On Achieving Unconditionally Secure Communications Via the Physical Layer Approaches

by

Hong Wen

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2018

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	YUGUAGN FANG
	Title: Professor, University of Florida
Supervisor(s):	PIN-HAN HO
	Title: Professor
Internal Member:	PATRICK MITRAN
	Title: Associate Professor
Internal Member:	MAHESH TRIPUNITARA
	Title: Associate Professor
Internal-external Member(s):	ALEXANDER WONG
	Title: Associate Professor

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Due to the broadcast nature, wireless links are open to malicious intrusions from outsiders, which makes the security issues a critical concern in the wireless communications over them. Physical-layer security techniques, which are based on the Shannon's unconditional secrecy model, are effective in addressing the security issue while meeting the required performance level. According to the Wyner's wiretap channel model, to achieve unconditionally security communication, the first step is to build up a wiretap channel with better channel quality between the legitimate communication peers than that of the eavesdropper; and the second step is to employ a robust security code to ensure that the legitimate users experience negligible errors while the eavesdropper is subject to 0.5 error probability.

Motivated by this idea, in this thesis, we build wiretap channels for the single antenna systems without resorting to the spatial degree in commonly observed the multiple-input multiple-output (MIMO) systems. Firstly, to build effective wiretap channels, we design a novel scheme, called multi-round two-way communications (MRTWC). By taking feedback mechanisms into the design of Low Density Parity Check (LDPC) codes, our scheme adds randomness to the feedback signals from the destination to keep the eavesdropper ignorant while adding redundancy with the LDPC codes so that the legitimate receiver can correctly receive and decode the signals. Then, the channel BERs are specifically quantified according to the crossover probability in the case of Binary Symmetric Channel (BSC), or the Signal to Noise Ratio (SNR) in the case of AWGN and Rayleigh channels. Thus, the novel scheme can be utilized to address the security and reliability. Meanwhile, we develop a cross-layer approach to building the wiretap channel, which is suitable for high dynamic scenarios. By taking advantage of multiple parameters freedom in the discrete fractional Fourier transform (DFRFT) for single antenna systems, the proposed scheme introduces a distortion parameter instead of a general signal parameter for

wireless networks based on DFRFT. The transmitter randomly flip-flops the uses of the distortion parameter and the general signal parameter to confuse the eavesdropper. An upper-layer cipher sequence will be employed to control the flip-flops. This cryptographic sequence in the higher layer is combined with the physical layer security scheme with random parameter fipping in DFRFT to guarantee security advantages over the main communication channel.

As the efforts on the second step, this thesis introduces a novel approach to generate security codes, which can be used for encoding with low complexity by taking advantage of a matrix general inverse algorithm. The novel constructions of the security codes are based on binary and non-binary resilient functions. With the proposed security codes, we prove that our novel security codes can ensure 0.5 error probability seen by the wiretapper while close to zero by the intended receiver if the error probability of the wiretapper's channel is over a derived threshold. Therefore, the unconditionally secure communication of legitimate partners can be guaranteed. It has been proved mathematically that the non-binary security codes could achieve closer to the security capacity bound than any other reported short-length security codes under BSC.

Finally, we develop the framework of associating the wiretap channel building approach with the security codes. The advantages between legitimate partners are extended via developing the security codes on top of our cross-layer DFRFT and feedback MRTWC security communication model. In this way, the proposed system could ensure almost zero information obtained by the eavesdroppers while still keeping rather lower error transmissions for legitimate users. Extensive experiments are carried out to verify the proposed security schemes and demonstrate the feasibility and implement ability. An USRP testbed is also constructed, under which the physical layer security mechanisms are implemented and tested. Our study shows that our proposed security schemes can be implemented in practical communications settings.

Acknowledgements

I would like to thank my beloved family for their spiritual and financial support through out my student career.

I would like to thank my supervisor, Prof. Pin-Han Ho, for his guidance and great help during the past 6 years, and also his suggestions for my future career.

I also would like to thank other research collaborators for their help to my research and study.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ADC	Analog to digital converter
AN	Artificial noise
AWGN	Additive white Gaussian noise
BCH	Bose Ray-Chaudhuri and Hocquenghem
BER	Bit error rate
BPSK	Binary phase shift keying
BSC	Binary symmetric channel
CC	Channel codes
CP	Cycle prefix
CSI	Channel state information
D2D	Device-to-Device
DAC	Digital to analog converter
DFRFT	Discrete fractional Fourier transform
DFT	Discrete Fourier transform
DMCs	Discrete memoryless channels
EVE	Eavesdropper
FFT	Fast Fourier transform

IFFT	Inverse fast Fourier transform
FRFT	Fractional Fourier transform
IDFRFT	Inverse discrete fractional Fourier transform
IFRFT	Inverse fractional Fourier transform
LabVIEW	Laboratory virtual instrument engineering workbench
LDPC	Low density parity check code
LLR	Log-likelihood ratios
LPI	Low probability-of-interception
MRC	Maximum ratio combining
MIMO	Multiple input multiple output
MB	MIMO beamforming
MIMOME	multiple-input-multiple-output and multiple-antenna eavesdropper
MRTWC	Multiple rounds two-way communication
MPDFRFT	multiple-parameter discrete fractional Fourier transform
OFDM	Orthogonal frequency division multiplexing
QAM	Quadarature amplitude modulation
QoS	Quality-of-service
RF	Radio frequency
SCs	Security codes
SER	Symbol error rate
SLC	Select combining
SNR	Signal-to-noise ratio
USRP	Universal softwar radio peripheral

List of Symbols

$\mathbf{S}$	Plaintext message
$\mathbf{X}$	Encoded sequence from $\mathbf{S}$
$\mathbf{Y}$	Received sequence of $\mathbf{X}$ by the legitimate receive
$\mathbf{Z}$	Received sequence of $\mathbf{X}$ by Eve
$\hat{\boldsymbol{S}}$	Decoded sequence from $\mathbf{Y}$ by the legitimate receive
$\tilde{\boldsymbol{S}}$	Decoded sequence from $\mathbf{Z}$ by Eve
$\tilde{\boldsymbol{S}}_e$	Decoded sequence from $\mathbf{Z}$ by Eve
P_e^m	The error rate that the legitimate received sequences
P_e^w	The error rate that the eavesdroppers received sequences
C_s	Security capacity
R_s	Transmit secrecy rate
p	Channel crossover probability
$H(\cdot)$	Entropy function
$H(\cdot\|\cdot)$	Conditional entropy function
$h(\cdot)$	Binary entropy function
χ_i	Security encoding function
ψ_i	Security decoding function

$\mathbf{C}$	Encoded sequence from $\mathbf{X}$ by the security encoding function
$\mathbf{V}$	Received sequence of $\mathbf{C}$ by the legitimate receive
$\mathbf{V}_e$	Received sequence of $\mathbf{C}$ by Eve
$Pr(\cdot)$	Probability
$\boldsymbol{Q}$	Random sequence
$\boldsymbol{E}$	Error vector of the legitimate receive
$\boldsymbol{E}_e$	Error vector of Eve
$\boldsymbol{T}$	Noisy version of $\boldsymbol{E}$
$\boldsymbol{T}_e$	Noisy version of $\boldsymbol{E}_e$
α_i	The error probability of the main channel
β_i	The error probability of the Eve channel
δ	Interactive communication rounds
ε_j^1	BERs of jth bit for Bob
ε_j^2	BERs of jth bit for Eve
$llr(v_j)$	Log-likelihood ratios of v_j
$P_b(e)$	The BER of BPSK signals
γ	The average SNR
N_i	Variance of the AWGN noise for the main channel
N_{e_i}	Variance of the AWGN noise for the Eve's channel
σ_1^2	Noise power for the main channel
σ_2^2	Noise power for the Eve's channel
$\mathbf{w}^j$	jth n-tuple binary sequence
p_w	The BER threshold probability
p_s	The SER threshold probability
p_{w_b}	The BER threshold probability of security codes

p_{w_s}	The SER threshold probability of security codes
$\mathbf{F}$	Resilient function
$\mathbf{D}$	An mn dimension matrix
$\overline{g}(x)$	The generator polynomial
P_{ir}	BER at the intended receiver after channel codes decoding
P_{Eve}	BER at the eavesdropper after channel codes decoding
P_{B_s}	SER at the intended receiver after security codes decoding
P_{E_s}	SER at the eavesdropper after security codes decoding
P_B	BER at the intended receiver after security codes decoding
P_E	BER at the eavesdropper after security codes decoding
$\frac{E_b}{N_0}$	Signal-to-noise ratio of per bit
$PE_{B,max}$	The maximum BER allowed for Bob at the input of the secure decoder
$PE_{E,min}$	The minimum input BER required for Eve at the decoder
$\tilde{u}$	the average SNR per receive antenna of the intended receiver
r	Instantaneous SNR of Eve
$\tilde{r}$	Average SNR of Eve
ρ_c	Transition probability
$\bar{t}$	Average error bits number
$P_{out}(\cdot)$	The probability of the secure transmit outage
$\Gamma(\cdot)$	Gamma function

Chapter 1

Introduction

1.1 Background

Securing communications is a challenging task. A first attempt at security involves learning basic cryptography, and applying encryption algorithms to make messages unintelligible to adversaries. However, rarely is the task of securing a message exchange so simple. When one steps back and contemplates how to secure the exchange of communications, one realizes that the challenge is fundamentally one of building a complete solution. The classical cryptography security methods are built without consideration to how communication takes place.

On the other side, all the classical cryptography schemes which are built on the upper layers can be broken if the computing resource and time are unlimited. Shannon [1] introduced the classic unbroken model of a cryptosystem as the unconditional security system and presented one time pad scheme as an example of the unconditional security system. However, it is impractical because the length of the key is same as the length of plaintext.

In fact, the classical cryptography schemes ignore the most fundamental of communication layers — the physical layer, whereby devices communicate through the encoding and modulation of information into waveforms. The cryptographic protocols are designed assuming that the physical layer has already been established and is error free. Cryptographic techniques may be used to provide security in a mobile environment, but these techniques do not directly leverage the unique properties of the wireless domain to address security threats. The physical properties of the wireless medium are a powerful source of domain-specific information that can be used to complement and enhance traditional security mechanisms.

The built-in security of the physical-layer is defined as that physical-layer transmissions guarantee Low Probability-of-Interception (LPI) based on transmission properties such as modulations, coding, signals and channels, without resorting to source data encryption, which is an approach to realize the the unconditionally security communication technology [1].

On the other hand, the physical-layer security is a novel approach to solve the wireless communication security [2, 3]. For the broadcasting nature of wireless communication, a eavesdropper can overhear the transmission. Thus, this unique physical-layer weakness calls for innovative physical-layer security designs in future mobile communication system, which aroused a lot of attention in recent years [2]-[8].

Wyner [9]-[11] first proposed the wiretap channel as an physical layer security model, in which a fact was proved that the unconditional security can be realised by taking advantages of the Security Codes (SCs) when the eavesdropper channel is a degraded version of the legitimate channel. From practical perspectives, however, it is generally hard to guarantee that the adversary's channel is noisier than the one taken by the legitimate partners. It is possible that the adversary's channel is better than that of legitimate partners.

Following this idea, many researches focused on the MIMO system [12], [13]-[16] are invested. The beamforming [17, 29, 18] and the artificial noise (AN) methods [19] are popular methods to construct the advanced main channel. Especially, there has been a great interest on the information-theoretic secrecy capacity of MIMO communication. Khisti and Wornell [20], [21], have discussed the achievable secrecy rate with beamforming in a multiple-input-single-output multiple-eavesdropper wiretap channel. The transmitter could directionally launch the optimal beamforming to create the biggest channel advantage for legitimate user. Khisti and Wornell [21], given an upper bound of achievable secrecy rate for the multiple-input-multiple-output and multiple-antenna eavesdropper (MIMOME) case in the asymptotic regime via signal-to-noise ratio (SNR) under such environment. The investigations on MIMO secrecy capacity were extended to various secure communication scenes such as the MIMO broadcast wiretap channel [22], some relay, and cooperate communication [23]-[28]. Ammari and Fortier [29] compared the secrecy of MIMO system employing transmit beamforming with maximum ratio combining (MRC) at legitimate receiver and either MRC or select combining (SLC) at the eavesdropper. By combining the CSI of both legitimates and eavesdroppers, the secure MIMO beamforming (MB) designs [20],[18] can calculate the optimum beamforming to weaken eavesdropper interception signal as much as possible meanwhile keeping the intended receiver signal at a special required quality level. the artificial noise (AN) methods [19] are considered mostly for this case by transmitting AN in the null space of the legitimate channel to obstruct the illegal receivers. On the basis of this, the quality of service (QoS)-based physical-layer security system [18],[100],[101] are usually considered focused on using only enough power to guarantee a certain QoS for Bob, and then use the remaining power to generate the artificial interference [101]. However, in some power limited system, the transmitter has to allocate part of power to send the AN, that may reduce the transmit efficiency and increase the computational complexity. Generally

in the AN system, the legitimates could hardly guarantee the eavesdropper BER close to 0.5 when the power of AN is limited, and some secret information may leak to the eavesdropper.

Another important factor is that a practical and implementable capacity approaching wiretap security code has never been available. Wyner [9] first introduced coset codes based on a random construction to solve the particular case when the main channel is noiseless and the wiretap channel is noisy BSC channel. However, no effective encoding and decoding algorithm was developed, such that the coset coding scheme can hardly be practically used. The only good results of security codes from polar codes and LDPC codes are too long to performance under wireless environment [31]-[35].

Therefore, building the advantage channel for the legitimate partners by the practical schemes is the first target of this thesis; while the novel security code construction methods will be investigated in the second step. By MIMO approaches to build the advanced channel [36]-[49] is a popular research area and be investigated widely. In some scenarios such as Device-to-Device (D2D) communication system [50]-[54], it is hard to support the multiple-antenna. How to build the advanced channel under the single antenna system? Maurer [55] is the first person to try to answer this problem and presents a feedback method to build an advantage for the main channel without MIMO scheme. In this thesis, we extend this method to Multiple Rounds Two-Way Communication (MRTWC) method for building a wiretap channel with larger advantages. We also develop the discrete fractional Fourier transform (DFRFT) [56, 57] cross-layer approach to build the advanced channel of the main channel under the single antenna system, which is suitable for the channel rapid variations scenarios such as moving at high speed. Meanwhile, this thesis explores developing the low-complexity encoding and decoding short-length security coding scheme via the resilient fanction [58, 59, 60] for wireless communication applications.

To achieve unconditional communications, the first step is to build up a practical wiretap channel by keeping better channel quality between the legitimate communication peers than that of the eavesdropper; while the second step is to achieve the unconditional secure communication by a robust security code scheme. However, the method for establishing such channel model and combining with the practice secret code [61]-[65], is not so obvious. we are motivated to investigate unconditionally secure communications building based on Wyner's model, where a wiretap channel is created first by using the approached of multi-round two-way communications and the DFRFT cross-layer communication systems, followed by novel constructed security codes from the resilient functions.

1.2 Contribution

The contribution of this thesis is listed as follows

- A novel wiretap channel built method called MRTWC is proposed, in which manipulating feedback mechanisms adds randomness to the transmitting signals from the destination for keeping the eavesdropper ignorant and redundancy is added and encoded by the LDPC codes such that a legitimate receiver can correctly receive and decode the signals;

- BERs of the proposed MRTWC method are derived according to the crossover probability in the case of BSC, or the Signal to Noise Ratio (SNR) in the case of AWGN and Rayleigh channels;

- The representation of bit Log-likelihood Ratios (LLR) for optimal soft information decoding and demodulation is extracted;

- A low complexity encoding method of security codes is developed by taking advantage of a matrix general inverse algorithm, which is suitable to all kinds of coset security codes;
- Several families of binary and non-binary security codes with low complexity are constructed by the binary and non-binary security resilient functions;
- The threshold probabilities of novel security codes are derived, which provide the strong security proof for the proposed security codes
- A cross-layer approach to build advantages of the main channel via DFRFT is proposed, in which the transmitter randomly flip-flops between the distorted signal parameter and the general signal parameter for confusing the attacker. An upper-layer pseudorandom sequence will be employed to control the flip-flops process;
- The security communication system model that combined the DFRFT cross-layer approach with the security codes is given.

1.3 Organization

The rest of this thesis is organized as follows. In Chapter 2, the Shannon's unconditional seurity model is given. Followed this model, Wyner is introduced, which is the first model to to realize the unconditional security model by the condition that is the main channel has advantage over the eavesdropper's channel. Then the security capacity that measures the advantage of the legitimate partner is introduced. Finally, a two-step unconditional security model is given, in which the first step is build the advanced main channel and followed step is to choose a suitable security codes.

Chapter 3 gives the details about building the wiretap channel by using feedback and LDPC codes. Most results focused on the MIMO approaches to build the advanced

channel. However, in some scenarios such as Device-to-Device (D2D) communication system, it is hard to support the multiple antennaes. By using feedback mechanisms adds randomness to the destination signals to degrade the eavesdroppers' channel and the manipulating several times feedback extends such degradation while the redundancy that is added by the LDPC codes encoding can let a legitimate receiver correctly receive and decode the signals. By this way the advantage of the main channel can be obtained without resorting to the MIMO scheme. The security capacity of such wiretap channel can be adjusted via setting the feedback rounds. BERs of the novel method are specifically quantified according to the crossover probability in the case of BSC, or the SNR in the case of AWGN and Rayleigh channels. The exact representation of bit Log-likelihood Ratios (LLR) is derive, which is necessary for optimal soft information decoding and demodulation.

The proposed novel security codes are described in Chapter 4. Firstly, Wyner's coset security codes are introduced. A novel encoding scheme with low complexity is proposed via a matrix general inverse algorithm, which can also provide low complexity benefit to Wyner's coset security codes and all other kinds of security codes. Then by manipulating both binary and non-binary resilient functions, novel security codes are generated. In particular, the proposed non-binary encoding construction is practically implementable due to low complexity and short code lengths, and is proved to yield the best achievable performance among all the reported short-length security codes over BSC. The threshold probabilities of novel security codes are derived, which provide the strong security proof for the proposed security codes. Finally, subsequently, the preliminary numerical results by combining the proposed wiretap model and the security codes are given.

In Chapter 5, a cross-layer approach to achieve unconditional communication security via DFRFT is investigated. The novel scheme introduces a distorted signal parameter instead of a general signal parameter for wireless networks based on DFRFT system. The

transmitter randomly flip-flops between the distorted signal parameter and the general signal parameter for confusing the attacker. An upper-layer cipher sequence will be employed to control the flip-flops process. The cryptographic sequence in the higher layer is combined with the physical layer security scheme using random parameters fipping of DFRFT to guarantee security advantages for the main channel. The advantages between legitimate partners building from the cross-layer scheme are extended via developing the security codes on top of our cross-layer DFRFT security communication model, aiming to achieve an error-free legitimate channel while preventing the eavesdropper from any useful information. Thus, a strong secure model is built. The extensive experiments are illustrated to verify the proposed security systems and demonstrate its feasibility and implement ability.

An USRP testbed of the unconditional security system is presented in Chapter 6, which is consisted of 5 sets of equipments. One equipment plays the role of the base station and other four sets equipment alternately play the role of the legitimate receivers and Eves. Security communication between users are successfully established and performance of this USRP platform shows that the security condition 2.3 and reliability 2.4 can be realized in the actual environment.

Finally, we conclude the proposal and outline the future research plans in Chapter 7.

Chapter 2

Unconditionally Security Communication Model

In this chapter, based on the theories of Shannon and Wyner, the two-step realized unconditional security model is given. According to Wyner's model, if and only if the eavesdropper's channel is a degraded version of the main channel, the physical layer security can be realized by certain security encoding and decoding scheme. Therefore, the first step is build the advanced main channel, whose superiority is measured by the security capacity which is also presented in this chapter.

2.1 Reliability and Security Condition of the Unconditionally Security Communication

Unconditionally security communication is based on the perfect secrecy model by Shannon [1], which is the strongest possible notion of security of a cryptosystem in effective resolving the boundary, efficiency, and link reliability issues. We will consider the follow-

ing scenario, which is illustrated in Figure 2.1. Alice wants to send a private message to Bob, which should be kept perfectly secret from Eve. Eve listens and tries to decode the message that Alice sends to Bob.

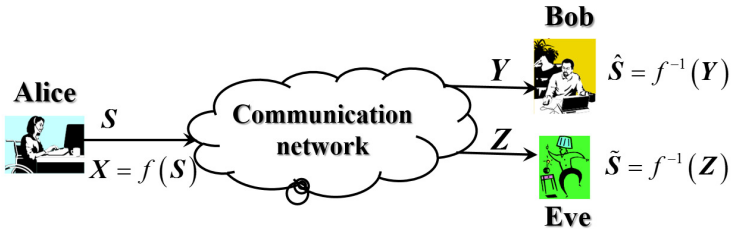


Figure 2.1: Communication system with a transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eve).

The source produces a message $\boldsymbol{S} = [s_1, s_2, \cdots, s_m]$, and encodes this message as a vector $\boldsymbol{X} = [x_1, x_2, \cdots, x_n]$, such that $\boldsymbol{X} = f(\boldsymbol{S})$. This vector is transmitted over the communication main channel and received as $\boldsymbol{Y} = [y_1, y_2, \cdots, y_n]$ by the destination. The eavesdropper has access to $t(t < n)$ symbols of $\boldsymbol{X}$ through a wiretap channel denoted as $\boldsymbol{Z} = [z_1, z_2, \cdots, z_n]$. The destination and eavesdropper can decode information as $\hat{\boldsymbol{S}} = [\hat{s}_1, \hat{s}_2, \cdots, \hat{s}_m]$ and $\tilde{\boldsymbol{S}} = [\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m]$ from $\boldsymbol{Y}$ and $\boldsymbol{Z}$, respectively.

A system has a perfect secrecy if and only if the plaintext message $\boldsymbol{S}$ is statistically independent of the ciphertext $\boldsymbol{Z}$, i.e., $I(\boldsymbol{S}; \boldsymbol{Z}) = 0$. In the classic model of a cryptosystem introduced by Shannon [1], both the sender and the intended receiver share a common secret key that is unknown to the wiretapper, and this key is used to encrypt and decrypt the message $\boldsymbol{S}$ at the sender and receiver, respectively. Shannon considered a scenario where both the intended receiver and the wiretapper have direct access to the transmitted signal. If the signal received by the wiretapper is $\boldsymbol{Z}$, unconditional security is achieved if $\boldsymbol{S}$ and $\boldsymbol{Z}$ are statistically independent. With $m \longrightarrow \infty$, if the error rate of the destination and eavesdropper are:

$$P_e^m = \frac{1}{m}\sum_{i=1}^{m} Pr(\hat{s}_i \neq s_i) \tag{2.1}$$

$$P_e^w = \frac{1}{m}\sum_{i=1}^{m} Pr(\tilde{s}_i \neq s_i) \tag{2.2}$$

The two conditions for security communication are:

$$P_e^m \longrightarrow 0 \tag{2.3}$$

$$P_e^w \longrightarrow 0.5 \tag{2.4}$$

Condition (2.3) is called *reliability condition* which implies that $\boldsymbol{X}$ must be solely determined by $\boldsymbol{S}$. Condition (2.4) is called *security condition* which ensures an eavesdropper unable to receive any useful information from the t intercepted symbols. The eavesdropper obtains no information about the source, and the system obtained perfect secrecy, which means that the transmitter can send information to the legitimate receiver in virtually unconditional secrecy without sharing a secret key with the legitimate receiver.

