transmitters to the fusion center and do not make any such assumption on the computational power of each terminal, thus the privacy and secrecy in our work is information theoretically secure.

5.2 System Model

In this chapter, we consider a problem of function computing with privacy and secrecy constraints. As illustrated in Fig.5.1, two legitimate terminals, Alice and Bob, are connected to the fusion center via two public noiseless channels in the presence of an eavesdropper Eve who has full access to the public channels. Alice, Bob, the fusion center and Eve observe n-length correlated source sequences X_1^n, X_2^n, Y^n and Z^n respectively. These sequences are

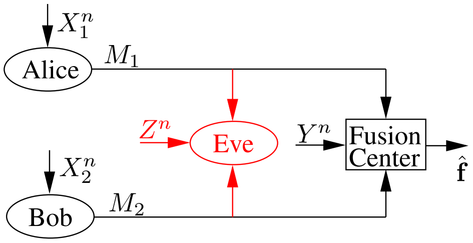


Figure 5.1: System model: the fusion center would like to compute a function f of (X_1^n, X_2^n, Y^n). Alice and Bob are connected to the fusion center via public noiseless channels, which Eve has full access to.

generated according to a given PMF $P_{X_1X_2YZ}$:

$$\Pr\{X_1^n, X_2^n, Y^n, Z^n\} = \prod_{i=1}^{n} P_{X_1X_2YZ}(X_{1i}, X_{2i}, Y_i, Z_i), \tag{5.1}$$

where (X_1, X_2, Y, Z) take values from finite alphabets $(\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}, \mathcal{Z})$ respectively.

The fusion center would like to compute a function $\mathbf{f}(X_1^n, X_2^n, Y^n)$ that consists of component-wise functions of $\{X_{1i}, X_{2i}, Y_i\}_{i=1}^n$, thus $\mathbf{f}(X_1^n, X_2^n, Y^n)$ can be written as

$$\mathbf{f}(X_1^n, X_2^n, Y^n) := \{f(X_{1i}, X_{2i}, Y_i)\}_{i=1}^n.$$

$\mathbf{f}(X_1^n, X_2^n, Y^n)$ is denoted by $\mathbf{f}$ in short and $f(X_{1i}, X_{2i}, Y_i)$ is denoted by f_i for all $i \in [1:n]$. Thus, we rewrite $\mathbf{f}(X_1^n, X_2^n, Y^n)$ as $\mathbf{f} := f^n$. To facilitate the computation of $\mathbf{f}$ at the fusion center, Alice and Bob will send messages M_1 and M_2 to the fusion center via the public channels respectively. Here M_1 is a function (could be stochastic) of the sequence X_1^n. Similarly M_2 is a function (could be stochastic) of the sequence X_2^n. After receiving these messages, the fusion center computes an estimated value $\hat{\mathbf{f}}$ of $\mathbf{f}$ as a function of M_1, M_2 and Y^n:

$$\hat{\mathbf{f}} := \hat{\mathbf{f}}(M_1, M_2, Y^n).$$

In the considered model, Alice and Bob have privacy constraints in the sense that they would like minimize privacy leakage to the fusion center and Eve about their observations while still enabling the fusion center to compute the function of interest. We use $I(X_1^n, X_2^n; M_1, M_2|Y^n)$ to measure additional private information leakage about (X_1^n, X_2^n) to the fusion center. As $I(X_1^n, X_2^n; M_1, M_2|Y^n) = H(X_1^n, X_2^n|Y^n) - H(X_1^n, X_2^n|M_1, M_2, Y^n)$, this quantity measures additional information about (X_1^n, X_2^n) that the fusion center learns from (M_1, M_2), and hence is the privacy price we pay in order to compute $\mathbf{f}$. We use $H(X_1^n, X_2^n|M_1, M_2, Z^n)$ to measure the equivocation of (X_1^n, X_2^n) at Eve.

Definition 5.1. Given arbitrary random variable alphabet $\mathcal{F}$ and its reconstruction alphabet $\hat{\mathcal{F}}$, the distortion measure is a mapping

$$d : \mathcal{F} \times \hat{\mathcal{F}} \to [0, \infty),$$

and the distortion between given sequences f^n and $\hat{f}^n$ is measured as

$$d(f^n, \hat{f}^n) = \sum_{i=1}^{n} d(f_i, \hat{f}_i).$$

Definition 5.2. Given a per-letter distortion measure mapping d, a tuple $(R_1, R_2, D, \Delta_1, \Delta_2)$ is said to be *achievable* if $\forall \epsilon > 0$, there exists an $n(\epsilon) \in I\!N$ and a sequence of $(n, R_1, R_2, D, \Delta_1, \Delta_2)$ codes such that

$$\frac{1}{n} E[d(\mathbf{f}, \hat{\mathbf{f}})] \leq D + \epsilon, \tag{5.2}$$

$$\frac{1}{n} H(M_i) \leq R_i + \epsilon, \ i = 1, 2, \tag{5.3}$$

$$\frac{1}{n} I(X_1^n, X_2^n; M_1, M_2|Y^n) \leq \Delta_1 + \epsilon, \tag{5.4}$$

$$\frac{1}{n} H(X_1^n, X_2^n|M_1, M_2, Z^n) \geq \Delta_2 - \epsilon, \tag{5.5}$$

$\forall n > n(\epsilon)$.

Note that the expectation in (5.2) is calculated over all $X_1^n \times X_2^n \times Y^n \in \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{Y}^n$, and (5.2) requires that the average distortion between the estimated value $\hat{\mathbf{f}}$ and the true value

$\mathbf{f}$ is less than a given positive parameter D, (5.3) measures the transmitted message rates at Alice and Bob respectively, (5.4) implies that the extra private leakage of (X_1^n, X_2^n) at the fusion center is less than Δ_1, and (5.5) measures the joint equivocation of (X_1^n, X_2) at Eve's side.

In Definition 5.2, in the case when $D = 0$, we replace (5.2) with the following condition:

$$\Pr\{\mathbf{f} \neq \hat{\mathbf{f}}\} \leq \epsilon, \tag{5.6}$$

while keeping the equations (5.3)-(5.5) unchanged. For this case, we rewrite the tuple $(n, R_1, R_2, D = 0, \Delta_1, \Delta_2)$ as $(n, R_1, R_2, \Delta_1, \Delta_2)$ in short. Obviously, the constraint defined by (5.6) is stricter than that defined by (5.2). We refer the case when $D = 0$ with constraints defined by (5.3)-(5.6) as *lossless function computing*, and the case with constraints defined by (5.2)-(5.5) as *lossy function computing*. The lossless function computing case can be viewed as a special case of the lossy function computing case, but with a stricter constraint, thus it deserves an independent investigation.

Definition 5.3. The set of all achievable tuple $(R_1, R_2, D, \Delta_1, \Delta_2)$ is defined as:

$$\mathcal{S} := \{(R_1, R_2, D, \Delta_1, \Delta_2) \in I\!R_+^5 : (R_1, R_2, D, \Delta_1, \Delta_2) \text{ is achievable } \}.$$

The goal in this chapter is to single-letter characterize the region $\mathcal{S}$.

5.3 A Special Case with $X_2 = \emptyset$

In this section, we study a special case when $X_2 = \emptyset$. In this case, for the convenience of presentation, we denote X_1 by X, and M_1 by M. The model is shown in Fig.5.2.

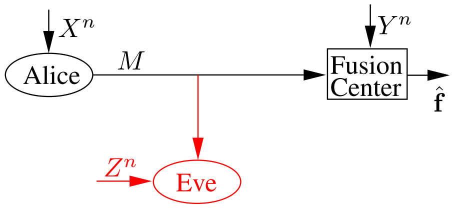


Figure 5.2: The case with $X_2 = \emptyset$: the fusion center would like to compute a value as a function of sequences X^n and Y^n. Alice is connected to the fusion center via a public noiseless channel, which Eve has full access to.

5.3.1 Lossless Function Computing

In this part, we study the lossless function computing problem. As mentioned in Section 5.2, the lossless function computing case has a stricter constraint compared with the normal special case when $D = 0$ in the lossy function computing.

Before proceeding to the main results, we introduce the following definition, which is similar as that introduced in [70], that will simplify the presentation of the theorems in the sequel.

Definition 5.4. A random variable U is said to be *admissible* with respect to random variables X, Y and function f (we may write U is admissible in short), if it satisfies

(1) $U \to X \to Y$;

(2) U and Y determine f, i.e., $H(f|U,Y) = 0$.

Furthermore, a sequence U^n is said to be an admissible sequence if each component of U^n is admissible.

Here, condition 1) denotes that random variables U, X and Y form a Markov chain in this order. Condition 2) is equivalent to the condition that there exists a deterministic function g such that $g(U,Y) = f(X,Y), \forall (X,Y)$ with $P_{XY}(X,Y) > 0$, according to [16, Chapter 2].

To facilitate understanding, we first assume that Eve has no side information, i.e., $\mathcal{Z} = \emptyset$, and we have the following result.

Theorem 5.1. The achievable tuple set $\mathcal{S}$ in the case when Eve has no side information is given by

$$\mathcal{S} = \Big\{(R, \Delta_1, \Delta_2) : R \geq I(X;U) - I(Y;U), \tag{5.7}$$

$$\Delta_1 \geq I(X;U|Y), \tag{5.8}$$

$$\text{and } \Delta_2 \leq H(X|U) + I(Y;U), \tag{5.9}$$

$$\text{for someadmissible } U \text{ w.r.t.} X, Y \text{ and } f.\Big\}. \tag{5.10}$$

Proof. Please see Appendix C.1. □

Intuitively, to reduce the additional information leakage to the fusion center and to increase the equivocation at Eve, Alice should reduce the information of X^n contained in the public message M. She first chooses an appropriate sequence U^n, and encodes it into a codeword containing the least information of X^n under the conditions that the fusion center can decode U^n correctly and U^n together with Y^n can determine f^n. We will show that stochastic encoding does not help in increasing the equivocation at Eve or reducing the privacy information leakage to the fusion center. Thus, deterministic encoding is sufficient. Detailed proof is provided in Appendix C.

Obviously, the set of all possible random variables U is not empty: X belongs to this set. In addition, we can see, from Theorem 5.1, that there is no tradeoff between (R, Δ_1, Δ_2) in this case. In particular, when R achieves it optimal value denoted by R^*, the values of Δ_1 and Δ_2 can be R^* and $H(X) - R^*$ respectively, which are the corresponding optimal values. In other words, there exists a U that achieves lower bounds on R and Δ_1, and the upper bound for Δ_2, simultaneously. Set

$$U^* = \arg \min_{U \text{ is admissible}} I(X;U) - I(Y;U),$$

then the set $\mathcal{S}$ in Theorem 5.1 can be rewritten as

$$\begin{aligned}\mathcal{S} = \Big\{(R, \Delta_1, \Delta_2) : R &\geq I(X;U^*) - I(Y;U^*),\\ \Delta_1 &\geq I(X;U^*|Y),\\ \text{and } \Delta_2 &\leq H(X|U^*) + I(Y;U^*).\end{aligned}$$

However, as shown in the sequel, the situation is different in the case when $\mathcal{Z} \neq \emptyset$.

In addition, given PMF P_{XY} and function $f(X,Y)$, the range of U can be written in an alternative manner by introducing conditional characteristic graph as shown [70]. [70] focuses on characterizing the least message rate and does not take Δ_1 and Δ_2 into consideration. As a special case when we only care about R, the result in Theorem 5.1 is consistent with the result obtained in [70].

For the case when Eve has side information, i.e., $\mathcal{Z} \neq \emptyset$, Eve can use both Z^n and the public discussion to infer the sequence X^n, thus, the equivocation of X^n at Eve reduces. We have the following result in this case.

Theorem 5.2. The achievable tuple set $\mathcal{S}$ for the case when Eve has side information is given by

$$\mathcal{S} = \Big\{ (R, \Delta_1, \Delta_2) : R \geq I(X;U) - I(Y;U), \tag{5.11}$$

$$\Delta_1 \geq I(X;U|Y) \tag{5.12}$$

$$\Delta_2 \leq H(X|U,Z) + [I(Y;U|V) - I(Z;U|V)]^+, \tag{5.13}$$

for some admissible U and a r.v. V with

$$V \rightarrow U \rightarrow X \rightarrow (Y,Z).\Big\} \tag{5.14}$$

Proof. Please see Appendix C.2. □

The existence of side-information Z^n provides more information to Eve about X^n. Thus, it is necessary to introduce an additional random variable V that serves as stochastic encoding to confuse Eve. Compared with the result in Theorem 5.1, there exists a tradeoff among the tuple (R, Δ_1, Δ_2): in general, there does not exist an optimal solution (U^*, V^*) that minimizes R and Δ_1, and maximizes Δ_2 simultaneously.

The result in Theorem 5.2 can be further simplified if the source random variables satisfy the Markov chain relationship $X \to Y \to Z$.

Corollary 5.3. If $X \to Y \to Z$ holds, the achievable tuple set $\mathcal{S}$ is given by

$$\mathcal{S} = \Big\{ (R, \Delta_1, \Delta_2) : R \geq I(X;U) - I(Y;U), \tag{5.15}$$

$$\Delta_1 \geq I(X;U|Y), \tag{5.16}$$

$$\Delta_2 \leq H(X|U,Z) + I(Y;U) - I(Z;U), \tag{5.17}$$

$$\text{for some admissible } U. \Big\}$$

Proof. For the convenience of notation, we rename the region stated in Theorem 5.2 as $\hat{\mathcal{S}}$ and the region in the corollary as $\tilde{\mathcal{S}}$, under the condition that $X \to Y \to Z$ holds. On the one hand, that $\tilde{\mathcal{S}} \subseteq \hat{\mathcal{S}}$ is trivial since we can set $V = \emptyset$ to obtain $\tilde{\mathcal{S}}$ from $\hat{\mathcal{S}}$.

On the other hand, we show that $\hat{\mathcal{S}} \subseteq \tilde{\mathcal{S}}$. It suffices to show that $H(X|U,Z)+[I(Y;U|V)$ $-I(Z;U|V)]^+ \leq H(X|U,Z) + I(Y;U) - I(Z;U)$, which is equivalent to

$$\begin{aligned} & I(Y;U|V) - I(Z;U|V) \leq I(Y;U) - I(Z;U) \\ \Leftrightarrow \quad & I(Y;V) \geq I(Z;V). \end{aligned}$$

And that $I(Y;V) \geq I(Z;V)$ is true due to the Markov chain $V \to U \to X \to Y \to Z$. Hence, we have $\hat{\mathcal{S}} = \tilde{\mathcal{S}}$, and this completes the proof. □

5.3.2 Lossy Function Computing

In this section, we focus on the lossy function computing case, i.e., the case with $D > 0$. In this case, the fusion center is not required to recover the value of function $\mathbf{f}$ exactly, it only needs to compute **f** to within a prefixed allowed distortion level for a given distortion metric. This relaxed requirement allows us to reduce the message rate and privacy leakage.

Given a distortion measure mapping d on the alphabets of **f** and its reconstruction, we have the following result.

Theorem 5.4. Given distortion measure mapping d, the achievable tuple set $\mathcal{S}$ for the coding of lossy function computation is given by

$$\begin{aligned}\mathcal{S} = \Big\{ & (R, D, \Delta_1, \Delta_2) : R \geq I(X;U) - I(Y;U), && (5.18)\\ & D \geq E[d(f(X,Y), g(U,Y))], && (5.19)\\ & \Delta_1 \geq I(X;U|Y), && (5.20)\\ & \Delta_2 \leq H(X|U,Z) + [I(Y;U|V) - I(Z;U|V)]^+, && (5.21)\\ & \text{for some function } g \text{ and r.v. } U, V \text{ with}\\ & V \to U \to X \to (Y,Z).\Big\} && (5.22)\end{aligned}$$

Proof. Please see Appendix C.3. □

Although there is a function g in the description of the region, the form of g is implicitly determined by the choice of U. In particular, for any PMF P_{XYZUV} and function f, we can always find an optimal function g^* as follows:

$$g^*(U,Y) = \arg\min_g E[d(f(X,Y), g(U,Y))].$$

Consider the case with hamming distance as an example. Here, we take the function f as a variable (denoted by F) and its value as to realization (denoted by f).

$$\begin{aligned}E[d(F, g(U,Y))] &= \sum_{f,u,y} P_{FUY}(f,u,y) d(f, g(u,y))\\ &\geq 1 - \sum_{u,y} P_{FUY}(\hat{f}, u, y),\end{aligned}$$

where $\hat{f} := \arg\max_{f} P_{F|UY}(f|u,y)$. Thus, $\forall(u,y) \in \mathcal{U} \times \mathcal{Y}$, we can obtain the optimal function g as

$$g^*(u,y) := \arg\max_{f} P_{F|UY}(f|u,y). \tag{5.23}$$

When P_{XYZUV} and function f are given, the PMF P_{FUY} is given and it is straightforward to find the solution to (5.23).

Note that, unlike the lossless case, the random variable U here is not required to be admissible w.r.t (X,Y) and f anymore. As shown in [70] that in the lossless case, there are many scenarios where the fusion center needs to decode X^n exactly so that it can compute f. However, when a certain amount of distortion is allowed, there always exists random variable U other than X, such that the decoder only needs to decode the sequence U^n. This sequence serves as distortion mapping of X^n, which helps in increasing the equivocation of X^n at Eve and reducing privacy leakage to the fusion center.

Comparing the results in Theorems 5.2 and 5.4, we observe that the region given in Theorem 5.4, when $D = 0$, is the same as that in Theorem 5.2, even though the requirement in the lossless function computing case is stricter than that in the lossy case, i.e., (5.6) is stricter than setting $D = 0$ to (5.2). In addition, similar to Corollary 5.3, we have the following Corollary when $X \to Y \to Z$ holds in the lossy function computing case.

Corollary 5.5. If $X \to Y \to Z$ holds, the achievable tuple set $\mathcal{S}$ in the lossy function computing case is given by

$$\begin{aligned}\mathcal{S} = \Big\{(R, D, \Delta_1, \Delta_2) : R &\geq I(X;U) - I(Y;U), && (5.24)\\
D &\geq E[d(f(X,Y), g(U,Y))], && (5.25)\\
\Delta_1 &\geq I(X;U|Y), && (5.26)\\
\Delta_2 &\leq H(X|U,Z) + I(Y;U) - I(Z;U), && (5.27)\\
&\text{for some function } g \text{ and r.v. } U \text{ with } U \to X \to Y \to Z).\Big\} && (5.28)\end{aligned}$$

The proof follows similar steps as that in the derivative of Corollary 5.3, thus is omitted here.

5.4 The Case when $X_2 \neq \emptyset$

In this section, we study the case when $X_2 \neq \emptyset$. Despite being much more complicated than the case when $X_2 = \emptyset$, the techniques developed in the previous section can be generalized to this case.

We first consider the lossless function computing case, for which we have both inner and outer bounds on the region of achievable tuples as follows.

Theorem 5.6. (Converse) For lossless function computing at the fusion center, if the tuple $(R_1, R_2, \Delta_1, \Delta_2)$ is achievable, then there exist auxiliary random variables (U_1, V_1) and (U_2, V_2), for which $V_1 \to U_1 \to X_1 \to (X_2, Y, Z)$ and $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$ form Markov chains in the indicated orders, and

$$R_1 \geq I(V_1; X_1|Y, V_2) + I(U_1; X_1|Y, U_2, V_1) - I(V_1; V_2|Y, X_1) - I(U_1; U_2|X_1, Y, V_1), \quad (5.29)$$

$$R_2 \geq I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2) - I(V_1; V_2|Y, X_2) - I(U_1; U_2|X_2, Y, V_2), \quad (5.30)$$

$$R_1 + R_2 \geq I(V_1; X_1|Y) + I(V_2; X_2|Y, V_1) + I(U_1; X_1|Y, V_1, V_2) + I(U_2; X_2|Y, U_1, V_2), \quad (5.31)$$

$$\Delta_1 \geq I(X_1, X_2; U_1, U_2|Y), \quad (5.32)$$

$$\Delta_2 \leq H(X_1, X_2|U_1, U_2, Z) + \big[I(U_1, U_2; Y|V_1, V_2) - I(U_1, U_2; Z|V_1, V_2)\big]^+, \quad (5.33)$$

$$H(f|U_1, U_2, Y) = 0. \quad (5.34)$$

(Achievability) Furthermore, for random variables (U_1, V_1) and (U_2, V_2) satisfying

$$P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$$

and $H(f|U_1, U_2, Y) = 0$, then the tuple $(R_1, R_2, \Delta_1, \Delta_2)$ subject to (5.29)-(5.33) is achievable.

Proof. Please see Appendix C.4. □

In general, the converse and achievable bounds do not match because the region of U_1, V_1 and U_2, V_2 defined by $V_1 \to U_1 \to X_1 \to (X_2, Y, Z)$ and $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$ in the converse bound is larger than that defined by

$$P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$$

in the achievability bound.

Note that, the minus terms on the right-hand sides of (5.29) and (5.30) are zeros if $P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$, since we have

$$(V_1, U_1) \to X_1 \to (Y, U_2, V_2),$$
$$(V_2, U_2) \to X_2 \to (Y, U_1, V_1),$$

in this case. By setting $V_1 = V_2 = \emptyset$, we observe that the achievability result of the message rate region defined by (5.29)-(5.31) and (5.34) recovers the inner bound obtained in [78, Prop. 1]. In addition, it is consistent with a special case of the result obtained in [80, Theorem 2] when the rooted directed tree involves with only three nodes: one root and two children.

Given $P_{U_1V_1U_2V_2X_1X_2YZ}$, the main idea of our achievable scheme is that there exist auxiliary sequences U_1^n, V_1^n and U_2^n, V_2^n such that $\mathbf{f}(X_1^n, X_2^n, Y^n) = \hat{\mathbf{f}}(U_1^n, U_2^n, Y^n)$ if $(R_1, R_2, \Delta_1, \Delta_2)$ is achievable. Thus, the function $\mathbf{f}$ will be correctly computed at the fusion center as long as it can correctly decodes (U_1^n, U_2^n), and (5.29)-(5.31) define the region of (R_1, R_2), such that (U_1^n, U_2^n) can be correctly decoded with some scheme. And sequences V_1^n, V_2^n are used to increase the equivocation of (X_1^n, X_2^n) at Eve.

Under certain scenarios where we need to correctly decode X_1^n and X_2^n, i.e., f is a invertible function with respect to X_1 and X_2: $U_1 = X_1$, $U_2 = X_2$ [78], and when we only care about the region of (R_1, R_2), we have the following corollary.

Corollary 5.7. Given $P_{X_1X_2Y}$, sequences (X_1^n, X_2^n) can be correctly decoded, if and only if

$$\begin{aligned} R_1 &\geq H(X_1|Y) - I(X_1;X_2|Y) \\ R_2 &\geq H(X_2|Y) - I(X_1;X_2|Y) \\ R_1 + R_2 &\geq H(X_1|Y) + H(X_2|Y) - I(X_1;X_2|Y). \end{aligned}$$

Corollary 5.7 recovers the result in [78, Rate Region - Invertible Function]. In addition, it recovers the distributed source coding problem when $Y = \emptyset$ as well, and the result is consistent with the Slepian-Wolf coding theorem [16, Chap. 15].

For the lossy function computing case with a given distortion metric d, we have the following result regarding the tradeoffs between message rates, information leakage, equivocation and distortion.

Theorem 5.8. (Achievability) Given a distortion mapping d, the tuple $(R_1, R_2, D, \Delta_1, \Delta_2)$ is achievable if

$$R_1 \geq I(V_1;X_1|Y,V_2) + I(U_1;X_1|Y,U_2,V_1) - I(V_1;V_2|Y,X_1) - I(U_1;U_2|X_1,Y,V_1), \tag{5.35}$$

$$R_2 \geq I(V_2;X_2|Y,V_1) + I(U_2;X_2|Y,U_1,V_2) - I(V_1;V_2|Y,X_2) - I(U_1;U_2|X_2,Y,V_2), \tag{5.36}$$

$$R_1 + R_2 \geq I(V_1;X_1|Y) + I(V_2;X_2|Y,V_1) + I(U_1;X_1|Y,V_1,V_2) + I(U_2;X_2|Y,U_1,V_2), \tag{5.37}$$

$$\Delta_1 \geq I(X_1,X_2;U_1,U_2|Y), \tag{5.38}$$

$$\Delta_2 \leq H(X_1,X_2|U_1,U_2,Z) + \left[I(U_1,U_2;Y|V_1,V_2) - I(U_1,U_2;Z|V_1,V_2)\right]^+, \tag{5.39}$$

$$D \geq E\left[d\left(f(X_1,X_2,Y), g(U_1,U_2,Y)\right)\right], \tag{5.40}$$

for some function g and auxiliary random variables U_1, V_1 and U_2, V_2 with $P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}\, P_{U_1|X_1} P_{V_1|U_1} P_{U_2|X_2} P_{V_2|U_2}$.

(Converse) If the tuple $(R_1, R_2, \Delta_1, \Delta_2)$ is achievable, there exist some function g and auxiliary random variables, U_1, V_1 and U_2, V_2, for which $V_1 \to U_1 \to X_1 \to (X_2, Y, Z)$

and $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$ form Markov chains in the indicated orders, such that (5.35)-(5.40) hold.

Proof. Please see Appendix C.5. □

Similar to the relationship between Theorems 5.2 and 5.4, Theorem 5.8 recovers Theorem 5.6 when $D = 0$.

5.5 Concluding Remarks

In this chapter, we have considered the problem of function computation with distortion under privacy constraints. We have first considered the special scenario where $X_2 = \emptyset$, and have characterized the corresponding region for both the lossless and the lossy function computation cases. Then, we have generalized the obtained results into the more general scenario and provided both outer bounds and inner bounds for the corresponding lossless and lossy cases.

Chapter 6

Conclusion and Extension

In this chapter, we summarize the contributions we have made in this dissertation and propose certain potential directions in the field of information theoretic security and privacy.

6.1 Summary of the Dissertation

The aim of this dissertation is to explore information theoretic approaches to solve several open problems related to security and privacy issues in communication networks.

In the first part, we have designed efficient algorithms to check simulatability condition. In particular, we have constructed a LP problem and showed that simulatability condition holds if and only if the optimal value obtained from the constructed LP is zero, for any given joint PMF. In addition, we have constructed another LP and showed that the minimizer of the constructed LP is a valid attack strategy. Finally, we have further showed that simulatability condition is not sensitive on the knowledge about Eve's observations.