2.2 Wyner's Model

A famous approach for achieving Shannon's unconditional security is by Wyner's model [9, 10, 11]. Wyner introduced the wire tap channel, which has matured into a system depicted in Figure 2.2. In a wiretap channel, the honest parties Alice and Bob are separated by a main channel. The important modification when compared to Shannon's study of security is that any eavesdropper observes information transmitted by Alice through the wiretapper's channel. The main channel and the eavesdropper's channel are assumed to be Discrete Memoryless Channels (DMCs). Wyner [9] showed that if the eavesdropper's channel is a degraded version of the main channel condition (2.3) and

condition (2.4) can be realized by certain security encoding and decoding scheme. Under this condition, it is possible to establish a perfectly secure source-destination link without relying on a pre-shared secret key.

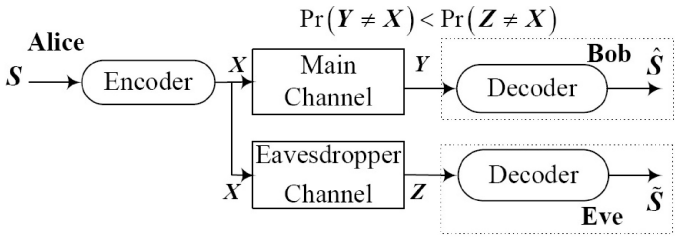


Figure 2.2: Block diagram of a Wyner's model.

2.3 Security Capacity

In this section, we briefly recap the results of [66, 67] to provide a simple expression of the secrecy capacity C_s in the case where the main channel and the eavesdropper's channel are symmetric DMCs and the eavesdropper's channel is degraded with respect to the main channel.

The notation of secrecy capacity, as introduced by [9], has an operational meaning of being the maximum possible rate of information transmission between Alice and Bob that still enables Eve to be kept totally ignorant. The secrecy capacity C_s for a general wiretap channel can be calculated as follows [66]:

$$C_s = \max \left\{ \; [I(\boldsymbol{S}; \boldsymbol{Y}) - I(\boldsymbol{S}; \boldsymbol{Z})], 0 \; \right\} \tag{2.5}$$

where the inner maximum is over all possible random variables $\boldsymbol{S}$ in joint distribution with $\boldsymbol{X}$, $\boldsymbol{Y}$, and $\boldsymbol{Z}$ such that $\boldsymbol{S} \to \boldsymbol{X} \to (\boldsymbol{Y}, \boldsymbol{Z})$ is a Markov chain. Note that C_s could turn out to be zero in cases where the maximization over $\boldsymbol{S} \to \boldsymbol{X} \to (\boldsymbol{Y}, \boldsymbol{Z})$ turns out

to be negative. At present, the calculation of secrecy capacity is an unsolved problem when the main channel and the eavesdropper's channel are general DMCs. However, the calculation of secrecy capacity can be simplified for some special cases that impose restrictions on the wiretap channel with respect to the main channel.

If $I(\boldsymbol{S};\boldsymbol{Y}) \geq I(\boldsymbol{S};\boldsymbol{Z})$ for all Markov chains $\boldsymbol{S} \rightarrow \boldsymbol{X} \rightarrow (\boldsymbol{Y}$, the main channel is said to be less noisy than the wire tap channel. Then [66]:

$$C_s = \max_{P_{\boldsymbol{X}}(x)} [I(\boldsymbol{S};\boldsymbol{Y}) - I(\boldsymbol{S};\boldsymbol{Z})] \tag{2.6}$$

where the maximum is over all possible distributions $P_{\boldsymbol{X}}(x)$ of $\boldsymbol{X}$. Moreover, as shown in [68], $I(\boldsymbol{S};\boldsymbol{Y}) - I(\boldsymbol{S};\boldsymbol{Z})$ is a convex function of $P_{\boldsymbol{X}}(x)$ where the main channel is less noisy than the wire tap channel; hence, the secrecy capacity can be calculated using convex optimization methods. It was further shown in [68] that if $I(\boldsymbol{S};\boldsymbol{Y})$ and $I(\boldsymbol{S};\boldsymbol{Z})$ are individually maximized by the same $P_{\boldsymbol{X}}(x)$, and the main channel ($\boldsymbol{X} \rightarrow \boldsymbol{Y}$) is less noisy than the wiretap channel ($\boldsymbol{X} \rightarrow \boldsymbol{Z}$), then

$$C_s = Capacity(\boldsymbol{X} \rightarrow \boldsymbol{Y}) - Capacity(\boldsymbol{X} \rightarrow \boldsymbol{Z}) \tag{2.7}$$

where $Capacity(\cdot)$ refers to the usual channel capacity. The capacity of a symmetric channel is given by

$$C_s = H(\boldsymbol{X}) - H(\boldsymbol{X}\,|\,\boldsymbol{Y}) \tag{2.8}$$

where the random variable X at the input to the channel is uniform distribution and Y is the corresponding random variable at the channel output. When the main channel and the eavesdropper's channel are symmetric and the eavesdropper's channel is degraded with respect to the main channel, a simple expression for C_s was given by [67]:

$$C_s = H(\boldsymbol{X}|\boldsymbol{Z}) - H(\boldsymbol{X}\,|\,\boldsymbol{Y}) \tag{2.9}$$

An important example of a symmetric channel is the BSC channel. Let a BSC channel with crossover probability p be denoted by $BSC(p)$. If the main channel is $BSC(p_1)$ while

the eavesdropper's channel is $BSC(p_2)$, then the secrecy capacity is given by

$$C_s = \begin{cases} h(p_2) - h(p_1), & p_2 > p_1 \\ 0, & otherwise \end{cases} \tag{2.10}$$

where h denotes the binary entropy function defined by

$$h(p) = -p \log_2 p - (1-p) \log_2 (1-p)$$

2.4 Proposed Unconditional Security Model

In this section, we present the proposed unconditional security model in detail, where two steps are given for realizing unconditionally security communication, the first step is to build up a practical wiretap channel and the second step is to extend the advantages to achieve the unconditional secure communication by a security code scheme.

The unconditionally secure communications model targeted in this thesis is shown in Figure 2.3, where Alice sends m bits message $\boldsymbol{S} = \{s_1, s_2, \cdots, s_m\}$ to Bob. Firstly, Alice encodes the message such that

$$\boldsymbol{X} = \chi_1(\boldsymbol{S}) \tag{2.11}$$

where χ_1 is the security encoder function. Alice continues to encode $\boldsymbol{X}$ such that.

$$\boldsymbol{C} = \chi_2(\boldsymbol{X}) \tag{2.12}$$

where χ_2 is the channel encoder function. The channel coding step is optional. Then Alice and Bob perform the feedback as defined in next section. After several rounds two-way communication between Alice and Bob, the sequence $\boldsymbol{V}$ received by Bob is the noisy version of sequence $\boldsymbol{C}$. Meanwhile, Eve can also observe the noisy sequence $\boldsymbol{V}_e$. Bob and Eve perform channel decoding as:

$$\boldsymbol{Y} = \psi_2(\boldsymbol{V}) \tag{2.13}$$

$$\boldsymbol{Z} = \psi_2(\boldsymbol{V}_e) \tag{2.14}$$

where ψ_2 is channel decoding function, which is an invertible function of the channel encoding function χ_2. Then security decoding is performed as following:

$$\tilde{\boldsymbol{S}} = \psi_1(\boldsymbol{Y}) \tag{2.15}$$

$$\tilde{\boldsymbol{S}}_e = \psi_1(\boldsymbol{Z}) \tag{2.16}$$

where ψ_1 is security decoding function, which is an invertible function of security encoding function χ_1. In Eqs. (2.15) and (2.16), the eavesdropper uses the same decoding function ψ_1 as that of the legitimate. The decoding function ψ_1 that the legitimate used is the optimal receiving method. Therefore, if the eavesdropper want to get the optimal receiving result, he has to take this decoding function ψ_1 as his receiver. By security decoding, Bob gets the message estimation $\tilde{\boldsymbol{S}}$ with error probability $Pr(\tilde{\boldsymbol{S}} \neq \boldsymbol{S}) \to 0$ and Eve gets the message estimation $\tilde{\boldsymbol{S}}_e$ with error probability $Pr(\tilde{\boldsymbol{S}}_e \neq \boldsymbol{S}) \to 0.5$ at the same time. Therefore, the security of Alice's message $\boldsymbol{S}$ is guaranteed.

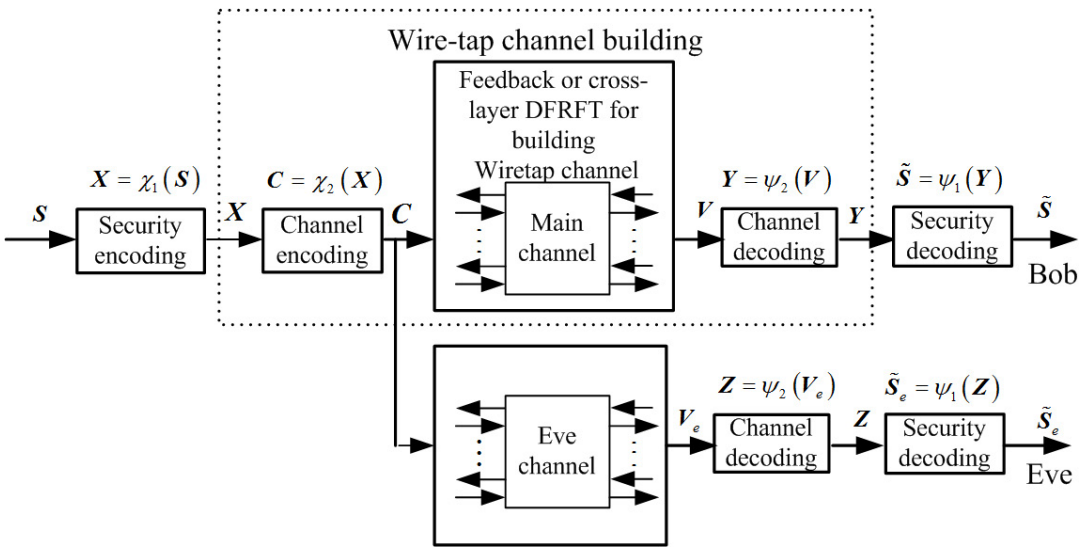


Figure 2.3: The unconditional communication model

Chapter 3

MRTWC Method for Building Wiretap Channels

Wyner [9, 10] proved that the transmitter could send information to the legitimate receiver in virtually perfect secrecy without sharing a secret key with the legitimate receiver if the eavesdropper's channel is a degraded version of the main channel. However, the assumption that the adversary only receives a degraded signal from the legitimate receiver is generally unrealistic. Wyner also did not mention how to build such advantages for the legitimate partners. This became a major problem in taking advantage of the advances in the wiretap channel model theory.

Most results focused on the MIMO approaches to build the advanced channel [36]-[49]. However, in some scenarios such as Device-to-Device (D2D) communication system [50]-[54], it is hard to support the multiple antennas. Maurer [55] is the first person to present a method to build an advantages for the legitimate partners without MIMO scheme. Maurer only presented one round feedback in his paper [55] under BSC channel, which has a drawback that the advantage of the main channel is less when the channel

noise is small. In this chapter, we develop this method to Multiple Rounds Two-Way Communication (MRTWC) method for building a wiretap channel in detail to enhance the advantage of the main channel. We also present the BER analysis for both one round feedback and novel MRTWC method under AWGN and Rayleigh channel.

3.1 Two-way Communication for Building Wire-tap Channel

[55] introduced two-way communications scheme, in which feedback signals from the destination play the role of private keys that initiate secure communications. An example is shown as follows.

Alice intends to send a sequence $\boldsymbol{S} = \{s_0, s_1, \cdots, s_{n-1}\}$ to Bob. To initiate a secure communication, firstly Bob sends a random sequence $\boldsymbol{Q} = \{q_0, q_1, \cdots, q_{n-1}\}$ to Alice, i.e. $Pr(q_i = 0) = Pr(q_i = 1) = 0.5$. Let $\boldsymbol{E} = \{e_0, e_1, \cdots, e_{n-1}\}$ and $\boldsymbol{E}_e = \{e_{e\_0}, e_{e\_1}, \cdots, e_{e\_n-1}\}$ denote the error vectors of the Alice's and the eavesdropper's channel, respectively. The received signals of Alice and the eavesdropper are

$$\boldsymbol{T} = \boldsymbol{E} + \boldsymbol{Q} \tag{3.1a}$$

and

$$\boldsymbol{T}_e = \boldsymbol{E}_e + \boldsymbol{Q} \tag{3.1b}$$

respectively, where $\boldsymbol{T} = \{t_0, t_1, \cdots, t_{n-1}\}, t_i = q_i \oplus e_i$ and $\boldsymbol{T}_e = \{t_{e_0}, t_{e_1}, \cdots, t_{e_{n-1}}\}, t_{e_i} = q_i \oplus e_{e_i}$. Then Alice uses the received signal $\boldsymbol{T}$ to calculate

$$\boldsymbol{U} = \boldsymbol{T} + \boldsymbol{S} \tag{3.2}$$

where $\boldsymbol{U} = \{u_0, u_1, \cdots, u_{n-1}\}, u_i = t_i \oplus m_i$. Alice encodes $\boldsymbol{U}$ such that

$$\boldsymbol{W} = \phi(\boldsymbol{U}) \tag{3.3}$$

where ϕ is the encoder function. Alice sends $\boldsymbol{W}$ over the channel. Bob and the eavesdropper receive the noise version of $\boldsymbol{W}$ as $\boldsymbol{W'}$ and decode $\boldsymbol{W'}$ as

$$\hat{\boldsymbol{U}} = \psi(\boldsymbol{W'}) \tag{3.4}$$

where ψ is the decoder function. We assume the decoding error probability $Pr(\hat{\boldsymbol{U}} \neq \boldsymbol{U}) \rightarrow 0$. Bob and the eavesdropper received $\boldsymbol{U}$ with almost error free. Bob knows the random sequence $\boldsymbol{Q}$, so he can add wise $\boldsymbol{Q}$ to $\boldsymbol{U}$ as

$$\boldsymbol{Y} = \boldsymbol{U} \oplus \boldsymbol{Q} = \boldsymbol{S} \oplus \boldsymbol{E} \tag{3.5}$$

where $\boldsymbol{Y} = \{y_0, y_1, \cdots, y_{n-1}\}$. The eavesdropper only knows $\boldsymbol{T}_e$ that is the noise version of $\boldsymbol{Q}$ and he only can add wise Eq. (3.1b) to $\boldsymbol{U}$ as:

$$\boldsymbol{Z} = \boldsymbol{U} \oplus \boldsymbol{T}_e = \boldsymbol{S} \oplus \boldsymbol{E} \oplus \boldsymbol{E}_e \tag{3.6}$$

where $\boldsymbol{Z} = \{z_0, z_1, \cdots, z_{n-1}\}$. By comparing Eq. (3.5) with Eq. (3.6), $\boldsymbol{E}_e$ becomes extra noise. Therefore, after the two-way communication in Figure 3.1, the direction of the main channel is inverted when the eavesdropper has a better channel at the beginning.

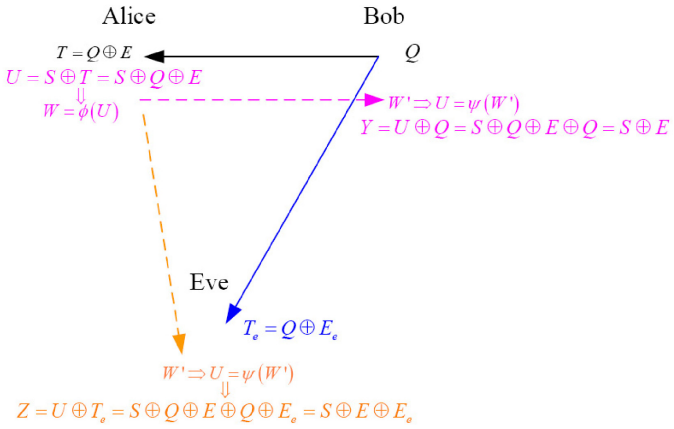


Figure 3.1: Two way communication

Lemma 3.1: Let the error probability of $\boldsymbol{E} = \{e_0, e_1, \cdots, e_i, \cdots, e_{n-1}\}$ in (3.1a) be $Pr(e_i = 1) = \alpha$ and the error probability of $\boldsymbol{E}_e = \{e_{e\_0}, e_{e\_1}, \cdots, e_{e\_i}, \cdots, e_{e\_n-1}\}$ in (3.1b)

be $Pr(e_{e\_i} = 1) = \beta$. After a round-trip two-way communication, the error probability of the main channel is α, and the error probability of the eavesdropper's channel is β, $\alpha + \beta - 2\alpha\beta$.

Proof: Since

$$Pr(y_i \neq s_i) = Pr(e_i = 1) = \alpha,$$

and

$$\begin{aligned} Pr(z_i \neq s_i) &= Pr(e_i = 1) \cdot Pr(e_{e_i} = 0) + Pr(e_i = 0) \cdot Pr(e_{e_i} = 1) \\ &= \alpha \cdot (1 - \beta) + (1 - \alpha) \cdot \beta \end{aligned}$$

Thus $Pr(z_i \neq s_i) = \alpha + \beta - 2\alpha\beta$.

Because $\alpha \leq 0.5$ and $\beta \leq 0.5$, so we have $\alpha \leq \alpha + \beta - 2\alpha\beta$, the equality holds for $\alpha = 0.5$ or $\beta = 0$.

According to the secret capacity C_s in (2.10), we know that the secrecy capacity C_s is very small when β is very small. The secret level of the system is very weak. it is clear that after a round-trip two-way communication, only the main channel quality is improved while the attacker's channel will still be as noisy as it was. Thus, there could be a method for changing the situation by continuing performing the two-way communication or parallel channel feedbacks round by round, where the advantage of the main channel will be increased accordingly. A wiretap channel can thus be built when the legitimate user's channel is better than that of the attacker by some extent. Based on the above observations, this thesis will present multiple rounds two-way communication for building the wiretap channel in the following section.

3.2 MRTWC Method for Building Wire-tap Channel

Following Maurer's two-way communication method [55] , this section proposed a multiple rounds two-way communication to extend the advantages of the legitimate partners. Obviously, we can not repeat the one round feedback again and again. Otherwise, the Eves can attack every one round feedback separately and the advantage of the main channel is not enhanced. As shown in Figure 3.2, our contribution is to put a channel coding on the top of the information and split the encoded sequence into multi streams randomly and let such random streams to perform the one way feedback in Figure 3.1. Eve can not get any useful information by attacking any stream. Instead, he has to add all the streams together and recovers the information from the added stream while the extra noise is accumulated, which degraded the Eve's channel.

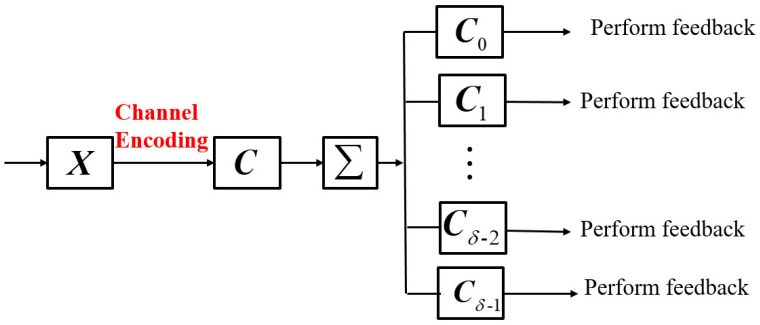


Figure 3.2: Encoded stream is split into multi streams

Alice wants to transmit m_1 bits message $\boldsymbol{X}$ to Bob, she selects a (n_1, m_1) linear binary code $\boldsymbol{C} = (c_0, c_1, \cdots, c_{n_1-1})$ such that

$$\boldsymbol{C} = \chi(\boldsymbol{X}) \tag{3.7}$$

where χ is the channel encoder function. Then Alice randomly chooses $\boldsymbol{C}_0, \boldsymbol{C}_1, \cdots, \boldsymbol{C}_{\delta-2}$

, where $\boldsymbol{C}_i = (c_i^0, c_i^1, \cdots, c_i^{n_1-1}), 0 \leq i < \delta - 2$ and δ is interactive communication rounds which determined by the channel noisy level [83]. The vector $\boldsymbol{C}_{\delta-1}$ can be calculated from encoded vector $\boldsymbol{C}$ in (3.7):

$$\boldsymbol{C}_{\delta-1} = \boldsymbol{C}_0 \oplus \boldsymbol{C}_1 \oplus \cdots \oplus \boldsymbol{C}_{\delta-2} \oplus \boldsymbol{C} \tag{3.8}$$

Following Eq. (3.8), Bob randomly generates δ sequences $\boldsymbol{Q}_i = (q_i^0, q_i^1, \cdots, q_i^{n_1-1})$, $i = 0, 1, 2, \cdots, \delta - 1$. The scheme may take two steps to complete the information exchange:

1)$Bob \rightarrow Alice$: $\boldsymbol{Q}_i = (q_i^0, q_i^1, \cdots, q_i^{n_1-1}), i = 0, 1, 2, \cdots, \delta - 1$. The received signals of Alice and the eavesdropper are $\boldsymbol{T}_i = \boldsymbol{Q}_i \oplus \boldsymbol{E}_i$ and $\boldsymbol{T}_{e\_i} = \boldsymbol{Q}_i \oplus \boldsymbol{E}_{e\_i}$, respectively, where $\boldsymbol{E}_i = (e_i^0, e_i^1, \cdots, e_i^{n_1-1})$ and $\boldsymbol{E}_{e\_i} = (e_{e\_i}^0, e_{e\_i}^1, \cdots, e_{e\_i}^{n_1-1})$ denote the error vectors of the Alice's and the eavesdropper's channel correspond to the transmitted the random sequence $\boldsymbol{Q}_i$, respectively.

2)$Alice \rightarrow Bob$: $\boldsymbol{U}_i = \boldsymbol{C}_i \oplus \boldsymbol{T}_i, i = 0, 1, 2, \cdots, \delta - 1$. Alice send $\boldsymbol{U}_i$ to Bob by the error free channel which can be obtained by using a powerful error correcting code. After Bob receives $\boldsymbol{U}_i$, he will use δ random sequences $\boldsymbol{Q}_i$ to calculate as

$$\boldsymbol{V}_i = \boldsymbol{U}_i \oplus \boldsymbol{Q}_i = \boldsymbol{C}_i \oplus \boldsymbol{T}_i \oplus \boldsymbol{Q}_i = \boldsymbol{C}_i \oplus \boldsymbol{E}_i \tag{3.9}$$

He sums the $\boldsymbol{V}_i, i = 0, 1, 2, \cdots, \delta - 1$ as

$$\boldsymbol{V} = \sum_{i=0}^{\delta-1} \boldsymbol{V}_i = \sum_{i=0}^{\delta-1} \boldsymbol{C}_i \oplus \sum_{i=0}^{\delta-1} \boldsymbol{E}_i \tag{3.10}$$

According to (3.8), we have:

$$\boldsymbol{V} = \boldsymbol{C} \oplus \sum_{i=0}^{\delta-1} \boldsymbol{E}_i \tag{3.11}$$

At the same time, Eve intercept $\boldsymbol{U}_i$. Instead of known the random sequence $\boldsymbol{Q}_i$, Eve only knows $\boldsymbol{T}_{e\_i}$. Therefore, Eve calculates as

$$\boldsymbol{V}_{e\_i} = \boldsymbol{U}_i \oplus \boldsymbol{T}_{e\_i} = \boldsymbol{C}_i \oplus \boldsymbol{E}_i \oplus \boldsymbol{E}_{e\_i} \tag{3.12}$$

Eve also can sum the $\boldsymbol{V}_{e\_i}, i = 0, 1, 2, \cdots, \delta - 1$ as

$$\boldsymbol{V}_e = \sum_{i=0}^{\delta-1} \boldsymbol{V}_{e\_i} = \sum_{i=0}^{\delta-1} \boldsymbol{C}_i \oplus \sum_{i=0}^{\delta-1} \boldsymbol{E}_i \oplus \sum_{i=0}^{\delta-1} \boldsymbol{E}_{e\_i} \tag{3.13}$$

$$\boldsymbol{V}_e = \boldsymbol{C} \oplus \sum_{i=0}^{\delta-1} \boldsymbol{E}_i \oplus \sum_{i=0}^{\delta-1} \boldsymbol{E}_{e\_i} \tag{3.14}$$

Finally, Bob perform channel decoding as:

$$\tilde{\boldsymbol{C}} = \psi(\boldsymbol{V}) \tag{3.15}$$

where ψ is the decoding function, which is an invertible function of χ. At the same time, Eve also can perform channel decoding as:

$$\tilde{\boldsymbol{C}}_e = \psi(\boldsymbol{V}_e) \tag{3.16}$$

Because of extra noise term $\sum_{i=0}^{\delta-1} \boldsymbol{E}_{e\_i}$ in (3.14), we have:

$$Pr(\tilde{\boldsymbol{C}} \neq \boldsymbol{C}) < Pr(\tilde{\boldsymbol{C}}_e \neq \boldsymbol{C}) \tag{3.17}$$

As a result, the adversary's channel is noisier than the one taken by the legitimate partner with sufficient rounds of such two-way communications. This scheme is shown in Figure 3.3.

3.3 BER and LLR Extraction of the MRTWC under Different Channels

The method of MRTWC provides a novel approach of creating wiretap channels, but the channel BER needs to be specifically quantified according to the crossover probability in the case of BSC, or the SNR in the case of AWGN and Rayleigh channels, before it can

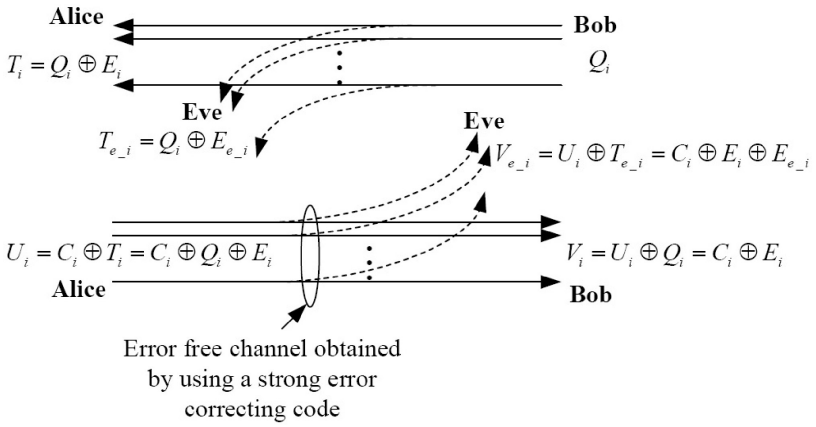


Figure 3.3: The MRTWC method employed in the study for creating wiretap channel.

be projected to the security and reliability conditions in (2.3) and (2.4), respectively. It is also necessary to derive the exact representation of bit Log-likelihood Ratios (LLR) for optimal soft information decoding and demodulation. Therefore, this section provides the BER extraction of the BSC, AWGN, and Rayleigh channels and LLR extraction under the MRTWC method.

3.3.1 BER over BSC

Let the error probability of $\boldsymbol{E}_i = (e_i^0, e_i^1, \cdots, e_i^{n-1})$ in (3.10) be denoted as $Pr(e_i^j = 1) = \alpha_i, i = 0, 1, 2, \cdots, \delta - 1$, and the error probability of $\boldsymbol{E}_{e\_i} = (e_{e\_i}^0, e_{e\_i}^1, \cdots, e_{e\_i}^{n-1})$ in (3.13) be denoted as $Pr(e_{e\_i}^j = 1) = \beta_i, i = 0, 1, 2, \cdots, \delta - 1$, which means that α_i and β_i are the crossover probabilities of the main channel and the eavesdropper channel, respectively. By considering single round ($i.e., \delta = 1$). The error probability of $\boldsymbol{V} = (v_0, v_1, \cdots, v_{n-1})$ in (3.10) and $\boldsymbol{V}_e = (v_{e\_0}, v_{e\_1}, \cdots, v_{e\_n-1})$ in (3.13) are:

$$Pr(v_j \neq c_j) = Pr(e_0^j = 1) = \alpha_0$$

$$\begin{aligned} Pr(v_{e\_j} \neq c_j) &= Pr(e_0^j = 1) \cdot Pr(e_{e\_0}^j = 0) + Pr(e_0^j = 0) \cdot Pr(e_{e\_0}^j = 1) \\ &= \alpha_0 \cdot (1 - \beta_0) + \beta_0 \cdot (1 - \alpha_0) = \alpha_0 + \beta_0 - 2\alpha_0\beta_0 \end{aligned} \tag{3.18}$$

Let α_i^j and β_i^j be jth received signal's error probabilities of the main channel and the eavesdropper channel under ith round communication, respectively. With (3.18), we can get the general case of the multiple rounds of two-way communication as following theory.

Lemma 3.2: After δ round-trip two-way communication, the bit-error rates (BERs) of the legitimate receiver and the eavesdropper are $1 - \frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\alpha_i^j)\right)$ and $1 - \frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\alpha_i^j)(1 - 2\beta_i^j)\right)$, respectively.

Proof: Following from (3.11), we have that Bobs BER ε_j^1 is

$$\varepsilon_j^1 = P_r(v_j \neq c_j) = P_r\left(\sum_{i=0}^{\delta-1} \oplus e_i^j = 1\right) = 1 - P_r\left(\sum_{i=0}^{\delta-1} \oplus e_i^j = 0\right). \tag{3.19}$$

Since the probability that an even number of digits in $\{e_0^j, e_1^j, \cdots, e_{\delta-1}^j\}$ are "1" is $\frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\alpha_i^j)\right)$ [69], thus (3.19) can be rewritten as

$$\varepsilon_j^1 = 1 - \frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\alpha_i^j)\right), \tag{3.20}$$

where $\alpha_i^j = P_r(e_i^j = 1)$.

Similarly, according to (3.14), we get that the BER ε_j^2 for Eve is

$$\begin{aligned} \varepsilon_j^2 = P_r(v_{e\_j} \neq c_j) &= P_r\left(\sum_{i=0}^{\delta-1} \oplus e_i^j \oplus \sum_{i=0}^{\delta-1} \oplus e_{e\_i}^j = 1\right) \\ = 1 - P_r(v_{e\_j} = c_j) &= P_r\left(\sum_{i=0}^{\delta-1} \oplus e_i^j \oplus \sum_{i=0}^{\delta-1} \oplus e_{e\_i}^j = 0\right). \end{aligned} \tag{3.21}$$

The probability that an even number of digits in $\{e_0^j, e_1^j, \cdots, e_{\delta-1}^j, e_{e\_0}^j, e_{e\_1}^j, \cdots, e_{e\_(\delta-1)}^j\}$ are "1" is [69]

$$\frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)\prod_{i=0}^{\delta-1}(1-2\beta_i^j)\right)=\frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)(1-2\beta_i^j)\right), \tag{3.22}$$

then (3.21) can be modified as

$$\varepsilon_j^2 = P_r(v_{e\_j}\neq c_j) = 1-\frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)(1-2\beta_i^j)\right), \tag{3.23}$$

where $\beta_i^j = P_r(e_{e\_i}^j = 1)$.

Hence, we obtain the statement of the theorem; Q.E.D.

(3.20) and (3.23) derived in Lemma 3.2 are essentially the same as (12a) and (12b) in [65], respectively. The only difference is in representation. Let $\delta = 1$, we have that the BERs of Bob and Eve are

$$\left.\begin{aligned}\varepsilon^1 &= 1-\tfrac{1}{2}(1+(1-2\alpha))\\ \varepsilon^2 &= 1-\tfrac{1}{2}(1+(1-2\alpha)(1-2\beta)) = \alpha+\beta-2\alpha\beta\end{aligned}\right\} \tag{3.24}$$

In (3.24), we obtain *lemma* 1 in [65].

According to (3.24), we can conclude that the BER of Bob after interaction is no more than that of Eve.

Lemma 3.3: After δ round-trip two-way communication, we can prove two statements about the relationship between ε^1 and ε^2.

Statements:

1) ε^1 is no more than ε^2, i.e., $\varepsilon^1 \leq \varepsilon^2$;

2) The equality in 1) holds for $\alpha = 0.5$, $0 \leq j \leq \delta - 1$, $1 \leq i \leq n$ or $\sum_{i=0}^{\delta-1} \oplus e_{e\_i}^{j} = 0$.

Proof: To prove the first statement, we note that

$$\prod_{i=0}^{\delta-1}(1-2\alpha_i^j) \geq \prod_{i=0}^{\delta-1}(1-2\alpha_i^j)(1-2\beta_i^j),$$

then

$$\frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)\right) \geq \frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)(1-2\beta_i^j)\right).$$

So that

$$1-\frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)\right) \leq 1-\frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)(1-2\beta_i^j)\right).$$

Hence we obtain $\varepsilon^1 \leq \varepsilon^2$.

To prove the second statement, let $\varepsilon^1 = \varepsilon^2$, we get

$$1-\frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)\right) = 1-\frac{1}{2}\left(1+\prod_{i=0}^{\delta-1}(1-2\alpha_i^j)(1-2\beta_i^j)\right). \tag{3.25}$$

From (3.25), we can obtain that $\varepsilon^1 = \varepsilon^2 = 0.5$. if $\alpha_i^j = 0.5$, $0 \leq j \leq \delta - 1$, $1 \leq i \leq n$.

Following from (3.19) and (3.21), we can obtain the fact that if $\sum_{i=0}^{\delta-1} \oplus e_{e\_i}^{j} = 0$, the equality in

$$\sum_{i=0}^{\delta-1} \oplus e_i^j = \sum_{i=0}^{\delta-1} \oplus e_i^j \oplus \sum_{i=0}^{\delta-1} \oplus e_{e\_i}^j \tag{3.26}$$

holds. Then we conclude that $\varepsilon^1 = \varepsilon^2$ on condition of $\sum_{i=0}^{\delta-1} \oplus e_{e\_i}^{j} = 0$.

Hence, we obtain the statement of the theorem; Q.E.D.

Lemma 3.4: For given $\{\alpha_i^j, \beta_i^j | \alpha_i^j = 0.5, 0 \leq i \leq \delta - 1, 1 \leq j \leq n\}$, the probability that the BER of the legitimate receiver equals to that of the eavesdropper is $\frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\beta_i^j)\right)$.

Proof: Following from *Lemma* 3.3, we have that

$$P_r(\varepsilon_j^1 = \varepsilon_j^2) = P_r\left(\sum_{i=0}^{\delta-1} \oplus e_{e\_i}^j = 0\right). \tag{3.27}$$

Note that the probability that an even number of digits are "1" is

$$\frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\beta_i^j)\right), \tag{3.28}$$

then

$$P_r(\varepsilon_j^1 = \varepsilon_j^2) = \frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\beta_i^j)\right). \tag{3.29}$$

Hence, we obtain the statement of the theorem; Q.E.D.

3.3.2 LLRs Extraction over BSC

The soft decoding algorithm is the optimum decoding method. For permitting the security, Bob should know the decoding performance under the optimum decoding method. However, LLRs of the received signals are necessary for performing the soft decoding algorithms. In this section, we give the method of the LLRs extraction of the received signals as following.

Lemma 3.5: After δ round-trip two-way communication, the LLR for c_j of the legitimate receiver is

$$llr(v_j) = \begin{cases} \ln \frac{\varepsilon_j^1}{1-\varepsilon_j^1}, \text{if } v_j = 0 \\ \ln \frac{1-\varepsilon_j^1}{\varepsilon_j^1}, \text{if } v_j = 1 \end{cases}, \tag{3.30}$$

and that for the eavesdropper is

$$llr(v_{e\_j}) = \begin{cases} \ln \frac{\varepsilon_j^2}{1-\varepsilon_j^2}, \text{if } v_{e\_j} = 0 \\ \ln \frac{1-\varepsilon_j^2}{\varepsilon_j^2}, \text{if } v_{e\_j} = 1 \end{cases}. \tag{3.31}$$

Proof: As for Bob, the LLR of c_j is give by [70]

$$llr(v_j) = \ln \frac{P_r(c_j = 1|v_j)}{P_r(c_j = 0|v_j)}. \tag{3.32}$$

According to *Lemma* 3.3, if $v_j = 0$, (3.32) can be modified as

$$llr(v_j) = \ln \frac{P_r(c_j = 1|v_j)}{P_r(c_j = 0|v_j)} = \ln \frac{P_r(v_j \neq c_j)}{P_r(v_j = c_j)} = \ln \frac{1 - \frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1-2\alpha_i^j)\right)}{\frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1-2\alpha_i^j)\right)} = \ln \frac{\varepsilon_j^1}{1-\varepsilon_j^1}. \tag{3.33}$$

If $v_j = 1$, (3.32) is now rewritten as

$$llr(v_j) = \ln \frac{P_r(c_j = 1|v_j)}{P_r(v_j = 0|v_j)} = \ln \frac{P_r(v_j = c_j)}{P_r(v_j \neq c_j)} = \ln \frac{\frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1-2\alpha_i^j)\right)}{1 - \frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1-2\alpha_i^j)\right)} = \ln \frac{1-\varepsilon_j^1}{\varepsilon_j^1}. \tag{3.34}$$

Similarly, the LLRs for c_{e_j} of Eve is

$$
\begin{aligned}
llr(v_{e\_j}) &= \ln \frac{P_r(c_j = 1|v_{e\_j})}{P_r(c_i = 0|v_{e\_j})} = \ln \frac{P_r(v_{e\_j} \neq c_j)}{P_r(v_{e\_j} = c_j)} \\
&= \ln \frac{1 - \frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\alpha_i^j)(1 - 2\beta_i^j)\right)}{\frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\alpha_i^j)(1 - 2\beta_i^j)\right)} = \ln \frac{\varepsilon_j^2}{1 - \varepsilon_j^2}.
\end{aligned} \tag{3.35}
$$

and

$$
\begin{aligned}
llr(v_{e\_j}) &= \ln \frac{P_r(c_j = 1|v_{e\_j})}{P_r(c_j = 0|v_{e\_j})} = \ln \frac{P_r(v_{e\_j} = c_j)}{P_r(v_{e\_j} \neq c_j)} \\
&= \ln \frac{\frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\alpha_i^j)(1 - 2\beta_i^j)\right)}{1 - \frac{1}{2}\left(1 + \prod_{i=0}^{\delta-1}(1 - 2\alpha_i^j)(1 - 2\beta_i^j)\right)} = \ln \frac{1 - \varepsilon_j^2}{\varepsilon_j^2}.
\end{aligned} \tag{3.36}
$$

for $v_{e\_j} = 0$ and $v_{e\_j} = 1$, respectively.

Hence, we obtain the statement of the theorem; Q.E.D.

Based on the above description, the process for building wiretap channel via multiple round two-way communication under the BSC is depicted in Table 3.1.

Table 3.1: Detailed process for building wiretap channel on the feedback

Algorithm 1 Building Wiretap Channel on the Feedback

1: Randomly generate m-bit secret messages $\boldsymbol{S}$;Set multiple round parameter δ
2: Compute $\boldsymbol{C}$ with (3.7)
3: **for** i from 0 to $\delta - 2$ **do**
4: Randomly generate binary sequence $\boldsymbol{C}_i$
5: **end for**
6: Compute $\boldsymbol{C}_{\delta-1}$ with (3.8)
7: **for** i from 0 to $\delta - 1$ **do**
8: Bob randomly generates binary sequence $\boldsymbol{Q}_i$ and sends to the wireless channel
9: Alice and Eve receive the noisy version of $\boldsymbol{Q}_i$ as $\boldsymbol{T}_i$
10: Alice calculates $\boldsymbol{U}_i$ as $\boldsymbol{U}_i = \boldsymbol{C}_i + \boldsymbol{T}_i$ and send $\boldsymbol{U}_i$ to the "error free" wireless channel
11: Bob and Eve receive $\boldsymbol{U}_i$ and get $\boldsymbol{V}_i$ and $\boldsymbol{V}_{e\_i}$ according to (3.9) and (3.12), respectively
12: **end for**
13: **for** j from 0 to $n - 1$ **do**
14: Compute $llr(v_j)$ according to (3.33) or (3.34)
15: Compute $llr(v_{e\_j})$ according to (3.35) or (3.36)
16: **end for**
17: The legitimate receiver computes $\tilde{\boldsymbol{C}}$ by soft decoding with $\{llr(v_1), \cdots, llr(v_n)\}$
18: The Eve computes $\tilde{\boldsymbol{C}}_e$ by the soft decoding with $\{llr(v_{e\_1}), \cdots, llr(v_{e\_n})\}$
19: The legitimate receiver and Eve recover the secret messages

3.3.3 BER over AWGN

Under an AWGN channel, the attack model considered in this thesis is that the wiretapper can demodulate every intercepted transmission and process the obtained information, which is the most aggressive attack that the wiretapper can possibly launch. Without

loss of generality, we consider that the transmissions are modulated under Binary Phase Shift Keying (BPSK), and our target is to map the SNR under AWGN to BER. The same approach can be applied to any other modulation scheme. The BER of BPSK signals on AWGN channels with coherent detection, denoted as $p_b(e)$, is given by [94]:

$$P_b(e) = \boldsymbol{Q}(\sqrt{\frac{2E_s}{N_0}}) \tag{3.37}$$

where E_s is the transmitted energy per bit, $N_0 = 2\sigma^2$ is the noise power spectral density and $\boldsymbol{Q}(\cdot)$ function is defined as:

$$\boldsymbol{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-t^2/2} dt, x \geq 0$$

Let γ denote the average SNR. (3.37) can also be written as

$$P_b(e) = \boldsymbol{Q}(\sqrt{\gamma}) \tag{3.38}$$

The BER of AWGN channels with other modulation methods can refer [94].

The model of MRTWC over the AWGN channel is shown in Figure 3.4, which is extended from the model in Figure 3.3. We have:

$$\boldsymbol{T}_i = \boldsymbol{Q}_i + \boldsymbol{N}_i \tag{3.39}$$

$$\boldsymbol{T}_{e\_i} = \boldsymbol{Q}_i + \boldsymbol{N}_{e\_i} \tag{3.40}$$

where $i = 0, 1, 2, \cdots, \delta - 1$. The ith signal received by Bob and Eve is:

$$\boldsymbol{V}_i = \boldsymbol{C}_i + \boldsymbol{T}_i + \boldsymbol{Q}_i = \boldsymbol{C}_i + \boldsymbol{Q}_i + \boldsymbol{N}_i + \boldsymbol{Q}_i = \boldsymbol{C}_i + \boldsymbol{N}_i \tag{3.41}$$

and

$$\begin{aligned} \boldsymbol{V}_{e\_i} &= \boldsymbol{C}_i + \boldsymbol{T}_i + \boldsymbol{T}_{e\_i} + \boldsymbol{Q}_i \\ &= \boldsymbol{C}_i + \boldsymbol{Q}_i + \boldsymbol{N}_i + \boldsymbol{Q}_i + \boldsymbol{N}_{e\_i} = \boldsymbol{C}_i + \boldsymbol{N}_i + \boldsymbol{N}_{e\_i} \end{aligned} \tag{3.42}$$

where $\boldsymbol{N}_i$ and $\boldsymbol{N}_{e\_i}$ are independent AWGN samples with zero mean, and variances σ_i^2 and $\sigma_{e\_i}^2$, respectively. Bob and Eve sum $\boldsymbol{V}_i$ and $\boldsymbol{V}_{e\_i}$ as:

$$\boldsymbol{V} = \sum_{i=0}^{\delta-1} \boldsymbol{V}_i = \sum_{i=0}^{\delta-1} \boldsymbol{C}_i + \sum_{i=0}^{\delta-1} \boldsymbol{N}_i \tag{3.43}$$

$$\boldsymbol{V}_e = \sum_{i=0}^{\delta-1} \boldsymbol{V}_{e\_i} = \sum_{i=0}^{\delta-1} \boldsymbol{C}_i + \sum_{i=0}^{\delta-1} \boldsymbol{N}_i + \sum_{i=0}^{\delta-1} \boldsymbol{N}_{e\_i} \tag{3.44}$$

We assumed that the random sequence $\boldsymbol{Q}_i$ is transmitted with equal power. Let the average transmitted power of ith random sequence $\boldsymbol{Q}_i$ be denoted as $\boldsymbol{P}_i$ and the ith noise power of receive branch be denoted as σ_i^2. The average SNR of $\boldsymbol{T}_i$ in (3.39) is equal to the ratio of the transmitted power and the noise power per receiver. Thus it can be written as:

$$\gamma_i = \frac{P_i}{\sigma_i^2} \tag{3.45}$$

The SNR of $\boldsymbol{T}_{e\_i}$ in (3.40) can be written as:

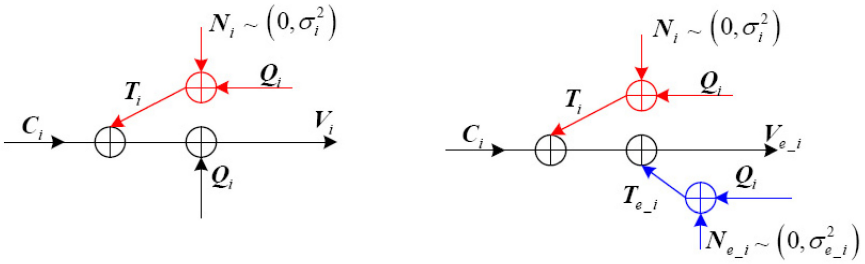
$$\gamma_{e\_i} = \frac{P_i}{\sigma_{e\_i}^2} \tag{3.46}$$

By construction the model of MRTWC over AWGN channels in Figure 3.3, the bit error probabilities for both the main channel and the Eves channel are mapped from the SNR under AWGN. Then the same calculation steps can be taken from subsection 3.3.1. With(3.38), we have the bit error probabilities of $\boldsymbol{T}_i$ and $\boldsymbol{T}_{e\_i}$ as $Pr(\boldsymbol{T}_i) = \boldsymbol{Q}(\gamma_i) = \alpha_{A\_i}$ and $Pr(\boldsymbol{T}_{e\_i}) = \boldsymbol{Q}(\gamma_{e\_i}) = \beta_{A\_i}$, respectively. Then we have the bit error probabilities of $\boldsymbol{V}_i$ and $\boldsymbol{V}_{e\_i}$ as:

$$Pr(\boldsymbol{V}_i) = \alpha_{A\_i} \tag{3.47}$$

$$Pr(\boldsymbol{V}_{e\_i}) = \alpha_{A\_i} + \beta_{A\_i} - 2\alpha_{a\_i}\beta_{a\_i} \tag{3.48}$$

The BER of $\boldsymbol{V}$ in (3.43) and $\boldsymbol{V}_e$ in (3.44) can be calculated according (3.19) to (3.21)



(a) Action of Bob (b) Action of Eve

Figure 3.4: The model of MRTWC over AWGN Channels

3.3.4 LLRs Extraction over AWGN

After a round-trip two-way communication, let $\boldsymbol{C} = (c_0, c_1, \cdots, c_j, \cdots, c_{n-1})$ be the information that Alice sends to Bob, $\boldsymbol{Q} = \{q_0, q_1, \cdots, q_{n-1}\}$ be a random sequence that Bob sends to Alice , and $\boldsymbol{V} = (v_0, v_1, \cdots, v_j, \cdots, v_{n-1})$ and $\tilde{\boldsymbol{V}} = (\tilde{v}_0, \tilde{v}_1, \cdots, \tilde{v}_j, \cdots, \tilde{v}_{n-1})$ be the Bob's received sequence after interaction and decoded sequence, respectively.