In Chapter 3, we have investigated the problem of simultaneously generating multiple secret keys in joint source-channel models. In this problem, we have first studied a simplified model in which Eve has no side information, and provided a full characterization on the secret-key capacity region. Then, we generalized it into a more general model where Eve has side information, and have single-letter characterized secret-key capacity region as well.

The obtained results summarize many existing works in the field of key generation as special cases.

In Chapter 4, we have discussed the problem of keyless authentication. Different from most existing models on authentication, we assumed that the legitimate terminals have no pre-shared key. Instead, we exploited the statistical properties of the physical channels to analyze the authentication exponent and the authenticated channel capacity of the noisy channel connecting the legitimate terminals. By interpreting the message authentication as a hypothesis testing problem, we fully characterized the authentication exponent for the zero-rate message case and provided both an upper bound and a lower bound on the exponent for the non-zero message rate case. In the authenticated capacity problem, we studied the largest data transmission rate under which the attacker's optimal successful attack probability can still be made arbitrarily small. In addition, we provided efficient algorithms to check simulatability condition related to the noisy channels and we showed that the obtained results are robust to modeling uncertainties about the eavesdropper's channels connecting to the legitimate terminals.

Finally, we considered both secrecy and privacy issues in Chapter 5. We put both a secrecy and a privacy constraints in the problem of function computation, and we characterized the rate region of those parameters including message rates, private information leakage, equivocation of source and the computed function distortion. The obtained results showed that there exists a trade-off among those parameters, which provides a guide for us to select which criterion we hope to achieve.

6.2 Future Directions

The research presented in this dissertation can be extended in many interesting directions. Here we point out some of them.

- *Simultaneously generating multiple keys in a joint source-channel network with multi-*

ple recipients: the simultaneously generating multiple key problem studied in Chapter 3 can be extended into many interesting models. As we only considered one legitimate recipient (i.e., Carol) at the output of the wiretap channel in Chapter 3, it can be generalized by including multiple recipients. In this model, Alice and Bob would like to share different keys with different recipients. For this model, we can first consider a simple scenario with only two recipients. We can then further enhance the model by allowing public discussion between these two recipients. Finally, we can study the model with more than two recipients.

- *Sufficient condition on keyless authentication exponent*: as discussed in Chapter 4, it is important to characterize the authentication exponent for the message authentication problem over noisy channels, and we fully characterized the authentication exponent for the zero-rate message case and provide both an upper bound and a lower bound on the authentication exponent for the nonzero-rate case. We realize that it is difficult to characterize the authentication exponent for the general case, but we clarify a condition that if $f(P_X)+I(X;Y)$ is convex in P_X, as stated in Corollary 4.8, the provided lower and upper bounds match. However, we did not provide an explicit statement on when it is convex. As a continued research work, it is interesting to further study the statistical properties of the channels $W(Y|X)$ and $V(Y|Z)$, and provide precise conditions on $W(Y|X)$ and $V(Y|Z)$, under which $f(P_X) + I(X;Y)$ is convex in P_X.

- *Secure function computation with secrecy and privacy constraints*: as stated in Chapter 5, [97] considers the problem of secure function computation under a multi-terminal source model. It characterizes the secure computability of the function, i.e., when the computed value of the function is secure from the adversary who has full access to the public discussion. Our work in Chapter 5 focuses on both the privacy of the sources at the fusion center and the secrecy at Eve. However, to the best of our knowledge, no work exists to simultaneously consider both the secrecy of the computed function and the privacy of sources. It would be interesting to take these issues into consideration together.

Appendix A

Chapter 3

A.1 Proof of Theorem 3.1

A.1.1 Converse

Here, we provide the converse proof of Theorem 3.1. Before going further, we first introduce a lemma from [3], which will be used frequently in the following.

Lemma A.1 (Lemma 4.1 of [3])**.** For arbitrary RVs $U,\ V$ and sequences of RVs $Y^n,\ Z^n$ we have

$$I(U;Y^n|V)-I(U;Z^n|V)=\sum_{i=1}^{n}\Big[I(U;Y_i|Y^{i-1}Z_{i+1}^n,V)-I(U;Z_i|Y^{i-1}Z_{i+1}^n,V)\Big]. \quad \text{(A.1)}$$

Converse of Theorem 3.1. In this part, we will show that any achievable pair (R_1,R_2) must be in the union defined by the right hand side of (3.9).

According to the setup, the following Markov relationships are true:

$$V^N\to U^N\to \mathbf{F}\to(Y^n,Z^n), \quad \text{(A.2)}$$

$$V^N\to U^N\to(\mathbf{F},K_2)\to(Y^n,Z^n). \quad \text{(A.3)}$$

Let $\epsilon > 0$ be arbitrary, we have

$$\begin{aligned}
H(K_1) &= H(K_1|Y^n, V^N) + I(K_1; Y^n, V^N) \\
&\leq I(K_1; Y^n, V^N) + n\epsilon \\
&= I(K_1; Y^n) + I(K_1; V^N|Y^n) + n\epsilon \\
&\leq I(K_1; \mathbf{F}) + I(K_1; V^N|Y^n) + n\epsilon \\
&\leq \sum_{i=1}^{N} I(K_1; V_i|Y^n, V^{i-1}) + 2n\epsilon \\
&\leq \sum_{i=1}^{N} I(K_1, U_{i+1}^n, V^{i-1}, Y^n; V_i) + 2n\epsilon \\
&= \sum_{i=1}^{N} I(S_{1i}; V_i) + 2n\epsilon \\
&= \sum_{i=1}^{N} I(S_{1Q}; V_Q|Q = i) + 2n\epsilon \\
&= N \sum_{i=1}^{N} \frac{1}{N} I(S_{1Q}; V_Q|Q = i) + 2n\epsilon \\
&= NI(S_{1Q}; V_Q|Q) + 2n\epsilon \\
&= NI(S_{1Q}, Q; V_Q) - NI(Q; V_Q) + 2n\epsilon \\
&= NI(S_1; V) + 2n\epsilon, \qquad \text{(A.4)}
\end{aligned}$$

in which $S_{1i} \triangleq (K_1, U_{i+1}^n, V^{i-1}, Y^n)$, $S_1 \triangleq (S_{1Q}, Q)$, and Q is an independent RV uniformly distributed over $[1 : N]$.

Thus, we have

$$R_1 \leq \frac{1}{\beta} I(S_1; V) + 2\epsilon. \qquad \text{(A.5)}$$

Furthermore, $S_1 \to U \to V$ is true as

$$(U^{i-1}, U_{i+1}^N, V^{i-1}) \to U_i \to V_i$$

$$
\begin{aligned}
&\Rightarrow \quad (U^N, V^{i-1}) \to U_i \to V_i \\
&\Rightarrow \quad (K_1, \mathbf{F}, U_{i+1}^N, V^{i-1}) \to U_i \to V_i \\
&\overset{(a)}{\Rightarrow} \quad (K_1, Y^n, U_{i+1}^N, V^{i-1}) \to U_i \to V_i \\
&\Leftrightarrow \quad S_{1i} \to U_i \to V_i, \qquad \text{(A.6)}
\end{aligned}
$$

in which (a) is true as Y^n can be seen as a function of $(\mathbf{F}, \theta)$ (θ is some RV which is independent with all variables in (A.6)).

Now, we prove (3.7). We have

$$
\begin{aligned}
H(K_2) &\leq H(K_2) - I(K_2; Z^n, \mathbf{F}) + 2n\epsilon \\
&\overset{(a)}{=} H(K_2) - I(K_2; Z^n, \mathbf{F}, V^N) + 2n\epsilon \\
&= H(K_2|Y^n, \mathbf{F}, V^N) + I(K_2; Y^n, \mathbf{F}, V^N) - I(K_2; Z^n, \mathbf{F}, V^N) + 2n\epsilon \\
&\leq I(K_2; Y^n, \mathbf{F}, V^N) - I(K_2; Z^n, \mathbf{F}, V^N) + 3n\epsilon \\
&= I(K_2; Y^n|\mathbf{F}, V^N) - I(K_2; Z^n|\mathbf{F}, V^N) + 3n\epsilon \\
&= \sum_{i=1}^{n} \Big[I(K_2; Y_i|Y^{i-1}, Z_{i+1}^n, \mathbf{F}, V^N) - I(K_2; Z_i|Y^{i-1}, Z_{i+1}^n, \mathbf{F}, V^N) \Big] + 3n\epsilon \\
&= \sum_{i=1}^{n} \left[I(S_{2i}; Y_i|T_{2i}) - I(S_{2i}; Z_i|T_{2i}) \right] + 3n\epsilon \\
&= \sum_{i=1}^{n} \Big[I(S_{2J}; Y_J|T_{2J}, J=i) - I(S_{2J}; Z_J|T_{2J}, J=i) \Big] + 3n\epsilon \\
&= n \left[I(S_2; Y|T_2) - I(S_2; Y|T_2) \right] + 3n\epsilon. \qquad \text{(A.7)}
\end{aligned}
$$

Here, $S_{2i} \triangleq (K_2, V^N, Y^{i-1}, Z_{i+1}^n, \mathbf{F})$, $T_{2i} \triangleq (V^N, Y^{i-1}, Z_{i+1}^n, \mathbf{F})$, $S_2 \triangleq (S_{2J}, J)$, $T_2 \triangleq (T_{2J}, J)$, and J is an independent RV uniformly distributed over $[1:n]$. (a) is true due to

$$
\begin{aligned}
&\begin{cases} V^N \to \mathbf{F} \to K_2 \\ V^N \to (\mathbf{F}, K_2) \to Z^n \end{cases} \\
\Rightarrow \quad & V^N \to \mathbf{F} \to (Z^n, K_2)
\end{aligned}
$$

$$\begin{aligned} \Rightarrow &\quad V^N \to (\mathbf{F}, Z^n) \to K_2 \\ \Leftrightarrow &\quad (V^N, Z^n, \mathbf{F}) \to (\mathbf{F}, Z^n) \to K_2. \end{aligned} \tag{A.8}$$

Hence, we have

$$R_2 \leq I(S_2; Y|T_2) - I(S_2; Y|T_2) + 3\epsilon. \tag{A.9}$$

Furthermore, we can easily show that $T_2 \to S_2 \to X \to (Y, Z)$.

Now, to prove (3.8), we first have

$$\begin{aligned} & I(U^N; Y^n) - I(V^N; Y^n) \\ \leq & \ I(\mathbf{F}; Y^n) - I(V^N; Y^n) \\ = & \ I(\mathbf{F}, V^N; Y^n) - I(V^N; Y^n|\mathbf{F}) - I(V^N; Y^n) \\ = & \ I(\mathbf{F}; Y^n|V^N) - I(V^N; Y^n|\mathbf{F}) \\ = & \ I(\mathbf{F}; Y^n|V^N) \\ = & \sum_{i=1}^{n} I(\mathbf{F}; Y_i|Y^{i-1}, V^N) \\ \leq & \sum_{i=1}^{n} I(\mathbf{F}, Y^{i-1}, Z_{i+1}^n, V^N; Y_i) \\ = & \sum_{i=1}^{n} I(T_{2i}; Y_i) \\ = & \ nI(T_2; Y). \end{aligned} \tag{A.10}$$

On the other hand, we have

$$\begin{aligned} & I(U^N; Y^n) - I(V^N; Y^n) \\ = & \ I(U^N; Y^n, K_1) - I(V^N; Y^n, K_1) - I(U^N; K_1|Y^n) + I(V^N; K_1|Y^n) \\ = & \ I(U^N; Y^n, K_1) - I(V^N; Y^n, K_1) + H(K_1|Y^n, U^N) - H(K_1|Y^n, V^N) \\ \geq & \ I(U^N; Y^n, K_1) - I(V^N; Y^n, K_1) - n\epsilon \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{N} \Big(I(Y^n, K_1; U_i | U_{i+1}^N, V^{i-1}) - I(Y^n, K_1; V_i | U_{i+1}^N, V^{i-1}) \Big) - n\epsilon \\
&= \sum_{i=1}^{N} \Big(I(Y^n, K_1, U_{i+1}^N, V^{i-1}; U_i) - I(Y^n, K_1, U_{i+1}^N, V^{i-1}; V_i) \Big) - n\epsilon \\
&= \sum_{i=1}^{N} I(S_{1i}; U_i) - I(S_{1i}; V_i) - n\epsilon \\
&= N\big(I(S_1; U) - I(S_1; V) \big) - n\epsilon. \qquad \text{(A.11)}
\end{aligned}
$$

Combining (A.10) and (A.11), we have

$$I(S_1; U) - I(S_1; V) \leq \beta I(T_2; Y) + \beta\epsilon. \qquad \text{(A.12)}$$

□

A.1.2 Achievability

In this part, we will show that $\mathcal{R}(P_{S_1|U}, P_{T_2 S_2} P_{X|S_2})$ is an achievable region. It suffices to show that there exists at least one scheme such that the pair (R_1, R_2) with

$$
\begin{aligned}
R_1 = & \frac{1}{\beta}[I(S_1; V) - \epsilon], R_2 = \big[I(S_2; Y|T_2) - I(S_2; Z|T_2) \big]^{+} - \epsilon \\
\text{s.t.} \quad & I(S_1; U) - I(S_1; V) < \beta I(T_2; Y), \qquad \text{(A.13)}
\end{aligned}
$$

is achievable. Without loss of generality, we assume $I(S_2; Y|T_2) - I(S_2; Z|T_2) > 0$.

Codebook Construction:

$\mathcal{C}_A$ *at Alice*. Given $P_{S_1|U} P_{UV}$ (suppose $I(S_1; U) - I(S_1; V) < \beta I(T_2; Y)$), randomly and independently generate 2^{NR_0} sequences S_1^N according to $\prod_{i=1}^{N} P_{S_1}(S_{1i})$. These sequences are indexed by (f, ϕ) with $f \in [1 : 2^{NR_{01}}]$, $\phi \in [1 : 2^{NR_{02}}]$.

$\mathcal{C}_B$ *at Bob*. Given $P_{T_2 S_2} P_{X|S_2} P_{YZ|X}$ randomly and independently generate $2^{nR_{11}}$ sequences T_2^n according to $\prod_{i=1}^{n} P_{T_2}(T_{2i})$. These sequences are indexed by (f, φ) with $\varphi \in [1 : 2^{nR_{12}}]$. For each $T_2^n(f, \varphi)$, randomly and independently generate $2^{nR_{13}}$ sequences S_2^n

which are indexed by (γ, ψ) with $\gamma \in [1 : 2^{nR_{14}}]$ and $\psi \in [1 : 2^{nR_{15}}]$, according to $\prod_{i=1}^{n} P_{S_2|T_2}(S_{2i}|T_{2i})$. Here, we set

$$R_0 = I(S_1;U) + \epsilon, \quad R_{01} = I(S_1;U) - I(S_1;V) + 2\epsilon, \tag{A.14}$$

$$R_{02} = I(S_1;V) - \epsilon, \quad R_{11} = I(T_2;Y) - \epsilon, \tag{A.15}$$

$$R_{12} = I(T_2;Y) - \epsilon - \frac{1}{\beta}\left(I(S_1;U) - I(S_1;V) + 2\epsilon\right), \quad R_{13} = I(S_2;Y|T_2) - \epsilon, \tag{A.16}$$

$$R_{14} = I(S_2;Z|T_2) + \epsilon R_{15} = I(S_2;Y|T_2) - I(S_2;Z|T_2) - 2\epsilon. \tag{A.17}$$

Encoding: After observing sequence U^N, Alice selects a sequence S_1^N that is jointly P_{S_1U} typical with U^N in $\mathcal{C}_A$. If there is more than one of such S_1^Ns, she randomly select one. If there is no such sequence, randomly select one from the whole codebook. We denote the selected sequence by $S_1^N(f, \phi)$. Alice sends the index f to Bob. Upon receiving f, Bob refers to $\mathcal{C}_B$, randomly generates a value for φ, and then looks into the sequences S_2^n generated by $T_2^n(f, \varphi)$, randomly selects one $S_2^n(\gamma, \psi)$, and finally transmits it to Carol via the channel $P_{X|S_2}P_{YZ|X}$.

Decoding: Upon receiving sequence Y^n, Carol first tries to find a unique $T_2^n(\hat{f}, \hat{\varphi})$ that is jointly typical with Y^n in $\mathcal{C}_B$: If there is more than one of such sequences T_2^n, she randomly selects one. If there exists no such sequence, she declares an error. Then Carol looks into those S_2^ns generated by $T_2^n(\hat{f}, \hat{\varphi})$, trying to find a unique $S_2^n(\hat{\gamma}, \hat{\psi})$ that is jointly typical with $(T_2^n(\hat{f}, \hat{\varphi}), Y^n)$. If there is more than one of such sequences S_2^n, she randomly picks one. If there exists no such T_2^n, she declares an error. After decoding $\hat{f}$, Carol tries to find a unique $S_1^N(\hat{f}, \hat{\phi})$ that is jointly typical with V^N.

Key Generation: Alice sets $K_1 = \phi$; Bob sets $K_2 = \psi$; Carol sets $K_1' = \hat{\phi}$ and $K_2' = \hat{\psi}$.

Key Rates Analysis: According to the codebook constructed above, we know that ϕ and ψ are uniformly distributed in $[1 : 2^{NR_{02}}]$ and $[1 : 2^{nR_{15}}]$, respectively. Thus,

$$R_1 = \frac{N}{n} R_{02} = \frac{1}{\beta}[I(S_1;V) - \epsilon], \tag{A.18}$$

$$R_2 = I(S_2;Y|T_2) - I(S_2;Z|T_2) - 2\epsilon. \tag{A.19}$$

Error Analysis: Denote

$$\xi \triangleq \{K_1 \neq K_1' \text{ or } K_2 \neq K_2'\}, \tag{A.20}$$

$$\xi_1 \triangleq \{T_2^n(f,\varphi) \neq T_2^n(\hat{f},\hat{\varphi})\}, \tag{A.21}$$

$$\xi_2 \triangleq \{S_2^n(\gamma,\psi) \neq S_2^n(\hat{\gamma},\hat{\psi})\}, \tag{A.22}$$

$$\xi_3 \triangleq \{S_1^N(f,\phi) \neq S_1^N(\hat{f},\hat{\phi})\}. \tag{A.23}$$

Then, we have

$$\begin{aligned}
\text{Pr}\{\xi\} &\leq \text{Pr}\{\xi_1 \cup \xi_2 \cup \xi_3\} \\
&= \text{Pr}\{\xi_1\} + \text{Pr}\{\xi_2|\xi_1^c\} + \text{Pr}\{\xi_3|(\xi_2 \cup \xi_1)^c\} \\
&\overset{(a)}{=} \text{Pr}\{\xi_1\} + \text{Pr}\{\xi_2|\xi_1^c\} + \text{Pr}\{\xi_3|\xi_1^c\}, \qquad (A.24)
\end{aligned}$$

in which (a) is true since ξ_2 and ξ_3 are independent given ξ_1^c according to the above encoding approach. In the following, we bound each term in (A.24) one by one.

In our scheme, each T_2^n is randomly and independently generated according to $\prod_{i=1}^{n} P_{T_2}(T_{2i})$ and the total number of T_2^n sequences is $2^{nR_{11}}$. Furthermore, Y^n is equivalently generated by $T_2^n(f,\varphi)$ according to $\prod_{i=1}^{n} P_{Y|T_2}(Y_i|T_{2i})$, with $P_{Y|T_2} = P_{S_2|T_2}P_{X|S_2}P_{Y|X}$. Hence, it's easy to show that with high probability, $(T_2^n(f,\varphi), Y^n)$ is jointly typical and there will be no other T_2^n sequences that are jointly typical with Y^n (one may refer to Chapter 7 in[16]). Thus,

$$\text{Pr}\{\xi_1\} \leq \epsilon/3,$$

when n is sufficiently large.

Given ξ_1^c, which is equivalent to that $T_2^n(f,\varphi)$ is given, there are $2^{nR_{13}}$ sequences S_2^n, each randomly and independently generated by $T_2^n(f,\varphi)$ according to $\prod_{i=1}^{n} P_{S_2|T_2}(S_{2i}|T_{2i})$. In addition, Y^n is equivalently generated by $S_2^n(\gamma,\psi)$ according to $\prod_{i=1}^{n} P_{Y|S_2}(Y_i|S_{2i})$, with $P_{Y|S_2} = P_{X|S_2}P_{Y|X}$. We can show that with high probability, $T_2^n(f,\varphi)$, $(S_2^n(\gamma,\psi)$ and $Y^n)$ are jointly typical and there will be no other sequences S_2^n that are jointly typical with Y^n according to the Packing Lemma [23]. Thus, we can conclude

$$\text{Pr}\{\xi_2|\xi_1^c\} \leq \epsilon/3,$$

when n is sufficiently large.

Since there are 2^{NR_0} sequences S_1^N, which are randomly and independently generated according to $\prod_{i=1}^{N} P_{S_1}(S_{1i})$, we can show that with high probability there exists at least one S_1^N that is jointly typical with U^N (also jointly typical with V^N since $S_1 \to U \to V$). Besides, given $T_2^n(f,\varphi)$, which indicates f is given, there are a total of $2^{NR_{02}}$ sequences $S_1^N(f,\cdot)$. Thus, with high probability there will be no other sequences S_1^N that are jointly typical with V^N. Then, we have

$$\text{Pr}\{\xi_2|\xi_1^c\} \leq \epsilon/3,$$

when N is sufficiently large.

Hence,

$$\text{Pr}\{\xi\} \leq \epsilon. \tag{A.25}$$

Information Leakage Analysis: Since ϕ and f are independent, and that $\phi \to f \to Z^n$,

$$I(K_1; f, Z^n|\mathcal{C}_A, \mathcal{C}_B) = I(\phi; f, Z^n|\mathcal{C}_A, \mathcal{C}_B) = I(\phi; f|\mathcal{C}_A) = 0.$$

To bound $I(K_2; U^N, f, Z^n|\mathcal{C}_A, \mathcal{C}_B)$, we have

$$I(K_2; U^N, f, Z^n|\mathcal{C}_A, \mathcal{C}_B) = I(\psi; U^N, f, Z^n|\mathcal{C}_A, \mathcal{C}_B)$$

$$
\begin{aligned}
&\overset{(a)}{=} I(\psi; f, Z^n|\mathcal{C}_A, \mathcal{C}_B)\\
&\leq I(\psi; T_2^n, Z^n|\mathcal{C}_B)\\
&= I(\psi; T_2^n|\mathcal{C}_B) + I(\psi; Z^n|T_2^n, \mathcal{C}_B)\\
&= I(\psi; Z^n|T_2^n, \mathcal{C}_B), \qquad \text{(A.26)}
\end{aligned}
$$

in which (a) is true due to

$$
\begin{aligned}
&\begin{cases} U^N \to f, \psi \to Z^n, \\ U^N \to f \to \psi \end{cases}\\
\Rightarrow \quad & U^N \to f \to \psi, Z^n\\
\Rightarrow \quad & U^N \to f, Z^n \to \psi\\
\Leftrightarrow \quad & U^N, Z^n \to f, Z^n \to \psi. \qquad \text{(A.27)}
\end{aligned}
$$

Now, we have

$$
\begin{aligned}
I(\psi; Z^n|T_2^n, \mathcal{C}_B) &= H(Z^n|T_2^n, \mathcal{C}_B) - H(Z^n|T_2^n, \psi, \mathcal{C}_B)\\
&= H(Z^n|T_2^n, \mathcal{C}_B) - H(S_2^n, Z^n|T_2^n, \psi, \mathcal{C}_B) + H(S_2^n|Z^n, T_2^n, \psi, \mathcal{C}_B)\\
&= H(Z^n|T_2^n, \mathcal{C}_B) - H(S_2^n|T_2^n, \psi, \mathcal{C}_B)\\
&\quad - H(Z^n|S_2^n, T_2^n, \psi, \mathcal{C}_B) + H(S_2^n|Z^n, T_2^n, \psi, \mathcal{C}_B)\\
&= H(Z^n|T_2^n, \mathcal{C}_B) - H(S_2^n|T_2^n, \psi, \mathcal{C}_B)\\
&\quad - H(Z^n|S_2^n, \mathcal{C}_B) + H(S_2^n|Z^n, T_2^n, \psi, \mathcal{C}_B). \qquad \text{(A.28)}
\end{aligned}
$$

We can easily obtain that

$$
\begin{aligned}
&H(Z^n|T_2^n, \mathcal{C}_B) \leq nH(Z|T_2) + n\epsilon,\\
&H(Z^n|S_2^n, \mathcal{C}_B) \geq nH(Z|S_2) - n\epsilon, \qquad \text{(A.29)}
\end{aligned}
$$

and according to Lemma A.2 below, we have

$$\begin{aligned} I(\psi;Z^n|T_2^n,\mathcal{C}_B) &\leq n(H(Z|T_2) - H(Z|S) + I(S_2;Z|T_2) + 3\epsilon) \\ &= 3n\epsilon. \end{aligned} \tag{A.30}$$

Thus, we have

$$I(K_2;U^N,f,Z^n|\mathcal{C}_A,\mathcal{C}_B) \leq 3n\epsilon.$$

Lemma A.2. If $R_{15} + I(S_2;Z|T_2) < \frac{1}{n}H(S_2^n|T_2^n,\mathcal{C}_B)$, then

$$\frac{1}{n}H(S_2^n|Z^n,T_2^n,\psi,\mathcal{C}_B) \leq \frac{1}{n}H(S_2^n|T_2^n,\psi,\mathcal{C}_B) - I(S_2;Z|T_2) + \epsilon.$$

Proof. See Appendix A.2. □

Finally, using standard information theoretic arguments, we can conclude that there exists a particular code such that (A.13) is achievable and hence $\mathcal{R}(P_{S_1|U}, P_{T_2S_2}P_{X|S_2})$ is an achievable region.

A.2 Proof of Lemma A.2

The proof here follows similar steps as those in the proof of [23, Lemma 22.3].

Given T_2^n, denote $\mathcal{T}_\epsilon^n(S_2Z|T_2^n)$ as the set of pairs (S_2^n, Z^n) which are jointly typical with T_2^n. Define

$$E_1 = \begin{cases} 1, \ (S_2^n, Z^n) \in \mathcal{T}_\epsilon^n(S_2Z|T_2^n); \\ 0, \ (S_2^n, Z^n) \notin \mathcal{T}_\epsilon^n(S_2Z|T_2^n). \end{cases}$$

Then, according to the Law of Large Numbers, we have

$$\Pr\{E_1 = 0\} \overset{n\to\infty}{\longrightarrow} 0, \tag{A.31}$$

since $T_2 \to S_2 \to Z$.