We have:

$$v_j = (2c_j - 1) + (2q_j - 1) + n_j, n_j \sim CN(0, \sigma_1^2) \tag{3.49}$$

$$\tilde{v}_j = v_j - (2q_j - 1) = 2c_j - 1 + n_j. \tag{3.50}$$

Similarly, we denote Eves received sequence after interaction as $\boldsymbol{V}_e = (v_{e\_0}, v_{e\_1}, \cdots, v_{e\_j}, \cdots, v_{e\_(n-1)})$ and $\tilde{\boldsymbol{V}}_e = (\tilde{v}_{e\_0}, \tilde{v}_{e\_1}, \cdots, \tilde{v}_{e\_j}, \cdots, \tilde{v}_{e\_(n-1)})$ as the sequence for Eves decoding, and then we can have

$$\tilde{v}_{e\_j} = v_{e\_j} - (2q_j - 1 + n_{e\_j}) = 2c_j - 1 + n_j - n_{e\_j}, \tag{3.51}$$

where $n_{e\_j} \sim CN(0, \sigma_2^2)$.

Lemma 3.6: After a round-trip two-way communication, the bit LLR derived from v_j is $2v_j/\sigma_1^2$, and that derived from v_{e_j} is $2v_{e\_j}/(\sigma_1^2 + \sigma_2^2)$.

Proof: Following from (3.50), we get that the bit LLR derived from v_j is $2v_j/\sigma_1^2$ [70]. Note that $(n_j - n_{e\_j}) \sim CN(0, \sigma_1^2 + \sigma_2^2)$, then the LLR derived from v_{e_j} is $2v_{e\_j}/(\sigma_1^2 + \sigma_2^2)$ following from (3.51) [70].

Hence, the statement of the theorem is achieved; Q.E.D.

From *lemma* 3.6, we conclude that if the two feedback channel conditions are the same, i.e., $\sigma_1^2 = \sigma_2^2 = \sigma^2$, the LLRs derived from v_j and v_{e_j} are $2v_j/\sigma^2$ and v_{e_j}/σ^2, respectively. Moreover, if the feedback channel between Bob and Eve is error-free, the BERs of Bob and Eve will be the same after interaction. Otherwise, the Bobs BER is smaller than Eves.

Let $\boldsymbol{C} = (\boldsymbol{C}_0, \boldsymbol{C}_1, \cdots, \boldsymbol{C}_i, \cdots, \boldsymbol{C}_{(\delta-1)})$ be n-dimensional encoded vectors that Alice aims to send to Bob in (3.8) and $\boldsymbol{Q} = (\boldsymbol{Q}_0, \boldsymbol{Q}_1, \cdots, \boldsymbol{Q}_i, \cdots, \boldsymbol{Q}_{(\delta-1)})$ be n-dimensional vectors that Bob randomly generates and sends to Alice, where ith vector can be denoted as $\boldsymbol{C}_i = (c_i^0, c_i^1, \cdots, c_i^j, \cdots, c_i^{n-1})$ and $\boldsymbol{Q}_i = (q_i^0, q_i^1, \cdots, q_i^j, \cdots, q_i^{n-1}))$. Within δ round-trip two-way communication, the received δ n-dimensional vectors $\boldsymbol{V} = (\boldsymbol{V}_0, \boldsymbol{V}_1, \cdots, \boldsymbol{V}_i, \cdots, \boldsymbol{V}_{(\delta-1)})$ of Bob after interaction and ith vector can be denoted as

$$\boldsymbol{V}_i = (v_i^0, v_i^1, \cdots, v_i^j, \cdots, v_i^{n-1}),\ 0 \le i \le \delta - 1,\ 0 \le j \le n - 1 \tag{3.52}$$

where

$$v_i^j = (2c_i^j - 1) + (2q_i^j - 1) + n_i^j,\ n_i^j \sim CN(0, \sigma_1^2). \tag{3.53}$$

Thus, the n-dimensional decoded vectors of Bob are $\tilde{\boldsymbol{V}} = (\tilde{\boldsymbol{V}}_0, \tilde{\boldsymbol{V}}_1, \cdots, \tilde{\boldsymbol{V}}_i, \cdots, \tilde{\boldsymbol{V}}_{(\delta-1)})$ and ith vector can be given by

$$\tilde{\boldsymbol{V}}_i = (\tilde{v}_i^0, \tilde{v}_i^1, \cdots, \tilde{v}_i^j, \cdots, \tilde{v}_i^{n-1}) \tag{3.54}$$

where

$$\tilde{v}_i^j = (2c_i^j - 1) + n_i^j. \tag{3.55}$$

In a similar way, we denote the δ n-dimensional vectors $\boldsymbol{V}_e = (\boldsymbol{V}_{e\_0}, \boldsymbol{V}_{e\_1}, \cdots, \boldsymbol{V}_{e\_i}, \cdots, \boldsymbol{V}_{e\_(\delta-1)})$ of Bob after interaction and ith vector can be denoted as

$$\boldsymbol{V}_{e\_i} = (v_{e\_i}^0, v_{e\_i}^1, \cdots, v_{e\_i}^j, \cdots, v_{e\_i}^{n-1}),\ 0 \le i \le \delta - 1,\ 0 \le j \le n-1 \tag{3.56}$$

where $v_{e\_i}^j = (2c_i^j - 1) + (2q_i^j - 1) + n_i^j$. Then, the n-dimensional decoded vectors of Eve are $\tilde{\boldsymbol{V}}_e = (\tilde{\boldsymbol{V}}_{e\_0}, \tilde{\boldsymbol{V}}_{e\_1}, \cdots, \tilde{\boldsymbol{V}}_{e\_i}, \cdots, \tilde{\boldsymbol{V}}_{e\_(\delta-1)})$ and ith vector can be given by

$$\tilde{\boldsymbol{V}}_{e\_i} = (\tilde{v}_{e\_i}^0, \tilde{v}_{e\_i}^1, \cdots, \tilde{v}_{e\_i}^j, \cdots, \tilde{v}_{e\_i}^{n-1}) \tag{3.57}$$

Then, we can have $\tilde{v}_{e\_i}^j = (2c_i^j - 1) + n_i^j - n_{e\_i}^j$.

Lemma 3.7: After δ round-trip two-way communication, the LLR of bit c_j for the legitimate receivers decoding can be given by

$$2\text{arc}\tanh\left(\prod_{i=0}^{\delta-1}\tanh\left(\frac{v_i^j}{\sigma_1^2}\right)\right)$$

and that for the eavesdropper can be written as

$$2\text{arc}\tanh\left(\prod_{i=0}^{\delta-1}\tanh\left(\frac{v_{e\_i}^j}{\sigma_1^2+\sigma_2^2}\right)\right)$$

.

Proof: From (3.8), we note $\boldsymbol{C} = \overset{\delta-1}{\underset{i=0}{\oplus}}\boldsymbol{C}_i$, and then we get $c^i \oplus \overset{\delta-1}{\underset{i=0}{\oplus}} c_i^j = 0$. That is to say, $(c_i^0, c_i^1, c_i^2, \cdots, c_i^{\delta-1}, c_i)$ is a codeword of the binary $(\delta, \delta-1)$ single-parity-check (SPC) code [70, 72, 73].

From (3.54), we note that the ith column of $\tilde{\boldsymbol{V}}_i$ is exactly the corresponding channel receive vector of $(c_i^0, c_i^1, c_i^2, \cdots, c_i^{n-1}),\ 0 \le i \le \delta - 1$ for Bob. Then, the LLR of bit c_i^j is [70, 72]

$$2\text{arc}\tanh\left(\prod_{i=0}^{\delta-1}\tanh\left(\frac{\tilde{v}_i^j}{\sigma_1^2}\right)\right), \tag{3.58}$$

where $\operatorname{arc}\tanh x$ is the inverse function of $\tanh x$ defined as

$$\tanh x = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

Similarly, we observe that the column of $\tilde{\boldsymbol{V}}_{e\_i}$ is the corresponding channel receive vector of $(c_i^0, c_i^1, c_i^2, \cdots, c_i^{n-1})$, $0 \leq i \leq \delta - 1$ for Eve following from (3.57). Therefore, the LLR of bit c_i^j is [70, 72]

$$2\operatorname{arc}\tanh\left(\prod_{i=0}^{\delta-1}\tanh\left(\frac{\tilde{v}_{e\_i}^j}{\sigma_1^2+\sigma_2^2}\right)\right). \tag{3.59}$$

Hence, the statement of the theorem is achieved; Q.E.D.

3.3.5 BER over Rayleigh Channel

Similar to the case of the AWGN, we consider the model of MRTWC over Rayleigh channels as shown in Figure 3.5. We have:

$$Pr(\boldsymbol{T}_i) = \lambda_i \boldsymbol{Q}_i + \boldsymbol{N}_i \tag{3.60}$$

$$Pr(\boldsymbol{T}_{e\_i}) = \lambda_{e\_i} \boldsymbol{Q}_i + \boldsymbol{N}_{e\_i} \tag{3.61}$$

where $i = 0, 1, 2, \cdots, \delta - 1$; λ_i is the fading coefficient magnitude between Bob and Alice, and λ_{e_i} is the fading coefficient magnitude between Bob and Eve. The corresponding ith signal received by Bob and Eve, respectively, can be expressed as:

$$\boldsymbol{V}_i = \boldsymbol{C}_i + \boldsymbol{T}_i + \boldsymbol{Q}_i = \boldsymbol{C}_i + \lambda_i \boldsymbol{Q}_i + \boldsymbol{N}_i + \boldsymbol{Q}_i \tag{3.62}$$

and

$$\boldsymbol{V}_{e\_i} = \boldsymbol{C}_i + \boldsymbol{T}_i + \boldsymbol{T}_{e\_i} = \boldsymbol{C}_i + \lambda_i \boldsymbol{Q}_i + \boldsymbol{N}_i + \lambda_{e\_i} \boldsymbol{Q}_i + \boldsymbol{N}_{e\_i} \tag{3.63}$$

where $\boldsymbol{N}_i$ and $\boldsymbol{N}_{e\_i}$ are the AWGN sample with zero mean and variances denoted as σ_i^2 and $\sigma_{e\_i}^2$, respectively. Bob and Eve sum $\boldsymbol{V}_i$ and $\boldsymbol{V}_{e\_i}$ as:

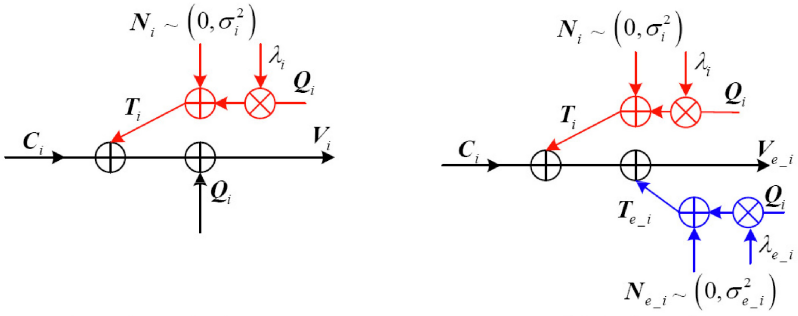
$$\boldsymbol{V} = \sum_{i=0}^{\delta-1} \boldsymbol{V}_i = \sum_{i=0}^{\delta-1} \boldsymbol{C}_i + \sum_{i=0}^{\delta-1} (\lambda_i + 1)\, \boldsymbol{Q}_i + \sum_{i=0}^{\delta-1} \boldsymbol{N}_i \tag{3.64}$$

$$\boldsymbol{V}_e = \sum_{i=0}^{\delta-1} \boldsymbol{V}_{e\_i} = \sum_{i=0}^{\delta-1} \boldsymbol{C}_i + \sum_{i=0}^{\delta-1} (\lambda_i + \lambda_{e\_i})\, \boldsymbol{Q}_i + \sum_{i=0}^{\delta-1} \boldsymbol{N}_i + \sum_{i=0}^{\delta-1} \boldsymbol{N}_{e\_i} \tag{3.65}$$

For a given fading attenuation coefficient λ , the average SNR per bit is defined as:

$$\bar{\gamma} = E(\lambda^2) \frac{E_s}{N_0} \tag{3.66}$$

where $E(\cdot)$ denotes the expectation operation. For a Rayleigh fading channel, the average



(a) Action of Bob (b) Action of Eve

Figure 3.5: The model of MRTWC over Rayleigh Channels

BER of BPSK signals is given by [94]

$$P_b(e) = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}}{1+\bar{\gamma}}}\right) \tag{3.67}$$

Let $\bar{\gamma}_i$ and $\bar{\gamma}_{e\_i}$ be the SNR of $\boldsymbol{T}_i$ in (3.60) and $\boldsymbol{T}_{e\_i}$ in (3.61), respectively. We have the BER of $\boldsymbol{T}_i$ and $\boldsymbol{T}_{e\_i}$ as:

$$Pr(\boldsymbol{T}_i) = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_i}{1+\bar{\gamma}_i}}\right) = \alpha_{R\_i}$$

$$Pr(\boldsymbol{T}_{e\_i}) = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_{e\_i}}{1+\bar{\gamma}_{e\_i}}}\right) = \beta_{R\_i}$$

Thus, the BER of $\boldsymbol{V}_i$ and $\boldsymbol{V}_{e\_i}$ can be written as:

$$Pr(\boldsymbol{V}_i) = \alpha_{R\_i} \tag{3.68}$$

$$Pr(\boldsymbol{V}_{e\_i}) = \alpha_{R\_i} + \beta_{R\_i} - 2\alpha_{R\_i}\beta_{R\_i} \tag{3.69}$$

The BER of $\boldsymbol{V}$ in (3.64) and $\boldsymbol{V}_e$ in (3.65) can be calculated according (3.19) to (3.21)

Chapter 4

A Novel Security Code Construction

To achieve the unconditional security system in Figure 2.3, a security encoding and decoding function (i.e., χ_1 and ψ_1) with short code lengths, low complexity, and high achievable security capacity should be in place for wireless applications. For this purpose, the thesis constructs a novel big family of security codes with good properties from both binary and non-binary resilient functions in this chapter.

4.1 Coset Security Codes

Wyner [9] firstly introduced the coset code based on a random construction to solve the particular case when the main channel is noiseless and the wiretap channel is noisy BSC channel. It was significantly extended and generalized in [71, 31]. However, no effective encoding and decoding algorithm was developed, such that the coset coding scheme can hardly be practically used. But the coset code are still the basis to construct the other good security codes. Here we present its construction as following.

To transmit k bits message $\boldsymbol{S}^j = \{s_1^j, s_2^j, \cdots, s_k^j\}, j = 1, 2, \cdots, 2^k$, a $(n, n-k)$ linear

Table 4.1: Coset code

		$\boldsymbol{Ce}^1$	$\boldsymbol{Ce}^2$	$\cdots$	$\boldsymbol{Ce}^i$	$\cdots$	$\boldsymbol{Ce}^{2^{(n-k)}}$
$\boldsymbol{S}^1 \rightarrow \boldsymbol{V}^1$	$\boldsymbol{w}^1$	$\boldsymbol{w}^1 \oplus \boldsymbol{Ce}^1$	$\boldsymbol{w}^1 \oplus \boldsymbol{Ce}^2$	$\cdots$	$\boldsymbol{w}^1 \oplus \boldsymbol{Ce}^i$	$\cdots$	$\boldsymbol{w}^1 \oplus \boldsymbol{Ce}^{2^{(n-k)}}$
$\boldsymbol{S}^2 \rightarrow \boldsymbol{V}^2$	$\boldsymbol{w}^2$	$\boldsymbol{w}^2 \oplus \boldsymbol{Ce}^1$	$\boldsymbol{w}^2 \oplus \boldsymbol{Ce}^2$	$\cdots$	$\boldsymbol{w}^2 \oplus \boldsymbol{Ce}^i$	$\cdots$	$\boldsymbol{w}^2 \oplus \boldsymbol{Ce}^{2^{(n-k)}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$\boldsymbol{S}^j \rightarrow \boldsymbol{V}^j$	$\boldsymbol{w}^j$	$\boldsymbol{w}^j \oplus \boldsymbol{Ce}^1$	$\boldsymbol{w}^j \oplus \boldsymbol{Ce}^2$	$\cdots$	$\boldsymbol{w}^j \oplus \boldsymbol{Ce}^i$	$\cdots$	$\boldsymbol{w}^j \oplus \boldsymbol{Ce}^{2^{(n-k)}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$\boldsymbol{S}^{2^k} \rightarrow \boldsymbol{V}^{2^k}$	$\boldsymbol{w}^{2^k}$	$\boldsymbol{w}^{2^k} \oplus \boldsymbol{Ce}^1$	$\boldsymbol{w}^{2^k} \oplus \boldsymbol{Ce}^2$	$\cdots$	$\boldsymbol{w}^{2^k} \oplus \boldsymbol{Ce}^i$	$\cdots$	$\boldsymbol{w}^{2^k} \oplus \boldsymbol{Ce}^{2^{(n-k)}}$

binary code $\boldsymbol{Ce}$ with coset $\boldsymbol{V} = \{\boldsymbol{V}^1, \boldsymbol{V}^2, \cdots, \boldsymbol{V}^{2^k}\}$ is chosen. Let each message $\boldsymbol{M}^j$ correspond to a coset $\boldsymbol{V}^j = \{\boldsymbol{V}_1^j, \boldsymbol{V}_2^j, \cdots, \boldsymbol{V}_{2^{n-k}}^j\}$, where n-tuple $\boldsymbol{V}_i^j$ such that

$$\boldsymbol{V}_i^j = \boldsymbol{w}^j \oplus \boldsymbol{Ce}^i, i = 2^{n-k}, j = 2^k, \tag{4.1}$$

$\boldsymbol{w}^j$ and $\boldsymbol{Ce}^i \in \{0,1\}^n$, $\boldsymbol{Ce}^i$ is codeword of $(n, n-k)$ linear binary code. We construct the encoder such that the encoder output $\boldsymbol{V}_i^j \in \{0,1\}^n$ is a randomly chosen member of the coset when the sending message is $\boldsymbol{S}^j$. Therefore, message $\boldsymbol{S}^j$ and $\boldsymbol{w}^j$ corresponding the syndrome and error vector of the code $\boldsymbol{Ce}$, respectively. This scheme can refer as Table 4.1.

Clearly, the decoder of the legitimate receiver can recover $\boldsymbol{S}^j$ from output $\boldsymbol{V}_i^j$ perfectly if the legitimate communication partners hold an error free channel. Now we turn to eavesdroppers who observe the noisy version $\boldsymbol{Z}e^j \in \{0,1\}^n$, which is the output of the BSC corresponding to the input $\boldsymbol{V}_i^j$. Let $\boldsymbol{S} = \{s_1, s_2, \cdots, s_k\}$, $\hat{\boldsymbol{S}} = \{\hat{s}_1, \hat{s}_2, \cdots, \hat{s}_k\}$ and $\hat{\boldsymbol{S}}_e = \{\hat{s}_{e_1}, \hat{s}_{e_2}, \cdots, \hat{s}_{e_k}\}$ be vectors denoting Alice's message, Bob's decoded message and Eve's decoded message, respectively. We can state the security criterion to guarantee security of Alice's message $\boldsymbol{S}^j$ as following lemma.

Lemma 4.1: The average BER of the recovering message $\boldsymbol{S}^j$ from $\boldsymbol{Z}e^j$ equals to 0.5,

i.e., $Pr(s_i^j \neq \hat{s}_{e_i}^j) = 0.5$, when the received noisy version $\boldsymbol{Z}e^j$ has the equal probability to fall into one of cosets $\boldsymbol{V}$, i.e., $Pr(\boldsymbol{Z}e^j \in \boldsymbol{V}^j) = 2^{-k}$, for $j = 1, 2, \cdots, 2^k$.

The proof of this lemma can refer [83].

following the Wyner's coset security codes, there are some researched results about the novel security codes construction. [32] presented security codes derived from polar codes, which asymptotically achieve the whole capacity equivocation region for the wiretap channel. [61] presented a channel-state-aware security code construction for achieving the secrecy capacity under a wide range of wiretap channels. By using polar codes, [32, 61] yield a code length of 2^{20} bits, which is not practical in wireless communications. [33, 34] is the only study on a practical solution via LDPC codes to asymptotically achieve the whole capacity equivocation region for the wiretap channel. But it is on the Binary Erasure Channel (BEC) instead the BSC, which is not considered a reasonable channel model. Note that the bound provided by [33] is the best result among all the reported ones for the short security codes under BSC channel. All these security codes construction are based on the coset codes construction. [79] provided the connection between security codes and binary resilient functions. But it did not provide an effective encoding method for the developed security codes. Apparently, how to construct the security code close to security capacity under BSC while being practically low-complexity implementable, is still an open problem. However, also these results can be catalogued into the coset security codes.

In this research, it is the first time to explore developing the low-complexity encoding and decoding short-length security coding scheme via the resilient fanction for wireless communication applications.

4.2 Binary Security Code Construction from Resilient Functions

4.2.1 Binary Resilient Functions

Resilient functions were firstly introduced and studied in [58, 59, 60], and were originally applied respectively to the key distribution and generation of random strings in presence of faulty processors. The definition of binary resilient functions is as follows.

Definition 4.1 [58]: Let $n \geq m \geq 1$ be integers and suppose:

$$f\colon \{0,1\}^n \longrightarrow \{0,1\}^m \tag{4.2}$$

where f is a function that accepts n input bits and produces m output bits. Let $t \leq n$ be an integer. Suppose $(x_1, x_2, \cdots, x_n) \in \{0,1\}^n$, where t arbitrary input bits out of n are fixed by an adversary, and the remaining $n-t$ input bits are chosen independently at random. Then f is said to be t-resilient by which an output of every possible m-tuple is equally likely to occur. Formally, the property can be stated as follows: Suppose $f(x_1, x_2, \cdots, x_n) = (s_1, s_2, \cdots, s_m)$ and let $(z_1, z_2, \cdots, z_n) \in \{0,1\}^n$ be an accepted input by an adversary. For every t-subset $(i_1, i_2, \cdots, i_t) \subseteq \{1, 2, \cdots, n\}$, we have:

$$Pr(f(z_1, z_2, \cdots, z_n) = (s_1, s_2, \cdots, s_m) | x_{i_j} = z_{i_l}) = \frac{1}{2^m} \tag{4.3}$$

where $0 \leq j, l \leq t$. Such a function f is called as a binary (n, m, t) resilient function.

Theorem 4.1: Let us consider the model in Figure 4.1. Let n-tuple $\boldsymbol{X} = (x_1, x_2, \cdots, x_n)$ pass a BSC channel and $\boldsymbol{Z} = (z_1, z_2, \cdots, z_n)$ is a noisy version of $\boldsymbol{X}$. Let f be an (n, m, t) resilient function, and set $(s_1, s_2, \cdots, s_m) = f(x_1, x_2, \cdots, x_n)$ and $(\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m) = f(z_1, z_2, \cdots, z_n)$. Let the channel crossover probability be p , i.e. $Pr(x_i \neq z_i) = p$. If:

$$p \geq \frac{(n-t)}{2n} \tag{4.4}$$

then we have:

$$Pr((\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m) = (s_1, s_2, \cdots, s_m)) = \frac{1}{2^m} \tag{4.5}$$

Proof: Let us firstly consider n-tuple $\boldsymbol{X} = (x_1, x_2, \cdots, x_n)$ and $\boldsymbol{Z} = (z_1, z_2, \cdots, z_n)$. If $\boldsymbol{Z}$ takes exact arbitray t bits from $\boldsymbol{X}$, it is obviously that there are randomly and independently t bits correctly taken in $\boldsymbol{Z}$, and a half of the remaining $n-t$ bits as correct and the other half as incorrect. Therefore, the total correct bits in $\boldsymbol{Z}$ are $\frac{1}{2}(n+t)$ and the total error bits in $\boldsymbol{Z}$ are $\frac{1}{2}(n-t)$, which leads to $Pr(x_i \neq z_i) = \frac{n-t}{2n}$. If $Pr(x_i \neq z_i) \geq \frac{n-t}{2n}$, it means no more than t bits in $\boldsymbol{Z}$ are correctly taken from $\boldsymbol{X}$. From **Definition** 4.1 the output $(\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$ recovered from $\boldsymbol{Z}$ is uniform distribution over m-tuple vector space. Thus (4.4) and (4.5) hold immediately.

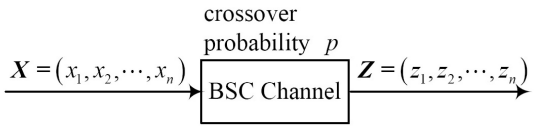


Figure 4.1: BSC channel with crossover probability p

Lemma 4.2: Let $(s_1, s_2, \cdots, s_m)$ in **Theorem** 4.1 be uniformly distributed over am m-tuple vector space. When Eqs (4.4) or (4.5) hold on, the average BER of recovering message $(\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$ from $\boldsymbol{Z} = (z_1, z_2, \cdots, z_n)$ is approaches to 0.5 with $n \to \infty$, i.e., $Pr(\tilde{s}_i \neq s_i) = 0.5$.

Proof: Because $(s_1, s_2, \cdots, s_m)$ is uniformly distributed over an m-tuple vector space, let $\boldsymbol{S}_j = (s_1, s_2, \cdots, s_m)_j, 1 \leq j \leq 2^m$ represent a distinct binary sequence of length m.

Then the average BER of the recovering message $(\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$ is:

$$\begin{aligned} Pr(\tilde{s}_i \neq s_i | \boldsymbol{Z}) &= \frac{Average\ \sharp\ of\ erroneous\ bits}{m} \\ &= \sum_{j=1}^{2^m} Pr(\boldsymbol{S}_j) \frac{1}{m} \sum_{k \neq j} Pr((\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m) = \boldsymbol{S}_k) d(\boldsymbol{S}_j, \boldsymbol{S}_k) \\ &= \frac{1}{m} \sum_{k \neq j} Pr((\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m) = \boldsymbol{S}_k) d(\boldsymbol{S}_j, \boldsymbol{S}_k) \end{aligned}$$

Form Eq (4.5), we have $Pr((\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m) = \boldsymbol{S}_k) = \frac{1}{2^m}$. Then we can get:

$$Pr(\tilde{s}_i \neq s_i \mid \boldsymbol{Z}) = \frac{1}{2^m} \cdot \frac{1}{m} \sum_{k \neq j} d(\boldsymbol{S}_j, \boldsymbol{S}_k) \tag{4.6}$$

where $d(\boldsymbol{S}_j, \boldsymbol{S}_k)$ is the Hamming distance between $\boldsymbol{S}_j$ and $\boldsymbol{S}_k$. Let $\boldsymbol{A}_a$ denotes the number of m dimension vectors which have distance a with vector$(\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$, we have:

$$\sum_{k \neq j} d(\boldsymbol{S}_j, \boldsymbol{S}_k) = \sum_{a=1}^{m} (\boldsymbol{A}_a \cdot a) = \sum_{a=1}^{m} (\begin{pmatrix} m \\ a \end{pmatrix} \cdot a) = \sum_{a=1}^{m} (\frac{m!}{a!(m-a)!} \cdot a) \tag{4.7}$$

From the mean of the binomial distribution, we have:

$$\sum_{a=1}^{m} (\frac{m!}{a!(m-a)!} \cdot a \cdot p^a \cdot (1-p)^{(m-a)}) = mp$$

Let $p = \frac{1}{2}$, we have:

$$\begin{aligned} &\sum_{a=1}^{m} (\frac{m!}{a!(m-a)!} \cdot a \cdot (\frac{1}{2})^m) = m \cdot \frac{1}{2} \\ \Longrightarrow\ &(\frac{1}{2})^m \cdot \sum_{a=1}^{m} (\frac{m!}{a!(m-a)!} \cdot a) = m \cdot \frac{1}{2} \\ \Longrightarrow\ &\sum_{a=1}^{m} (\frac{m!}{a!(m-a)!} \cdot a) = m \cdot 2^{m-1} \end{aligned} \tag{4.8}$$

(4.7) becomes:

$$\sum_{k \neq j} d(\boldsymbol{S}_j, \boldsymbol{S}_k) = m \cdot 2^{m-1}$$

Therefore, (4.6) becomes:

$$Pr(\tilde{s}_i \neq s_i \mid \boldsymbol{Z}) = \frac{1}{2^m} \cdot \frac{1}{m} \cdot m \cdot 2^{m-1} = \frac{1}{2}$$

4.2.2 Security Code Construction

[79] provided an example of security codes from resilient functions by assuming that the encoding function can be obtained via the inverse of decoding functions. However in most cases, it is not tractable to find the inverse of decoding functions. For example, [79] could not find the encoding function even with a very short code length as 16 bits. Thus the research outcome becomes impractical without a systematic way to obtain the encoding function of the security codes. In this section, we introduce a number of classes of security codes generated by binary linear resilient functions by taking advantage of matrix general inverse algorithms in [80, 81].

Let function f in Eq. (4.2) be a linear function, and $\boldsymbol{S}^T$ be the transpose of $\boldsymbol{S}$. $\boldsymbol{S} = (s_1, s_2, \cdots, s_m) = f(x_1, x_2, \cdots, x_n)$ can be denoted as:

$$\boldsymbol{S}^T = \boldsymbol{D}(x_1, x_2, \cdots, x_n)^T \tag{4.9}$$

where $\boldsymbol{D}$ is an $m \times n$ dimension matrix:

$$\boldsymbol{D} = [d_1, d_2, \cdots, d_m] = \begin{bmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,n} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{m,1} & d_{m,2} & \cdots & d_{m,n} \end{bmatrix}$$

where $d_{i,j} \in \{0, 1\}$

Example 4.1: An $(7, 3, 3)$ linear resilient function f is:

$$f(x_1, x_2, \cdots, x_7) = (x_4 + x_5 + x_6 + x_7, x_2 + x_3 + x_6 + x_7, x_1 + x_3 + x_5 + x_7)$$

Then we have:

$$\boldsymbol{S} = (s_1, s_2, \cdots, s_m) = f(x_1, x_2, \cdots, x_7) = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} (x_1, x_2, \cdots, x_7)^T$$

From (n, m, t) resilient functions, we have following encoding construction for the security code.

Construction 4.1: Let $\boldsymbol{D}$ be an $m \times n$ matrix from a (n, m, t) resilient function. Let $\boldsymbol{G}$ be an $m \times n$ matrix such that $\boldsymbol{D} \cdot \boldsymbol{G}^T \cdot \boldsymbol{D} = \boldsymbol{D}$. Given $\boldsymbol{S} = (s_1, s_2, \cdots, s_m)$ as the secret information launched by the legitimate user, the encoding function on $\boldsymbol{S}$ should be:

$$\boldsymbol{X} = (x_1, x_2, \cdots, x_n) = \boldsymbol{S} \cdot \boldsymbol{G} + \boldsymbol{V} \tag{4.10}$$

where $\boldsymbol{V}$ is an arbitrary n dimension vector such that $\boldsymbol{D} \cdot \boldsymbol{V}^T = 0$, and $\boldsymbol{X}$ is (n, m) security code.

To derive $\boldsymbol{G}$, we firstly perform row and column permutations on $\boldsymbol{D}$:

$$\boldsymbol{D} = \boldsymbol{Q}_L [\boldsymbol{I}_m \ \boldsymbol{0}] \boldsymbol{Q}_R \tag{4.11}$$

where $\boldsymbol{I}_m$ is $m \times m$ identity matrix, $\boldsymbol{0}$ is $m \times (n - m)$ all zero matrix, $\boldsymbol{Q}_L$ and $\boldsymbol{Q}_R$ are $m \times m$ and $n \times n$ matrix, respectively. Note that such an operation can be performed only if $\boldsymbol{D}$ has a full column rank, i.e., $r = m$, where r is the rank of $\boldsymbol{D}$. Then $\boldsymbol{G}$ can be calculated as [80, 81]:

$$\boldsymbol{G}^T = \boldsymbol{Q}_R^{-1} [\boldsymbol{I}_m \ \boldsymbol{B}]^T \boldsymbol{Q}_L^{-1} \tag{4.12}$$

where $\boldsymbol{B}$ is $m \times (n - m)$ matrix and can be chosen randomly, which means $\boldsymbol{G}$ is not unique. Here we randomly choose one to calculate the encoded security information bits $\boldsymbol{S}$ as $\boldsymbol{S} \cdot \boldsymbol{G}$.

If $\boldsymbol{D}$ is not fully column ranked (i.e., $r < m$), $\boldsymbol{D}$ can be transferred into the form:

$$\boldsymbol{D} = \boldsymbol{Q}_L \begin{bmatrix} \boldsymbol{I}_r & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{bmatrix} \boldsymbol{Q}_R \tag{4.13}$$

where $\boldsymbol{I}_r$ is $r \times r$ identity matrix, then $\boldsymbol{G}$ can be calculated as:

$$\boldsymbol{G}^T = \boldsymbol{Q}_R^{-1} \begin{bmatrix} \boldsymbol{I}_r & \boldsymbol{B}_{12} \\ \boldsymbol{B}_{21} & \boldsymbol{B}_{22} \end{bmatrix} \boldsymbol{Q}_L^{-1} \tag{4.14}$$

where $\boldsymbol{B}_{12}$, $\boldsymbol{B}_{21}$ and $\boldsymbol{B}_{22}$ are $r \times (m-r)$, $(n-r) \times r$ and $(n-r) \times (m-r)$ matrix, respectively, which can be chosen randomly to calculate $\boldsymbol{S} \cdot \boldsymbol{G}$.

The rate of the secret code from **Construction** 4.1 is r/n. If $\boldsymbol{D}$ has a full column rank, the rate of the secret code is m/n .

One method in finding vector $\boldsymbol{V}$ in (4.10) is shown as following. Let $\boldsymbol{D}_H$ be a $(n-m) \times n$ matrix such that

$$\boldsymbol{D}_H \cdot \boldsymbol{D}^T = \boldsymbol{0} \tag{4.15}$$

where $\boldsymbol{0}$ is $(n-m) \times m$ all-zero matrix. Let an $n-m$ dimension vector denoted as $\boldsymbol{K}$ be randomly selected for computing $\boldsymbol{V} = \boldsymbol{K} \cdot \boldsymbol{D}_H$, which means that one source message $\boldsymbol{S}$ will correspond to numerous outputs $\boldsymbol{X}$ when a matrix $\boldsymbol{G}$ is given. From (4.10) to (4.15), all arithmetic is done in $GF(2)$.

By launching $\boldsymbol{X}$ into the channel, the receivers will receive $\boldsymbol{Z} = (z_1, z_2, \cdots, z_n)$ which is the noisy version of $\boldsymbol{X}$. Decoding the secret information $\tilde{\boldsymbol{S}} = (\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$ from $\boldsymbol{Z}$ yields:

$$\tilde{\boldsymbol{S}} = (z_1, z_2, \cdots, z_n)\boldsymbol{D}^T \tag{4.16}$$

Theorem 4.2: A security code generated from **Construction** 4.1 can ensure secret information $\boldsymbol{S}$ from leaking to any eavesdropper under BSC channel when the crossover probability of the wiretape channel is p_w where $p_w \geq \frac{(n-t)}{2n}$. In other words, the average error rate at the eavesdropper (i.e., P_e^w in (2.2) and (2.4)) approaches to 0.5 with $n \to \infty$ if $p_w \geq \frac{(n-t)}{2n}$.

The proof of **Theorem** 4.2 directly follows by combining **Theorem** 4.1 with *Lemma* 4.2. We call this crossover probability p_w as the *threshold probability*, and denote the security code accordingly as (n, m, p_w). From this theorem we can know that the proposed security codes satisfaction security condition (2.4).

4.3 Non-Binary Security Code Construction

4.3.1 Preliminaries

The binary security codes developed in the previous section are feasible and practically implementable for our purpose. However, its threshold probabilities could be way larger than that in [33] which gives

$$p_w \geq 1 - 2^{-R} \tag{4.17}$$

which leads to low security capacity. In the effort of searching for solutions with smaller threshold probabilities, we observed that an (n, m, d) linear code meeting the Singleton bound [84], also referred to as Maximum Distance Separable (MDS) codes, can be used to form an $(n, m, d-1)$ resilient function [60]; and the security codes generated by such resilient functions will yield a threshold probabilities $R/2$, where $R = m/n$ is defined as the rate of the codes. In the following, *Lemma* 4.3 and 4.4 support the above statements, respectively.

Lemma 4.3: Let $\boldsymbol{D}$ be a generating matrix for an (n, m, d) linear code. Define a function $f\colon [\boldsymbol{GF}(2)]^n \to [\boldsymbol{GF}(2)]^m$ by the rule:

$$f(x_1, x_2, \cdots, x_n) = (x_1, x_2, \cdots, x_n) \cdot \boldsymbol{D}^T \tag{4.18}$$

Then f is an $(n, m, d-1)$ resilient function.

The proof of this lemma can be seen in [60].

Lemma 4.4: If a security code is constructed from the resilient function derived from the MDS codes, we have its threshold probability as $\frac{R}{2}$.

Proof: According to [84], an (n, m, d) MDS code meets the Singleton bound and follows the relation:

$$d = n - m + 1 \tag{4.19}$$

Therefore, the security code constructed from $(n, m, d-1)$ resilient function corresponding to the MDS code has its *threshold probability* as:

$$p_w \geq \frac{n-d+1}{2n} = \frac{R}{2} \tag{4.20}$$

Lemma 4.5: The threshold probability of a security code in turn derives from a resilient function corresponding to a MDS code is always better (or smaller) than that by [33], i.e., $(1-2^{-R}) \geq \frac{R}{2}$ for $0 \leq R \leq 1$.

Proof: Define $y(R) = (1-2^{-R}) - \frac{R}{2}$. $y'(R) = \frac{\partial y(R)}{\partial R} = 2^{-R} \cdot ln(2) - \frac{1}{2} = 0$ occurs when $R = 1 + log_2(ln2)$. Obviously, we have $y'(R) \geq 0$ with $R \in [0, 1+\log_2(\ln 2)]$, which means that $y(R)$ increases monotonically, and $y(R) \geq 0$ with $R \in [0, 1+\log_2(\ln 2)]$ since $y(0) = 0$. Similarly we have $y'(R) \leq 0$ with $R \in [1+\log_2(\ln 2), 1]$; thus $y(0) \geq 0$ with $R \in [1+\log_2(\ln 2), 1]$.

To summarize the above three lemmas, the security codes derive from the resilient functions corresponding to the MDS codes always yield better threshold probabilities than that of [33], which is the best reported for short length security codes under BSC so far. However, to the best of our knowledge, all binary MDS codes are *trivial* codes that are not practically implementable. This motivates us to explore the possibility of using non-binary MDS codes as the vehicle toward the desired security codes.

4.3.2 Nonbinary Resilient Functions

In this section, we extend the notions of resilient functions to functions over finite alphabet, and similarly, we follow the definition on non-binary resilient function given in [85].

Definition 4.2 [85]: Let q be the power of a certain prime number, Define function $\boldsymbol{F}: \boldsymbol{GF}(q)^n \rightarrow \boldsymbol{GF}(q)^m, 1 \leq m \leq n$. Let $\boldsymbol{S} = (s_1, s_2, \cdots, s_m)$ be the set of random input

variables assuming values from $\boldsymbol{GF}(q)$ with uniform distributions (that is, every possible input vector occurs with an equal probability $1/q^m$). Let $\boldsymbol{X} = (x_1, x_2, \cdots, x_n) \in \boldsymbol{GF}(q)^n$ and $\boldsymbol{Z} = (z_1, z_2, \cdots, z_n) \in \boldsymbol{GF}(q)^n$ denote the set of output variables of the function $\boldsymbol{F}$. Given $\boldsymbol{F}(x_1, x_2, \cdots, x_n) = (s_1, s_2, \cdots, s_m)$, we need to have:

$$Pr(\boldsymbol{F}(z_1, z_2, \cdots, z_n) = (s_1, s_2, \cdots, s_m) | x_{i_j} = z_{i_l}) = \frac{1}{q^m} \tag{4.21}$$

where $0 \leq j, l \leq t$, for any t-subset $(i_1, i_2, \cdots, i_t) \subseteq \{1, 2, \cdots, n\}$. Such a function $\boldsymbol{F}$ is called a non-binary (q, n, m, t) resilient function. In other words, if $\boldsymbol{Z}$ intercepts t or less symbols from $\boldsymbol{X}$, $\boldsymbol{F}(z_1, z_2, \cdots, z_n)$ only has a probability of $\frac{1}{q^m}$ to obtain vector $(s_1, s_2, \cdots, s_m)$.

Samilar to **Theorem** 4.1, **Theorem** 4.3 provides the threshold on the Symbol Error Rate (SER) for the wiretapper above which no information will be intercepted.

Theorem 4.3: Let $\boldsymbol{Z} = (z_1, z_2, \cdots, z_n)$ be a noisy version of $\boldsymbol{X} = (x_1, x_2, \cdots, x_n)$. $\boldsymbol{X}$ and $\boldsymbol{Z}$ take values from $\boldsymbol{GF}(q)$. Let $\boldsymbol{F}$ be an (q, n, m, t) resilient function. Let $\boldsymbol{F}(x_1, x_2, \cdots, x_n) = (s_1, s_2, \cdots, s_m)$, and $\boldsymbol{F}(z_1, z_2, \cdots, z_n) = (\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$. Let the SER between $\boldsymbol{X}$ and $\boldsymbol{Z}$ be denoted as p_s , i.e.$Pr(x_i \neq z_i) = p_s$. If:

$$p_s \geq \frac{q-1}{q} \cdot \frac{(n-t)}{n} \tag{4.22}$$

then we have:

$$Pr((\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m) = (s_1, s_2, \cdots, s_m)) = \frac{1}{q^m} \tag{4.23}$$

Proof: Obviously, there are randomly and independently t symbols correctly taken by $\boldsymbol{Z}$ and $1/q$ of the remaining $n-t$ symbols correctly taken by $\boldsymbol{Z}$ too, while the other $\frac{(n-t)(q-1)}{q}$ symbols being incorrectly taken. Therefore, the total correct symbols in $\boldsymbol{Z}$ are $t + \frac{n-t}{q}$, and the total error bits in $\boldsymbol{Z}$ are $\frac{q-1}{q} \cdot (n-t)$. Thus we have $Pr(x_i \neq z_i) = \frac{q-1}{q} \cdot \frac{n-t}{n}$. Combining with **Definition** 4.2, we can get the results immediately.

4.3.3 Non-binary Resilient Functions Construction

The resilient functions used in numeric cryptography are subject to stringent requirements on high orders of resiliency, nonlinearity, and algebraic degree [91]. However, in the targeted scenario of this study, an (q, n, m, t) resilient function is desired to have as large m as possible with a given n and t, where the nonlinearity and algebraic degree are completely not a concern. (4.19) and (4.20) indicate that a non-binary resilient function (q, n, m, t) derived from a MDS code can provide optimal parameter m.

Among very few reported non-binary resilient function constructions, the study considers the one derived from non-binary linear codes. The relationship between non-binary linear codes and non-binary resilient functions is given in *Lemma* 4.5, which is a simple extension from *Lemma* 4.2.

Lemma 4.6 [91]: $\boldsymbol{D}$ is a generating matrix for an (n, m, d) linear code over $\boldsymbol{GF}(q)$ if and only if the function $\boldsymbol{F} : [\boldsymbol{GF}(q)^n] \rightarrow [\boldsymbol{GF}(q)^m]$ defined by the rule $\boldsymbol{F}(x_1, x_2, \cdots, x_n) = (x_1, x_2, \cdots, x_n) \cdot \boldsymbol{D}^T$ is an (q, n, m, t) - resilient function.

An optimal resilient function (i.e., with the optimal m) can be obtained from the corresponding MDS code. Without loss of generality, the study employs Reed-Solomon codes (or RS codes) [92] which is the most commonly used MDS codes, for construction of the resilient functions. Note that any other MDS codes such as rank metric codes [93] can serve for the same purpose.