Thus, we have

$$\begin{aligned}
H(S_2^n|Z^n,T_2^n,\psi,\mathcal{C}_B) &\le H(S_2^n,E_1|Z^n,T_2^n,\psi,\mathcal{C}_B)\\
&= H(E_1|Z^n,T_2^n,\psi,\mathcal{C}_B) + H(S_2^n|Z^n,E_1,T_2^n,\psi,\mathcal{C}_B)\\
&\le 1 + \text{Pr}\{E_1=0\}H(S_2^n|Z^n,E_1=0,T_2^n,\psi,\mathcal{C}_B)\\
&\quad +\text{Pr}\{E_1=1\}H(S_2^n|Z^n,E_1=1,T_2^n,\psi,\mathcal{C}_B)\\
&\le 1 + \text{Pr}\{E_1=0\}H(S_2^n|Z^n,E_1=0,T_2^n,\psi,\mathcal{C}_B)\\
&\quad + \sum_{z^n,t_2^n,\psi}\text{Pr}\{z^n,t_2^n,\psi|E_1=1\}H(S_2^n|z^n,E_1=1,t_2^n,\psi,\mathcal{C}_B)\\
&\le n\epsilon + \sum_{z^n,t_2^n,\psi}\text{Pr}\{z^n,t_2^n,\psi|E_1=1\}H(S_2^n|z^n,E_1=1,t_2^n,\psi,\mathcal{C}_B).
\end{aligned}$$

Now, given t_2^n,ψ,z^n and $E_1=1$, define $\text{Num}(z^n,t_2^n)$ as the number of $S_2^n \in S_2^n(\cdot,\psi|t_2^n)\cap \mathcal{T}_\epsilon^n(S_2|z^n)$ ($S_2^n(\cdot,\psi|t_2^n)$ denotes the sequences S_2^ns generated by t_2^n, with second index ψ), we can easily show that

$$\begin{aligned}
&\mathbb{E}(\text{Num}(z^n,t_2^n)) = 2^{-nI(S_2;Z|T_2)}|S_2^n(\cdot,\psi|t_2^n)|,\\
&\text{Var}(\text{Num}(z^n,t_2^n)) \le 2^{-nI(S_2;Z|T_2)}|S_2^n(\cdot,\psi|t_2^n)|,
\end{aligned} \tag{A.32}$$

where

$$\log|S_2^n(\cdot,\psi|t_2^n)| = H(S_2^n|T_2^n,\mathcal{C}_B) - nR_{15}.$$

Thus, we have

$$\text{Pr}\{\text{Num}(z^n,t_2^n) \ge 2\mathbb{E}(\text{Num}(z^n,t_2^n))\} \le 2^{-(H(S_2^n|T_2^n,\mathcal{C}_B)-nR_{15}-nI(S_2;Z|T_2))}. \tag{A.33}$$

Then, we have

$$H(S_2^n|z^n,E_1=1,t_2^n,\psi,\mathcal{C}_B) \le n\epsilon + H(S_2^n|T_2^n,\mathcal{C}_B) - nR_{15} - nI(S_2;Z|T_2)$$

$$= n\epsilon + H(S_2^n|T_2^n, \psi, \mathcal{C}_B) - nI(S_2; Z|T_2). \tag{A.34}$$

Hence, we have

$$H(S_2^n|Z^n, T_2^n, \psi, \mathcal{C}_B) \leq 2n\epsilon + H(S_2^n|T_2^n, \psi, \mathcal{C}_B) - nI(S_2; Z|T_2).$$

A.3 Converse Proof of Theorem 3.2

Similar to the converse proof of Theorem 3.1, we will show that for any achievable pair (R_1, R_2), there exists $(P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2})$ s.t. $(R_1, R_2) \in \mathcal{R}(P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2})$.

First, we have

$$\begin{aligned}
H(K_1) &= H(K_1|Y^n, V^N) + I(K_1; Y^n, V^N) \\
&\leq I(K_1; Y^n, V^N) + n\epsilon \\
&\leq I(K_1; Y^n, V^N) - I(K_1; Z^n, W^N, \mathbf{F}) + 2n\epsilon \\
&\leq I(K_1; Y^n, V^N) - I(K_1; W^N, \mathbf{F}) + 2n\epsilon \\
&\overset{(a)}{=} I(K_1; Y^n, V^N) - I(K_1; Y^n, W^N, \mathbf{F}) + 2n\epsilon \\
&\leq I(K_1; Y^n, V^N) - I(K_1; Y^n, W^N) + 2n\epsilon \\
&\leq I(K_1; V^N|Y^n) - I(K_1; W^N|Y^n) + 2n\epsilon \\
&= \sum_{i=1}^{N} \left[I(K_1; V_i|V^{i-1}, W_{i+1}^N, Y^n) - I(K_1; W_i|V^{i-1}, W_{i+1}^N, Y^n)\right] + 2n\epsilon \\
&= \sum_{i=1}^{N} \left[I(S_{1i}; V_i|T_{1i}) - I(S_{1i}; W_i|T_{1i})\right] + 2n\epsilon \\
&= N\left[I(S_1; V|T_1) - I(S_1; W|T_1)\right] + 2n\epsilon,
\end{aligned} \tag{A.35}$$

in which $S_{1i} \triangleq (K_1, V^{i-1}, W_{i+1}^N, Y^n),\ T_{1i} \triangleq (V^{i-1}, W_{i+1}^N, Y^n)$ and $S_1 \triangleq (S_{1Q}, Q),\ T_1 \triangleq$

(T_{1Q}, Q). (a) is true because of

$$\begin{aligned} & W^N \to U^N \to \mathbf{F} \to Y^n \\ \Rightarrow \quad & (U^N, W^N) \to \mathbf{F} \to Y^n \\ \Rightarrow \quad & (K_1, W^N) \to \mathbf{F} \to Y^n \\ \Rightarrow \quad & K_1 \to (W^N, \mathbf{F}) \to Y^n. \end{aligned} \tag{A.36}$$

Thus, we have

$$R_1 \leq \frac{1}{\beta}\big[I(S_1; V|T_1) - I(S_1; W|T_1)\big] + 2\epsilon. \tag{A.37}$$

Furthermore, similar to (A.6), we can show that $T_1 \to S_1 \to U \to (V, W)$.

The derivation of R_2 is exactly the same as in (A.9), thus, we have

$$R_2 \leq I(S_2; Y|T_2) - I(S_2; Y|T_2) + 3\epsilon, \tag{A.38}$$

where $S_2 \triangleq (K_2, V^N, Y^{J-1}, Z_{J+1}^n, \mathbf{F}, J)$, and $T_2 \triangleq (V^N, Y^{J-1}, Z_{J+1}^n, \mathbf{F}, J)$.

Next, we show (3.12). From (A.11), we conclude

$$I(U^N; Y^n) - I(V^N; Y^n) \tag{A.39}$$

$$\geq \sum_{i=1}^{N} \Big[I(Y^n, K_1, U_{i+1}^N, V^{i-1}; U_i) - I(Y^n, K_1, U_{i+1}^N, V^{i-1}; V_i)\Big] - n\epsilon. \tag{A.40}$$

Now, since

$$\begin{aligned} & W_{i+1}^N \to U_{i+1}^N \to (U^N, V^i) \\ \Rightarrow \quad & W_{i+1}^N \to U_{i+1}^N \to (K_1, \mathbf{F}, U_i, V^i) \\ \Rightarrow \quad & W_{i+1}^N \to U_{i+1}^N \to (K_1, Y^n, U_i, V^i) \\ \Rightarrow \quad & W_{i+1}^N \to (Y^n, K_1, U_{i+1}^N, V^{i-1}) \to (U_i, V_i) \end{aligned}$$

$$\Rightarrow \quad \begin{cases} W_{i+1}^N \to (Y^n, K_1, U_{i+1}^N, V^{i-1}) \to U_i \\ W_{i+1}^N \to (Y^n, K_1, U_{i+1}^N, V^{i-1}) \to V_i \end{cases}, \tag{A.41}$$

and

$$\begin{aligned}
& (U^N, V^{i-1}, W_{i+1}^N) \to U_i \to V_i \\
\Rightarrow \quad & (K_1, \mathbf{F}, U_{i+1}^N, V^{i-1}, W_{i+1}^N) \to U_i \to V_i \\
\Rightarrow \quad & (K_1, Y^n, U_{i+1}^N, V^{i-1}, W_{i+1}^N) \to U_i \to V_i \\
\Rightarrow \quad & U_{i+1}^N \to (Y^n, K_1, V^{i-1}, W_{i+1}^N, U_i) \to V_i,
\end{aligned} \tag{A.42}$$

we have

$$\begin{aligned}
& \sum_{i=1}^N \Big[I(Y^n, K_1, U_{i+1}^N, V^{i-1}; U_i) - I(Y^n, K_1, U_{i+1}^N, V^{i-1}; V_i) \Big] \\
&= \sum_{i=1}^N \Big[I(Y^n, K_1, U_{i+1}^N, V^{i-1}, W_{i+1}^N; U_i) - I(Y^n, K_1, U_{i+1}^N, V^{i-1}, W_{i+1}^N; V_i) \Big] \\
&= \sum_{i=1}^N \Big[I(Y^n, K_1, V^{i-1}, W_{i+1}^N; U_i) - I(Y^n, K_1, V^{i-1}, W_{i+1}^N; V_i) \Big] \\
&\quad + \sum_{i=1}^N \Big[I(U_{i+1}^N; U_i | Y^n, K_1, V^{i-1}, W_{i+1}^N) - I(U_{i+1}^N; V_i | Y^n, K_1, V^{i-1}, W_{i+1}^N) \Big] \\
&= \sum_{i=1}^N \Big[I(Y^n, K_1, V^{i-1}, W_{i+1}^N; U_i) - I(Y^n, K_1, V^{i-1}, W_{i+1}^N; V_i) \Big] \\
&\quad + \sum_{i=1}^N \Big[I(U_{i+1}^N; Y^n, K_1, V^{i-1}, W_{i+1}^N, U_i, V_i) - I(U_{i+1}^N; Y^n, K_1, V^{i-1}, W_{i+1}^N, V_i) \Big] \\
&\geq \sum_{i=1}^N \Big[I(Y^n, K_1, V^{i-1}, W_{i+1}^N; U_i) - I(Y^n, K_1, V^{i-1}, W_{i+1}^N; V_i) \Big] \\
&= \sum_{i=1}^N \Big[I(S_{1i}; U_i) - I(S_{1i}; V_i) \Big] \\
&= N \Big[I(S_1; U) - I(S_1; V) \Big].
\end{aligned} \tag{A.43}$$

Thus, it follows

$$I(U^N;Y^n) - I(V^N;Y^n) \geq N\Big[I(S_1;U) - I(S_1;V)\Big] - n\epsilon.$$

On the other hand, same as (A.10), we conclude

$$I(U^N;Y^n) - I(V^N;Y^n) \leq nI(T_2;Y).$$

Hence,

$$\begin{aligned} & N\Big[I(S_1;U) - I(S_1;V)\Big] - n\epsilon \leq nI(T_2;Y) \\ \Rightarrow \quad & I(S_1;U) - I(S_1;V) \leq \beta I(T_2;Y) + \beta\epsilon. \end{aligned} \tag{A.44}$$

Combining the fact that ϵ in each term is an arbitrary small number, we can conclude that there exists such $(P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2})$ that $(R_1, R_2) \in \mathcal{R}(P_{S_1|U}P_{T_1|S_1}, P_{T_2S_2}P_{X|S_2})$.

Appendix B

Chapter 4

B.1 Proof of Theorem 4.4

To simplify the presentation of the proof of Thereom 4.4, we first introduce a concept from [31] and its property.

Definition B.1 ([31])**.** Let X be a random variable with PMF P. For a given $r \geq 0$, a sequence X^n is called a r-divergent sequence for P if

$$D(\text{tp}(X^n)||P) \leq r.$$

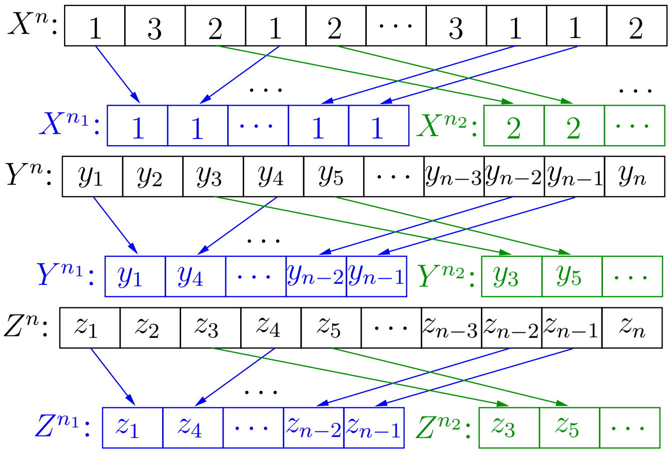
We also denote the set of all r-divergent sequences for P as $S_r^n(P)$.

Lemma B.1 ([31])**.** Fix $r \geq 0$, then

$$P^n(S_r^n(P)) \geq 1 - (n+1)^{|\mathcal{X}|} \exp(-nr).$$

Now, we proceed to our proof of Theorem 4.4.

Proof of Theorem 4.4. The proof has two major steps: 1) Step 1: For any given ϕ, we characterize the optimal ψ, g_I and the corresponding error exponent; 2) Step 2: Characterize the



X^n:
1 3 2 1 2 $\cdots$ 3 1 1 2
X^{n_1}:
1 1 $\cdots$ 1 1
X^{n_2}:
2 2 $\cdots$
Y^n:
y_1 y_2 y_3 y_4 y_5 $\cdots$ y_{n-3} y_{n-2} y_{n-1} y_n
Y^{n_1}:
y_1 y_4 $\cdots$ y_{n-2} y_{n-1}
Y^{n_2}:
y_3 y_5 $\cdots$
Z^n:
z_1 z_2 z_3 z_4 z_5 $\cdots$ z_{n-3} z_{n-2} z_{n-1} z_n
Z^{n_1}:
z_1 z_4 $\cdots$ z_{n-2} z_{n-1}
Z^{n_2}:
z_3 z_5 $\cdots$

Figure B.1: An illustration of the 1th segment for a general sequence X^n.

optimal ϕ.

Step 1: Characterizing optimal ψ and g_I for any given ϕ: In this step, we suppose ϕ is fixed (i.e., the codeword X^n for the message is given), and assume tp$(X^n) = P_X$. Analyzing this case involves two phases. In the first phase, we show that we can construct ψ such that $\beta_I(0_1, \epsilon)$ goes to zero exponentially with a rate $\min_{\{P_{Z,i}\}_{i\in\mathcal{X}}} \sum_i P_X(i) \cdot D(P_{Y,i}||Q_{Y,i})$. In the second phase, we show there is no scheme that can achieve an exponent larger than $\min_{\{P_{Z,i}\}_{i\in\mathcal{X}}} \sum_i P_X(i) \cdot D(P_{Y,i}||Q_{Y,i})$.

Step 1.1: For a given ϕ, construct a particular ψ and characterize the corresponding optimal attack strategy g_I: Fix a selected codeword X^n with type tp$(X^n) = P_X$. We need to characterize which attack sequences Z^n are optimal to minimize the error exponent. All our analysis is based on separating X^n in to $|\mathcal{X}|$ sub-sequences such that each element within the same sub-sequence has the same realization. Thus, without any loss of generality, we assume $X^n = 1^{n_1}2^{n_2}\cdots|\mathcal{X}|^{n_{|\mathcal{X}|}}$, in which $n_i = nP_X(i), i \in \mathcal{X}$. In the following, we denote the positions of i^{n_i} in X^n as the ith segment. For a general X^n, the sequence in the ith segment is denoted by X^{n_i}. And Y^{n_i} and Z^{n_i} are defined in the same manner, see Fig.B.1.

In the ith segment, since $X^{n_i} = i^{n_i}$ and that the channel $W(Y|X)$ is memoryless, Y^{n_i} obtained by passing X^{n_i} through the channel $W(Y|X)$ can be seen as generated i.i.d. according to $P_{Y,i} \triangleq W(Y|i)$. Now, we set the acceptance region, which in return determines

ψ, as

$$\mathscr{A}_n(X^n) = \{Y^{n_1} \cdots Y^{n_{|\mathcal{X}|}} : Y^{n_i} \in \mathscr{A}_i, i \in \mathcal{X}\}, \tag{B.1}$$

in which

$$\mathscr{A}_i \triangleq S_r^{n_i}(P_{Y,i})$$

is defined in the ith segment with

$$r = \max_{i \in \mathcal{X}} -\frac{1}{n_i} \log \frac{\epsilon}{|\mathcal{X}|}(n_i + 1)^{-|\mathcal{X}|}. \tag{B.2}$$

With this r, we have, according to Lemma B.1, that

$$P_{Y,i}^{n_i}(S_r^{n_i}(P_{Y,i})) \geq 1 - \frac{\epsilon}{|\mathcal{X}|}, \forall i \in \mathcal{X}.$$

Then, we have

$$\text{Pr}\{\mathscr{A}_n(X^n)|X^n\} \geq \prod_{i \in \mathcal{X}} \left(1 - \frac{\epsilon}{|\mathcal{X}|}\right) > 1 - \epsilon.$$

Thus,

$$\text{Pr}(H_1|H_0) \leq \epsilon.$$

Hence using this particular ψ, the constraint (4.7) is satisfied.

In the following, we analyze the successful attack probability and characterize the optimal g_I (equivalently the optimal choice of the attack sequence Z^n) for this particular ψ. For any sequence Z_0^n selected by Eve, we denote the successful attack probability as

$\Pr\{\mathscr{A}_n(X^n)|Z_0^n\}$. We realize that, due to the symmetric construction of $\mathscr{A}_n(X^n)$, we have

$$\Pr\{\mathscr{A}_n(X^n)|Z_0^n\} = \prod_{i\in\mathcal{X}} \Pr\{\mathscr{A}_i|Z_0^{n_i}\}.$$

Suppose $\text{tp}(Z_0^{n_i}) = P_{Z,i}$, then according to the construction of $\mathscr{A}_i$, all Z^{n_i}s with $\text{tp}(Z^{n_i}) = P_{Z,i}$ result in the same success probability:

$$\Pr\{\mathscr{A}_i|Z^{n_i}\} = \Pr\{\mathscr{A}_i|Z_0^{n_i}\},\ \forall Z^{n_i} : \text{tp}(Z^{n_i}) = P_{Z,i}. \tag{B.3}$$

Thus, we have

$$\begin{aligned}\Pr\{\mathscr{A}_i|Z_0^{n_i}\} &= \sum_{Y^{n_i}\in\mathscr{A}_i} \Pr\{Y^{n_i}|Z_0^{n_i}\}.\\ &= \sum_{Z^{n_i}\in\mathcal{T}_Z^{n_i}(P_{Z,i})} \Pr\{Z^{n_i}|P_{Z,i}\} \sum_{Y^{n_i}\in\mathscr{A}_i} \Pr\{Y^{n_i}|Z_0^{n_i}\}\\ &\overset{(a)}{=} \sum_{Z^{n_i}\in\mathcal{T}_Z^{n_i}(P_{Z,i})} \Pr\{Z^{n_i}|P_{Z,i}\} \sum_{Y^{n_i}\in\mathscr{A}_i}\Pr\{Y^{n_i}|Z^{n_i}\},\end{aligned} \tag{B.4}$$

where $\Pr\{Z^{n_i}|P_{Z,i}\}$ can be any arbitrary conditional probability distribution of Z^{n_i} given $\text{tp}(Z^{n_i}) = P_{Z,i}$, and (a) holds due to (B.3).

To further analyze $\Pr\{\mathscr{A}_i|Z_0^{n_i}\}$, we first investigate the relationship between $\Pr\{\mathscr{A}_i|Z_0^{n_i}\}$ and $Q_{Y,i}^{n_i}(\mathscr{A}_i)$, in which

$$Q_{Y,i} = \sum_{j\in\mathcal{Z}} V(Y|j)\cdot P_{Z,i}(j) \tag{B.5}$$

with $P_{Z,i} = \text{tp}(Z_0^{n_i})$. Thus, $Q_{Y,i}$ is equivalent to being the distribution of the corresponding Y if Eve generates Z^{n_i} i.i.d. according to $P_{Z,i}$. We can decompose $Q_{Y,i}^{n_i}(A_i)$ as follows

$$Q_{Y,i}^{n_i}(\mathscr{A}_i) = \sum_{Z^{n_i}\in\mathcal{Z}^{n_i}} P_{Z,i}^{n_i}(Z^{n_i})\cdot\Pr\{\mathscr{A}_i|Z^{n_i}\}$$

$$
\begin{aligned}
&= \sum_{Z^{n_i}\in\mathcal{Z}^{n_i}} P_{Z,i}^{n_i}(Z^{n_i}) \sum_{Y^{n_i}\in\mathscr{A}_i} \text{Pr}\{Y^{n_i}|Z^{n_i}\}\\
&= \sum_{\tilde{P}_{Z,i}\in\mathcal{T}_Z} \sum_{Z^{n_i}\in\mathcal{T}_Z^{n_i}(\tilde{P}_{Z,i})} P_{Z,i}^{n_i}(Z^{n_i}|\tilde{P}_{Z,i}) P_{Z,i}^{n_i}(\mathcal{T}_Z^{n_i}(\tilde{P}_{Z,i})) \cdot \sum_{Y^{n_i}\in\mathscr{A}_i} \text{Pr}\{Y^{n_i}|Z^{n_i}\}\\
&= \sum_{\tilde{P}_{Z,i}\in\mathcal{T}_Z} P_{Z,i}^{n_i}(\mathcal{T}_Z^{n_i}(\tilde{P}_{Z,i})) \sum_{Z^{n_i}\in\mathcal{T}_Z^{n_i}(\tilde{P}_{Z,i})} P_{Z,i}^{n_i}(Z^{n_i}|\tilde{P}_{Z,i}) \cdot \sum_{Y^{n_i}\in\mathscr{A}_i} \text{Pr}\{Y^{n_i}|Z^{n_i}\}\\
&\geq P_{Z,i}^{n_i}(\mathcal{T}_Z^{n_i}(P_{Z,i})) \sum_{Z^{n_i}\in\mathcal{T}_Z^{n_i}(P_{Z,i})} P_{Z,i}^{n_i}(Z^{n_i}|P_{Z,i}) \cdot \sum_{Y^{n_i}\in\mathscr{A}_i} \text{Pr}\{Y^{n_i}|Z^{n_i}\}.\\
&\overset{(a)}{=} P_{Z,i}^{n_i}(\mathcal{T}_Z^{n_i}(P_{Z,i})) \cdot \text{Pr}\{\mathscr{A}_i|Z_0^{n_i}\}, \qquad \text{(B.6)}
\end{aligned}
$$

where (a) is true because of (B.4). On the other hand, according to [16, Theorem 11.1.4], we have

$$
\begin{aligned}
P_{Z,i}^{n_i}(\mathcal{T}_Z^{n_i}(P_{Z,i})) &\geq \frac{1}{(n_i+1)^{|\mathcal{Z}|}} \cdot 2^{-n_i D(P_{Z,i}||P_{Z,i})}\\
&= \frac{1}{(n_i+1)^{|\mathcal{Z}|}}.
\end{aligned}
$$

Thus, we conclude that

$$
\text{Pr}\{\mathscr{A}_i|Z_0^{n_i}\} \leq (n_i+1)^{|\mathcal{Z}|} Q_{Y,i}^{n_i}(\mathscr{A}_i). \qquad \text{(B.7)}
$$

In the following, we bound $Q_{Y,i}^{n_i}(\mathscr{A}_i)$ from above. First, it follows

$$
Q_{Y,i}^{n_i}(\mathscr{A}_i) = \sum_{\text{tp}(Y^{n_i}):\mathcal{T}_Y^{n_i}(\text{tp}(Y^{n_i}))\subseteq S_r^{n_i}(P_{Y,i})} Q_{Y,i}^{n_i}(\text{tp}(Y^{n_i})), \qquad \text{(B.8)}
$$

and by Lemma B.2 in Appendix B.3, $\forall$ tp$(Y^{n_i}) : \mathcal{T}_Y^{n_i}(\text{tp}(Y^{n_i})) \subseteq S_r^{n_i}(P_{Y,i})$, we have

$$
D(\text{tp}(Y^{n_i})||Q_{Y,i}) \geq D(P_{Y,i}||Q_{Y,i}) - \delta(r), \qquad \text{(B.9)}
$$

with $\delta(r)$ goes to zero as r decreases. Thus,

$$\begin{aligned} Q_{Y,i}^{n_i}(\text{tp}(Y^{n_i})) &\leq 2^{-n_i D(\text{tp}(Y^{n_i})||Q_{Y,i})} \\ &\leq 2^{-n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))}. \end{aligned} \quad \text{(B.10)}$$

Combine (B.10) and (B.8), and we have

$$\begin{aligned} Q_{Y,i}^{n_i}(\mathscr{A}_i) &\leq \sum_{\text{tp}(Y^{n_i}):\mathcal{T}_Y^{n_i}(\text{tp}(Y^{n_i}))\in S_r^{n_i}(P_{Y,i})} 2^{-n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))} \\ &\leq (n_i+1)^{|\mathcal{Y}|}2^{-n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))}. \end{aligned} \quad \text{(B.11)}$$

Combining (B.11) and (B.7), we obtain

$$\begin{aligned} \Pr\{\mathscr{A}_i|Z_0^{n_i}\} &\leq (n_i+1)^{|\mathcal{Y}|+|\mathcal{Z}|}2^{-n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))} \\ &\leq n^{|\mathcal{Y}|+|\mathcal{Z}|}2^{-n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))}. \end{aligned} \quad \text{(B.12)}$$

Thus, we have

$$\begin{aligned} \Pr\{\mathscr{A}_n(x^n)|Z_0^n\} &\leq n^{|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)}\prod_{i\in\mathcal{X}}2^{-n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))} \\ &= n^{|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)}2^{\sum_i -n_i(D(P_{Y,i}||Q_{Y,i})-\delta(r))} \\ &= n^{|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)}2^{-n(\sum P_X(i)D(P_{Y,i}||Q_{Y,i})-\delta(r))}, \end{aligned} \quad \text{(B.13)}$$

which implies

$$-\frac{1}{n}\log\Pr\{\mathscr{A}_n(x^n)|Z_0^n\} \geq \sum P_X(i)D(P_{Y,i}||Q_{Y,i}) - \delta(r) - \frac{|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)}{n}\log n. \text{(B.14)}$$

Inequality (B.14) implies that for our particular choice of ψ as specified in (B.1), the smallest exponent that Eve can hope for is

$$\min_{\{P_{Z,i}\}_{i\in\mathcal{X}}} \sum P_X(i)D(P_{Y,i}||Q_{Y,i}). \tag{B.15}$$

Now, we show that Eve can indeed achieve (B.15). Let $P_{Z^*,i}$ be the minimizer for (B.15) and $Q^*_{Y,i}$ be the corresponding value computed from (4.23). Similarly as (B.9), we also have, from Lemma B.2 in Appendix B.3, that $\forall$ tp(Y^{n_i}) : $\mathcal{T}^{n_i}_Y(\text{tp}(Y^{n_i})) \subseteq S^{n_i}_r(P_{Y,i})$,

$$D(\text{tp}(Y^{n_i})||Q^*_{Y,i}) \leq D(P_{Y,i}||Q^*_{Y,i}) + \delta(r),$$

in which $\delta(r)$ goes to zero as r decreases. Thus,

$$\begin{aligned} Q^{*,n_i}_{Y,i}(\mathscr{A}_i) &\geq Q^{*,n_i}_{Y,i}(\text{tp}(Y^{n_i})) \\ &\overset{(a)}{\geq} \frac{1}{(n_i+1)^{|\mathcal{Y}|}} 2^{-n_i D(\text{tp}(Y^{n_i})||Q^*_{Y,i})} \\ &\geq \frac{1}{(n+1)^{|\mathcal{Y}|}} 2^{-n_i(D(P_{Y,i}||Q^*_{Y,i})+\delta(r))}, \end{aligned} \tag{B.16}$$

in which (a) is due to Theorem 11.1.4 in [16]. Now, consider a particular attack strategy g^*_I, in which Eve generates Z^{n_i} i.i.d. according to $P_{Z^*,i}$ in the ith segment, $\forall i \in \mathcal{X}$. With this particular attack strategy, from (B.16), the success probability is

$$P^*_I \geq \frac{1}{(n+1)^{|\mathcal{X}||\mathcal{Y}|}} 2^{-n(\sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q^*_{Y,i})+\delta(r))}, \tag{B.17}$$

which implies that

$$-\frac{1}{n}\log P^*_I \leq \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q^*_{Y,i}) + \delta(r) - \frac{|\mathcal{X}||\mathcal{Y}|}{n}\log n. \tag{B.18}$$

As both $\delta(r)$ and $-\frac{|\mathcal{X}||\mathcal{Y}|}{n}\log n$ go to zero as n increases, we conclude that g^*_I achieves (B.15), the best Eve can hope for. Hence, for our particular choice of ψ, g^*_I is the optimal attack strategy.

Step 1.2: Show ψ constructed in Step 1.1 is optimal: Consider any acceptance region $\mathscr{A}_n$ with $\Pr\{\mathscr{A}_n|X^n\} \geq 1-\epsilon$, we will show that the particular attack strategy g_I^* discussed above will achieve an exponent specified in (B.15). Here $\Pr\{\mathscr{A}_n|X^n\} \geq 1-\epsilon$ is due to the fact that $\Pr\{\mathscr{A}_n|X^n\} = 1-\Pr(H_1|H_0)$ as well as the requirement defined by (4.7). We denote the set of the ith segment sequences of $Y^n \in \mathscr{A}_n$ by $\mathscr{A}_i, i \in \mathcal{X}$. Then we have

$$\begin{aligned}
1-\epsilon &\leq \Pr\{\mathscr{A}_n|X^n\} \\
&= \sum_{Y^n \in \mathscr{A}_n} \Pr\{Y^n|X^n\} \\
&= \sum_{Y^n \in \mathscr{A}_n} \prod_{i \in \mathcal{X}} \Pr\{Y^{n_i}|i^{n_i}\} \\
&= \sum_{Y^n \in \mathscr{A}_n} \prod_{i \in \mathcal{X}} P_{Y,i}^{n_i}(Y^{n_i}) \\
&= \sum_{Y_k^n \in \mathscr{A}_k} \sum_{Y^{n \setminus n_k} \in \mathscr{A} \setminus \mathscr{A}_k} P_{Y,k}^{n_k}(Y^{n_k}) \prod_{i \in \mathcal{X} \setminus k} P_{Y,i}^{n_i}(Y^{n_i}) \\
&= \sum_{Y_k^n \in \mathscr{A}_k} P_{Y,k}^{n_k}(Y^{n_k}) \sum_{Y^{n \setminus n_k} \in \mathscr{A} \setminus \mathscr{A}_k} \prod_{i \in \mathcal{X} \setminus k} P_{Y,i}^{n_i}(Y^{n_i}) \\
&\leq \sum_{Y_k^n \in \mathscr{A}_k} P_{Y,k}^{n_k}(Y^{n_k}) \\
&= \Pr\{\mathscr{A}_k|(X=k)^{n_k}\}.
\end{aligned}$$

Now, consider the attack strategy g_I^* discussed above. Using Lemma B.3 in Appendix B.3, we have

$$Q_{Y,k}^{n_k}(\mathscr{A}_k) \geq (1-2\epsilon)2^{-n_k(D(P_{Y,k}||Q_{Y,k}^*)+\epsilon)}.$$

Then, it follows

$$\begin{aligned}
P_I^* &\geq \prod_{i \in \mathcal{X}} (1-2\epsilon)2^{-n_i(D(P_{Y,i}||Q_{Y,i}^*)+\epsilon)} \\
&= (1-2\epsilon)^{|\mathcal{X}|} 2^{\sum_{i \in \mathcal{X}} -n_i(D(P_{Y,i}||Q_{Y,i}^*)+\epsilon)}
\end{aligned}$$

$$= (1-2\epsilon)^{|\mathcal{X}|} 2^{-n(\sum\limits_{i\in\mathcal{X}} P_X(i) D(P_{Y,i}||Q^*_{Y,i})+\epsilon)}.$$

Since P_I^* is obtained by the particular attack strategy g_I^*, it must be less or equal to that from the optimal attack strategy (denote the optimal attack sequence by $Z^{\star n}$)with respect to $\mathscr{A}_n$, i.e. $\Pr\{\mathscr{A}_n|Z^{\star n}\} \geq P_I^*$. Thus, we have

$$-\frac{1}{n}\log \Pr\{\mathscr{A}_n|Z^{\star n}\} \leq \sum_{i\in\mathcal{X}} P_X(i) D(P_{Y,i}||Q_{Y,i}) + \epsilon - \frac{|\mathcal{X}|}{n}\log(1-2\epsilon). \tag{B.19}$$

Combining (B.14) and (B.19) with the fact that Eve can always select a Z^n with the optimal types $\{P_{Z,i}\}_{i\in\mathcal{X}}$ in corresponding segments, we conclude that the exponent of the successful attack probability when X^n is given, denoted by $\theta_I(X^n)$, is

$$\theta_I(X^n) = \min_{\{P_{Z,i}\}_{i\in\mathcal{X}}} \sum_i P_X(i)\cdot D(P_{Y,i}||Q_{Y,i}).$$

Step 2: Characterize the optimal ϕ: Now, we optimize over ϕ. We obtain

$$\begin{aligned}\theta_I(0_1,\epsilon) &= \max_{X^n}\theta_I(X^n) = \max_{P_X}\theta_I(X^n)\\ &= \max_{P_X}\min_{\{P_{Z,i}\}_{i\in\mathcal{X}}}\sum_i P_X(i)\cdot D(P_{Y,i}||Q_{Y,i})\\ &= \max_{i\in\mathcal{X}}\min_{P_{Z,i}} D(P_{Y,i}||Q_{Y,i}),\end{aligned}$$

in which the last step is true as $\sum\limits_i P_X(i)\cdot D(P_{Y,i}||Q_{Y,i})$ is a linear function of $P_X(i), i = 1,\cdots,|\mathcal{X}|$. This completes the proof. □

B.2 Proof of Theorem 4.7

This proof has two main parts: First, we will show that, $\min\limits_{P_Z}\max\limits_{P_X\in\mathcal{P}_R} D(P_Y||Q_Y)$ is an upper bound on the authentication exponent of any scheme; Second, we will construct a scheme to achieve an authentication exponent $\max\limits_{P_X\in\mathcal{P}_R}\min\limits_{P_Z} D(P_Y||Q_Y)$.

Upper-bounding the authentication exponent for any scheme by (4.26)**:** Consider an arbitrary triplet (ϕ, ψ, φ) that satisfy the conditions in (4.7) and (4.9). Suppose 2^{nR_m} sequences X^n are selected as the codewords by the encoder ϕ. Define the acceptance region determined by ψ as $\mathscr{A}_n$. As there are at most $(n+1)^{|\mathcal{X}|}$ different types of sequences X^n, there must exist at least $(n+1)^{-|\mathcal{X}|}2^{nR_m}$ codewords that have the same type. We denote this particular type as P_X and the set of these codewords as C_{P_X}.

For any arbitrary testing function ψ and decoding function φ, we define $A(X^n) \subset \mathcal{Y}^n$ as the set of sequences Y^n that are accepted and decoded to X^n with a probability larger than $\frac{1}{2}$. For each X^n, we must have $\Pr\{A(X^n)|X^n\} \geq 1 - 2\epsilon$, otherwise, the decoding error for X^n is larger than ϵ, which violates the condition (4.7). It is easy to see that

$$A(X^n) \cap A(\tilde{X}^n) = \emptyset,\ \forall\, X^n, \tilde{X}^n \in C_{P_X} : X^n \neq \tilde{X}^n. \tag{B.20}$$

In Appendix B.5, we show that we must have

$$R_m \leq I(X;Y), \tag{B.21}$$

in which the mutual information $I(X;Y)$ is computed from this particular P_X and $P_Y = \sum\limits_{i \in \mathcal{X}} P_X(i) W(Y|i)$. Meanwhile, we also have

$$\mathscr{A}_n \supseteq \bigcup_{X^n \in C_{P_X}} A(X^n), \tag{B.22}$$

which follows from the fact that for any $Y^n \notin \mathscr{A}_n$, Y^n will be rejected by Bob, let alone be decoded to a codeword in C_{P_X}, and thus $Y^n \notin \bigcup\limits_{X^n \in C_{P_X}} A(X^n)$.

Now suppose Eve initiates an impersonation attack by generating a sequence Z^n with each component generated i.i.d. according to some PMF P_Z, and define

$$Q_Y = \sum_{j \in \mathcal{Z}} P_Z(j) V(Y|j). \tag{B.23}$$

With this particular attack, the success probability is

$$\Pr\{\mathscr{A}_n|Z^n\} \overset{(a)}{\geq} \Pr\left\{\bigcup_{X^n \in C_{P_X}} A(X^n)|Z^n\right\} \tag{B.24}$$

$$\overset{(b)}{=} \sum_{X^n \in C_{P_X}} \Pr\{A(X^n)|Z^n\}, \tag{B.25}$$

in which (a) follows from (B.22) and (b) is true due to (B.20).

On the other hand, according to the proof in Theorem 4.4 (in particular, the proof of (B.17)), we have, for each $X^n \in C_{P_X}$, that

$$\begin{aligned}\Pr\{A(X^n)|Z^n\} &\geq 2^{-n(\sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_{Y,i})+\varepsilon)} \\ &= 2^{-n(\sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y)+\varepsilon)},\end{aligned}$$

since $\Pr\{A(X^n)|X^n\} \geq 1 - 2\epsilon$. And the last step is true due to the fact that $\forall\ i \in \mathcal{X}$, $Q_{Y,i} = Q_Y$ is fixed under this attack ($P_{Y,i}$ and $Q_{Y,i}$ are defined in Section 4.4.1). Thus, we have

$$\begin{aligned}\Pr\{\mathscr{A}_n|Z^n\} &\geq \sum_{x^n \in C_{P_X}} 2^{-n(\sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y)+\varepsilon)} \\ &\geq (n+1)^{-|\mathcal{X}|} 2^{nR_m} 2^{-n(\sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y)+\varepsilon)} \\ &= (n+1)^{-|\mathcal{X}|} 2^{-n(\sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y)-R_m+\varepsilon)}.\end{aligned}$$

Since $\Pr\{\mathscr{A}_n|Z^n\}$ is obtained by one specific attack strategy, it must be less than or equal to the successful attack probability of the optimal attack strategy, $\Pr\{\mathscr{A}_n|Z^{\star n}\}$. Thus, we have

$$-\frac{1}{n}\log \Pr\{\mathscr{A}_n|Z^{\star n}\} \leq \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m + \varepsilon + \frac{|\mathcal{X}|}{n}\log(n+1)$$

$$= \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m + \varepsilon', \tag{B.26}$$

where $\varepsilon' \triangleq \varepsilon + \frac{|\mathcal{X}|}{n}\log(n+1)$. From (B.21) and (B.26), we see that for any given (ϕ, φ, ψ) (thus P_X is given), Eve can select an arbitrary distribution $P_Z \in \mathcal{P}_Z$ to initiate an impersonation attack as described above, and the corresponding exponent of the successful attack probability is upper bounded by the right-hand side of (B.26). Thus, the largest exponent of the successful attack probability (corresponding to the smallest successful attack probability) Alice and Bob can expect in the worst case when Eve selects the optimal distribution P_Z based on the given P_X, is given by $\min\limits_{P_Z} \sum\limits_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m$. Hence, we conclude that

$$\theta_I(R_m, \epsilon) \leq \max_{P_X\in\mathcal{P}_R} \min_{P_Z} \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m,$$

since ε' is an arbitrary small number as $n \to \infty$. And we have

$$\begin{aligned}\theta_I(R_m, \epsilon) &\leq \max_{P_X\in\mathcal{P}_R} \min_{P_Z} \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m \\ &\overset{(a)}{=} \min_{P_Z} \max_{P_X\in\mathcal{P}_R} \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m. \qquad \text{(B.27)}\end{aligned}$$

Here, (a) is proved in Appendix B.6.

Given any $P_Z \in \mathcal{P}_Z$ (thus, Q_Y is given), we first focus on the maximization sub-problem:

$$\max_{P_X\in\mathcal{P}_R} \sum_{i\in\mathcal{X}} P_X(i)D(P_{Y,i}||Q_Y) - R_m, \qquad \text{(B.28)}$$

In Appendix B.7, we show that, for the optimization problem (B.28), an optimizer P_X^* with $I(X^*;Y) = R_m$ can always be found. On the other hand, we have

$$\begin{aligned}&\sum_i P_X(i)D(P_{Y,i}||Q_Y) - R_m \\ &= \sum_i P_X(i) \sum_Y P_{Y,i} \log \frac{P_{Y,i}}{Q_Y} - R_m\end{aligned}$$

$$
\begin{aligned}
&= \sum_i P_X(i) \sum_Y W(Y|i) \log \frac{W(Y|i)}{Q_Y} - R_m \\
&= \sum_{i,Y} P_X(i) W(Y|i) \log \frac{W(Y|i)}{Q_Y} \frac{P_Y}{P_Y} - R_m \\
&= \sum_{i,Y} P_X(i) W(Y|i) \log \frac{P_Y}{Q_Y} + \sum_{i,Y} P_X(i) W(Y|i) \log \frac{W(Y|i)}{P_Y} - R_m \\
&= \sum_Y P_Y \log \frac{P_Y}{Q_Y} + \sum_{i,Y} P_X(i) W(Y|i) \log \frac{P_X(i) W(Y|i)}{P_X P_Y} - R_m \\
&= D(P_Y||Q_Y) + \sum_{i,Y} P_{XY} \log \frac{P_{XY}}{P_X \cdot P_Y} - R_m \\
&= D(P_Y||Q_Y) + I(X;Y) - R_m.
\end{aligned}
$$

Thus, (B.27) is equivalent to

$$
\begin{aligned}
\theta_I(R_m, \epsilon) &\le \min_{P_Z} \max_{P_X \in \mathcal{P}_R} \sum_{i \in \mathcal{X}} P_X(i) D(P_{Y,i}||Q_Y) - R_m \\
&\overset{(a)}{=} \min_{P_Z} \max_{P_X \in \partial \mathcal{P}_R} D(P_Y||Q_Y) \\
&\overset{(b)}{=} \min_{P_Z} \max_{P_X \in \mathcal{P}_R} D(P_Y||Q_Y), \qquad \text{(B.29)}
\end{aligned}
$$

in which $\partial \mathcal{P}_R := \{P_X : I(X;Y) = R_m\}$. Here step (a) is true because as discussed above, the optimizer P_X^* satisfies $I(X^*;Y) = R_m$. Step (b) is true, because for any given P_Z, $D(P_Y||Q_Y)$ is convex in P_Y while P_Y is an affine function of P_X, then $D(P_Y||Q_Y)$ is convex in P_X, thus the optimal solution of $\max\limits_{P_X \in \mathcal{P}_R} D(P_Y||Q_Y)$ is obtained on the boundary $\partial \mathcal{P}_R$ [96].

Construct a scheme to achieve (4.27)**:** In this part, for any given P_X (thus P_Y is fixed), we will construct a scheme such that the successful attack probability of any attack strategy is less than $2^{-n(\min\limits_{P_Z} D(P_Y||Q_Y) - \varepsilon)}$.

Codebook construction: Fix P_X, generate 2^{nR_m} sequences X^n as the codewords, i.i.d. according to the PMF P_X, with $R_m \le I(X;Y)$. And each codeword is assigned to one message. We use $X^n(M)$ to denote the M-th codeword.

Encoder ϕ: If Alice needs to send a message M to Bob, she transmits $X^n(M)$ into the channel.

Testing function ψ: Upon receiving a sequence Y^n, Bob first determines whether Y^n is from Alice or not. He declares it to be from Alice if Y^n is P_Y-typical, in which $P_Y = \sum\limits_{i\in\mathcal{X}} P_X(i)W(Y|i)$ for the given P_X; Otherwise, Bob declares that the message is from Eve, and abandons it. Hence, the acceptance region is $\mathscr{A} = T_\epsilon^n(Y)$. It is easy to show that for any given ϵ, there exists an r such that

$$\mathscr{A} \subseteq S_r^n(P_Y). \tag{B.30}$$

Furthermore, r goes to zero as ϵ decreases.

Decoder φ: If Y^n is tested to be from Alice, Bob tries to find a unique sequence $X^n(\hat{M})$ from the codebook such that $(X^n(\hat{M}), y^n)$ are jointly typical according to $W(Y|X)P_X$. If there are more than one such sequences X^n, he randomly picks one and declares it as the transmitted message; If there is no such sequence, he declares an error.

Error analysis: Since the acceptance region is $\mathscr{A} = T_\epsilon^n(Y)$, and all Y^n sequences that are jointly typical with X^n are included in $\mathscr{A}$, thus, we can easily show that

$$\Pr\{\hat{M} \neq M, H_0|H_0\} \leq \frac{\epsilon}{2},$$
$$\Pr\{H_1|H_0\} \leq \frac{\epsilon}{2}.$$

Using similar argument as that of the proof of Theorem 7.7.1[16], we can obtain that there exists at least one codebook such that (4.7) is satisfied.

Authentication exponent analysis: First, for any attack sequence Z^n with type P_Z chosen by Eve, we have

$$\Pr\{\mathscr{A}|Z^n\} \leq \Pr\{S_r^n(P_Y)|Z^n\},$$

which is true due to (B.30). Furthermore, following the same derivation as that in Appendix B.4, we have

$$\begin{aligned}\text{Pr}\{S_r^n(P_Y)|Z^n\} &\leq n^{|\mathcal{Y}|+|\mathcal{Z}|}2^{-n(D(P_Y||Q_Y)-\delta(r))}\\ &\leq n^{|\mathcal{Y}|+|\mathcal{Z}|}2^{-n(\min\limits_{P_Z} D(P_Y||Q_Y)-\delta(r))}.\end{aligned} \tag{B.31}$$

Thus, we have

$$\text{Pr}\{\mathscr{A}|Z^n\} \leq n^{|\mathcal{Y}|+|\mathcal{Z}|}2^{-n(\min\limits_{P_Z} D(P_Y||Q_Y)-\delta(r))},$$

which indicates that

$$-\frac{1}{n}\log \text{Pr}\{\mathscr{A}|Z^n\} \geq \min_{P_Z} D(P_Y||Q_Y) - \delta(r) - \frac{|\mathcal{Y}|+|\mathcal{Z}|}{n}\log n.$$

Finally, we conclude that

$$\theta_I(R_m,\epsilon) \geq \max_{P_X\in\mathcal{P}_R}\min_{P_Z} D(P_Y||Q_Y), \tag{B.32}$$

and this completes the proof.

B.3 Lemma B.2

Lemma B.2. Let P^*, P and Q be three distributions on random variable X, and $r \geq 0$, then if $D(P^*||P) \leq r$ and $0 < D(P||Q) < \infty$, then

$$D(P^*||Q) \geq D(P||Q) - \delta(r),$$

$$D(P^*||Q) \leq D(P||Q) + \delta(r).$$

in which $\delta(r) \downarrow 0$ as $r \downarrow 0$.

In order to prove Lemma B.2, techniques from [16] are utilized.

Lemma B.3 ([16])**.** 1. (*Pinsker's Inequality*) Let P and Q be any two distributions on X, then

$$D(P||Q) \geq \frac{1}{2\ln 2}||P - Q||_1^2,$$

in which $||P - Q||_1 = \sum_{x \in \mathcal{X}} |P(x) - Q(x)|$.

2. Let B_n be any set of sequences X^n, such that $P^n(B_n) > 1 - \epsilon$. Let Q be any other distribution such that $D(P||Q) < \infty$, then

$$Q^n(B_n) > (1 - 2\epsilon)2^{-n(D(P||Q)+\epsilon)}.$$

Proof of Lemma B.2. If $Q(i) = 0$ for some $i \in \mathcal{X}$, then $P(i) = 0$ and $P^*(i) = 0$, since $D(P||Q) < \infty$ and $D(P^*||P) \leq r$. Thus, the existence of $\{i \in \mathcal{X} : Q(i) = 0\}$ has no influence on the final result. Hence, to facilitate the presentation, we assume that $Q(i) > 0, \forall i \in \mathcal{X}$.

Since $r \geq D(P^*||P) \geq \frac{1}{2\ln 2}||P^* - P||_1^2$, then we have

$$\sum_{i \in \mathcal{X}} |P^*(i) - P(i)| \leq \sqrt{2\ln 2 \cdot r},$$

which indicates

$$|P^*(i) - P(i)| \leq \sqrt{2\ln 2 \cdot r}, \forall i \in \mathcal{X}.$$

Define a set $A := \{i \in \mathcal{X} : P(i) > Q(i) + \sqrt{2\ln 2 \cdot r}\}$, and $\bar{A} := \mathcal{X} \backslash A$. Then we have

$$D(P^*||Q) = \sum_{i \in \mathcal{X}} P^*(i) \log \frac{P^*(i)}{Q(i)}$$

$$
\begin{aligned}
&= \sum_{i\in A} P^*(i) \log \frac{P^*(i)}{Q(i)} + \sum_{i\in \bar{A}} P^*(i) \log \frac{P^*(i)}{Q(i)} \\
&\overset{(a)}{\geq} \sum_{i\in A} (P(i) - \sqrt{2r\ln 2}) \log \frac{P(i) - \sqrt{2r\ln 2}}{Q(i)} \\
&\quad + \sum_{i\in \bar{A}} (P(i) + \sqrt{2r\ln 2}) \log \frac{P(i) - \sqrt{2r\ln 2}}{Q(i)} \\
&= \sum_{i\in \mathcal{X}} P(i) \log \frac{P(i) - \sqrt{2r\ln 2}}{Q(i)} - \sqrt{2r\ln 2} \cdot \\
&\left(\sum_{i\in A} \log \frac{P(i) - \sqrt{2r\ln 2}}{Q(i)} - \sum_{i\in \bar{A}} \log \frac{P(i) - \sqrt{2r\ln 2}}{Q(i)} \right) \qquad \text{(B.33)} \\
&= \sum_{i\in \mathcal{X}} P(i) \log \frac{P(i) - \sqrt{2r\ln 2}}{Q(i)} - \delta'(r) \qquad \text{(B.34)} \\
&= \sum_{i\in \mathcal{X}} P(i) \log \frac{P(i)}{Q(i)} + \sum_{i\in \mathcal{X}} P(i) \log \frac{P(i) - \sqrt{2r\ln 2}}{P(i)} - \delta'(r) \\
&\overset{(b)}{\geq} D(P||Q) - \sum_{i\in \mathcal{X}} P(i) \frac{2\sqrt{2r\ln 2}}{P(i)\ln 2} - \delta'(r) \\
&= D(P||Q) - \delta_1(r),
\end{aligned}
$$

in which step (a) follows from the facts that $\log(\cdot)$ is an increasing function of its argument, and that

$$
\begin{aligned}
\log \frac{P(i) - \sqrt{2r\ln 2}}{Q(i)} &> 0, \ \forall i \in A; \\
\log \frac{P(i) - \sqrt{2r\ln 2}}{Q(i)} &\leq 0, \ \forall i \in \bar{A}.
\end{aligned}
$$

In addition, step (b) is true due to the fact that $\ln(1-\gamma) \geq -2\gamma$ when γ $(\gamma \geq 0)$ is small enough. Then, we only need to show $\delta_1(r)$ vanishes as $r \rightarrow 0$, which is equivalent to show $\delta'(r) \downarrow 0$ as $r \downarrow 0$. From (B.33) to (B.34), $\delta'(r) := \varepsilon \cdot (\sum_{i\in A} \log \frac{P(i)-\varepsilon}{Q(i)} - \sum_{i\in \bar{A}} \log \frac{P(i)-\varepsilon}{Q(i)})$ by setting $\varepsilon = \sqrt{2r\ln 2}$. Since the sizes of sets A and $\bar{A}$ are finite, we only need to show $\log \frac{P(i)-\varepsilon}{Q(i)}$ is finite when ε is small enough. And that $\forall i \in \mathcal{X}, \log \frac{P(i)-\varepsilon}{Q(i)}$ is finite is obvious, because of the assumption that $P(i) > 0, Q(i) > 0$.