By taking the prime as 2, we have $q = 2^k$, where k is any positive integer. Let α be a primitive element in $\boldsymbol{GF}(q)$. A t_d -error correcting RS code has the generator polynomial:

$$\bar{g}(x) = \prod_{j=b}^{b+2t_d-1} (x - \alpha^j) \tag{4.24}$$

where b is an integer, usually $b = 0$ or $b = 1$. RS codes are also a kind of cyclic codes. Therefore, The $q-1$ dimension vectors associated with the coefficients of the polynomials

$\bar{g}(x), x\bar{g}(x), x^2\bar{g}(x), \cdots, x^{q-2t_d-2}\bar{g}(x)$ can be used as rows of the generating matrix $\boldsymbol{D}$. This code is a $(q-1, q-2t_d-1, 2t_d+1)$ RS code. The function $\boldsymbol{F} : [\boldsymbol{GF}(q)^n] \rightarrow [\boldsymbol{GF}(q)^m]$ defined as $\boldsymbol{F}(x_1, x_2, \cdots, x_n) = (x_1, x_2, \cdots, x_n) \cdot \boldsymbol{D}^T$ is in fact a $(q, q-1, q-2t_d-1, 2t_d)$ resilient function, in which $n = q-1$ and $m = q-2t_d-1$.

4.3.4 Non-binary Security Code Construction

The results of the binary case can immediately generalize to functions over $\boldsymbol{GF}(q)$.

Construction 4.2: Let $\boldsymbol{D}$ be an $m \times n$ dimension matrix from an (q, n, m, t) resilient function. By (4.11) to (4.14) in **Construction** 4.1, we can find matrix $\boldsymbol{G}$ from $\boldsymbol{D}$ over $\boldsymbol{GF}(q)$ such that $\boldsymbol{D} \cdot \boldsymbol{G}^T \cdot \boldsymbol{D} = \boldsymbol{D}$. Then we take matrix $\boldsymbol{G}$ to encode the secret information $\boldsymbol{S} = (s_1, s_2, \cdots, s_m)$ as:

$$\boldsymbol{X} = (x_1, x_2, \cdots, x_n) = \boldsymbol{S} \cdot \boldsymbol{G} + \boldsymbol{V} \tag{4.25}$$

where $\boldsymbol{V}$ is an n dimension vector which is randomly chosen such that $\boldsymbol{D} \cdot \boldsymbol{V}^T = \boldsymbol{0}$. Here all the arithmetic operations are done in $\boldsymbol{GF}(q)$. Then we get a q -ray (q, n, m) security code from the (q, n, m, t) resilient function.

The rate of the secret code from **Construction** 4.2 is the same as that of the code from **Construction** 4.1. The method to find vector $\boldsymbol{V}$ in **Construction** 4.1 also can be used here. The encoded vector $\boldsymbol{X}$ is sent through the channel, and the wiretapper will receive $\boldsymbol{Z} = (z_1, z_2, \cdots, z_n)$ which is the a noisy version of $\boldsymbol{X}$. Similar to the binary case, decoding the estimate sequence of the secret information $\boldsymbol{S} = (\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$ from $\boldsymbol{Z}$ yields:

$$\boldsymbol{S} = (z_1, z_2, \cdots, z_n)\boldsymbol{D}^T \tag{4.26}$$

From **Theorem** 4.3, if the SER between $\boldsymbol{X}$ and $\boldsymbol{Z}$ is equal to or larger than $\frac{q-1}{q} \cdot \frac{(n-t)}{n}$ the decoding result $\tilde{\boldsymbol{S}} = (\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$ will become uniformly distributed over

$\boldsymbol{GF}(q)^m$. Given $q = 2^k$ and for every k-bit vector $\boldsymbol{V}_\omega$ there is a corresponding element $\omega \in \boldsymbol{GF}(2^k)$ due to isomorphism between $\boldsymbol{GF}(2^k)$ and $\{0,1\}^k$ such that $\boldsymbol{V}_{\omega_j} \in \{0,1\}^k \Leftrightarrow \omega_j \in \boldsymbol{GF}(2^k)$, $0 \le j \le 2^k - 1$. By Considering the model in Figure 4.2, $k \times m$ bits $\boldsymbol{S}_b = (s_1^1, s_1^2, \cdots, s_1^k, s_2^1, s_2^2, \cdots, s_2^k, \cdots, s_m^1, s_m^2, \cdots, s_m^k)$ are first converted into m symbols $\boldsymbol{S} = (s_1, s_2, \cdots, s_m)$, where $s_i = (s_i^1, s_i^2, \cdots, s_i^k), 1 \le i \le m$; then $(s_1, s_2, \cdots, s_m)$ is further encoded to $\boldsymbol{X} = (x_1, x_2, \cdots, x_n)$ via (4.25), which becomes noisy version $\boldsymbol{Z} = (z_1, z_2, \cdots, z_n)$ after passing a channel with SER p_s. For simplicity and without loss of generality, we ignore the effect due to modulation.

According to (4.26), $(z_1, z_2, \cdots, z_n)$ is decoded as $\tilde{\boldsymbol{S}} = (\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$. Finally, by mapping the symbols of $\boldsymbol{GF}(2^k)$ into binary vectors of length k we get output as $k \times m$ bits $\tilde{\boldsymbol{S}}_b = (\tilde{s}_1^1, \tilde{s}_1^2, \cdots, \tilde{s}_1^k, \tilde{s}_2^1, \tilde{s}_2^2, \cdots, \tilde{s}_2^k, \cdots, \tilde{s}_m^1, \tilde{s}_m^2, \cdots, \tilde{s}_m^k)$ from $(\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m)$.

From the perspective of the BSC, the encoded sequence $\boldsymbol{X} = (x_1, x_2, \cdots, x_n)$ can also be mapped into $k \times m$ bits $\boldsymbol{X}_b = (x_1^1, x_1^2, \cdots, x_1^k, x_2^1, x_2^2, \cdots, x_2^k, \cdots, x_m^1, x_m^2, \cdots, x_m^k)$, and launched in the BSC with a crossover probability p_b which yields the noisy version $\boldsymbol{Z}_b = (z_1^1, z_1^2, \cdots, z_1^k, z_2^1, z_2^2, \cdots, z_2^k, \cdots, z_m^1, z_m^2, \cdots, z_m^k)$. Then we can get $(z_1, z_2, \cdots, z_n)$ by mapping k bits into one symbol.

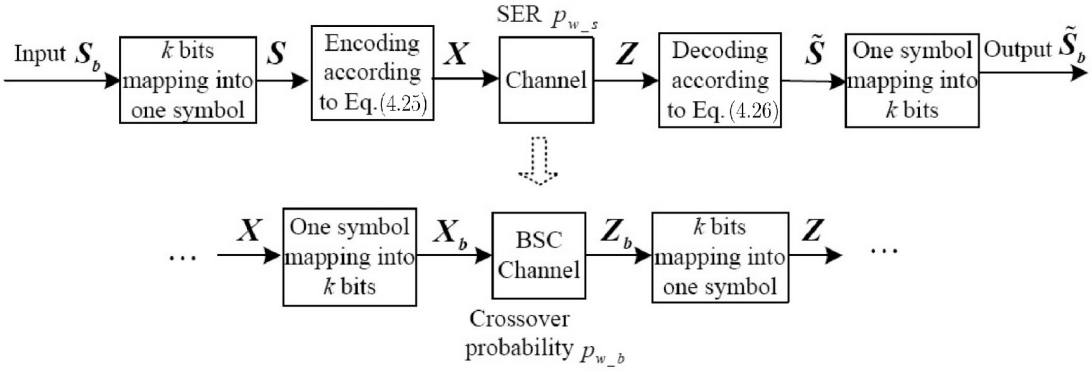


Figure 4.2: The non-binary security encoding and decoding model

Theorem 4.4: In the model of Figure 4.2, with the following condition on symbol

error probability p_{w_s}:

$$Pr(x_i \neq z_i) = p_{w\_s} \geq \frac{q-1}{q} \cdot \frac{(n-t)}{n}, q = 2^k \tag{4.27}$$

we have: (i) the average BER at the eavesdropper is approaches to 0.5 with $n \to \infty$, i.e. $Pr(s_i^j \neq \tilde{s}_i^j) = p_e = 0.5, 1 \leq i \leq m, 1 \leq j \leq k$; and (ii) the corresponding crossover probability of BSC, i.e., $Pr(x_i^j \neq z_i^j) = p_{w\_b}$, is subject to the condition:

$$p_{w\_b} \geq \frac{(n-t)}{2n} \tag{4.28}$$

Proof: (i) **Theorem** 4.3 shows that with $p_{w\_s} \geq \frac{q-1}{q} \cdot \frac{(n-t)}{n}$, we have $Pr((\tilde{s}_1, \tilde{s}_2, \cdots, \tilde{s}_m) = (s_1, s_2, \cdots, s_m)) = \frac{1}{q^m}$. Similar to the proof of *Lemma* 4.2, let $\boldsymbol{S}_{b\_j} = (s_1^1, s_1^2, \cdots, s_1^k, s_2^1, s_2^2, \cdots, s_2^k, \cdots, s_m^1, s_m^2, \cdots, s_m^k)_j$ and $\boldsymbol{S}_j = (s_1, s_2, \cdots, s_m)_j$ represent a distinct binary sequence of length km and symbol sequence of length m, respectively. Because $\boldsymbol{S}_j$ is uniformly distributed over $\boldsymbol{GF}(q)^m$, every vector $\boldsymbol{S}_j$ occurs with a probability $Pr(\boldsymbol{S}_j) = \frac{1}{q^m}$, which also means every vector $\boldsymbol{S}_{b\_j}$ occurs with probability $Pr(\boldsymbol{S}_{b\_j}) = \frac{1}{q^m}$. Thus the average BER of the recovering message $\tilde{\boldsymbol{S}}_{b\_j}$ is:

$$\begin{aligned} Pr(s_i^j \neq \tilde{s}_i^j | \boldsymbol{Z}) &= \frac{Average\ \sharp\ of\ erroneous\ bits}{km} \\ &= \sum_{j=1}^{q^m} Pr(\boldsymbol{S}_{b\_j}) \frac{1}{km} \sum_{k \neq j} Pr(\tilde{\boldsymbol{S}}_b = \boldsymbol{S}_{b\_k}) d(\boldsymbol{S}_{b\_j}, \boldsymbol{S}_{b\_k}) \\ &= \frac{1}{km} \sum_{k \neq j} \frac{1}{q^m} \cdot d(\boldsymbol{S}_{b\_j}, \boldsymbol{S}_{b\_k}) \qquad ; \\ &= \frac{1}{km} \cdot \frac{1}{q^m} \sum_{k \neq j} d(\boldsymbol{S}_{b\_j}, \boldsymbol{S}_{b\_k}) \end{aligned}$$

Form (4.8), we have:

$$Pr(s_i^j \neq \tilde{s}_i^j \mid \boldsymbol{Z}) = \frac{1}{km} \cdot \frac{1}{q^m} \cdot (km) \cdot 2^{km-1} = \frac{1}{2} \tag{4.29}$$

(ii) To prove the condition on crossover probability, we firstly argue that all symbol errors are equiprobable and occur with a probability:

$$\frac{p_{w\_s}}{q-1} \tag{4.30}$$

Thus with $z_i = (z_i^1, z_i^2, \cdots, z_i^k), 1 \leq i \leq m$, there are $\begin{pmatrix} k \\ a \end{pmatrix}$ ways in which a bits out of k are in error. Hence, the average number of bit errors per k-bit symbol is:

$$p_{w\_b} = \sum_{a=1}^{k} a \cdot \begin{pmatrix} k \\ a \end{pmatrix} \cdot \frac{p_{w\_s}}{q-1}/k \tag{4.31}$$

From (4.8) and (4.27), we have:

$$p_{w\_b} \geq k \cdot 2^{k-1} \cdot \frac{q-1}{q(q-1)} \cdot \frac{(n-t)}{n} \cdot \frac{1}{k} = \frac{(n-t)}{2n} \tag{4.32}$$

This result is the same as that of the binary case in **Theorem** 4.2.

Theorem 4.4 defines two *thresholds* on the SER p_{w_s} and BSC crossover probability p_{w_b} for a $(2^k, n, m)$ security code derived from a $(2^k, n, m, t)$ resilient function. We define the kind of security codes generated from **Construction** 4.2 as $(2^k, n, m, p_{w\_b})$. From this theorem we can know that the proposed non-binary security codes satisfaction security condition (2.4).

4.4 Security Code Performance

In this section, numerical results through case studies are presented to demonstrate the performance evaluation using the proposed approach.

4.4.1 Binary Security Codes

Construction 4.1 is based on binary resilient functions $(n, m, d-1)$, which can be generated by a corresponding linear code (n, m, d) [60]. In the experiment we implemented simplex codes $(2^m - 1, m, 2^{m-1})$, which are the dual of Hamming codes, so as to yield

a $(2^m - 1, m, 2^{m-1} - 1)$ linear resilient function. Figure 4.3 shows the BER after applying the security codes versus the crossover probability p of the BSC before applying the security codes.

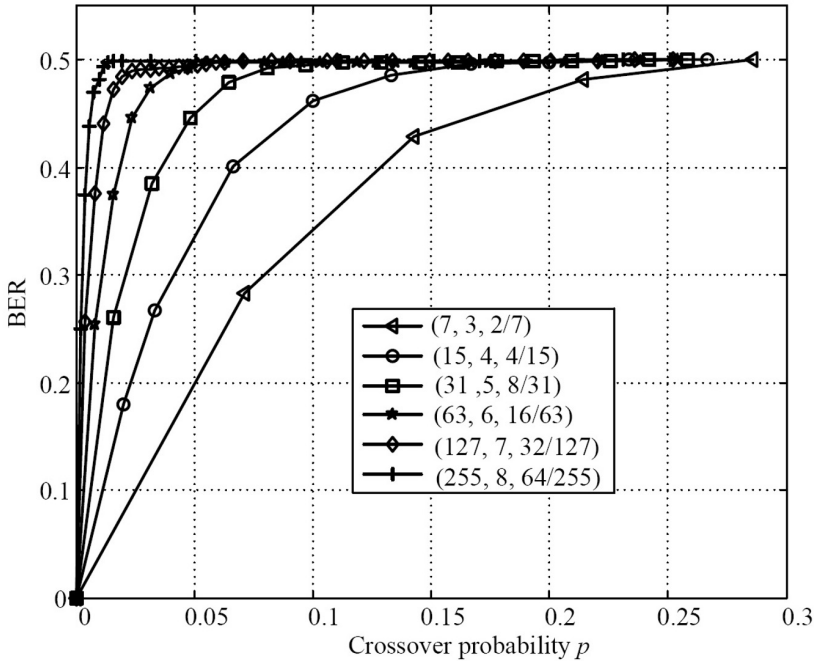


Figure 4.3: The performance of security codes generated by **Construction** 4.1

4.4.2 Non-binary Security Codes

In the experiment, a family of $(2^k, 2^k - 1, 2^k - 2t_d - 1, \frac{1}{2} - \frac{t_d}{2^k - 1})$ non-binary security codes were generated by the non-binary resilient functions $(2^k - 1, 2^k - 2t_d - 1, 2t_d)$ via **Construction** 4.2, which is in turn derived by RS codes $(2^k - 1, 2^k - 2t_d - 1, 2t_d + 1)$, where t_d is an integer such that $1 \leq t_d < 2^k - 1$. Figure 4.4 and Figure 4.5 show the SER and BER of the generated non-binary security codes with short code lengths versus channel error rate.

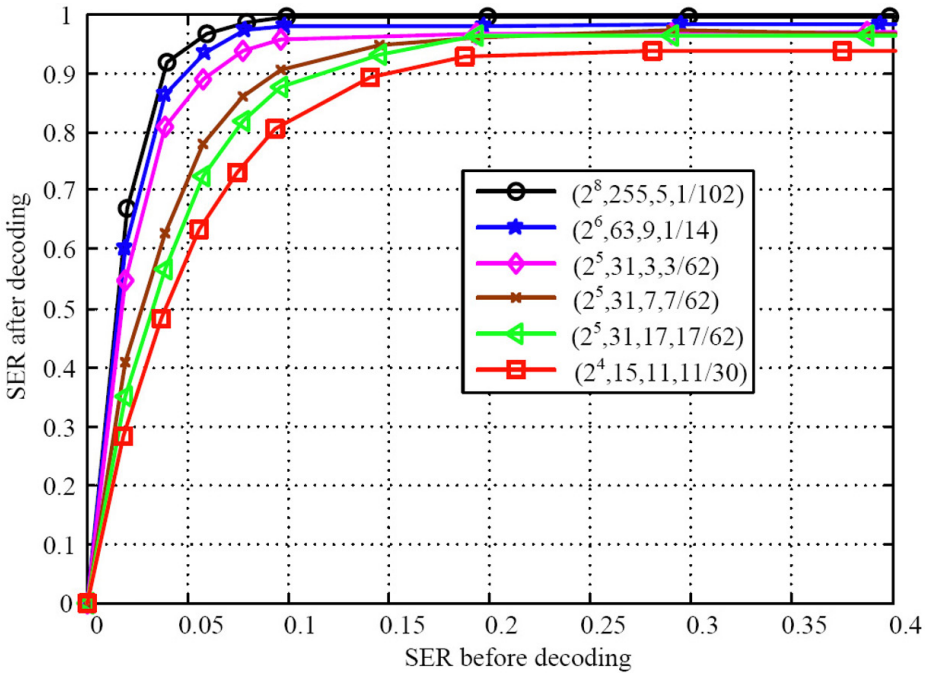


Figure 4.4: The SER performance of non-binary security codes derived from non-binary resilient function corresponding to RS codes

By using doubly extended RS codes, we can get a family of q-ary code with a wider range of parameter selection. Let $q = 2^k$, α be a primitive element in $\boldsymbol{GF}(q)$ and t_d be an integer such that $1 \leq t_d \leq 2^k - 1$. The doubly extended RS codes of dimension $m = 2^k - 1 - 2t_d$ are the codes defined over $\boldsymbol{GF}(q)$ with a generating matrix:

$$\boldsymbol{D} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 0 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} & 0 & 0 \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(q-2)2} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{m-2} & \alpha^{2(m-2)} & \cdots & \alpha^{(q-2)(m-2)} & 0 & 0 \\ 1 & \alpha^{m-1} & \alpha^{2(m-1)} & \cdots & \alpha^{(q-2)(m-1)} & 0 & 1 \end{bmatrix}$$

This family of codes is $(q+1, m, q-m+2)$ q-ary codes, where the first $n \leq q+1$

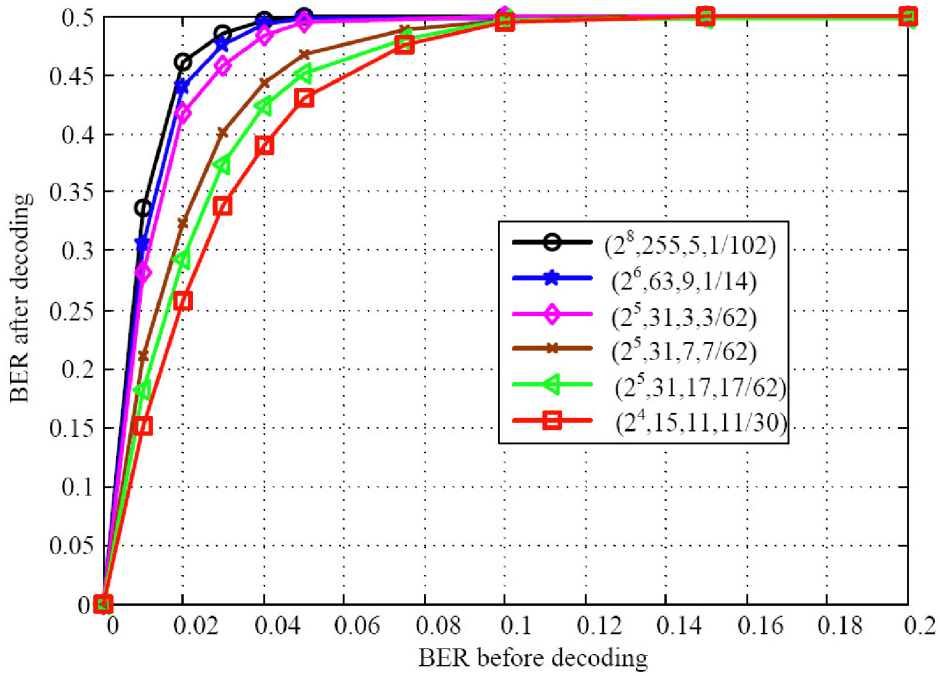


Figure 4.5: The BER performance of non-binary security codes derived from non-binary resilient function corresponding to RS codes

columns of $\boldsymbol{D}$ form the generating matrix $\boldsymbol{D}_0$ for the $(n, m, n-m+1)$ q-ary code. The function $\boldsymbol{F}: \boldsymbol{GF}(q)^n \rightarrow \boldsymbol{GF}(q)^m$ defined as $\boldsymbol{F}(\boldsymbol{X}) = \boldsymbol{X}(\boldsymbol{D}_0)^T$ is in fact a $(q, n, m, n-m)$ resilient function, by which we can derive the family of q-ary security codes denoted as $\left(q, n, m, \frac{m}{2n}\right)$. The performance of proposed security codes is shown in Figure 4.6 and Figure 4.7.

A comparison of proposed non-binary security codes with reported security codes under BSC is given in Table I. We assume that the error probability of the main channel is 10^{-3} and the crossover probability of eavesdropper channel is 0.5. The security capacity C_s is calculated according to (2.10). Table 4.2 shows that the rate of proposed security codes is lower than that of security codes derived from polar codes, but the proposed security codes have much shorter code lengths which is key point for energy limitation

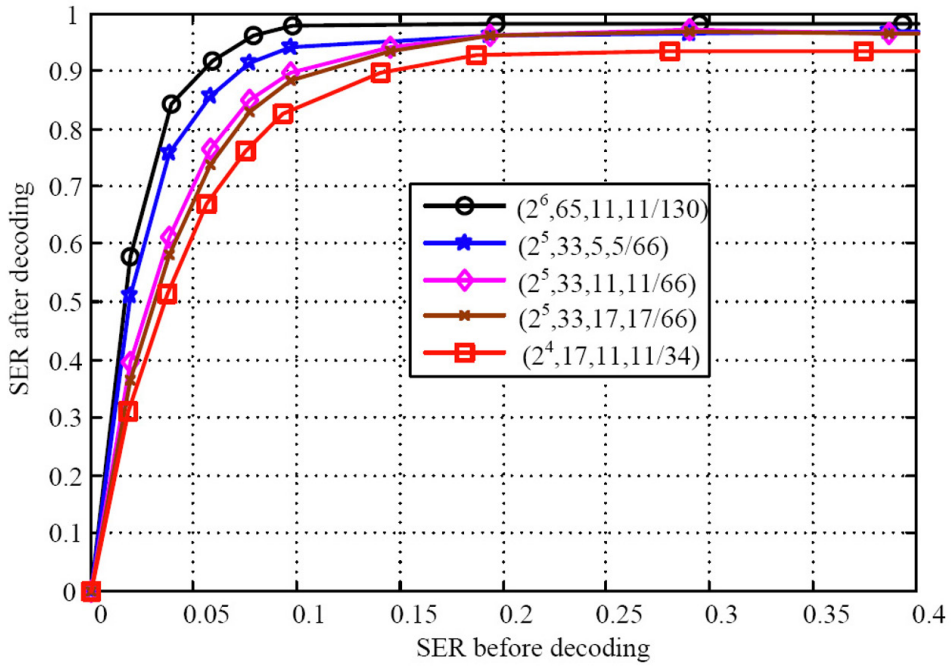


Figure 4.6: The SER performance of non-binary security codes derived from non-binary resilient function corresponding to doubly extended RS codes

wireless applications.

4.5 Security System Performance

Without loss of generality, the study considers LDPC [96] as the encoding scheme χ_2 in (3.7). Note that LDPC exhibits a threshold phenomenon under a certain decoding method, which determines the asymptotic behavior of the ensemble of the code. In specific, Parallel Concatenated LDPC (PC-LDPC) codes [96] are adopted in our performance evaluation, which demonstrates rate compatibility and adaptation to varying channel qualities. The parity-check matrix $\boldsymbol{H}$ of the PC-LDPC codes can be expressed as:

Table 4.2: A comparison of proposed non-binary security codes with reported security codes under BSC

p_w	Polar codes [61]			Proposed security codes			Rate in [33]	
	Code length	Rate R	% of C_s	Security codes	Rate R	% of C_s	Security codes	Rate R
0.45	2^{20}	0.933	95.1%	$\left(2^5, 33, 29, \frac{29}{66}\right)$	0.879	89.6%	$(65, 56)$	0.863
0.4		0.822	91.9%	$\left(2^4, 17, 13, \frac{13}{34}\right)$	0.765	79.7%	$(65, 48)$	0.737
0.35		0.817	88.5%	$\left(2^5, 33, 23, \frac{23}{66}\right)$	0.697	75.5%	$(29, 18)$	0.622
0.3		0.738	84.8%	$\left(2^4, 15, 9, \frac{9}{30}\right)$	0.6	69%	$(31, 16)$	0.515
0.25		0.647	80.9%	$\left(2^5, 31, 15, \frac{15}{62}\right)$	0.484	60.6%	$(65, 27)$	0.415
0.2		0.543	76.4%	$\left(2^5, 33, 13, \frac{13}{66}\right)$	0.394	55.5%	$(65, 21)$	0.323
0.15		0.425	71.1%	$\left(2^4, 17, 5, \frac{5}{34}\right)$	0.294	49.2%	$(17, 4)$	0.235
0.1		0.293	64.0%	$\left(2^4, 15, 3, \frac{1}{10}\right)$	0.2	43.7%	$(33, 5)$	0.152

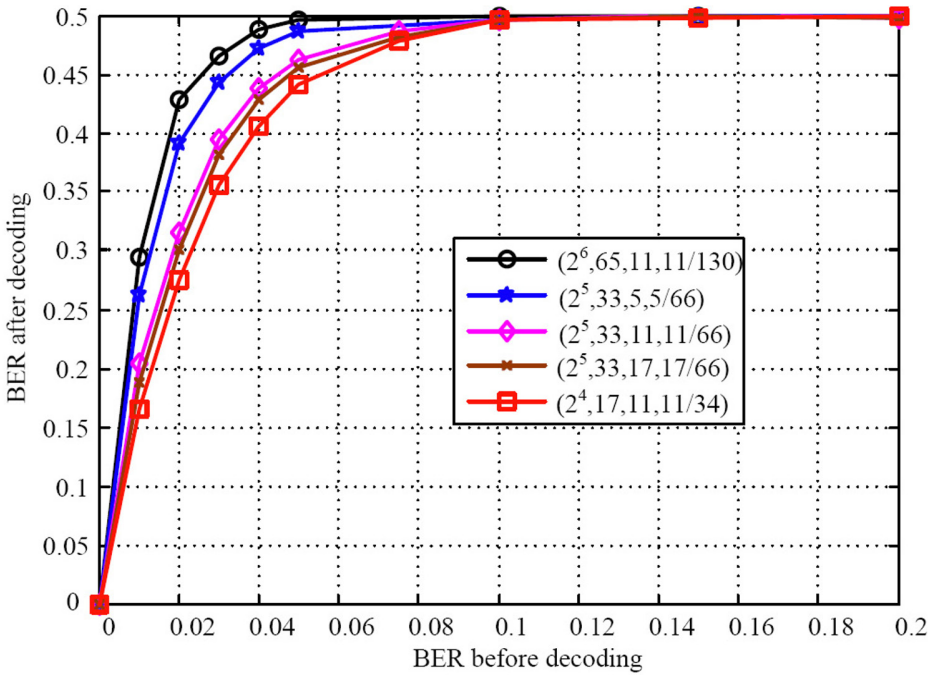


Figure 4.7: The BER performance of non-binary security codes derived from non-binary resilient function corresponding to doubly extended RS codes

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_1^d & \boldsymbol{H}_1^p & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{H}_2^d & \boldsymbol{0} & \boldsymbol{H}_2^p & \cdots & \boldsymbol{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{H}_s^d & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{H}_s^p \end{bmatrix} \tag{4.33}$$

We employ seven random LDPC codes with rate 1/2 as component codes. The overall code (mother code) length and rate are 10000 and 1/8 , respectively. The source block has 1250 bits. The component matrixes $\boldsymbol{H}_i^d$ and $\boldsymbol{H}_i^p$ in (4.33) have 1250 columns and 1250 rows with 3 weight for every column and row. By puncture the component matrixes $\boldsymbol{H}_i^p$ from the mother code matrix $\boldsymbol{H}$, we can get the LDPC codes with a length from 2500 to 10000 and the rate from 1/2 to 1/8. The belief propagation iterative decoding

algorithm is used and maximum number of iterations is 200. Figure 4.8 and Figure 4.9 show the performances of these codes over BSC, AWGN channel and Rayleigh Channel, respectively. With the LPDC implementation, performances are launched by taking

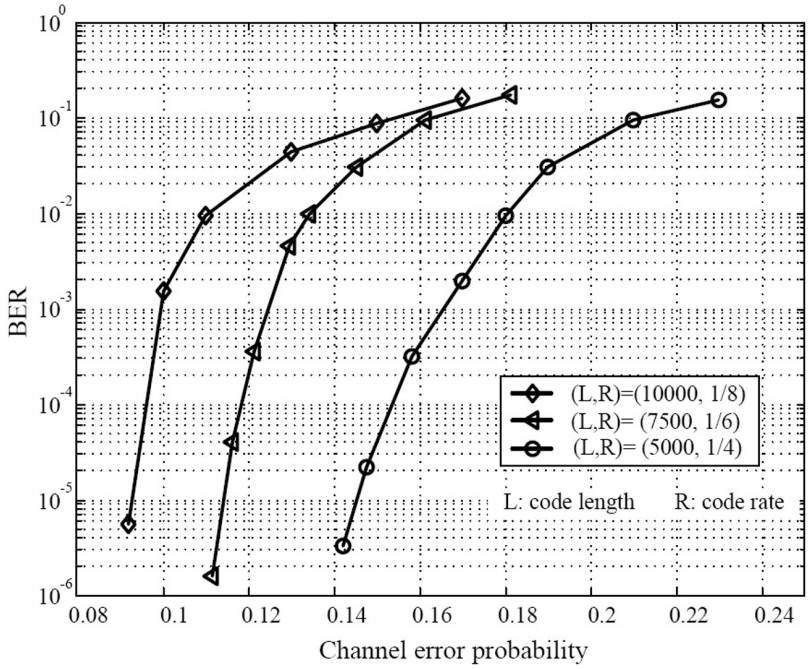


Figure 4.8: The BER performances of LDPC codes under BSC channel

$\delta = 1$ (one round interactive communication [55]) and $\delta = 2$ (two rounds interactive communication) over the three different channels. The results are shown in Tables 4.3-4.8. The second line of Table 4.3 is the performance results for the scheme in [55] under BSC. Table 4.5 and Table 4.7 are the performance results for the one-round scheme under AWGN and Rayleigh channel, which is our extended research results from [55]. Table 4.4, Table 4.6 and Table 4.8 are the performance results for the novel MRTWC scheme under the three different channels.

The BER due to the LDPC decoding process is given in the tables, where P_{ir} and P_{Eve} denotes the BER at the intended receiver and the eavesdropper after Channel Codes

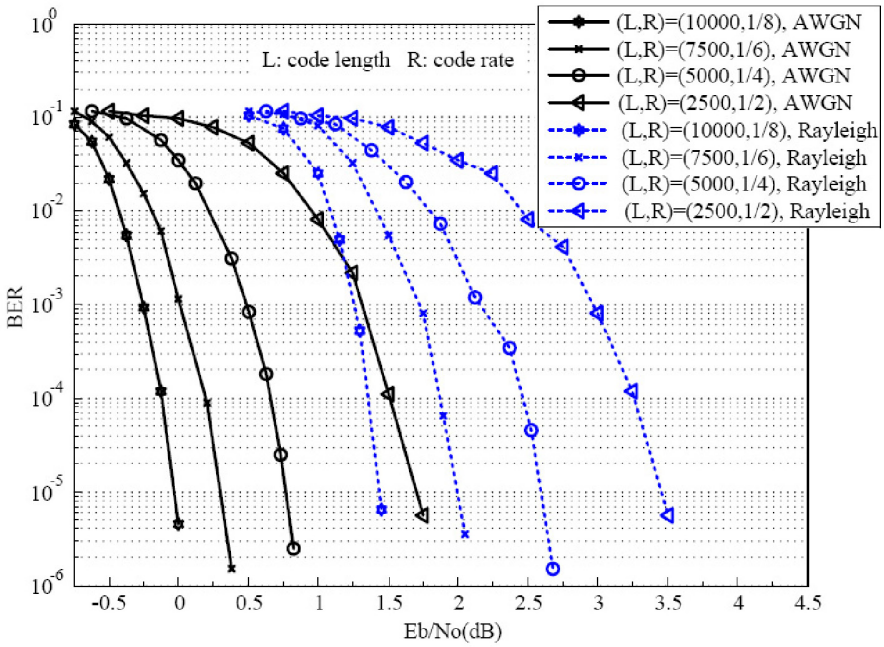


Figure 4.9: The BER performances of LDPC codes under AWGN and Rayleigh channels

(CC) decoding, respectively. P_{B_s} and P_{E_s} denote the SER of Bob and Eve after Security Codes (SC) decoding, respectively; while P_B and P_E denote the BER of Bob and Eve after security codes decoding, respectively. **SC** and **CC** are the logogram of security code and channel code.

Under AWGN channel and Rayleigh channel, corresponding to $\frac{E_b}{N_0}$ in Figure 4.7, SNR γ in Table 4.5 to Table 4.8 was calculated as:

$$\gamma = \frac{E_b}{N_0} + 10\log_{10} R \tag{4.34}$$

where R is the code rate of LDPC codes. For example, in table 4.5, with $\gamma_1 = -1dB$ and $\gamma_{e\_1} = -1dB$ the BER of the main channel and eavesdropper's channel are $Pr(\boldsymbol{V}) = 0.105$ and $Pr(\boldsymbol{V}_e) = 0.188$ by (3.47) and (3.48), which corresponding to $\gamma = -1dB$ and $\gamma = -4.06dB$ from (3.38). If we consider $R = \frac{1}{2}$, by (4.34) we can get $\frac{E_b}{N_0} = 2.0103dB$ and

Table 4.3: The performance under BSC channel ($\delta = 1$)

Crossover Probability	$\alpha = 0.06$ $\beta = 0.06$	$\alpha = 0.08$ $\beta = 0.04$	$\alpha = 0.08$ $\beta = 0.08$	$\alpha = 0.15$ $\beta = 0.075$	$\alpha = 0.15$ $\beta = 0.15$
BER after interaction	$Pr(\boldsymbol{V}) = 0.06$ $Pr(\boldsymbol{V}_e) = 0.1128$	$Pr(\boldsymbol{V}) = 0.08$ $Pr(\boldsymbol{V}_e) = 0.1136$	$Pr(\boldsymbol{V}) = 0.15$ $Pr(\boldsymbol{V}_e) = 0.1472$	$Pr(\boldsymbol{V}) = 0.15$ $Pr(\boldsymbol{V}_e) = 0.2138$	$Pr(\boldsymbol{V}) = 0.15$ $Pr(\boldsymbol{V}_e) = 0.255$
LDPC code	$(5000, 1/4)$	$(5000, 1/4)$	$(10000, 1/8)$	$(10000, 1/8)$	$(10000, 1/8)$
BER after CC decoding	$P_{ir} < 1.5 \times 10^{-5}$ $P_{Eve} = 0.0105$	$P_{ir} < 1.5 \times 10^{-5}$ $P_{Eve} = 0.0113$	$P_{ir} < 1.5 \times 10^{-5}$ $P_{Eve} = 0.077$	$P_{ir} < 3.5 \times 10^{-4}$ $P_{Eve} = 0.085$	$P_{ir} < 3.5 \times 10^{-4}$ $P_{Eve} = 0.198$
C_s	0.0838	0.089	0.3913	0.4150	0.7134
Security codes	$(2^8, 255, 5, \frac{1}{102})$	$(2^8, 255, 5, \frac{1}{102})$	$(2^5, 33, 5, \frac{5}{66})$	$(2^5, 33, 5, \frac{5}{62})$	$(2^5, 33, 5, \frac{13}{66})$
SER after SC decoding	$P_{B\_s} < 1.265 \times 10^{-4}$ $P_{E\_s} = 0.9961$	$P_{B\_s} < 1.265 \times 10^{-4}$ $P_{E\_s} = 0.9961$	$P_{B\_s} < 2.044 \times 10^{-4}$ $P_{E\_s} = 0.96975$	$P_{B\_s} < 4.40 \times 10^{-3}$ $P_{E\_s} = 0.96875$	$P_B < 9.881 \times 10^{-3}$ $P_{E\_s} = 0.96875$
BER after SC decoding	$P_B < 6.35 \times 10^{-5}$ $P_E = 0.5$	$P_B < 6.35 \times 10^{-5}$ $P_E = 0.5$	$P_B < 1.055 \times 10^{-4}$ $P_E = 0.5$	$P_B < 2.271 \times 10^{-3}$ $P_E = 0.5$	$P_B < 5.1 \times 10^{-3}$ $P_E = 0.5$

$\frac{E_b}{N_0} = -1.0497dB$ corresponding to $\gamma = -1dB$ and $\gamma = -4.06dB$. From Figure 4.6, the BER of $(2500, 1/2)$ LDPC code is 5.6×10^{-5} when $\frac{E_b}{N_0} = 1.75dB$. Therefore, $(2500, 1/2)$ LDPC code is chosen and the BER of the intended receiver and the eavesdropper after channel codes decoding are $P_{ir} < 5.6 \times 10^{-5}$ and $P_{Eve} = 0.112$, respectively.

From Table 4.3 to 4.8 we can know that the eavesdropper is subject to an error probability close to 0.5 while the main channel is almost error-free even if the eavesdropper has better channel. The results demonstrated the effectiveness of the proposed security codes and MRTWC mechanisms for achieving unconditionally secure communications.

Table 4.4: The performance under BSC channel ($\delta = 2$)

Crossover Probability	$\alpha_1 = \alpha_2 = 0.04$ $\beta_1 = \beta_2 = 0.04$	$\alpha_1 = \alpha_2 = 0.06$ $\beta_1 = \beta_2 = 0.04$	$\alpha_1 = \alpha_2 = 0.06$ $\beta_1 = \beta_2 = 0.06$	$\alpha_1 = \alpha_2 = 0.08$ $\beta_1 = \beta_2 = 0.04$	$\alpha_1 = \alpha_2 = 0.08$ $\beta_1 = \beta_2 = 0.08$
BER after interaction	$P(\boldsymbol{Y}) = 0.0768$ $P(\boldsymbol{Z}) = 0.1418$	$P(\boldsymbol{Y}) = 0.1128$ $P(\boldsymbol{Z}) = 0.1723$	$P(\boldsymbol{Y}) = 0.1128$ $P(\boldsymbol{Z}) = 0.2002$	$P(\boldsymbol{Y}) = 0.1472$ $P(\boldsymbol{Z}) = 0.201$	$P(\boldsymbol{Y}) = 0.1472$ $P(\boldsymbol{Z}) = 0.251$
LDPC code	(5000,1/4)	(7500,1/6)	(7500,1/6)	(10000,1/8)	(10000,1/8)
BER after CC decoding	$P_{ir} < 1.5 \times 10^{-5}$ $P_{Eve} = 0.073$	$P_{ir} < 1.16 \times 10^{-5}$ $P_{Eve} = 0.125$	$P_{ir} < 1.16 \times 10^{-5}$ $P_{Eve} = 0.172$	$P_{ir} = 1.9 \times 10^{-5}$ $P_{Eve} = 0.051$	$P_{ir} = 1.9 \times 10^{-5}$ $P_{Eve} = 0.195$
C_s	0.3804	0.5434	0.6621	0.288	0.6713
Security codes	$(2^6, 63, 9, \frac{1}{14})$	$(2^5, 31, 7, \frac{7}{62})$	$(2^5, 33, 11, \frac{1}{6})$	$(2^5, 31, 3, \frac{3}{62})$	$(2^5, 33, 11, \frac{1}{6})$
SER after SC decoding	$P_{B\_s} = 1.727 \times 10^{-4}$ $P_{E\_s} = 0.9844$	$P_{B\_s} = 3.993 \times 10^{-4}$ $P_{E\_s} = 0.96875$	$P_{B\_s} = 8.738 \times 10^{-4}$ $P_{E\_s} = 0.96875$	$P_{B\_s} = 4.067 \times 10^{-3}$ $P_{E\_s} = 0.96875$	$P_{B\_s} = 1.048 \times 10^{-3}$ $P_{E\_s} = 0.96875$
BER after SC decoding	$P_B = 8.77 \times 10^{-5}$ $P_E = 0.5$	$P_B = 2.061 \times 10^{-4}$ $P_E = 0.5$	$P_B = 4.516 \times 10^{-4}$ $P_E = 0.5$	$P_B = 2.099 \times 10^{-3}$ $P_E = 0.5$	$P_B = 5.411 \times 10^{-3}$ $P_E = 0.5$

Table 4.5: The performance under AWGN channel ($\delta = 1$)

SNR	$\gamma_1 = -1dB$ $\gamma_{e\_1} = -1dB$	$\gamma_1 = -5dB$ $\gamma_{e\_1} = -2dB$	$\gamma_1 = -5dB$ $\gamma_{e\_1} = -5dB$	$\gamma_1 = -7dB$ $\gamma_{e\_1} = -3dB$	$\gamma_1 = -9db$ $\gamma_{e\_1} = -9db$
BER after interaction	$Pr(\boldsymbol{V}) = 0.105$ $Pr(\boldsymbol{V}_e) = 0.188$	$Pr(\boldsymbol{V}) = 0.212$ $Pr(\boldsymbol{V}_e) = 0.288$	$Pr(\boldsymbol{V}) = 0.212$ $Pr(\boldsymbol{V}_e) = 0.334$	$Pr(\boldsymbol{V}) = 0.266$ $Pr(\boldsymbol{V}_e) = 0.340$	$Pr(\boldsymbol{V}) = 0.307$ $Pr(\boldsymbol{V}_e) = 0.426$
LDPC codes	$(2500, 1/2)$	$(5000, 1/4)$	$(5000, 1/4)$	$(7500, 1/6)$	$(10000, 1/8)$
BER after CC decoding	$P_{ir} < 5.6 \times 10^{-5}$ $P_{Eve} = 0.112$	$P_{ir} < 2.7 \times 10^{-5}$ $P_{Eve} = 0.308$	$P_{ir} < 2.7 \times 10^{-5}$ $P_{Eve} = 0.354$	$P_{ir} < 1.72 \times 10^{-5}$ $P_{Eve} = 0.379$	$P_{ir} < 4.5 \times 10^{-5}$ $P_{Eve} = 0.456$
C_s	0.505	0.8904	0.9371	0.9570	0.9937
Security codes	$\left(2^5, 33, 7, \frac{7}{66}\right)$	$\left(2^5, 31, 19, \frac{19}{62}\right)$	$\left(2^4, 17, 11, \frac{11}{34}\right)$	$\left(2^4, 15, 11, \frac{11}{30}\right)$	$\left(2^4, 15, 13, \frac{13}{30}\right)$
SER after SC decoding	$P_{B\_s} < 1.033 \times 10^{-3}$ $P_{E\_s} = 0.96875$	$P_{B\_s} < 1.187 \times 10^{-3}$ $P_{E\_s} = 0.96875$	$P_{B\_s} < 5.348 \times 10^{-4}$ $P_{E\_s} = 0.9375$	$P_{B\_s} < 3.032 \times 10^{-4}$ $P_{E\_s} = 0.9375$	$P_{B\_s} < 1.266 \times 10^{-3}$ $P_{E\_s} = 0.9375$
BER after SC decoding	$P_B < 5.335 \times 10^{-4}$ $P_E = 0.5$	$P_B < 6.127 \times 10^{-4}$ $P_E = 0.5$	$P_B < 2.852 \times 10^{-4}$ $P_E = 0.5$	$P_B < 1.617 \times 10^{-4}$ $P_E = 0.5$	$P_B < 6.753 \times 10^{-4}$ $P_E = 0.5$

Table 4.6: The performance under AWGN channel ($\delta = 2$)

SNR	$\gamma_1 = \gamma_2 = 1dB$ $\gamma_{e\_1} = \gamma_{e\_2} = 1dB$	$\gamma_1 = \gamma_2 = -1dB$ $\gamma_{e\_1} = \gamma_{e\_2} = 2dB$	$\gamma_1 = \gamma_2 = -3dB$ $\gamma_{e\_1} = \gamma_{e\_2} = -1dB$	$\gamma_1 = \gamma_2 = -4dB$ $\gamma_{e\_1} = \gamma_{e\_2} = -4dB$
BER after interaction	$Pr(\boldsymbol{V}) = 0.106$ $Pr(\boldsymbol{V}_e) = 0.1895$	$Pr(\boldsymbol{V}) = 0.188$ $Pr(\boldsymbol{V}_e) = 0.232$	$Pr(\boldsymbol{V}) = 0.266$ $Pr(\boldsymbol{V}_e) = 0.353$	$Pr(\boldsymbol{V}) = 0.304$ $Pr(\boldsymbol{V}_e) = 0.423$
LDPC codes	$(2500, 1/2)$	$(5000, 1/4)$	$(7500, 1/6)$	$(10000, 1/8)$
BER after CC decoding	$P_{ir} < 5.6 \times 10^{-5}$ $P_{Eve} = 0.281$	$P_{ir} < 2.7 \times 10^{-5}$ $P_{Eve} = 0.032$	$P_{ir} < 1.72 \times 10^{-5}$ $P_{Eve} = 0.393$	$P_{ir} < 4.5 \times 10^{-5}$ $P_{Eve} = 0.457$
C_s	0.8559	0.2039	0.9664	0.9939
Security codes	$\left(2^5, 31, 17, \frac{17}{62}\right)$	$\left(2^6, 63, 3, \frac{1}{42}\right)$	$\left(2^4, 15, 11, \frac{11}{30}\right)$	$\left(2^4, 15, 13, \frac{13}{30}\right)$
SER after SC decoding	$P_{B\_s} < 1.845 \times 10^{-3}$ $P_{E\_s} = 0.96875$	$P_{B\_s} < 2.431 \times 10^{-4}$ $P_{E\_s} = 0.9844$	$P_{B\_s} < 3.032 \times 10^{-4}$ $P_{E\_s} = 0.9375$	$P_{B\_s} < 1.266 \times 10^{-3}$ $P_{E\_s} = 0.9375$
BER after SC decoding	$P_B < 9.522 \times 10^{-4}$ $P_E = 0.5$	$P_B < 1.235 \times 10^{-4}$ $P_E = 0.5$	$P_B < 1.617 \times 10^{-4}$ $P_E = 0.5$	$P_B < 6.753 \times 10^{-4}$ $P_E = 0.5$