Following similar steps as above, we can also show that

$$D(P^*||Q) \leq D(P||Q) + \delta_2(r).$$

Finally, by setting $\delta(r) = \max\{\delta_1(r), \delta_2(r)\}$, we complete the proof. □

B.4 Proof of (4.25)

For any sequence Z_0^n selected by Eve, we denote the successful attack probability as $\text{Pr}\{\mathscr{A}_n|Z_0^n\}$. We realize that, for any given value $\epsilon > 0$, there exists an r, with r vanishing as ϵ goes to zero, such that

$$\mathscr{A}_n \in S_r^n(P_Y),$$

which implies that

$$\text{Pr}\{\mathscr{A}_n|Z_0^n\} \leq \text{Pr}\{S_r^n(P_Y)|Z_0^n\}.$$

Denote the type of sequence Z_0^n by $P_Z \triangleq \text{tp}(Z_0^n)$. Due to the symmetry of $S_r^n(P_Y)$, we have

$$\text{Pr}\{S_r^n(P_Y)|Z^n\} = \text{Pr}\{S_r^n(P_Y)|Z_0^n\},\ \forall Z^n : \text{tp}(Z^n) = P_Z.$$

Furthermore, denote

$$Q_Y = \sum_{j \in \mathcal{Z}} V(Y|j) \cdot P_Z(j),$$

and we have

$$\begin{aligned} Q_Y^n(S_r^n(P_Y)) &= \sum_{Z^n \in \mathcal{Z}^n} P_Z^n(Z^n) \cdot \text{Pr}\{S_r^n(P_Y)|Z^n\} \\ &= \sum_{Z^n \in \mathcal{Z}^n} P_Z^n(Z^n) \sum_{Y^n \in S_r^n(P_Y)} \text{Pr}\{Y^n|Z^n\} \end{aligned}$$

$$\begin{aligned}
&= \sum_{\tilde{P}_Z\in\mathcal{T}_Z}\ \sum_{Z^n\in\mathcal{T}_Z^n(\tilde{P}_Z)} P_Z^n(Z^n|\tilde{P}_Z)P_Z^n(\mathcal{T}_Z^n(\tilde{P}_Z))\cdot \sum_{Y^n\in S_r^n(P_Y)} \Pr\{Y^n|Z^n\}\\
&= \sum_{\tilde{P}_Z\in\mathcal{T}_Z} P_Z^n(\mathcal{T}_Z^n(\tilde{P}_Z)) \sum_{Z^n\in\mathcal{T}_Z^n(\tilde{P}_Z)} P_Z^n(Z^n|\tilde{P}_Z)\cdot \sum_{Y^n\in S_r^n(P_Y)} \Pr\{Y^n|Z^n\}\\
&\geq P_Z^n(\mathcal{T}_Z^n(P_Z)) \sum_{Z^n\in\mathcal{T}_Z^n(P_Z)} P_Z^n(Z^n|P_Z)\cdot \sum_{Y^n\in S_r^n(P_Y)} \Pr\{Y^n|Z^n\}.\\
&= P_Z^n(\mathcal{T}_Z^n(P_Z)) \sum_{Z^n\in\mathcal{T}_Z^n(P_Z)} P_Z^n(Z^n|P_Z)\cdot \sum_{Y^n\in S_r^n(P_Y)} \Pr\{Y^n|Z_0^n\}.\\
&= P_Z^n(\mathcal{T}_Z^n(P_Z))\cdot \Pr\{S_r^n(P_Y)|Z_0^n\}\\
&\geq \frac{1}{(n+1)^{|\mathcal{Z}|}}\cdot \Pr\{S_r^n(P_Y)|Z_0^n\}.
\end{aligned}$$

Thus, it follows that

$$\Pr\{S_r^n(P_Y)|Z_0^n\} \leq (n+1)^{|\mathcal{Z}|}Q_Y^n(S_r^n(P_Y)).$$

On the other hand, we have

$$\begin{aligned}
Q_Y^n(S_r^n(P_Y)) &= \sum_{\text{tp}(Y^n):\mathcal{T}_Y^n(\text{tp}(Y^n))\subseteq S_r^n(P_Y)} Q_Y^n(\text{tp}(Y^n))\\
&\leq \sum_{\text{tp}(Y^n):\mathcal{T}_Y^n(\text{tp}(Y^n))\subseteq S_r^n(P_Y)} 2^{-nD(\text{tp}(Y^n)||Q_Y)}\\
&\leq \sum_{\text{tp}(Y^n):\mathcal{T}_Y^n(\text{tp}(Y^n))\subseteq S_r^n(P_Y)} 2^{-n(D(P_Y||Q_Y)-\delta(r))}\\
&\leq (n+1)^{|\mathcal{Y}|}2^{-n(D(P_Y||Q_Y)-\delta(r))}.
\end{aligned}$$

Thus, it follows

$$\Pr\{S_r^n(P_Y)|Z_0^n\} \leq (n+1)^{|\mathcal{Y}|+|\mathcal{Z}|}2^{-n(D(P_Y||Q_Y)-\delta(r))},$$

which indicates that

$$2^{-n\theta_I(0,\epsilon)} = \limsup_{Z_0^n} \Pr\{S_r^n(P_Y)|Z_0^n\}$$

$$\leq \max_{P_Z}(n+1)^{|\mathcal{Y}|+|\mathcal{Z}|}2^{-n(D(P_Y||Q_Y)-\delta(r))}$$
$$= 2^{-n(\min_{P_Z} D(P_Y||Q_Y)-\epsilon')},$$

where ϵ' is a small number.

B.5 Proof of (B.21)

According to the conditional typicality property, we have

$$\text{Pr}\{T_\epsilon(Y^n|X^n)|X^n\} \geq 1-\epsilon.$$

Thus,

$$\text{Pr}\{A(X^n) \cap T_\epsilon(Y^n|X^n)|X^n\} \geq 1-3\epsilon.$$

In addition, for each $Y^n \in T_\epsilon(Y^n|X^n)$, we have

$$2^{-n(H(Y|X)+\epsilon)} \leq \text{Pr}\{Y^n|X^n\} \leq 2^{-n(H(Y|X)-\epsilon)}.$$

Thus, we have

$$|A(X^n) \cap T_\epsilon(Y^n|X^n)| \geq (1-3\epsilon)2^{n(H(Y|X)-2\epsilon)}.$$

Since for each $X^n \in C_{P_X}$, we have $T_\epsilon(Y^n|X^n) \subseteq T_\epsilon(Y^n)$, then,

$$T_\epsilon(Y^n) \supseteq \bigcup_{X^n \in C_{P_X}} A(X^n) \cap T_\epsilon(Y^n|X^n).$$

In addition, from (B.20), $\forall\, X^n, \tilde{X}^n \in C_{P_X}, X^n \neq \tilde{X}^n$ we have

$$A(X^n) \cap T_\epsilon(Y^n|X^n) \bigcap A(\tilde{X}^n) \cap T_\epsilon(Y^n|\tilde{X}^n) = \emptyset.$$

Thus, we have

$$\begin{aligned} |T_\epsilon(Y^n)| &\geq \sum_{X^n \in C_{P_X}} |A(X^n) \cap T_\epsilon(Y^n|X^n)| \\ &\geq \sum_{X^n \in C_{P_X}} (1-3\epsilon) 2^{n(H(Y|X)-2\epsilon)} \\ &\geq (n+1)^{-|\mathcal{X}|} 2^{nR_m} (1-3\epsilon) 2^{n(H(Y|X)-2\epsilon)}. \end{aligned}$$

Since that $|T_\epsilon(Y^n)| \leq 2^{n(H(Y)+\epsilon)}$, we have

$$2^{n(H(Y)+\epsilon)} \geq (n+1)^{-|\mathcal{X}|}(1-3\epsilon) 2^{n(H(Y|X)+R_m-2\epsilon)},$$

thus,

$$R_m \leq I(X;Y) + 4\epsilon + \frac{|\mathcal{X}|}{n} \log n (1-2\epsilon).$$

The proof is complete.

B.6 Proof of (B.27)

Define

$$\begin{aligned} &S := \{P_X : I(X;Y) \geq R_m\}, \\ &T := \{Q_Y : Q_Y = \sum_{j \in \mathcal{Z}} P_Z(j) V(Y|j), \forall P_Z \in \mathcal{P}_Z\}. \end{aligned}$$

Since Q_Y is an affine function of P_Z, we can rewrite the $\max \min$ problem in (B.27) as

$$\max_{P_X \in S} \min_{Q_Y \in T} F(P_X, Q_Y),$$

where $F(P_X, Q_Y) := \sum\limits_{i \in \mathcal{X}} P_X(i) D(P_{Y,i} || Q_Y) - R_m$. Thus, we need to show

$$\max_{P_X \in S} \min_{Q_Y \in T} F(P_X, Q_Y) = \min_{Q_Y \in T} \max_{P_X \in S} F(P_X, Q_Y) \tag{B.35}$$

is true.

Before going further, we need to introduce Sion's minimax theorem as follows.

Lemma B.4 (Sion's minimax theorem [85])**.** Let B be a convex subset of a topological vector space and D a compact convex subset of a topological vector space. And f is a real-valued function defined on $B \times D$ with

1. $f(b, \cdot)$ is lower semicontinuous and quasi-convex on D, $\forall b \in B$, and

2. $f(\cdot, d)$ is upper semicontinuous and quasiconcave on B, $\forall d \in D$.

Then

$$\max_{b \in B} \min_{d \in D} f(b, d) = \min_{d \in D} \max_{b \in B} f(b, d).$$

According to Sion's minimax theorem, in order to obtain (B.35), we need to prove

a) S and T are convex;

b) Given P_X, $F(P_X, \cdot)$ is convex on T;

c) Given Q_Y, $F(\cdot, Q_Y)$ is quasiconcave on S.

Now, we provide the proofs one by one.

Proof of a). That T is convex is obvious, since Q_Y is an affine function of P_Z, and $\mathcal{P}_Z$ is convex.

Then, we show S is convex. Suppose $P_{X1} \in S$ and $P_{X2} \in S$ (denote the corresponding mutual information by $I(X1;Y)$ and $I(X2;Y)$ respectively), thus we have

$$\begin{aligned} I(X1;Y) &\geq R_m, \\ I(X2;Y) &\geq R_m. \end{aligned}$$

Set $P_{X3} = \lambda P_{X1} + (1-\lambda)P_{X2}$ for arbitrary $\lambda \in [0,1]$. Since the conditional PMF $P_{Y|X}$ is fixed by the channel $W(Y|X)$ and that $I(X;Y)$ is concave in P_X for a fixed $P_{Y|X}$, we have

$$\begin{aligned} I(X3;Y) &\geq \lambda I(X1;Y) + (1-\lambda)I(X2;Y) \\ &\geq \lambda R_m + (1-\lambda)R_m \\ &= R_m. \end{aligned}$$

Thus, $P_{X3} \in S$. Then, we have that S is a convex set.

Proof of b). According to Theorem 2.7.2 of [16], $D(P_{Y,i}||Q_Y)$ is convex in $(P_{Y,i}, Q_Y)$. With a fixed $P_{Y,i}$, we obtain that $D(P_{Y,i}||Q_Y)$ is convex in Q_Y. Thus, suppose $Q_{Y1}, Q_{Y2} \in T$ and $Q_{Y3} = \lambda Q_{Y1} + (1-\lambda)Q_{Y2}$, and $\forall i \in \mathcal{X}$, we have

$$P_X(i)D(P_{Y,i}||Q_{Y3}) \leq P_X(i)(\lambda D(P_{Y,i}||Q_{Y1}) + (1-\lambda)D(P_{Y,i}||Q_{Y3})).$$

Thus

$$\begin{aligned} \sum_i P_X(i)D(P_{Y,i}||Q_{Y3}) &\leq \sum_i P_X(i)(\lambda D(P_{Y,i}||Q_{Y1}) + (1-\lambda)D(P_{Y,i}||Q_{Y2})) \\ &= \lambda \sum_i P_X(i)D(P_{Y,i}||Q_{Y1}) + (1-\lambda)\sum_i P_X(i)D(P_{Y,i}||Q_{Y2}). \end{aligned}$$

Then, we have

$$F(P_X, Q_{Y3}) \leq \lambda F(P_X, Q_{Y1}) + (1-\lambda)F(P_X, Q_{Y2}).$$

Thus, $F(P_X, \cdot)$ is convex on T.

Proof of c). Given Q_Y, we know $F(\cdot, Q_Y)$ is linear in P_X, thus, it's quasiconcave.

B.7 Proof of (B.28)

To assist the presentation, denote

$$\ell(P_X) \triangleq \sum_{i \in \mathcal{X}} P_X(i) h_i - R_m,$$

in which $h_i \triangleq D(P_{Y,i} || Q_Y)$. Since for each $i \in \mathcal{X}$, h_i is a constant, we have that $\ell(P_X)$ is linear in P_X.

Recall that $\mathcal{P}_R = \{P_X : I(X;Y) \geq R_m\}$. Suppose

$$P_X^* = \arg\max_{P_X \in \mathcal{P}_R} \ell(P_X), \tag{B.36}$$

and P_X^* is an interior point of $\mathcal{P}_R$, thus,

$$I(X^*;Y) > R_m.$$

Denote

$$\begin{aligned} &S_I \triangleq \{i \in \mathcal{X} : P_X^*(i) \neq 0\}, \\ &\hat{i} = \arg\min_{i \in S_I} h_i. \end{aligned}$$

Then, we have

$$\begin{aligned} \ell(P_X^*) &= \sum_{i \in S_I} P_X^*(i) h_i - R_m \\ &= \sum_{i \in S_I \setminus \hat{i}} P_X^*(i) h_i + P_X^*(\hat{i}) h_{\hat{i}} - R_m \end{aligned}$$

$$= \sum_{i \in S_I \backslash \hat{i}} P_X^*(i) h_i + \left(1 - \sum_{i \in S_I \backslash \hat{i}} P_X^*(i)\right) h_{\hat{i}} - R_m$$
$$= \sum_{i \in S_I \backslash \hat{i}} P_X^*(i)(h_i - h_{\hat{i}}) + h_{\hat{i}} - R_m.$$

Now, construct $\tilde{P}_X$ as

$$\tilde{P}_X(i) = P_X^*(i) + \epsilon, \quad \forall\, i \in S_I \backslash \hat{i};$$
$$\tilde{P}_X(i) = 0, \qquad \forall\, i \in \mathcal{X} \backslash S_I;$$
$$\tilde{P}_X(\hat{i}) = 1 - \sum_{i \in S_I \backslash \hat{i}} \tilde{P}_X(i).$$

Due to the continuity of $I(X;Y)$ in P_X, there exists some $\epsilon > 0$ such that

$$I(\tilde{X};Y) \geq R_m.$$

However, for this $\tilde{P}_X$, we have

$$\ell(\tilde{P}_X) = \ell(P_X^*) + \epsilon \sum_{i \in S_I \backslash \hat{i}} (h_i - h_{\hat{i}}) \geq \ell(P_X^*), \tag{B.37}$$

in which the equality holds only when $h_i = h_{\hat{i}}, \forall i \in S_I$. If the inequality in (B.37) is strict, then it contradicts the assumption in (B.36) that P_X^* is the maximizer for $\ell(P_X)$. Hence, the equality in (B.37) holds. In this case, all $\ell(P_X)$s with $P_X \in \{P_X : \forall i \in \mathcal{X} \backslash S_I, P_X(i) = 0\}$ have the same value as $\ell(P_X^*)$. Now, due to the continuity of $I(X;Y)$ in P_X, it's easy to conclude that there exists a $\hat{P}_X \in \{P_X : \forall i \in \mathcal{X} \backslash S_I, P_X(i) = 0\}$ such that $I(\hat{X};Y) = R_m$, as 1) $P_X^* \in \{P_X : \forall i \in \mathcal{X} \backslash S_I, P_X(i) = 0\}$ and $I(X^*;Y) > R_m$ from the assumption; and 2) there exists a $P_X^\star \in \{P_X : \forall i \in \mathcal{X} \backslash S_I, P_X(i) = 0\}$ (e.g. $P_X^\star$ is of the form $[0, \cdots, 1, 0, \cdots]$) such that $I(X^\star;Y) = 0$.

Hence, the optimal value can always be obtained on the boundary defined as

$$\{P_X : I(X;Y) = R_m\}.$$

This completes the proof.

B.8 Proofs of Lemmas

B.8.1 Proof of Lemma 4.10

Denote channels $W(Y|X)$ and $V(Y|Z)$ by matrice W and V in short. Define $P^1_{X,i} = [0, \cdots, 0, 1, 0, \cdots, 0]^T, i \in \mathcal{X}$, where 1 is on the ith row. Since simulatability condition holds, there exists $P^\triangle_{Z,i} \in \mathcal{P}_\mathcal{Z}$ such that

$$VP^\triangle_{Z,i} = WP^1_{X,i},\ \forall i \in \mathcal{X}.$$

In addition, given an arbitrary $P_X \in \mathcal{P}_X$, we have

$$P_X = [P_X(1), \cdots, P_X(|\mathcal{X}|)]^T = \sum_{i \in \mathcal{X}} P_X(i) P^1_{X,i}.$$

Set a virtual channel $\tilde{V}_{Z|\tilde{X}}$ by

$$\tilde{V}_{Z|\tilde{X}} = [P^\triangle_{Z,1}, P^\triangle_{Z,2}, \cdots, P^\triangle_{Z,|\mathcal{X}|}],$$

then, we have

$$\begin{aligned} WP_X &= W \sum_{i \in \mathcal{X}} P_X(i) P^1_{X,i} \qquad \text{(B.38)} \\ &= \sum_{i \in \mathcal{X}} WP_X(i) P^1_{X,i} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i\in\mathcal{X}} P_X(i) W P^1_{X,i} \\
&= \sum_{i\in\mathcal{X}} P_X(i) V P^{\triangle}_{Z,i} \\
&= V \sum_{i\in\mathcal{X}} P_X(i) P^{\triangle}_{Z,i} \\
&= V \tilde{V}_{Z|\tilde{X}} P_X. \qquad \text{(B.39)}
\end{aligned}
$$

Since here $P_X \in \mathcal{P}_X$ is arbitrarily given, we have

$$
W = V\tilde{V}_{Z|\tilde{X}}. \qquad \text{(B.40)}
$$

This completes the proof.

B.8.2 Proof of Lemma 4.11

The conclusion that if simulatability condition holds, then the equations defined by (4.34) hold is obvious, since $W(Y|i) = W(Y|X)P^1_{X,i}$, and $P^1_{X,i} \in \mathcal{P}_{\mathcal{X}}$ ($P^1_{X,i}$ is defined in the proof of Lemma 4.10).

On the other hand, as we have shown from (B.38) to (B.39), if (4.34) holds, then $\forall P_X \in \mathcal{P}_{\mathcal{X}}$, $P_Z = \sum_{i\in\mathcal{X}} P_X(i)P^{\triangle}_{Z,i}$ is always a valid choice.

B.8.3 Proof of Lemma 4.14

It suffices to show

$$
\min_{P_{Z,i^*}} ||\hat{V}(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1 > 0
$$

with constraints defined by (4.38).

$$
\begin{aligned}
\min_{P_{Z,i^*}} ||\hat{V}(Y|Z)P_{Z,i^*} - W(Y|i^*)||_1 &= \min_{P_{Z,i^*}} ||(V(Y|Z) + \Delta V(Y|Z))P_{Z,i^*} - W(Y|X)||_1 \\
&= \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|X) + \Delta V(Y|Z)P_{Z,i^*}||_1
\end{aligned}
$$

$$
\begin{aligned}
&\geq \min_{P_{Z,i^*}} ||V(Y|Z)P_{Z,i^*} - W(Y|X)||_1 - \max_{P_{Z,i^*}} ||\Delta V(Y|Z)P_{Z,i^*}||_1 \\
&= \rho - \max_{P_{Z,i^*}} ||\Delta V(Y|Z)P_{Z,i^*}||_1 \\
&\overset{(a)}{\geq} \rho - |\mathcal{Y}|\delta \\
&> 0,
\end{aligned}
$$

if $\delta < \frac{\rho}{|\mathcal{Y}|}$. (a) is true since the summation of each column of P_{Z,i^*} equals to 1.

Appendix C

Chapter 5

In the sequel, we use the term typicality as defined in [23, Chapter 2], i.e. a sequence X^n is said to be typical if

$$|\pi(x|X^n) - P_X(x)| \leq \epsilon P_X(x), \forall x \in \mathcal{X},$$

where $\pi(x|X^n) := |\{i : X_i = x\}|/n$ is the empirical PMF of X^n.

We first have the following lemma that is very useful for the achievability proofs.

Lemma C.1. Given a typical sequence x^n and an admissible variable U with joint PMF P_{UX}, then U^n is an admissible sequence if it is jointly typical with x^n according to P_{UX}.

Proof. Given $X = x$, we only need to consider realizations $y \in \mathcal{Y}$ with $p_{XY}(x, y) > 0$. According to Defi. 5.4, we have

$$\text{Pr}\{f(x, Y) = g(U, Y)\} = 1, \tag{C.1}$$

which is equivalent to that

$$\sum_{u \in \mathcal{U}} P_{U|X}(u|x)\text{Pr}\{f(x, Y) = g(u, Y)\} = 1,$$

which means that for all $u \in \mathcal{U}$, Pr$\{f(x, Y) = g(u, Y)\} = 1$ if $P_{U|X}(u|x) \neq 0$. Denote the support of the conditional PMF $P_{U|X}(U|x)$ by

$$S_{P_{UX}}(x) := \{u \in \mathcal{U} : P_{U|X}(u|x) > 0\}.$$

The typicality of x^n and U^n guarantees that the probability of $U_i \notin S_{P_{UX}}(x_i)$ is zero, since $\forall U_i \notin S_{P_{UX}}(x_i)$,

$$P_{UX}(U_i, x_i) = P_X(x)P_{U|X}(U_i|x_i) = 0,$$

and

$$\begin{aligned}
&|\pi((U_i, x_i)|(U^n, x^n)) - P_U X(U_i, x_i)| \leq \epsilon P_{U|X}(U_i|x_i) \\
&\Leftrightarrow | \ \ \pi((U_i, x_i)|(U^n, x^n))| \leq 0.
\end{aligned}$$

Thus, we can conclude that U^n is admissible. □

Now, we provide detailed proofs of theorems presented in this chapter.

C.1 Proof of Theorem 5.1

Achievability:

In this part, we will show that for a given $P_{UXY} = P_{XY}P_{U|X}$, in which U is an admissible random variable w.r.t. X, Y and f, there exists a function computation scheme such that the tuple (R, Δ_1, Δ_2) with

$$\begin{aligned}
&R = I(X;U) - I(Y;U) + \epsilon, \\
&\Delta_1 = I(X;U|Y) + \epsilon, \\
&\Delta_2 = H(X;U) + I(Y;U) - \epsilon,
\end{aligned}$$

is achievable.

(1) **Codebook $\mathcal{C}$ construction :** Given $P_{XYZ}P_{U|X}$, randomly and independently generate 2^{nR_0} sequences U^n according to $\prod_{i=1}^{n} P_U(u_i)$, and assign each U^n into 2^{nR} bins which are indexed by M, using a uniform distribution. Here, we use $b(M)$ to denote bin M, and set

$$R_0 = I(X;U) + \epsilon,$$
$$R = I(X;U) - I(Y;U) + 2\epsilon.$$

(2) **Encoding:** Upon observing a sequence X^n, Alice looks into the generated codebook trying to finding a U^n that is joint P_{UX}-typical with X^n. If there are more than one such U^n, she randomly picks up one, and sends the index, M, of the bin where U^n is to the fusion center. Otherwise, she declares an error.

(3) **Decoding:** After receiving M, the fusion center looks into $b(M)$ trying find a unique $\hat{U}^n$ that is joint P_{UY}-typical with Y^n. If there are more than one such sequence or no such sequence, it randomly selects a $\hat{U}^n$ as the decoded sequence.

(4) **Function computing:** The fusion center computes the estimated value $\hat{\mathbf{f}} := \{g(\hat{U}_i, Y_i)\}_{i=1}^{n}$.

(5) **Error analysis:** According to Lemma C.1, the fusion center can correctly compute $\mathbf{f}$ as long as U^n is jointly typical with X^n and $\hat{U}^n = U^n$. Thus, the error is upper bounded by

$$\Pr\{\text{No jointly typical } U^n \text{ is found}\} + \Pr\{\hat{U}^n \neq U^n\}.$$

Since there are $2^{n(I(U;X)+\epsilon)}$ sequences U^n generated in the codebook and there are $2^{n(I(U;Y)-\epsilon)}$ sequences in each bin, we can easily obtain that

$$\Pr\{\text{No jointly typical } U^n \text{ is found}\} \leq \epsilon/2,$$
$$\Pr\{\hat{U}^n \neq U^n\} \leq \epsilon/2,$$

following the standard random coding techniques as that in [16]. Thus, we have that

$$\text{Pr}\{\mathbf{f} \neq \hat{\mathbf{f}}\} \leq \epsilon.$$

(6) **Privacy leakage:** First, we have

$$\begin{aligned} I(X^n; M|\mathcal{C}) &= H(M|\mathcal{C}) - H(M|X^n, \mathcal{C}) \\ &\leq H(M) \\ &= I(X; U) - I(Y; U) + 2\epsilon. \end{aligned}$$

Thus

$$\begin{aligned} \frac{1}{n} H(X^n|M, \mathcal{C}) &= \frac{1}{n} H(X^n|\mathcal{C}) - \frac{1}{n} I(X^n; M|\mathcal{C}) \\ &\geq H(X|U) + I(Y; U) - 2\epsilon. \end{aligned}$$

Furthermore, it follows that

$$\begin{aligned} I(X^n; M|Y^n, \mathcal{C}) &= H(M|Y^n, \mathcal{C}) - H(M|X^n, Y^n, \mathcal{C}) \\ &\leq H(M|\mathcal{C}) \\ &= I(X; U) - I(Y; U) + 2\epsilon \\ &= I(X; U|Y) + 2\epsilon. \end{aligned}$$

In summary, following the standard information theoretic methods, we conclude that the achievability is complete.

Converse:

It suffices to prove that given any achievable tuple (R, Δ_1, Δ_2), there exists some admissible U w.r.t. X, Y and f, such that (5.7), (5.8) and (5.9) hold.

First of all, we have

$$\begin{aligned}
nR &\geq H(M) - n\epsilon \\
&\geq H(M|Y^n) - n\epsilon \\
&\geq H(M|Y^n) - H(M|X^n) - n\epsilon \\
&= I(M; X^n) - I(M; Y^n) - n\epsilon \\
&= \sum_{i=1}^{n} I(M; X_i|X^{i-1}, Y_{i+1}^n) - I(M; Y_i|X^{i-1}, Y_{i+1}^n) - n\epsilon \\
&= \sum_{i=1}^{n} I(M, X^{i-1}, Y_{i+1}^n; X_i) - I(M, X^{i-1}, Y_{i+1}^n; Y_i) - n\epsilon \\
&= \sum_{i=1}^{n} I(U_i; X_i) - I(U_i; Y_i) - n\epsilon \\
&= n\sum_{i=1}^{n} \frac{1}{n}[I(U_i; X_i|J=i) - I(U_i; Y_i|J=i)] - n\epsilon \\
&= n[I(U; X) - I(U; Y)] - n\epsilon, \qquad \text{(C.2)}
\end{aligned}$$

in which J is a random variable uniformly distributed over $[1:n]$, $U_i := (M, X^{i-1}, Y_{i+1}^n)$ and $U := (U_J, J)$. And from (C.2), we also obtain

$$\begin{aligned}
\Delta_2 &\leq \frac{1}{n}H(X^n|M) + \epsilon \\
&= \frac{1}{n}(H(X^n) - I(X^n; M)) + \epsilon \\
&\leq H(X) - [I(U; X) - I(U; Y)] + 2\epsilon \\
&= H(X|U) + I(U; Y) + 2\epsilon.
\end{aligned}$$

In addition, we can easily verify that $(M, X^{J-1}, Y_{J+1}^n) \to X_J \to Y_J$, thus it follows that $U \to X \to Y$.

Furthermore, according to Fano's Inequality, we have

$$n\epsilon \geq H(\mathbf{f}|\hat{\mathbf{f}})$$

$$\begin{aligned}
&\geq H(f^n|\hat{\mathbf{f}}, M, Y^n) \\
&= H(f^n|M, Y^n) \\
&= \sum_{i=1}^{n} H(f_i|f^{i-1}, M, Y^n) \\
&\geq \sum_{i=1}^{n} H(f_i|f^{i-1}, M, Y^n, X^{i-1}) \\
&\overset{(a)}{=} \sum_{i=1}^{n} H(f_i|M, Y^n, X^{i-1}) \\
&\overset{(b)}{=} \sum_{i=1}^{n} H(f_i|Y_i, M, Y_{i+1}^n, X^{i-1}) \\
&= \sum_{i=1}^{n} H(f_i|Y_i, U_i) \\
&= nH(f|Y, U),
\end{aligned} \tag{C.3}$$

where step (a) is true since f^{i-1} is a function of (X^{i-1}, Y^{i-1}), and step (b) follows from the Markov chain $f_i \to (Y_i, Y_{i+1}^n, X^{i-1}, M) \to Y^{i-1}$, which is indicated by

$$\begin{aligned}
& (X^n, Y_i^n) \to X^{i-1} \to Y^{i-1}, \\
\Rightarrow \quad & (M, X_i, Y_i^n) \to X^{i-1} \to Y^{i-1}, \\
\overset{(a)}{\Rightarrow} \quad & (X_i, Y_i) \to (M, Y_{i+1}^n, X^{i-1}) \to Y^{i-1},
\end{aligned} \tag{C.4}$$

in which (a) is due to the weak union property of the Markov chain [101]. Eq. (C.3) indicates that this particular choice of U is admissible w.r.t. X, Y and f.

Finally, we have

$$\begin{aligned}
n\Delta_1 &\geq I(X^n; M|Y^n) - n\epsilon \\
&= H(X^n|Y^n) - H(X^n|M, Y^n) - n\epsilon \\
&= nH(X|Y) - H(X^n|M, Y^n) - n\epsilon \\
&= nH(X|Y) - \sum_{i=1}^{n} H(X_i|M, Y^n, X^{i-1}) - n\epsilon
\end{aligned}$$

$$
\begin{aligned}
&\overset{(a)}{=} nH(X|Y) - \sum_{i=1}^{n} H(X_i|Y_i, M, Y_{i+1}^n, X^{i-1}) - 2n\epsilon \\
&= nH(X|Y) - \sum_{i=1}^{n} H(X_i|Y_i, U_i) - n\epsilon \\
&= nH(X|Y) - nH(X|Y, U) - n\epsilon \\
&= nI(X; U|Y) - n\epsilon, \qquad \text{(C.5)}
\end{aligned}
$$

where step (a) follows from the Markov chain defined in (C.4).

As ϵ is an arbitrarily small number, we conclude that the converse is complete.

C.2 Proof of Theorem 5.2

Achievability:

Given PMF $P_{XYZ}P_{U|X}P_{V|U}$ with U being admissible, the case when $I(Y; U|V) - I(Z; U|V) \leq 0$ is trivial since we can use the same scheme as stated in the achievability proof of Theorem 5.1, and under this scheme, we can show that $\Delta_2 = I(X; U, Z) + \epsilon$ is achievable. Thus, without loss of generality, we assume that $I(Y; U|V) - I(Z; U|V) > 0$. We will show that the tuple (R, Δ_1, Δ_2) with

$$
\begin{aligned}
&R = I(X; U) - I(Y; U) + 2\epsilon, \\
&\Delta_1 = I(X; U|Y) + \epsilon, \\
&\Delta_2 = H(X|U, Z) + [I(Y; U|V) - I(Z; U|V)] - 2\epsilon,
\end{aligned}
$$

is achievable.

(1) **Codebook $\mathcal{C}$ construction:** Randomly and independently generate 2^{nR_0} sequences V^n according to $\prod_{i=1}^{n} P_V(v_i)$, and assign each V^n into 2^{R_1} bins which are indexed by M', using a uniform distribution. We use $b(M')$ to denote bin M'; For each generated sequence V^n, randomly and independently generate 2^{nR_2} sequence U^n according

to $\prod_{i=1}^{n} P_{U|V}(u_i|v_i)$, and assign each U^n into 2^{nR_3} bins indexed by M'', using a uniform distribution. We use $b_{V^n}(M'')$ to denote the corresponding bin of sequences U^n. Besides, we set

$$\begin{aligned}
R_0 &= I(X;V) + \epsilon,\\
R_1 &= I(X;V) - I(Y;V) + 2\epsilon,\\
R_2 &= I(X;U|V) + \epsilon;\\
R_3 &= I(X;U|V) - I(Y;U|V) + 2\epsilon.
\end{aligned}$$

(2) **Encoding:** Upon observing a sequence X^n, Alice looks into the generated codebook trying to find a V^n which is joint P_{VX}-typical with X^n. After selecting V^n, Alice looks into those sequences U^n that are generated by V^n, trying to find a U^n that is joint P_{UVX}-typical with (V^n, X^n). During this process, if there are more than one such V^n or U^n, she randomly picks up one such sequence; if there is no such sequence, she declares an error. If Alice finds, she sends the bin indices, M' and M'', of V^n and U^n to the fusion center.

(3) **Decoding:** After receiving (M', M''), the fusion center first looks into $b(M')$ trying to find a unique $\hat{V}^n$ that is joint P_{VY}-typical with Y^n. Then, it looks into $b_{\hat{V}^n}(M'')$ trying to find a unique $\hat{U}^n$ that is joint P_{VUY}-typical with $(\hat{V}^n, Y^n)$. If there are more than one or no such sequence $\hat{V}^n(\hat{U}^n)$, it randomly selects a $\hat{U}^n$ as the decoded sequence.

(4) **Function computing:** The fusion center computes the estimated value $\hat{\mathbf{f}} := \{g(\hat{U}_i, Y_i)\}_{i=1}^{n}$.

(5) **Error analysis:** Similar as the analysis in the previous scheme, the error is upper bounded by

$$\text{Pr}\{\text{No jointly typical } U^n \text{ is found}\} + \text{Pr}\{\hat{U}^n \neq U^n\}.$$

Following the previous analysis, we can first obtain that there exists a V^n that is jointly typical with X^n and it can be correctly decoded. Then we can easily obtain that there exists a U^n which is generated by V^n and it is joinly typical with X^n using the Covering lemma, since there are $2^{n(I(X;U|V)+\epsilon)}$ sequences U^n. After that, we can also show that there is no other sequence jointly typical with (V^n, Y^n) (thus U^n is correctly decoded) using the Packing lemma, since there are $2^{n(I(Y;U|V)-\epsilon)}$ sequences in $b_{V^n}(M'')$.

(6) **Message rate**: The transmitted messages are (M', M''), thus, the rate is $I(X;V) - I(Y;V) + 2\epsilon + I(X;U|V) - I(Y;U|V) + 2\epsilon = I(X;U) - I(Y;U) + 4\epsilon$.

(7) **Privacy leakage:** Similar to that of the proof of Theorem 5.1, we can obtain

$$I(X^n; M', M''|Y^n, \mathcal{C}) \leq nI(X;U|Y) + n\epsilon.$$

Now we bound $I(X^n; M', M'', Z^n|\mathcal{C})$ as follows

$$\begin{aligned}
&I(X^n; M', M'', Z^n|\mathcal{C}) \\
&\quad \leq I(X^n; V^n, M'', Z^n|\mathcal{C}) \\
&\quad = H(X^n|\mathcal{C}) - H(X^n|V^n, M'', Z^n, \mathcal{C}) \\
&\quad = nH(X) - H(X^n, U^n|V^n, M'', Z^n, \mathcal{C}) + H(U^n|X^n, V^n, M'', Z^n, \mathcal{C}) \\
&\quad \overset{(a)}{\leq} nH(X) - H(X^n, U^n|V^n, M'', Z^n, \mathcal{C}) + n\epsilon \\
&\quad = nH(X) - H(U^n|V^n, Z^n, M'', \mathcal{C}) - H(X^n|Z^n, U^n, V^n, M'', \mathcal{C}) + n\epsilon \\
&\quad = nH(X) - H(U^n|V^n, Z^n, M'', \mathcal{C}) - H(X^n|Z^n, U^n, V^n, \mathcal{C}) + n\epsilon \\
&\quad \overset{(c)}{\leq} nI(X; Z, U) - H(U^n|V^n, Z^n, M'', \mathcal{C}) + 2n\epsilon \\
&\quad = nI(X; Z, U) - H(U^n|V^n, Z^n, \mathcal{C}) + I(U^n; M''|V^n, Z^n, \mathcal{C}) + 2n\epsilon,
\end{aligned}$$

where step (a) is true due to the fact that given V^n and M'', there are $2^{n(I(Y;U|V)-\epsilon)}$ sequences U^n in $b_{V^n}(M'')$, and the probability that there exists another $\bar{U}^n$ that is jointly typical with (X^n, V^n) is upper bounded by $2^{-n(I(X;U|V)-I(Y;U|V))} < \epsilon$, thus, it is easy to have

$$H(U^n|V^n, Z^n, M'', \mathcal{C}) \leq n\epsilon.$$

And step (c) follows from Lemma C.2 in the Appendix C.6. According to Lemma C.3 in the Appendix C.6, we have

$$H(U^n|V^n, Z^n, \mathcal{C}) \geq n(I(X;U|V) - I(Z;U|V)) - \epsilon.$$

On the other hand, we have that

$$\begin{aligned}
&I(U^n; M''|V^n, Z^n, \mathcal{C}) \\
&= H(M''|V^n, Z^n, \mathcal{C}) - H(M''|U^n, V^n, Z^n, \mathcal{C}) \\
&\leq H(M''|\mathcal{C}) \\
&= nI(X;U|V) - nI(Y;U|V) + 2n\epsilon.
\end{aligned}$$

Thus, we have that

$$\frac{1}{n} I(X^n; M', M'', Z^n|\mathcal{C}) \leq I(X; Z, U) - [I(Y;U|V) - I(Z;U|V)] + 5\epsilon,$$

which indicates that $\frac{1}{n}H(X^n|M', M'', Z^n, \mathcal{C}) \geq H(X; Z, U) + [I(Y;U|V) - I(Z;U|V)] - 5\epsilon$.

Hence, the achievability proof is complete.

Converse:

Similar to the converse proof of Theorem 5.1, we only need to show that any achievable tuple (R, Δ_1, Δ_2) is contained in $\mathcal{S}$, i.e. there exists some admissible U w.r.t. X, Y and f, as well as a random variable V, such that (5.11), (5.12), (5.13) and (5.14) hold.

As the first step, we have, according to (C.2), that

$$nR \geq \sum_{i=1}^{n} I(M, X^{i-1}, Y_{i+1}^{n}; X_i) - I(M, X^{i-1}, Y_{i+1}^{n}; Y_i) - n\epsilon.$$

On the other hand, the following Markov chains are true,

$$\begin{aligned} &X_i \to (M, X^{i-1}, Y_{i+1}^{n}) \to Z^{i-1}, \\ &Y_i \to (M, X^{i-1}, Y_{i+1}^{n}) \to Z^{i-1}, \end{aligned}$$

which are implied by

$$\begin{aligned} & (Y_i^n, X^n) \to X^{i-1} \to Z^{i-1}, \\ \Rightarrow\quad & (M, X_i, Y_i^n) \to X^{i-1} \to Z^{i-1}, \\ \Rightarrow\quad & (X_i, Y_i) \to (M, X^{i-1}, Y_{i+1}^{n}) \to Z^{i-1}. \end{aligned} \tag{C.6}$$

Thus, it follows that

$$\begin{aligned} nR &\geq \sum_{i=1}^{n} I(M, X^{i-1}, Y_{i+1}^{n}, Z^{i-1}; X_i) - I(M, X^{i-1}, Y_{i+1}^{n}, Z^{i-1}; Y_i) - n\epsilon \\ &= \sum_{i=1}^{n} I(U_i; X_i) - I(U_i; Y_i) - n\epsilon \\ &= n[I(U; X) - I(U; Y) - n\epsilon, \end{aligned} \tag{C.7}$$

in which U_i and U are defined by $U_i := (M, X^{i-1}, Y_{i+1}^{n}, Z^{i-1})$ and $U := (U_J, J)$, J is a independent random variable uniformly distributed over $[1 : n]$. And we can also verify that $U \to X \to Y$ holds.

Furthermore, following similar steps as that in (C.3), we conclude that

$$n\epsilon \geq \sum_{i=1}^{n} H(f_i | Y_i, M, Y_{i+1}^{n}, X^{i-1})$$

$$
\begin{aligned}
&\geq \sum_{i=1}^{n} H(f_i|Y_i, M, Y_{i+1}^n, X^{i-1}, Z^{i-1}) \\
&= \sum_{i=1}^{n} H(f_i|Y_i, U_i) \\
&= nH(f|Y, U).
\end{aligned}
\tag{C.8}
$$

Thus, we can claim that this constructed random variable U is admissible w.r.t. X, Y and f.

Furthermore, as (C.6) implies that the following Markov chain holds

$$
X_i \to (Y_i, M, X^{i-1}, Y_{i+1}^n) \to Z^{i-1},
$$

we have, according to (C.5), that

$$
\begin{aligned}
n\Delta_1 &\geq nH(X|Y) - \sum_{i=1}^{n} H(X_i|Y_i, M, Y_{i+1}^n, X^{i-1}) - n\epsilon \\
&= nH(X|Y) - \sum_{i=1}^{n} H(X_i|Y_i, M, Y_{i+1}^n, X^{i-1}, Z^{i-1}) - n\epsilon \\
&= nH(X|Y) - nH(X|Y, U) - n\epsilon \\
&= nI(X; U|Y) - n\epsilon.
\end{aligned}
\tag{C.9}
$$

As the final step, we now show (5.14). It follows that

$$
\begin{aligned}
&I(X^n; M, Z^n) \\
&\quad = I(M; X^n) + I(X^n; Z^n|M) \\
&\quad = I(M; X^n) - I(M; Y^n) + I(M; Y^n) - I(M; Z^n) + I(M; Z^n) + I(X^n; Z^n|M) \\
&\quad = I(M; X^n) - I(M; Y^n) + I(M; Y^n) - I(M; Z^n) + I(M, X^n; Z^n) \\
&\quad = I(M; X^n) - I(M; Y^n) + I(M; Y^n) - I(M; Z^n) + I(X^n; Z^n) \\
&\quad = I(M; X^n) - I(M; Y^n) + I(M; Y^n) - I(M; Z^n) + nI(X; Z).
\end{aligned}
\tag{C.10}
$$

In the right-hand side of (C.10), we have

$$\begin{aligned}
I(M;X^n)-I(M;Y^n) &= \sum_{i=1}^{n} I(M;X_i|X^{i-1},Y_{i+1}^n)-I(M;Y_i|X^{i-1},Y_{i+1}^n)\\
&= \sum_{i=1}^{n} I(M,X^{i-1},Y_{i+1}^n;X_i)-I(M,X^{i-1},Y_{i+1}^n;Y_i)\\
&= \sum_{i=1}^{n} I(M,X^{i-1},Y_{i+1}^n,Z^{i-1};X_i)-I(M,X^{i-1},Y_{i+1}^n,Z^{i-1};Y_i)\\
&= n[I(U;X)-I(U;Y)], \qquad \text{(C.11)}
\end{aligned}$$

and

$$\begin{aligned}
I(M;Y^n)-I(M;Z^n) &= \sum_{i=1}^{n} I(M;Y_i|Z^{i-1},Y_{i+1}^n)-I(M;Z_i|Z^{i-1},Y_{i+1}^n)\\
&= \sum_{i=1}^{n} I(M,Z^{i-1},Y_{i+1}^n;Y_i)-I(M,Z^{i-1},Y_{i+1}^n;Z_i)\\
&= \sum_{i=1}^{n} I(V_i;Y_i)-I(V_i;Z_i)\\
&= n[I(V;Y)-I(V;Z)], \qquad \text{(C.12)}
\end{aligned}$$

in which $V_i := (M,Y_{i+1}^n,Z^{i-1})$ and $V := (U_J,J)$, J is a independent random variable uniformly distributed over $[1:n]$. For this construction of V, we can conclude that $V \to U \to X \to (Y,Z)$ is true. Thus, it follows that

$$\begin{aligned}
I(X^n;M,Z^n) &= I(U;X)-I(U;Y)+I(V;Y)-I(V;Z)+I(X;Z)\\
&= I(U;X)-I(U;Y|V)-I(V;Z)+I(X;Z)\\
&= I(U;X)-I(U;Y|V)+I(X;Z|V)\\
&= I(U;X)-I(U;Y|V)+I(U,X;Z|V)\\
&= I(U;X)-I(U;Y|V)+I(U;Z|V)+I(X;Z|U,V)\\
&= I(U;X)-I(U;Y|V)+I(U;Z|V)+I(X;Z|U)
\end{aligned}$$

$$
\begin{aligned}
&= I(X;U,Z) - I(U;Y|V) + I(U;Z|V) \\
&\geq I(X;U,Z) - [I(U;Y|V) - I(U;Z|V)]^{+},
\end{aligned}
$$

which implies that

$$
\begin{aligned}
\Delta_2 &\leq \frac{1}{n} H(X^n|M,Z^n) + \epsilon \\
&= \frac{1}{n}(H(X^n) - I(X^n;M,Z^n)) + \epsilon \\
&\leq H(X) - I(X;U,Z) + [I(U;Y|V) - I(U;Z|V)]^{+} + \epsilon \\
&= H(X|U,Z) + [I(U;Y|V) - I(U;Z|V)]^{+} + \epsilon. \qquad \text{(C.13)}
\end{aligned}
$$

Hence, the converse is complete.

C.3 Proof of Theorem 5.4

Converse:

In this part, we show that any achievable tuple $(R, D, \Delta_1, \Delta_2)$ is contained in the region defined by (5.18)-(5.22).

First, according to (5.3), we have that

$$
\begin{aligned}
nR &\geq H(M) - \epsilon \\
&\geq I(M;X^n) - I(M;Y^n) - \epsilon \\
&= \sum_{i=1}^{n} \left[I(M;X_i|X^{i-1},Y_{i+1}^{n}) - I(M;Y_i|X^{i-1},Y_{i+1}^{n}) \right] - \epsilon \\
&= \sum_{i=1}^{n} \left[I(M,X^{i-1},Y_{i+1}^{n};X_i) - I(M,X^{i-1},Y_{i+1}^{n};Y_i) \right] - \epsilon \\
&\overset{(a)}{=} \sum_{i=1}^{n} \left[I(M,X^{i-1},Y_{i+1}^{n},Y^{i-1},Z^{i-1};X_i) - I(M,X^{i-1},Y_{i+1}^{n},Y^{i-1},Z^{i-1};Y_i) \right] - \epsilon
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} \left[I(U_i; X_i) - I(U_i; Y_i) \right] - \epsilon \\
&= n \left[I(U; X) - I(U; Y) \right] - \epsilon,
\end{aligned}
\tag{C.14}
$$

where step (a) follows from the following Markov chain

$$
(X_i, Y_i) \to (M, X^{i-1}, Y_{i+1}^{n}) \to (Y^{i-1}, Z^{i-1}),
\tag{C.15}
$$

which is implied by the following Markov chain

$$
(X^n, Y_i^n) \to (X^{i-1}) \to (Y^{i-1}, Z^{i-1}).
$$

Furthermore, U_i is defined as

$$
U_i := (M, X^{i-1}, Y_{i+1}^{n}, Y^{i-1}, Z^{i-1}),
$$

and we have $U_i \to X_i \to (Y_i, Z_i)$, which follows from

$$
\begin{aligned}
& (X^n, Y^{i-1}, Y_{i+1}^{n}, Z^{i-1}) \to X_i \to (Y_i, Z_i) \\
\Rightarrow \; & (M, X^{i-1}, Y_{i+1}^{n}, Y^{i-1}, Z^{i-1}) \to X_i \to (Y_i, Z_i).
\end{aligned}
\tag{C.16}
$$

Second, it follows from (5.2) that

$$
\begin{aligned}
D &\geq \frac{1}{n} E \left[d(\mathbf{f}(X^n, Y^n), \hat{\mathbf{f}}(M, Y^n)) \right] - \epsilon \\
&= \frac{1}{n} E \left[\sum_{i=1}^{n} d(f(X_i, Y_i), \hat{f}_i(M, Y^n)) \right] - \epsilon \\
&\overset{(a)}{\geq} \frac{1}{n} E \left[\sum_{i=1}^{n} d(f(X_i, Y_i), g(M, Y^n, X^{i-1}, Z^{i-1})) \right] - \epsilon \\
&= \frac{1}{n} E \left[\sum_{i=1}^{n} d(f(X_i, Y_i), g(U_i, Y_i)) \right] - \epsilon
\end{aligned}
$$

$$
\begin{aligned}
&= E\left[\sum_{i=1}^{n} \frac{1}{n} d(f(X_i,Y_i),g(U_i,Y_i))\right] - \epsilon \\
&= E\left[d(f(X,Y),g(U,Y))\right] - \epsilon,
\end{aligned}
$$

where step (a) is due to the fact that since $\hat{f}_i(M,Y^n)$ is a function of M and Y^n in general, there must exist some function, say g, such that the distortion decreases since more information is provided for each $i \in [1:n]$.

In addition, we have

$$
\begin{aligned}
n\Delta_1 &\geq I(X^n;M|Y^n) - n\epsilon \\
&= H(X^n|Y^n) - H(X^n|M,Y^n) - n\epsilon \\
&= nH(X|Y) - \sum_{i=1}^{n} H(X_i|M,Y^n,X^{i-1}) - n\epsilon \\
&\overset{(a)}{=} nH(X|Y) - \sum_{i=1}^{n} H(X_i|M,Y^n,X^{i-1},Z^{i-1}) - 2n\epsilon \\
&=nH(X|Y) - \sum_{i=1}^{n} H(X_i|Y_i,U_i) - n\epsilon \\
&=nH(X|Y) - nH(X|Y,U) - n\epsilon \\
&=nI(X;U|Y) - n\epsilon, \qquad \text{(C.17)}
\end{aligned}
$$

in which step (a) is true due to the following Markov chain

$$X_i \to (M,Y^n,X^{i-1}) \to Z^{i-1},$$

which is implied by (C.15) due to the decomposition property of Markov chain [101].

As the final step, the derivation is similar as the procedure from (C.10) to (C.13).

First, we have

$$I(X^n;M,Z^n) = I(M;X^n) - I(M;Y^n) + I(M;Y^n) - I(M;Z^n) + nI(X;Z). \qquad \text{(C.18)}$$

Furthermore, it follows from (C.14) that

$$I(M;X^n)-I(M;Y^n)=n[I(U;X)-I(U;Y)], \tag{C.19}$$

while

$$\begin{aligned} I(M;Y^n)-I(M;Z^n) &= \sum_{i=1}^{n} I(M;Y_i|Z^{i-1},Y_{i+1}^n)-I(M;Z_i|Z^{i-1},Y_{i+1}^n) \\ &= \sum_{i=1}^{n} I(V_i;Y_i)-I(V_i;Z_i) \\ &= n[I(V;Y)-I(V;Z)], \end{aligned} \tag{C.20}$$

with $V_i := (M, Y_{i+1}^n, Z^{i-1})$ and $V := (U_J, J)$, J is a independent random variable uniformly distributed over $[1:n]$. Based on the definition of U and V stated above, it's not difficult to obtain this Markov chain: $V \to U \to X \to (Y,Z)$ based on (C.16). Combine (C.18)-(C.20), and we have

$$\begin{aligned} I(X^n;M,Z^n) &= I(U;X)-I(U;Y)+I(V;Y)-I(V;Z)+I(X;Z) \\ &= I(X;U,Z)-I(U;Y|V)+I(U;Z|V) \\ &\geq I(X;U,Z)-[I(U;Y|V)-I(U;Z|V)]^+. \end{aligned}$$

Finally, we obtain

$$\begin{aligned} \Delta_2 &\leq \frac{1}{n}H(X^n|M,Z^n)+\epsilon \\ &= \frac{1}{n}(H(X^n)-I(X^n;M,Z^n))+\epsilon \\ &\leq H(X)-I(X;U,Z)+[I(U;Y|V)-I(U;Z|V)]^+ +\epsilon \\ &= H(X|U,Z)+[I(U;Y|V)-I(U;Z|V)]^+ +\epsilon. \end{aligned} \tag{C.21}$$

Hence, the converse proof is complete.

Achievability:

To prove the achievability for Theorem 5.4, we use the same achievability scheme as stated in the proof for Theorem 5.2. The only difference is the range of PMF $P_{XYZ}P_{U|X}P_{V|U}$. In this scheme, $P_{XYZ}P_{U|X}P_{V|U}$ is given, subject to that there exist a function g of (U,Y) achieving $E(d(f(X,Y),g(U,Y))) \leq D+\epsilon$ and the function g is fixed for function computing. Once $P_{XYZ}P_{U|X}P_{V|U}$ and g is fixed, we can follow the same procedures in the proof of Theorem 5.2 to obtain the desired result.

C.4 Proof of Theorem 5.6

Converse:

In the following, we define

$$\begin{aligned} U_{1i} &:= (M_1, X_1^{i-1}, Z^{i-1}, Y_{i+1}^n), V_{1i} := (M_1, Z^{i-1}, Y_{i+1}^n), \\ U_{2i} &:= (M_2, X_2^{i-1}, Z^{i-1}, Y_{i+1}^n), V_{2i} := (M_2, Z^{i-1}, Y_{i+1}^n). \end{aligned}$$

Furthermore, define $U_1 := (U_{1J}, J)$ with J being a random variable independent with all other random variables and uniformly distributed over $[1:n]$. Define V_1, U_2 and V_2 in the same manner. We can verify that the Markov chain $V_1 \to U_1 \to X_1 \to (X_2, Y, Z)$ holds, as we have

$$\begin{aligned} & (X_1^n, Z^{i-1}, Y_{i+1}^n) \to X_{1i} \to (X_{2i}, Y_i, Z_i) \\ \Rightarrow \quad & (M_1, X_1^{i-1}, Z^{i-1}, Y_{i+1}^n) \to X_{1i} \to (X_{2i}, Y_i, Z_i). \end{aligned}$$

Similarly, we can verify that $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$ holds.

In the following, we show (5.29)-(5.34) one by one. First, we have

$$
\begin{aligned}
nR_1 &\geq H(M_1) - n\epsilon \\
&\geq I(M_1; X_1^n) - I(M_1; Y^n) - n\epsilon \\
&= \sum_{i=1}^{n} [I(M_1; X_{1i}|X_1^{i-1}, Y_{i+1}^n) - I(M_1; Y_i|X_1^{i-1}, Y_{i+1}^n)] - n\epsilon \\
&= \sum_{i=1}^{n} [I(M_1, X_1^{i-1}, Y_{i+1}^n; X_{1i}) - I(M_1, X_1^{i-1}, Y_{i+1}^n; Y_i)] - n\epsilon \\
&= \sum_{i=1}^{n} [I(M_1, X_1^{i-1}, Z^{i-1}, Y_{i+1}^n; X_{1i}) - I(M_1, X_1^{i-1}, Z^{i-1}, Y_{i+1}^n; Y_i)] - n\epsilon \\
&= \sum_{i=1}^{n} [I(U_{1i}; X_{1i}) - I(U_{1i}; Y_i)] - n\epsilon \\
&= n[I(U_1; X_1) - I(U_1; Y)] - n\epsilon \\
&= n[I(U_1; X_1|Y) - n\epsilon \\
&= I(V_1; X_1|Y) + I(U_1; X_1|Y, V_1) - n\epsilon, \\
&= I(V_1;X_1,V_2|Y) - I(V_1;V_2|Y,X_1) + I(U_1;X_1,U_2|Y,V_1) - I(U_1;U_2|X_1,Y,V_1) - n\epsilon, \\
&\geq I(V_1;X_1|Y,V_2) + I(U_1;X_1|Y,U_2,V_1) - I(V_1;V_2|Y,X_1) - I(U_1;U_2|X_1,Y,V_1) - n\epsilon.
\end{aligned}
$$

Thus, we have

$$
R_1 \geq I(V_1;X_1|Y,V_2) + I(U_1;X_1|Y,U_2,V_1) - I(V_1;V_2|Y,X_1) - I(U_1;U_2|X_1,Y,V_1) - \epsilon.
$$

Similarly, we have

$$
R_1 + R_2 \geq I(V_1;X_1|Y) + I(V_2;X_2|Y,V_1) + I(U_1;X_1|Y,V_1,V_2) + I(U_2;X_2|Y,U_1,V_2) - \epsilon.
$$

In addition, it follows that

$$
R_1 + R_2 \geq \frac{1}{n} H(M_1) - \epsilon + \frac{1}{n} H(M_2) - \epsilon
$$

$$
\begin{aligned}
&\geq \frac{1}{n}H(M_1, M_2) - 2\epsilon \\
&\geq \frac{1}{n}I(M_1, M_2; X_1^n, X_2^n) - \frac{1}{n}I(M_1, M_2; Y^n) - 2n\epsilon \\
&= \frac{1}{n}\sum_{i=1}^{n}[I(M_1, M_2; X_{1i}, X_{2i}|X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n) + I(M_1, M_2; Y_i|X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n)] - 2n\epsilon \\
&= \frac{1}{n}\sum_{i=1}^{n}[I(M_1, M_2, X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n; X_{1i}, X_{2i}) + I(M_1, M_2, X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n; Y_i)] - 2n\epsilon \\
&= \frac{1}{n}\sum_{i=1}^{n}[I(M_1,M_2,X_1^{i-1},X_2^{i-1},Z^{i-1},Y_{i+1}^n;X_{1i},X_{2i}) + I(M_1,M_2,X_1^{i-1},X_2^{i-1},Z^{i-1},Y_{i+1}^n;Y_i)] - 2n\epsilon \\
&= I(U_1, U_2; X_1, X_2) - I(U_1, U_2; Y) - 2\epsilon \\
&= I(U_1, U_2; X_1, X_2|Y, V_1, V_2) - I(V_1, V_2; X_1, X_2|Y) - 2\epsilon \\
&= I(V_1;X_1,X_2|Y) + I(V_2;X_1,X_2|Y,V_1) + I(U_1;X_1,X_2|Y,V_1,V_2) + I(U_2;X_1,X_2|Y,U_1,V_2) - 2\epsilon \\
&\geq I(V_1; X_1|Y) + I(V_2; X_2|Y, V_1) + I(U_1; X_1|Y, V_1, V_2) + I(U_2; X_2|Y, U_1, V_2) - 2\epsilon.
\end{aligned}
$$

Furthermore, we have

$$
\begin{aligned}
n\Delta_1 &\geq I(X_1^n, X_2^n; M_1, M_2|Y^n) - n\epsilon \\
&= H(X_1^n, X_2^n|Y^n) - H(X_1^n, X_2^n|M_1, M_2, Y^n) - n\epsilon \\
&= nH(X_1, X_2|Y) - H(X_1^n, X_2^n|M_1, M_2, Y^n) - n\epsilon \\
&= nH(X_1, X_2|Y) - \sum_{i=1}^{n} H\Big(X_{1i}, X_{2i}\big|M_1, M_2, Y^n, X_1^{i-1}, X_2^{i-1}\Big) - n\epsilon \\
&\overset{(a)}{=} nH(X_1, X_2|Y) - \sum_{i=1}^{n} H\Big(X_{1i}, X_{2i}\big|M_1, M_2, Y_{i+1}^n, Z^{i-1}, X_1^{i-1}, X_2^{i-1}\Big) - n\epsilon \\
&= nH(X_1, X_2|Y) - \sum_{i=1}^{n} H(X_{1i}, X_{2i}\big|Y_i, U_{1i}, U_{2i}) - n\epsilon \\
&= nH(X_1, X_2|Y) - nH(X_1, X_2|Y, U_1, U_2) - n\epsilon \\
&= nI(X_1, X_2; U_1, U_2|Y) - n\epsilon, \qquad \text{(C.22)}
\end{aligned}
$$

in which step (a) is due to the following Markov chain:

$$\big((X_1)_i,(X_2)_i\big) \to \big(M_1,M_2,Y_{i+1}^n,X_1^{i-1},X_2^{i-1}\big) \to \big(Y^{i-1},Z^{i-1}\big).$$

In addition, following similar step from (C.10) to (C.13) by replacing X with (X_1, X_2), U with (U_1, U_2), V with (V_1, V_2) and M with (M_1, M_2), we can obtain

$$\Delta_2 \leq H(X_1, X_2|U_1, U_2, Z) + \big[I(U_1, U_2; Y|V_1, V_2) - I(U_1, U_2; Z|V_1, V_2)\big]^+ + \epsilon. \quad \text{(C.23)}$$

As the last step, it follows that

$$\begin{aligned}
n\epsilon &\geq H(f^n|M_1, M_2, Y^n) \\
&= \sum_{i=1}^n H(f_i|f^{i-1}, M_1, M_2, Y^n) \\
&\geq \sum_{i=1}^n H(f_i|f^{i-1}, M_1, M_2, Y^n, X_1^{i-1}, X_2^{i-1}, Z^{i-1}) \\
&\geq \sum_{i=1}^n H(f_i|M_1, M_2, Y^n, X_1^{i-1}, X_2^{i-1}, Z^{i-1}) \\
&= \sum_{i=1}^n H(f_i|M_1, M_2, Y_i^n, X_1^{i-1}, X_2^{i-1}, Z^{i-1}) \\
&= \sum_{i=1}^n H(f_i|Y_i, U_{1i}, U_{2i}) \\
&= nH(f|Y, U_1, U_2). \qquad \text{(C.24)}
\end{aligned}$$

Finally, the fact that ϵ is arbitrarily small number completes the converse proof.

Achievability:

In this part, we show that given any $P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$ with $H(f|U_1, U_2, Y) = 0$, any tuple $(R_1, R_2, \Delta_1, \Delta_2)$ satisfying the conditions from (5.29) to (5.34) is achievable. Since given $P_{U_1V_1U_2V_2X_1X_2YZ}$, the values of the right-hand side of

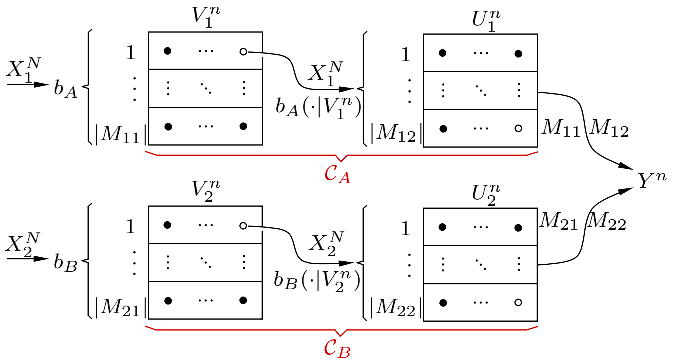


Figure C.1: Encoding scheme.

(5.32) and (5.33) are fixed, it suffices to consider the corner point with

$$R_1 = I(V_1; X_1|Y) + I(U_1; X_1|Y, V_1, V_2),$$

$$R_2 = I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2),$$

and the other corner point with

$$R_1 = I(V_1; X_1|Y, V_2) + I(U_1; X_1|Y, U_2, V_1),$$

$$R_2 = I(V_2; X_2|Y) + I(U_2; X_2|Y, V_1, V_2),$$

and at corner point, we need to guarantee that $\Delta_1 \leq I(X_1, X_2; U_1, U_2|Y) + \epsilon$ and $\Delta_2 \geq H(X_1, X_2|U_1, U_2, Z) + [I(U_1, U_2; Y|V_1, V_2) - I(U_1, U_2; Z|V_1, V_2)]^+ - \epsilon$. Due to the symmetry of the above two corner points, we only consider the former one.

(1) **Codebook $\mathcal{C}$ construction:**

$\mathcal{C}_A$ at Alice. Given $P_{X_1X_2YZ}\ P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$, randomly and independently generate $2^{nR_{10}}$ sequences V_1^n according to $\prod_{i=1}^{n} P_{V_1}(v_{1i})$, and assign each V_1^n into $2^{nR_{11}}$ bins (indexed by M_{11}) using a uniform distribution. For each generated sequence V_1^n

generate $2^{nR_{12}}$ sequences U_1^n according to $\prod_{i=1}^{n} P_{U_1|V_1}(u_{1i}|v_{1i})$ and assign each U_1^n into $2^{nR_{13}}$ sub-bins indexed by M_{12}, using a similar manner as above. In addition, we use $b_A(M_{11})$ and $b_A(M_{12}|V_1^n)$ to denote the corresponding bin and sub-bin indexed by M_{11} and M_{12} respectively, and set

$$\begin{aligned}
R_{10} &= I(V_1; X_1) + \epsilon, \\
R_{11} &= I(V_1; X_1) - I(V_1; Y) + 2\epsilon, \\
R_{12} &= I(U_1; X_1|V_1) + \epsilon, \\
R_{13} &= I(U_1; X_1|V_1) - I(U_1; Y, V_2|V_1) + 2\epsilon.
\end{aligned}$$

$\mathcal{C}_B$ at Bob. Similar to $\mathcal{C}_A$, generate $2^{nR_{20}}$ sequences V_2^n according to $\prod_{i=1}^{n} P_{V_2}(v_{2i})$, and assign these sequences into $2^{nR_{21}}$ bins indexed by M_{21}; For each V_2^n, generated $2^{nR_{22}}$ sequences U_2^n and assign each U_2^n into $2^{nR_{23}}$ sub-bins indexed by M_{22}. The bin and sub-bin are denoted by $b_B(M_{21})$ and $b_B(M_{22}|V_2^n)$, respectively, and set

$$\begin{aligned}
R_{20} &= I(V_2; X_2) + \epsilon, \\
R_{21} &= I(V_2; X_2) - I(V_2; YV_1) + 2\epsilon, \\
R_{22} &= I(U_2; X_2|V_2) + \epsilon, \\
R_{23} &= I(U_2; X_2|V_2) - I(U_2; YU_1|V_2) + 2\epsilon.
\end{aligned}$$

(2) **Encoding:** As shown in Fig.C.1, upon observing a sequence X_1^n, Alice looks into $\mathcal{C}_A$ trying to find a V_1^n that is joint $P_{V_1X_1}$-typical with X_1^n. After find the V_1^n, she looks into those sequences U_1^n generated by V_1^n, trying to find a U_1^n that is joint $P_{V_1U_1X_1}$-typical with (V_1^n, X_1^n). In each step, if there are more than one desired sequence, she randomly picks up one; Otherwise, she declares an error if no desired sequence is found. Then, Alice sends the bin index M_{11} of V_1^n and sub-bin index M_{12} of U_1^n to the fusion center.

Similar to the encoding procedures of Alice's side, Bob looks into $\mathcal{C}_B$ to find a V_2^n and a U_2^n, and sends the indices M_{21} and M_{22} to the fusion center.

(3) **Decoding:** After receiving messages M_{11}, M_{12}, M_{21} and M_{22}, the fusion center first looks into bin $b_A(M_{11})$, trying to find a unique $\hat{V}_1^n$ that is joint P_{V_1Y}-typical with Y^n. If there are more than one such sequence or no such sequence, Bob randomly selects a $\hat{V}_1^n$ as the decoded sequence. Using the same decoding strategy within corresponding bins/sub-bins, it take turns to decode $\hat{V}_2^n$ with $(Y^n, \hat{V}_1^n)$, $\hat{U}_1^n$ with $(Y^n, \hat{V}_1^n, \hat{V}_2^n)$ and $\hat{U}_2^n$ with $(Y^n, \hat{U}_1^n, \hat{V}_2^n)$.

(4) **Function computing:** The fusion center computes the estimated value $\hat{\mathbf{f}}$ based on $(\hat{U}_1^n, \hat{U}_2^n, Y^n)$.

(5) **Error analysis:** Without much modification to Lemma C.1, we can easily obtain that the fusion center can correctly compute $\mathbf{f}$ provided that U_1^n is jointly typical with X_1^n and U_2^n is jointly typical with X_2^n. Thus, the error probability is upper bounded by the two events: 1). (U_1^n, X_1^n) or (U_2^n, X_2^n) are not jointly typical; 2). The fusion center cannot decode (U_1^n, U_2^n) correctly.

First of all, based on the parameters provided in this scheme, we can easily verify that with a high probability, there exists at least one pair (U_1^n, U_2^n) such that (U_1^n, X_1^n) and (U_2^n, X_2^n) are jointly typical respectively. Furthermore, we can easily obtain that the fusion center can correctly decode (U_1^n, U_2^n) with a high probability following the similar analysis in the achievability part in Theorem 5.2. Thus, the fusion center can compute $\mathbf{f}$ with a high probability.

(6) **Message rates:** From the above scheme, we have

$$\begin{aligned}R_1 &= R_{11} + R_{13}\\ &= I(V_1; X_1) - I(V_1; Y) + I(U_1; X_1|V_1) - I(U_1; Y, V_2|V_1) + 4\epsilon\end{aligned}$$

$$= I(V_1; X_1|Y) + I(U_1, X_1|Y, V_1, V_2) + 4\epsilon,$$

and

$$\begin{aligned}
R_2 &= R_{21} + R_{23} \\
&= I(V_2; X_2) - I(V_2; Y, V_1) + I(U_2; X_2|V_2) - I(U_2; Y, U_1|V_2) + 4\epsilon \\
&= I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2) + 4\epsilon.
\end{aligned}$$

(7) **Privacy leakage:** At first, it is easy to obtain that

$$\begin{aligned}
&\frac{1}{n} I(X_1^n, X_2^n; M_{11}, M_{12}, M_{21}, M_{22}|Y^n, \mathcal{C}) \\
&\quad \le H(M_{11}, M_{12}, M_{21}, M_{22}|\mathcal{C}) \\
&\quad = I(V_1; X_1|Y) + I(U_1; X_1|Y, V_1, V_2) + I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2) + 8\epsilon \\
&\quad = I(V_1, V_2; X_1, X_2|Y) + I(U_1, U_2; X_1, X_2|Y, V_1, V_2) + 8\epsilon \\
&\quad = I(X_1, X_2; U_1, U_2|Y) + 8\epsilon.
\end{aligned}$$

Furthermore, we have

$$\begin{aligned}
&H(X_1^n, X_2^n|M_{11}, M_{12}, M_{21}, M_{22}, Z^n, \mathcal{C}) \\
&\ge H(X_1^n, X_2^n|V_1^n, V_2^n, M_{21}, M_{22}, Z^n, \mathcal{C}) \\
&\ge H(X_1^n, X_2^n, U_1^n, U_2^n|V_1^n, V_2^n, M_{21}, M_{22}, Z^n, \mathcal{C}) - n\epsilon \\
&= H(U_1^n, U_2^n|V_1^n, V_2^n, M_{21}, M_{22}, Z^n, \mathcal{C}) + H(X_1^n, X_2^n|U_1^n, U_2^n, V_1^n, V_2^n, M_{21}, M_{22}, Z^n, \mathcal{C}) - n\epsilon \\
&= H(U_1^n, U_2^n|V_1^n, V_2^n, M_{21}, M_{22}, Z^n, \mathcal{C}) + H(X_1^n, X_2^n|U_1^n, U_2^n, V_1^n, V_2^n, Z^n, \mathcal{C}) - n\epsilon \\
&\overset{(a)}{\ge} H(U_1^n, U_2^n|V_1^n, V_2^n, M_{21}, M_{22}, Z^n, \mathcal{C}) + nH(X_1, X_2|U_1, U_2, Z) - 2n\epsilon \\
&= nH(X_1, X_2|U_1, U_2, Z) + H(U_1^n, U_2^n|V_1^n, V_2^n, Z^n, \mathcal{C}) - I(U_1^n, U_2^n; M_{21}, M_{22}|V_1^n, V_2^n, Z^n, \mathcal{C}) - 2n\epsilon \\
&\ge nH(X_1, X_2|U_1, U_2, Z) + H(U_1^n, U_2^n|V_1^n, V_2^n, Z^n, \mathcal{C}) - H(M_{21}, M_{22}) - 2n\epsilon,
\end{aligned}$$

where step (a) can be easily verified following similar arguments that those in the proof of Lemma C.2.

Now, we bound each term above. First, we have

$$\begin{aligned}\frac{1}{n}&H(M_{21}, M_{22}) \leq R_{13} + R_{23}\\&= I(U_1; X_1|V_1) - I(U_1; Y, V_2|V_1) + I(U_2; X_2|V_2) - I(U_2; Y, U_1|V_2) + 4\epsilon\\&= I(U_1; X_1|Y, V_1, V_2) + I(U_2; X_2|Y, U_1, V_2) + 4\epsilon\\&= I(U_1, U_2; X_1, X_2|Y, V_1, V_2) + 4\epsilon.\end{aligned}$$

We bound the term $H(U_1^n, U_2^n|V_1^n, V_2^n, Z^n, \mathcal{C})$ as follows. Given V_1^n, there are $2^{nR_{12}}$ sequences U_1^n that are generated by V_1^n, and the probability of that each U_1^n is jointly typical with (V_1^n, V_2^n, Z^n) is $2^{-nI(U_1;V_2,Z|V_1)}$. Thus, there are around $2^{n(I(U_1;X_1|V_1)-I(U_1;V_2,Z|V_1))}$ sequences U_1^n that are jointly typical with (V_1^n, V_2^n, Z^n). Similarly, for each such U_1^n, there are around $2^{n(I(U_2;X_2|V_2)-I(U_2;U_1,Z|V_2)+\epsilon)}$ sequences U_2^n that are generated by V_2^n and jointly typical with $(U_1^n, V_1^n, V_2^n, Z^n)$. Hence, given (V_1^n, V_2^n, Z^n), there are around $2^{n(I(U_1;X_1|V_1)-I(U_1;V_2,Z|V_1)+I(U_2;X_2|V_2)-I(U_2;U_1,Z|V_2)+2\epsilon)}$ jointly typical pairs of (U_1^n, U_2^n) in the constructed codebook. Then, we can follow similar steps in Lemma C.3 to obtain that

$$\begin{aligned}\frac{1}{n}&H(U_1^n, U_2^n|V_1^n, V_2^n, Z^n, \mathcal{C})\\&\geq 3\epsilon + I(U_1; X_1|V_1) - I(U_1; V_2, Z|V_1) + I(U_2; X_2|V_2) - I(U_2; U_1, Z|V_2)\\&= I(U_1, U_2; X_1, X_2|Z, V_1, V_2) + 3\epsilon.\end{aligned}$$

Thus, it follows that

$$\frac{1}{n}H(X_1^n, X_2^n|M_{11}, M_{12}, M_{21}, M_{22}, Z^n, \mathcal{C})$$

$$\geq H(X_1,X_2|U_1,U_2,Z)+I(U_1,U_2;X_1,X_2|Z,V_1,V_2)-I(U_1,U_2;X_1,X_2|Y,V_1,V_2)-2\epsilon$$
$$\geq H(X_1,X_2|U_1,U_2,Z)+I(U_1,U_2;Y|V_1,V_2)-I(U_1,U_2;Z|V_1,V_2)-2\epsilon.$$

Similarly, we can obtain another scheme to achieve the other corner point, then we can use the time-sharing technique to show that the region defined by (5.29)-(5.33) is achievable.

C.5 Proof of Theorem 5.8

Given PMF $P_{X_1X_2Y}P_{U|X_1}P_{V|X_2}$ and a function g s.t. $D > E[d(f(X_1,X_2,Y),g(U,V,Y))]+\epsilon$, the achievability scheme is the same as that in the proof of Theorem 5.6, we only need to further analyze $\frac{1}{n}E[d(\mathbf{f}(X_1^n,X_2^n,Y^n),\mathbf{g}(\hat{U}^n,\hat{V}^n,Y^n))]$, which can be easily shown to be upper bounded by D with high probability when n is large enough. We now turn to the proof of the outer bound.

Outer Bound:

Following similar process of extending the proof of Theorem 5.2 to that of Theorem 5.4, the techniques used in Theorem 5.6 can be modified to prove Theorem 5.8 as follows. In this part, we set

$$(U_1)_i := (M_1,(X_1)^{i-1},Z^{i-1},Y^{i-1},Y_{i+1}^n),\ \ (V_1)_i := (M_1,Z^{i-1},Y_{i+1}^n)$$
$$(U_2)_i := (M_2,(X_2)^{i-1},Z^{i-1},,Y^{i-1},Y_{i+1}^n),(V_2)_i := (M_2,Z^{i-1},Y_{i+1}^n),$$

and the proof of (5.35)-(5.39) is straightforward following the above derivatives. Here, we only show (5.40) as follows. Give D, we have

$$D \geq \frac{1}{n}E\left[d(\mathbf{f}(X_1^n,X_2^n,Y^n),\hat{\mathbf{f}}(M_1,M_2,Y^n))\right]-\epsilon$$
$$=\frac{1}{n}E\left[\sum_{i=1}^n d(f(X_{1i},X_{2i},Y_i),\hat{f}_i(M_1,M_2,Y^n))\right]-\epsilon$$

$$
\begin{aligned}
&\overset{(a)}{\geq} \frac{1}{n} E\left[\sum_{i=1}^{n} d(f(X_{1i}, X_{2i}, Y_i), g(M_1, M_2, Y^n, Z^{i-1}, X_1^{i-1}, X_2{}^{i-1}))\right] - \epsilon \\
&= \frac{1}{n} E\left[\sum_{i=1}^{n} d(f(X_{1i}, X_{2i}Y_i), g((U_1)_i, (U_2)_i, Y_i))\right] - \epsilon \\
&= E\left[d(f(X_1, X_2, Y), g(U_1, U_2, Y))\right] - \epsilon,
\end{aligned}
$$

where step (a) follows from that, in general, $\hat{\mathbf{f}}$ is a function of (M_1, M_2, Y^n) in any achievable scheme, so is $\hat{f}_i(M_1, M_2, Y^n)$, thus there must exist some function, say g, such that the distortion decreases with more information is provided for each $i \in [1:n]$.

Hence, the converse proof is complete.

C.6 Lemmas

Lemma C.2. Given arbitrary $\epsilon > 0$, we have

$$
\liminf_{n\to\infty} \frac{1}{n} H(X^n|U^n, V^n, Z^n, \mathcal{C}) \geq H(X|U, Z) - \epsilon.
$$

Proof. Denote the ϵ-jointly typical set of sequence pairs (U^n, V^n, Z^n) by $\mathcal{T}_\epsilon^n(U, V, Z)$, and the notation $\mathcal{T}_\epsilon^n(V, Z)$ in the sequel, followS in a similar manner. Set $\theta_1 = 0$ if $(U^n, V^n, Z^n) \in \mathcal{T}_\epsilon^n(U, V, Z)$, and $\theta_1 = 1$ otherwise. According to the scheme, we have, according to Markov Lemma [23, Chapter 12], that Pr$\{\theta_1 = 0\} \to 0$ as $n \to \infty$. Thus, it follows that

$$
\begin{aligned}
&H(X^n|U^n, V^n, Z^n, \mathcal{C}) \geq H(X^n|U^n, V^n, Z^n, \theta_1, \mathcal{C}) \\
&= \Pr\{\theta_1 = 0\} H(X^n|U^n, V^n, Z^n, \theta_1 = 0, \mathcal{C}) + \Pr\{\theta_1 = 1\} H(X^n|U^n, V^n, Z^n, \theta_1 = 1, \mathcal{C}) \\
&\geq H(X^n|U^n, V^n, Z^n, \theta_1 = 0, \mathcal{C}) - n\delta(\epsilon) \\
&= \sum_{z^n, \{v^n, u^n\} \in \mathcal{C}} \Pr\{u^n, v^n, z^n|\theta_1 = 0\} H(X^n|u^n, v^n, z^n) - n\delta(\epsilon) \\
&\geq \sum_{z^n, v^n, u^n \in \mathcal{C}} \Pr\{u^n, z^n|\theta_1 = 0\} n(H(X|U, V, Z) - n\epsilon) - n\delta(\epsilon) \\
&\geq nH(X|U, V, Z) - 2\delta(\epsilon)
\end{aligned}
$$

$$= nH(X|U,Z) - 2\delta(\epsilon).$$

□

Lemma C.3. Given arbitrary $\epsilon > 0$, we have

$$\liminf_{n\to\infty} \frac{1}{n} H(U^n|V^n, Z^n, \mathcal{C}) \geq I(X;U|V) - I(Z;U|V) - \epsilon.$$

Proof. Set $\theta_2 = 0$ if $(V^n, Z^n) \in \mathcal{T}_\epsilon^n(V,Z)$, and $\theta_2 = 1$ otherwise. Following the proof of Lemma C.2, we have that

$$H(U^n|V^n, Z^n, \mathcal{C}) \geq \sum_{z^n, v^n \in \mathcal{C}} \Pr\{v^n, z^n|\theta_1 = 0\} H(U^n|v^n, z^n, \mathcal{C}) - n\epsilon.$$

Now, set $\theta_3 = 0$ if $(U^n, v^n, z^n) \in \mathcal{T}_\epsilon^n(U,V,Z)$, and $\theta_3 = 1$ otherwise. Again, according to the Markov lemma, we have $\Pr\{\theta_3 = 0\} \geq 1 - \epsilon$ when n is sufficiently large. Then we have

$$\begin{aligned}
H(U^n|v^n, z^n, \mathcal{C}) &\geq H(U^n|v^n, z^n, \theta_3, \mathcal{C}) \\
&= \Pr\{\theta_3 = 0\} H(U^n|v^n, z^n, \theta_3 = 0, \mathcal{C}) + \Pr\{\theta_3 = 1\} H(U^n|v^n, z^n, \theta_3 = 1, \mathcal{C}) \\
&\geq H(U^n|v^n, z^n, \theta_3 = 0, \mathcal{C}) - n\delta(\epsilon).
\end{aligned}$$

Denote $\text{Num}(U^n|v^n, z^n)$ the number of sequences U^n that are generated by v^n and are jointly typical with (v^n, z^n). It is easy to verify that $\frac{1}{n} H(U^n|v^n, z^n, \theta_3 = 0, \mathcal{C}) \geq \log \text{Num}(U^n|v^n, z^n) - \epsilon$, since each jointly typical U^n has the same, or close to be precise, probability to be the desired sequence. For each U^n generated by v^n, according the *Joint Typicality Lemma* [23, Chapter 2], we have

$$\begin{aligned}
\Pr\{(U^n, v^n, z^n) \in \mathcal{T}_\epsilon^n(U,V,Z)\} &\geq 2^{-n(I(U;Z|V)+\epsilon)}, \\
\Pr\{(U^n, v^n, z^n) \in \mathcal{T}_\epsilon^n(U,V,Z)\} &\leq 2^{-n(I(U;Z|V)-\epsilon)}
\end{aligned}$$

if $(v^n, z^n) \in \mathcal{T}_\epsilon^n(V, Z)$. Thus, it follows that

$$\mathbb{E}[\text{Num}((U^n|v^n, z^n))] \geq 2^{n(I(U;X|V)+\epsilon)} 2^{-n(I(U;Z|V)+\epsilon)} = 2^{n(I(U;X|V)-I(U;Z|V))},$$

and

$$\text{Var}[\text{Num}((U^n|v^n, z^n))] \leq 2^{n(I(U;X|V)-I(U;Z|V)+2\epsilon)}.$$

Thus, we have

$$\Pr\{\text{Num}((U^n|v^n, z^n)) \leq \frac{1}{2}\mathbb{E}[\text{Num}((U^n|v^n, z^n))]\} \leq 4 \cdot 2^{-n(I(U;X|V)-I(U;Z|V)-2\epsilon)} \leq \delta(\epsilon).$$

Hence, we have

$$H(U^n|v^n, z^n, \mathcal{C}) \geq (1 - \delta(\epsilon))n[I(U;X|V) - I(U;Z|V)],$$

which implies that

$$\frac{1}{n}H(U^n|V^n, Z^n, \mathcal{C}) \geq I(X;U|V) - I(Z;U|V) - 2\delta(\epsilon).$$

□

Bibliography

[1] Divesh Aggarwal and Ueli Maurer. Breaking RSA generically is equivalent to factoring. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 36–53, Cologne, Germany, Apr. 2009. Springer.

[2] Anurag Agrawal, Zouheir Rezki, Ashish Khisti, and Mohamed-Slim Alouini. Noncoherent capacity of secret-key agreement with public discussion. *IEEE Trans. Inf. Forensics Security*, 6(3):565–574, Sept. 2011.

[3] Rudolf Ahlswede and Imre Csisz*á*r. Common randomness in information theory and cryptography, part I: Secret sharing. *IEEE Trans. Inf. Theory*, 39(4):1121–1132, July 1993.

[4] Rudolf Ahlswede and Janos Korner. Source coding with side information and a converse for degraded broadcast channels. *IEEE Trans. Inf. Theory*, 21(6):629–637, Nov. 1975.

[5] James M Anderson. Why we need a new definition of information security. *Computers & Security*, 22(4):308–313, May 2003.

[6] Rathinakumar Appuswamy, Massimo Franceschetti, Nikhil Karamchandani, and Kenneth Zeger. Network coding for computing: Cut-set bounds. *IEEE Trans. Inf. Theory*, 57(2):1015–1030, Feb. 2011.

[7] Mikhail J Atallah and Wenliang Du. Secure multi-party computational geometry. In *Workshop on Algorithms and Data Structures*, pages 165–179, Providence, RI, Aug. 2001. Springer.

[8] Ola Ayaso, Devavrat Shah, and Munther A Dahleh. Information theoretic bounds for distributed computation over networks of point-to-point channels. *IEEE Trans. Inf. Theory*, 56(12):6020–6039, 2010.

[9] Joao Barros and Miguel RD Rodrigues. Secrecy capacity of wireless channels. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 356–360, Seattle, WA, Jul. 2006. IEEE.

[10] Iluminada Baturone, Miguel A Prada-Delgado, and Susana Eiroa. Improved generation of identifiers, secret keys, and random numbers from srams. *IEEE Trans. Inf. Forensics Security*, 10(12):2653–2668, Dec. 2015.

[11] Mokhtar S Bazaraa, John J Jarvis, and Hanif D Sherali. *Linear programming and network flows*. John Wiley & Sons, New York, 2011.

[12] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proceedings of the Workshop on New Security Paradigms*, pages 97–104, Cloudcroft, NM, Sept. 2001. ACM.

[13] Dan Boneh et al. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203–213, Feb. 1999.

[14] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, London, UK, 2004.

[15] Kan Chen, Balasubramaniam Bala Natarajan, and Steve Shattil. Secret key generation rate with power allocation in relay-based LTE-A networks. *IEEE Trans. Inf. Forensics Security*, 10(11):2424–2434, Nov. 2015.

[16] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. John Wiley & Sons, New York, 2006.

[17] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[18] Imre Csiszár and Prakash Narayan. The capacity of the arbitrarily varying channel revisited: Positivity, constraints. *IEEE Trans. Inf. Theory*, 34(2):181–193, Mar. 1988.

[19] Imre Csiszár and Prakash Narayan. Common randomness and secret key generation with a helper. *IEEE Trans. Inf. Theory*, 46:344–366, Mar. 2000.

[20] Imre Csiszár and Prakash Narayan. Secrecy capacities for multiple terminals. *IEEE Trans. Inf. Theory*, 50(12):3047–3061, Dec. 2004.

[21] Imre Csiszár and Prakash Narayan. Secrecy capacities for multiterminal channel models. *IEEE Trans. Inf. Theory*, 54(6):2437–2452, Jun. 2008.

[22] Wenliang Du and Mikhail J Atallah. Secure multi-party computation problems and their applications: a review and open problems. In *Proceedings of the New security paradigms workshop*, pages 13–22, Cloudcroft, NM, Sept. 2001. ACM.

[23] Abbas El Gamal and Yang-Han Kim. *Network Information Theory*. Cambridge University Press, New York, 2011.

[24] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, Jun. 1985.

[25] Arvind Giridhar and Praveen R Kumar. Computing and communicating functions over sensor networks. *IEEE J. Sel. Areas Commun.*, 23(4):755–764, Apr. 2005.

[26] Mario Goldenbaum, Holger Boche, and H Vincent Poor. On secure computation over the binary modulo-2 adder multiple-access wiretap channel. In *Proc. IEEE Inform. Theory Workshop*, pages 21–25, Cambridge, UK, Sept. 2016. IEEE.

[27] Mario Goldenbaum, Holger Boche, and H Vincent Poor. Secure computation of linear functions over linear discrete multiple-access wiretap channels. In *Proc. Asilomar Conf. on Signals, Systems and Computers*, pages 1670–1674, Pacific Grove, CA, Nov. 2016. IEEE.

[28] Clóvis C Gonzaga. *An algorithm for solving linear programming problems in $O(n^3L)$ operations*. Springer, New York, 1989.

[29] Lawrence A Gordon and Martin P Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457, Nov. 2002.

[30] Onur Gungor and Can Emre Koksal. RF-fingerprint based authentication: Exponents and achievable rates. In *Proc. IEEE Conf. on Communications and Network Security*, pages 97–102, San Francisco, CA, Oct. 2014.

[31] Te Sun Han and Kingo Kobayashi. Exponential-type error probabilities for multiterminal hypothesis testing. *IEEE Trans. Inf. Theory*, 35(1):2–14, Jan. 1989.

[32] Yong Hao, Yu Cheng, Chi Zhou, and Wei Song. A distributed key management framework with cooperative message authentication in VANETs. *IEEE J. Sel. Areas Commun.*, 29(3):616–629, Mar. 2011.

[33] Mohamed F Haroun and T Aaron Gulliver. Secret key generation using chaotic signals over frequency selective fading channels. *IEEE Trans. Inf. Forensics Security*, 10(8):1764–1775, Aug. 2015.

[34] Weikun Hou, Xianbin Wang, Jean-Yves Chouinard, and Ahmed Refaey. Physical layer authentication for mobile systems with time-varying carrier frequency offsets. *IEEE Trans. Communications*, 62(5):1658–1667, May 2014.

[35] Shaoquan Jiang. Keyless authentication in a noisy model. *IEEE Trans. Inf. Forensics Security*, 9(6):1024–1033, Apr. 2014.

[36] Thomas Johansson. Lower bounds on the probability of deception in authentication with arbitration. *IEEE Trans. Inf. Theory*, 40(5):1573–1585, Sep. 1994.

[37] David Kahn. *The codebreakers*. Weidenfeld and Nicolson, London, UK, 1974.

[38] Narendra Karmarkar. A new polynomial-time algorithm for linear programming. In *Proceedings of the sixteenth annual ACM symposium on Theory of computing*, pages 302–311. ACM, 1984.

[39] Ashish Khisti, Suhas N Diggavi, and Gregory W Wornell. Secret-key agreement with channel state information at the transmitter. *IEEE Trans. Inf. Forensics Security*, 6(3):672–681, Sept. 2011.

[40] Ashish Khisti, Suhas N Diggavi, and Gregory W Wornell. Secret-key generation using correlated sources and channels. *IEEE Trans. Inf. Theory*, 58(2):652–670, Feb. 2012.

[41] Hiroki Koga and Hirokazu Yamamoto. Coding theorems for secret-key authentication systems. *IEICE Trans. Fundamentals*, 83(8):1691–1703, Aug. 2000.

[42] Valery Korzhik, Viktor Yakovlev, Guillermo Morales-Luna, and Roman Chesnokov. Performance evaluation of keyless authentication based on noisy channel. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, pages 115–126, St. Petersburg, Russia, Sept. 2007. Springer.

[43] Hemant Kowshik and P. R Kumar. Optimal function computation in directed and undirected graphs. *IEEE Trans. Inf. Theory*, 58(6):3407–3418, Jun. 2012.

[44] Hemant Kowshik and P. R Kumar. Optimal computation of symmetric boolean functions in collocated networks. *IEEE J. Sel. Areas Commun.*, 31(4):639–654, Apr. 2013.

[45] Lifeng Lai, Hesham El Gamal, and H Vincent Poor. Authentication over noisy channels. *IEEE Trans. Inf. Theory*, 55(2):906–916, Feb. 2009.

[46] Lifeng Lai and Lauren Huie. Simultaneously generating multiple keys in many to one networks. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2394–2398, Istanbul, Turkey, July 2013.

[47] Lifeng Lai, Yingbin Liang, and Wenliang Du. Cooperative key generation in wireless networks. In *IEEE J. Sel. Areas Commun.*, volume 30, pages 1578–1588, Sep. 2012.

[48] Lifeng Lai, Yingbin Liang, and H Vincent Poor. A unified framework for key agreement over wireless fading channels. *IEEE Trans. Inf. Forensics Security*, 7(2):480–490, Mar. 2012.

[49] Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310, Nov. 1992.

[50] Junlin Li and Ghassan AlRegib. Rate-constrained distributed estimation in wireless sensor networks. *IEEE Trans. Signal Processing*, 55(5):1634–1643, May 2007.

[51] Shundong Li, Daoshun Wang, Yiqi Dai, and Ping Luo. Symmetric cryptographic solution to Yao's millionaires' problem and an evaluation of secure multiparty computations. *Information Sciences*, 178(1):244–255, Jan. 2008.

[52] Nan Ma and Prakash Ishwar. Some results on distributed source coding for interactive function computation. *IEEE Trans. Inf. Theory*, 57(9):6180–6195, Sept. 2011.

[53] Nan Ma and Prakash Ishwar. The infinite-message limit of two-terminal interactive source coding. *IEEE Trans. Inf. Theory*, 59(7):4071–4094, Jul. 2013.

[54] Nan Ma, Prakash Ishwar, and Piyush Gupta. Interactive source coding for function computation in collocated networks. *IEEE Trans. Inf. Theory*, 58(7):4289–4305, Jul. 2012.

[55] Ueli Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39(3):733–742, May 1993.

[56] Ueli Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39(3):733–742, May 1993.

[57] Ueli Maurer. Information-theoretically secure secret-key agreement by not authenticated public discussion. In *Advances in CryptologyEurocrypt97*, pages 209–225. Springer, 1997.

[58] Ueli Maurer. Authentication theory and hypothesis testing. *Information Theory, IEEE Transactions on*, 46(4):1350–1356, 2000.

[59] Ueli Maurer and Stefan Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory*, 45(2):499–514, 1999.

[60] Ueli Maurer and Stefan Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology-EUROCRYPT 2000*, pages 351–368. Springer, 2000.

[61] Ueli Maurer and Stefan Wolf. Secret key agreement over a non-authenticated channel - Part III: Privacy amplification. *IEEE Transactions on Information Theory*, 49(4):839–851, April 2003.

[62] Ueli Maurer and Stefan Wolf. Secret key agreement over unauthenticated public channels - Part I: Definitions and a completeness result. *IEEE Transactions on Information Theory*, 49(4):822–831, April 2003.

[63] Ueli Maurer and Stefan Wolf. Secret key agreement over unauthenticated public channels - Part II: The simulatability condition. *IEEE Transactions on Information Theory*, 49(4):832–838, April 2003.

[64] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516, Sept. 2012.

[65] Hans-Michael Möller. *Exact Computation of the Generalized Inverse and the Least-squares Solution*. Techn. Univ., Fak. für Mathematik, 1999.

[66] Renato DC Monteiro and Ilan Adler. Interior path following primal-dual algorithms. Part I: Linear programming. *Mathematical Programming*, 44:27–41, 1989.

[67] Renato DC Monteiro and Ilan Adler. Interior path following primal-dual algorithms. Part II: Convex quadratic programming. *Mathematical Programming*, 44:43–66, 1989.

[68] Bobak Nazer and Michael Gastpar. Computation over multiple-access channels. *IEEE Trans. Inf. Theory*, 53(10):3498–3516, Oct. 2007.

[69] Frédérique Oggier and Babak Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory*, 57(8):4961–4972, Aug. 2011.

[70] Alon Orlitsky and James R Roche. Coding for computing. *IEEE Trans. Inf. Theory*, 47(3):903–917, Mar. 2001.

[71] Thomas R Peltier. *Information security risk analysis*. Auerbach publications, Boca Raton, FL, 2005.

[72] H. Vincent Poor. *An Introduction to Signal Detection and Estimation*. Springer-Verlag, New York, 1994.

[73] Mahalingam Ramkumar. The subset keys and identity tickets (skit) key distribution scheme. *IEEE Trans. Inf. Forensics Security*, 5(1):39–51, Feb. 2010.

[74] C Radhakrishna Rao. Calculus of generalized inverses of matrices Part I: General theory. *Sankhyā: The Indian Journal of Statistics, Series A*, pages 317–342, 1967.

[75] Calyampudi Radhakrishna Rao and Sujit Kumar Mitra. *Generalized inverse of matrices and its applications*. John Wiley & Sons, New York, 1971.

[76] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, Feb. 1978.

[77] Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, New York, 1998.

[78] Milad Sefidgaran and Aslan Tchamkerten. Computing a function of correlated sources: A rate region. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 1856–1860, Saint Petersburg, Russia, Aug. 2011. IEEE.

[79] Milad Sefidgaran and Aslan Tchamkerten. On cooperation in multi-terminal computation and rate distortion. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 766–770, Cambridge, MA, Jul. 2012.

[80] Milad Sefidgaran and Aslan Tchamkerten. Distributed function computation over a rooted directed tree. *IEEE Trans. Inf. Theory*, 62(12):7135–7152, Dec. 2016.

[81] Claude E Shannon. Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4):656–715, Oct. 1949.

[82] Rashid Sheikh, Durgesh Kumar Mishra, and Beerendra Kumar. Secure multiparty computation: From millionaires problem to anonymizer. *Information Security Journal: A Global Perspective*, 20(1):25–33, Feb. 2011.

[83] Gustavus J Simmons. Authentication theory/coding theory. In *Proc. Advances in Cryptology*, pages 411–431, Linz, Austria, Apr. 1985.

[84] Gustavus J Simmons. A survey of information authentication. *Proc*, 76(5):603–620, May 1988.

[85] Maurice Sion. On general minimax theorems. *Pacific J. Math*, 8(1):171–176, Mar. 1958.

[86] Stefano Tomasin and Alberto Dall'Arche. Resource allocation for secret key agreement over parallel channels with full and partial eavesdropper CSI. *IEEE Trans. Inf. Forensics Security*, 10(11):2314–2324, Nov. 2015.

[87] Wenwen Tu, Mario Goldenbaum, Lifeng Lai, and H Vincent Poor. Simultaneously generating multiple keys over a cascade of a noiseless channel and a wiretap. In *Proc. IEEE Inform. Theory Workshop*, pages 206–210, Cambridge, UK, Sept. 2016.

[88] Wenwen Tu, Mario Goldenbaum, Lifeng Lai, and H Vincent Poor. On simultaneously generating multiple keys in a joint source-channel model. *IEEE Trans. Inf. Forensics Security*, 12(2):298–308, Feb. 2017.

[89] Wenwen Tu and Lifeng Lai. On the simulatability condition in key generation over a non-authenticated public channel. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 720–724, Hong Kong, China, Jun. 2015.

[90] Wenwen Tu and Lifeng Lai. Keyless authentication over noisy channel. In *Proc. Asilomar Conf. on Signals, Systems and Computers*, pages 1665–1669, Pacific Grove, CA, Nov. 2016.

[91] Wenwen Tu and Lifeng Lai. Function computation with privacy constraints. In *Proc. Asilomar Conf. on Signals, Systems and Computers*, pages 1672–1676, Pacific Grove, CA, Oct. 2017.

[92] Wenwen Tu and Lifeng Lai. On function computation with privacy and secrecy constraints. *IEEE Trans. Inf. Theory*, Jun. 2017. Submitted.

[93] Wenwen Tu and Lifeng Lai. Keyless authentication and authenticated capacity. *IEEE Trans. Inf. Theory*, 64(5):3696–3714, May 2018.

[94] Wenwen Tu and Lifeng Lai. On private lossy function computation. In *Proc. IEEE Workshop on Signal Processing Advances in Wireless Communication*, Kalamata, Greece, Jun. 2018.

[95] Jitendra K Tugnait. Wireless user authentication via comparison of power spectral densities. *IEEE J. Sel. Areas Commun.*, 31(9):1791–1802, Aug. 2013.

[96] Hoang Tuy. *Convex analysis and global optimization*. Springer Science & Business Media, Boston, MA, 2013.

[97] Himanshu Tyagi, Prakash Narayan, and Piyush Gupta. When is a function securely computable? *IEEE Trans. Inf. Theory*, 57(10):6337–6350, Oct. 2011.

[98] Himanshu Tyagi and Shun Watanabe. A bound for multiparty secret key agreement and implications for a problem of secure computing. In *Advances in Cryptology-EUROCRYPT*, pages 369–386, Copenhagen, Denmark, May 2014. Springer.

[99] Himanshu Tyagi and Shun Watanabe. Converses for secret key agreement and secure computing. *IEEE Trans. Inf. Theory*, 61(9):4809–4827, Sept. 2015.

[100] Wen-Guey Tzeng. Efficient 1-out-n oblivious transfer schemes. In *International Workshop on Public Key Cryptography*, pages 159–171, Paris, France, Feb 2002. Springer.

[101] Jiřina Vejnarová. Conditional independence and markov properties in possibility theory. In *Proceedings of the Sixteenth conference on Uncertainty in artificial intelligence*, pages 609–616, Stanford, CA, Jun. 2000.

[102] HS Venter and Jan HP Eloff. A taxonomy for information security technologies. *Computers & Security*, 22(4):299–307, May 2003.

[103] Michael Walker. Information-theoretic bounds for authentication schemes. *Journal of Cryptology*, 2(3):131–143, Jan. 1990.

[104] Ning Wang, Ning Zhang, and T Aaron Gulliver. Cooperative key agreement for wireless networking: Key rates and practical protocol design. *IEEE Trans. Inf. Forensics Security*, 9(2):272–284, Jan. 2014.

[105] Shun Watanabe and Yasutada Oohama. Secret key agreement from vector Gaussian sources by rate limited public communication. *IEEE Trans. Inf. Forensics Security*, 6(3):541–550, Sept. 2011.

[106] Rolf H Weber. Internet of things–new security and privacy challenges. *Computer law & security review*, 26(1):23–30, Jan. 2010.

[107] Hong Wen, P-H Ho, C Qi, and Guang Gong. Physical layer assisted authentication for distributed ad hoc wireless sensor networks. *IET inf. secur.*, 4(4):390–396, Dec. 2010.

[108] Michael J Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information theory*, 36(3):553–558, May 1990.

[109] Chan Wong Wong, Tan F Wong, and John M Shea. Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel. *IEEE Trans. Inf. Forensics Security*, 6(3):551–564, Sept. 2011.

[110] Thomas YC Woo and Simon S Lam. Authentication for distributed systems. *IEEE Computer Society*, (1):39–52, Jan. 1992.

[111] Xiaofu Wu and Zhen Yang. Physical-layer authentication for multi-carrier transmission. *IEEE Communications Letters*, 19(1):74–77, Jan. 2015.

[112] Aaron D. Wyner. On source coding with side information at the decoder. *IEEE Trans. Inf. Theory*, 21(3):294–300, May 1975.

[113] Aaron D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Oct. 1975.

[114] Aaron D. Wyner and Jacob Ziv. The rate-distortion function for source coding with side information at the decoder. *IEEE Trans. Inf. Theory*, 22(1):1–10, Jan. 1976.

[115] Liang Xiao, Larry J Greenstein, Narayan B Mandayam, and Wade Trappe. Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans. Wireless Communications*, 7(7):2571–2579, Jul. 2008.

[116] Zixiang Xiong, Angelos D Liveris, and Samuel Cheng. Distributed source coding for sensor networks. *IEEE Signal Processing Magazine*, 21(5):80–94, Sept. 2004.

[117] Zixiang Xiong, Angelos D Liveris, and Yang Yang. *Distributed source coding*. Wiley Online Library, 2006.

[118] Peng Xu, Zhiguo Ding, Xuchu Dai, and George Karagiannidis. Simultaneously generating secret and private keys in a cooperative pairwise independent network. *IEEE Trans. Inf. Forensics Security*, 11(6):1139–1150, Jan. 2016.

[119] Chunxuan Ye, Suhas Mathur, Alex Reznik, Yogendra Shah, Wade Trappe, and Narayan B Mandayam. Information-theoretically secret key generation for fading wireless channels. *IEEE Trans. Inf. Forensics Security*, 5(2):240–254, Jun. 2010.

[120] Chunxuan Ye and Prakash Narayan. The secret key-private key capacity region for three terminals. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2142–2146, Adelaide, Australia, Sept. 4-9, 2005.

[121] Chunxuan Ye and Prakash Narayan. Secret key and private key constructions for simple multiterminal source models. *IEEE Trans. Inf. Theory*, 58(2):639–651, Feb. 2012.

[122] Lei Ying, R Srikant, and Geir E Dullerud. Distributed symmetric function computation in noisy wireless sensor networks. *IEEE Trans. Inf. Theory*, 53(12):4826–4833, Dec. 2007.

[123] Huishuai Zhang, Lifeng Lai, Yingbin Liang, and Hua Wang. The capacity region of the source-type model for secret key and private key generation. *IEEE Trans. Inf. Theory*, 60(10):6389–6398, Jul. 2014.

[124] Heng Zhou, Lauren M Huie, and Lifeng Lai. Secret key generation in the two-way relay channel with active attackers. *IEEE Trans. Inf. Forensics Security*, 9(3):476–488, Mar. 2014.

[125] Ali Zibaeenejad. Key generation over wiretap models with non-causal side information. *IEEE Trans. Inf. Forensics Security*, 10(7):1456–1471, Jul. 2015.