Table 4.7: The performance under Rayleigh channel ($\delta = 1$)

SNR	$\gamma_1 = 2dB$ $\gamma_{e\_1} = 2dB$	$\gamma_1 = -1dB$ $\gamma_{e\_1} = 2dB$	$\gamma_1 = -3dB$ $\gamma_{e\_1} = -3dB$	$\gamma_1 = -5dB$ $\gamma_{e\_1} = -3dB$	$\gamma_1 = -7db$ $\gamma_{e\_1} = -7db$
BER after interaction	$Pr(\boldsymbol{V}) = 0.122$ $Pr(\boldsymbol{V}_e) = 0.214$	$Pr(\boldsymbol{V}) = 0.177$ $Pr(\boldsymbol{V}_e) = 0.256$	$Pr(\boldsymbol{V}) = 0.218$ $Pr(\boldsymbol{V}_e) = 0.341$	$Pr(\boldsymbol{V}) = 0.264$ $Pr(\boldsymbol{V}_e) = 0.367$	$Pr(\boldsymbol{V}) = 0.301$ $Pr(\boldsymbol{V}_e) = 0.421$
LDPC codes	$(2500, 1/2)$	$(5000, 1/4)$	$(5000, 1/4)$	$(7500, 1/6)$	$(10000, 1/8)$
BER after CC decoding	$P_{ir} < 5.85 \times 10^{-5}$ $P_{Eve} = 0.273$	$P_{ir} < 1.63 \times 10^{-5}$ $P_{Eve} = 0.025$	$P_{ir} < 1.63 \times 10^{-5}$ $P_{Eve} = 0.392$	$P_{ir} < 4.671 \times 10^{-5}$ $P_{Eve} = 0.387$	$P_{ir} < 6.331 \times 10^{-5}$ $P_{Eve} = 0.448$
C_s	0.8448	0.1684	0.9658	0.9621	0.9912
Security codes	$\left(2^5, 33, 17, \frac{17}{66}\right)$	$\left(2^6, 63, 3, \frac{1}{42}\right)$	$\left(2^4, 15, 11, \frac{11}{30}\right)$	$\left(2^4, 15, 11, \frac{11}{30}\right)$	$\left(2^4, 15, 13, \frac{13}{30}\right)$
SER after SC decoding	$P_{B\_s} < 1.812 \times 10^{-3}$ $P_{E\_s} = 0.96875$	$P_{B\_s} < 1.681 \times 10^{-4}$ $P_{E\_s} = 0.9844$	$P_{B\_s} < 2.61 \times 10^{-4}$ $P_{E\_s} = 0.9375$	$P_{B\_s} < 1.166 \times 10^{-3}$ $P_{E\_s} = 0.9375$	$P_{B\_s} < 1.562 \times 10^{-3}$ $P_{E\_s} = 0.9375$
BER after SC decoding	$P_B < 9.351 \times 10^{-4}$ $P_E = 0.5$	$P_B < 8.539 \times 10^{-5}$ $P_E = 0.5$	$P_B < 1.392 \times 10^{-4}$ $P_E = 0.5$	$P_B < 6.217 \times 10^{-4}$ $P_E = 0.5$	$P_B < 8.333 \times 10^{-4}$ $P_E = 0.5$

Table 4.8: The performance under Rayleigh channel ($\delta = 2$)

SNR	$\gamma_1 = \gamma_2 = 6dB$ $\gamma_{e\_1} = \gamma_{e\_2} = 6dB$	$\gamma_1 = \gamma_2 = 2dB$ $\gamma_{e\_1} = \gamma_{e\_2} = 6dB$	$\gamma_1 = \gamma_2 = 1dB$ $\gamma_{e\_1} = \gamma_{e\_2} = 2dB$	$\gamma_1 = \gamma_2 = -1dB$ $\gamma_{e\_1} = \gamma_{e\_2} = -1dB$
BER after interaction	$Pr(\boldsymbol{V}) = 0.139$ $Pr(\boldsymbol{V}_e) = 0.239$	$Pr(\boldsymbol{V}) = 0.214$ $Pr(\boldsymbol{V}_e) = 0.294$	$Pr(\boldsymbol{V}) = 0.256$ $Pr(\boldsymbol{V}_e) = 0.360$	$Pr(\boldsymbol{V}) = 0.291$ $Pr(\boldsymbol{V}_e) = 0.413$
LDPC codes	$(2500, 1/2)$	$(5000, 1/4)$	$(7500, 1/6)$	$(10000, 1/8)$
BER after CC decoding	$P_{ir} < 5.85 \times 10^{-5}$ $P_{Eve} = 0.286$	$P_{ir} < 1.63 \times 10^{-5}$ $P_{Eve} = 0.322$	$P_{ir} < 4.671 \times 10^{-5}$ $P_{Eve} = 0.382$	$P_{ir} < 6.331 \times 10^{-5}$ $P_{Eve} = 0.437$
C_s	0.8626	0.9063	0.9587	0.9875
Security codes	$\left(2^5, 33, 17, \frac{17}{66}\right)$	$\left(2^5, 31, 19, \frac{19}{62}\right)$	$\left(2^4, 15, 11, \frac{11}{30}\right)$	$\left(2^4, 15, 13, \frac{13}{30}\right)$
SER after SC decoding	$P_{B\_s} < 1.812 \times 10^{-3}$ $P_{E\_s} = 0.96875$	$P_{B\_s} < 6.822 \times 10^{-4}$ $P_{E\_s} = 0.96875$	$P_{B\_s} < 1.166 \times 10^{-3}$ $P_{E\_s} = 0.9375$	$P_{B\_s} < 1.562 \times 10^{-3}$ $P_{E\_s} = 0.9375$
BER after SC decoding	$P_B < 9.351 \times 10^{-4}$ $P_E = 0.5$	$P_B < 3.521 \times 10^{-4}$ $P_E = 0.5$	$P_B < 6.217 \times 10^{-4}$ $P_E = 0.5$	$P_B < 8.333 \times 10^{-4}$ $P_E = 0.5$

Chapter 5

A Cross-layer Approach to Achieving Unconditionally Secure Communication via DFRFT

This chapter investigates a cross-layer approach to achieve unconditional communication security via DFRFT. The cryptographic techniques implemented in the higher layer is combined with the physical layer security scheme using random parameters flipping of DFRFT to provide security advantages for legitimate partners. The proposed scheme introduces a distorted signal parameter instead of a general signal parameter for wireless networks based on DFRFT [56, 106, 107]. The transmitter randomly flip-flops between the distorted signal parameter and the general signal parameter for confusing the attacker. An upper-layer pseudorandom sequence will be employed to control the flip-flops process. In this approach the physical-layer can utilize upper-layer encryption techniques for security, while physical-layer security techniques can also assist the security design in the upper layers. The advantages between legitimate partners building from the cross-

layer scheme are extended via developing the security codes on top of our cross-layer DFRFT security communication model, aiming to achieve an error-free legitimate channel while preventing the eavesdropper from any useful information. Thus, a strong secure model is built.

5.1 Introduction

Cross-layer is another way to build the wiretap channel under the single antenna system. Reference [55, 114, 103, 104] presented that the physical-layer security under the information-theoretic security models can achieve exponentially close to perfect secrecy in theory if suitably long codes are used for privacy amplification. There are no computational restrictions to be placed on the eavesdropper in physical-layer security system. However, the information theoretic security is an average-information measure. The system can be designed and tuned for a specific level of security e.g., with very high probability a block is secure, but it may not be able to guarantee security with probability 1. And the application of the information-theoretic security models subjects to limitations under the channel rapid variations scenarios. In the other hand, the security in classical cryptography system is based on unproven assumptions regarding the hardness of certain computational tasks. Therefore, systems are insecure if assumptions are wrong or if efficient attacks are developed. So any deployment of a physical-layer security protocol in a classical system would be part of a "layered security" solution where security is provided at a number of different layers, each with a specific goal in mind. Innovative cross-layer security designs considering both physical-layer security and upper-layer traditional security techniques are desirable for wireless networks.

Discrete fractional Fourier transform (DFRFT) is a generalization and has been applied in optics, quantum mechanics, and signal processing areas [56, 106]. Pei and Hsue

[107] extended the DFRFT to propose multiple-parameter discrete fractional Fourier transform (MPDFRFT) which has all of the desired properties for fractional transforms [108]. They also exploited the multiple-parameter feature of DFRFT to serve as encrypting digital data via proposing the double random phase encoding. Amr [109] pointed out that all the building blocks are linear, and hence, breaking this scheme via known plaintext attack is equivalent to solving a set of linear equations. [110, 111, 112, 57, 113] proposed several approaches of digital image encryption based on the fractional Fourier transform and chaos.

A practical solutions toward the construction of unconditionally secure communication systems via cross-layer approach is presented by utilizing the multi dynamic parameters of DFRFT system. By introducing one or several distorted signal parameters, the sender randomly flip-flops between the distorted signal parameter and the general signal parameter with a pseudorandom sequence cipher, which is pre-shared between the legitimate partners.By this way, the advantages of the legitimate partners are guaranteed. This advantages of the main channel can be extended by putting the security codes on top of cross-layer DFRFT security communication model to achieve an reliability receiving of the legitimate channel while BER of the eavesdropper approaches to 0.5.

5.2 Discrete Fractional Fourier Transform

In this Section, following the definition of the continuous fractional Fourier transform (FRFT) [116], the definition of the discrete fractional Fourier transform (DFRFT) is given.

5.2.1 Continuous Fractional Fourier Transform

The pth order FRFT of a time domain signal $x(t)$ is defined as [56]:

$$X_p(u) = \int_{-\infty}^{+\infty} K_p(u,t)\, x(t)\, dt \tag{5.1}$$

where $K_p(u,t)$ is kernel given by

$$K_p(u,t) = A_\alpha \exp\left[j\pi\left(u^2 \cot\alpha - 2ut \csc\alpha + t^2 \cot\alpha\right)\right] \tag{5.2}$$

in which n is integer, $A_\alpha = \sqrt{1 - j\cot\alpha}$, and $\alpha = p\pi/2$ is the rotation angle of FRFT, $p \neq 2n$. When $p = 0$, $X_p(u)$ is the signal $x(t)$ itself after FRFT. When $p = 1$, FRFT is the conventional Fourier transform (FT).

The inverse of an FRFT (IFRFT) with an order p is the FRFT with order $-p$ according to the following relation:

$$x(t) = \int_{-\infty}^{+\infty} X_p(u)\, K_{-p}(t,u)\, du \tag{5.3}$$

5.2.2 Discrete Fractional Fourier Transform

Let $x(n)$ be a sampled periodic signal with a period Δt and $n = -N, -N+1, ..., N$, in which N is the sampling interval of the signal $x(n)$. If we have function $y(n) = x(n\Delta t)$, let Δu is the sampled period of $y(n)$, the pth order discrete fractional Fourier transform (DFRFT) of $x(n)$ is given by [56]:

$$X_p(m) = \sum_{n=-N}^{N} K_p^{\alpha,\Delta t,\Delta u}(m,n)\, x(n) \tag{5.4}$$

where $K_p^{\alpha,\Delta t,\Delta u}$ is DFRFT transform matrix and defined as:

$$\begin{aligned} K_p^{\alpha,\Delta t,\Delta u} =& \sqrt{\frac{|\sin\alpha| - j\,\mathrm{sgn}(\sin\alpha)\cos\alpha}{2M+1}} \\ & \times e^{\frac{j}{2}\cot\alpha m^2 \Delta u^2} e^{-j\frac{\mathrm{sgn}(\sin\alpha) 2\pi nm}{2M+1}} e^{\frac{j}{2}\cot\alpha n^2 \Delta t^2} \end{aligned} \tag{5.5}$$

in which $m = -M, -M+1, ..., M$ where M is the sampling interval of the function $y(n)$.

The inverse of an DFRFT (IDFRFT) with an order p is the DFRFT with inverse rotation angle $-\alpha$ and alternating Δu, Δt according to the following relation:

$$x(n) = \sum_{n=-N}^{N} K_p^{-\alpha,\Delta u,\Delta t}(n,m) X_p(m) \tag{5.6}$$

When $M = N$, $\alpha = \pi/2$, IDFRFT becomes the inverse of discrete Fourier transform (IDFT). When $M = N$, $\alpha = -\pi/2$, DFRFT becomes the discrete Fourier transform (DFT).

5.2.3 OFDM System Based on DFRFT

The orthogonal frequency division multiplexing (OFDM) systems based on the discrete fractional Fourier transform is introduced in [117]. In the system, the fast Fourier transform (FFT) and inverse of fast Fourier transform (IFFT) are the replaced by DFRFT and IDFRFT. Assuming the cyclic prefix (CP) length is N_g, the mth sample of the nth transmitted frame is given by

$$X_p^i(m) = \sqrt{\frac{N}{N+N_g}} \sum_{n=0}^{N-1} K_{p,i}^{-\alpha,\Delta u,\Delta t}(m,n) x^i(n) \tag{5.7}$$

where $-N_g \leq m < N$, $x^i(n)$ is the symbol to be sent, assuming that different symbols are independent and identically distributed with a zero mean and average power σ^2. $K_{p,i}^{-\alpha,\Delta u,\Delta t}(m,n)$ expresses the calculation elements in IDFRFT with sampling space in time domain, given by Eqs. (5.5) and (5.6), in which $\alpha = p \cdot \pi/2$, p is the fractional factor of the transform, Δu is the sampling space in fractional Fourier domain, and $\Delta u T_s = 2\pi |\sin\alpha| / N$. When $\alpha = \pi/2$, the system is traditional orthogonal frequency division multiplexing (OFDM) system.

Let $h(k,l)$ be the discrete expression of the channel impulse response (CIR). The power spectrum of the channel obeys classical power spectra, the cross-correlation function

of CIR can be described as:

$$E\left[h\left(p,l_1\right)\cdot h\left(q,l_2\right)\right] = \sigma_l^2 J_0\left(2\pi\Delta t f_d\right)\delta\left(l_1-l_2\right) \tag{5.8}$$

where $\Delta t = |p-q|\cdot T_s$, σ_l^2 is the total power of the lth path. J_0 is the zero-order Bessel function of the first kind, f_d is the maximum Doppler frequency shift, $\delta(\cdot)$ is a Kronecker delta function, $(\cdot)^*$ represents complex conjugate.

We assume that the frame synchronized at the kth sample of the jth received frame is written as:

$$r_j\left(k\right) = \sum_{i=-\infty}^{\infty}\sum_{n=-N_g}^{N-1} h_{i,j}\left(k,k-m\right)\cdot x_i\left(n\right)e^{i2\pi\varepsilon/N} + w\left(k\right) \tag{5.9}$$

where $0 \le k < N$, $w(k)$ is complex additive white Gaussian noise (AWGN) and unit variance, σ_k^2, $\varepsilon = \Delta f N T_s$ is the frequency offset relative to the inverse of symbol duration, Δf is the frequency offset. The CIR of the $\left(j\left(N+N_g\right)+n\right)T_s$ time and the $l_1+\left(j-i\right)\left(N+N_g\right)$th path is: $h_{i,j}\left(k,l\right) = h\left(j\left(N+N_g\right)+n, l+\left(j-i\right)\left(N+N_g\right)\right)$.

After removing the CP, the transformed signals of DFRFT can be expressed as:

$$X_p^j\left(\hat{m}\right) = \sum_{n=0}^{N-1} K_{p,j}^{\alpha,\Delta t,\Delta u}\left(\hat{m},n\right)\cdot r_j\left(n\right) \tag{5.10}$$

where $0 \le \hat{m} < N$.

5.3 Cross-layer Security Model Based on DFRFT

In the DFRFT-OFDM system, the rotation angle α is one of the most important parameters. If the rotation angle α is 5^o in the transmitter, the rotation angle α is 5^o and 4.85^o in the receivers, respectively. The error of demodulation is shown in Figure 5.1, when the signal to noise ratio (SNR) is 0dB (error free). From Figure 5.1 we can know that the correct signal constellation can be demodulated only and if only the rotation

angle α is correctly known. Based on this fact, we introduce a distorted signal parameter instead of a general signal parameter for the DFRFT-OFDM system. The transmitter randomly flip-flops between the distorted signal parameter and the general signal parameter for confusing the attacker. An upper-layer pseudorandom sequence will be employed to control the flip-flops process.

In our scheme, two different rotation angles are denotes as α_1 and α_2 in the transmitter. An upper layer sequence set will be used to decide which rotation angle, either α_1 or α_2, is used to calculate the sending signal. Let the control sequence be $Q_{control} = (q_1, q_2, ..., q_n)$, $q_i \in GF(2)$. Then

$$\begin{cases} if \quad q_i = 0, \quad \alpha_1 \text{ is taken;} \\ if \quad q_i = 1, \quad \alpha_2 \text{ is taken.} \end{cases} \tag{5.11}$$

The control sequence $Q_{control}$ will be the secret key stream between the transmitter and the intended receiver. An attacker does not know the control sequence $Q_{control}$, who possibly know the two different rotation angles α_1 and α_2. The attacker can not know when slot the rotation angle α_1 or α_2 will be taken, which illustrates the ambiguity in the conventional signal detector. The attacker will receive the signal using a random sequence instead of the control sequence $Q_{control}$. The attacker also can directly adopt the rotation angle α_1 or α_2 to perform demodulation.

Figure 5.2 to Figure 5.4 illustrate the received results under perfect channel situation when the rotation angle α_1 and α_2 taken different values. In Figure 5.2, the rotation angle α_1 taken 0^o and the rotation angle α_2 will change from α_1 to $\alpha_1 + 90^o$. In Figure 5.3 and Figure 5.4 the rotation angle α_1 takes 0^o and 272^o, respectively while the rotation angle α_2 will change from α_1 to $\alpha_1 + 0.1^o$. Even if the difference between α_1 and α_2 is very small, the legitimate partners may obtain the advantages over the attackers. From Figure 5.2 to Figure 5.4, we can know that the bit error rate (BER) of legitimate receivers approaches 0 when the BER of attackers is over 0.15 with the difference between α_1 and

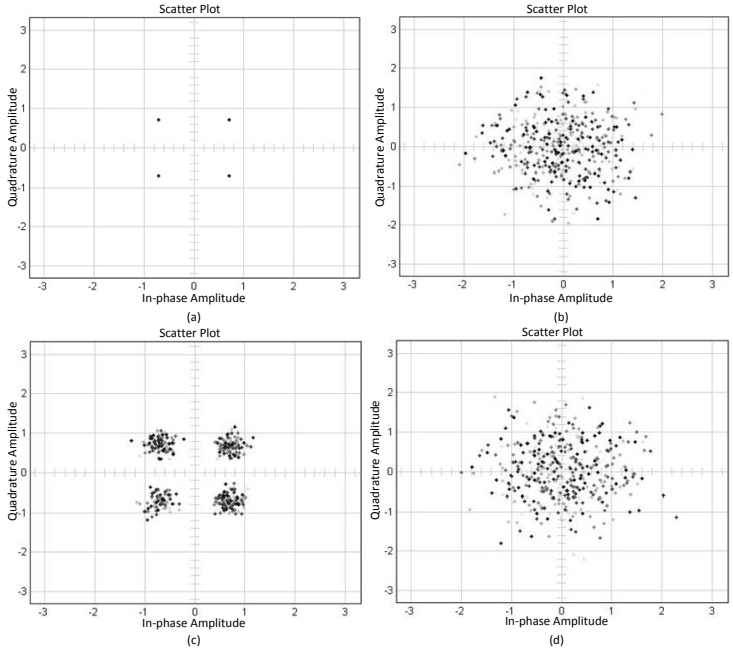


Figure 5.1: The signal constellation demodulation results with different parameters α. (a) The signal constellation before IDFRFT. (b) The signal constellation after IDFRFT. (c) The signal constellation after demodulation with $\alpha = 5^o$. (d) The signal constellation after demodulation with $\alpha = 4.85^o$.

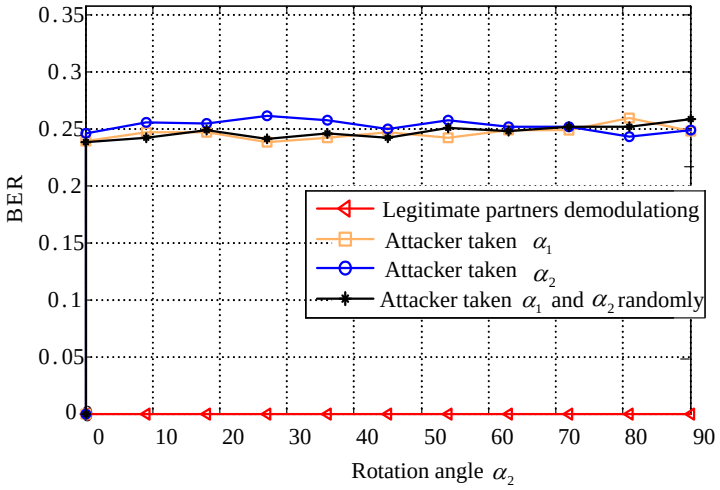


Figure 5.2: Received results of legitimate partners and attackers under $\alpha_1 = 0^o$ with α_2 changing from α_1 to $\alpha_1 + 90^o$.

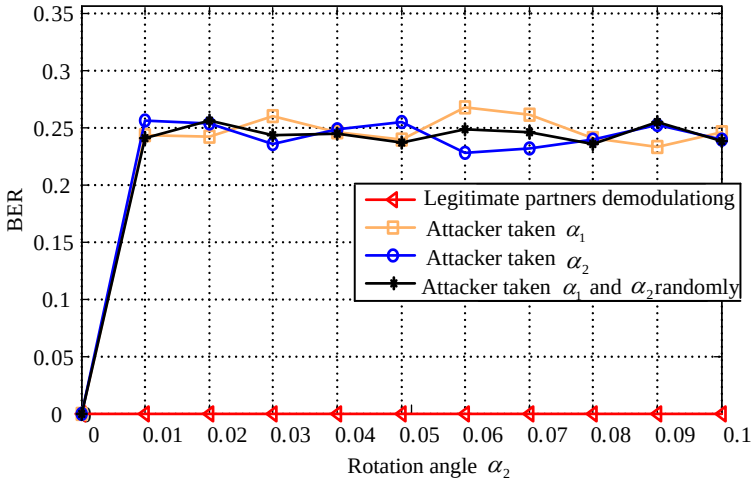


Figure 5.3: Received results of legitimate partners and attackers under $\alpha_1 = 0^o$ with α_2 changing from α_1 to $\alpha_1 + 0.1^o$.

α_2 over 0.01.

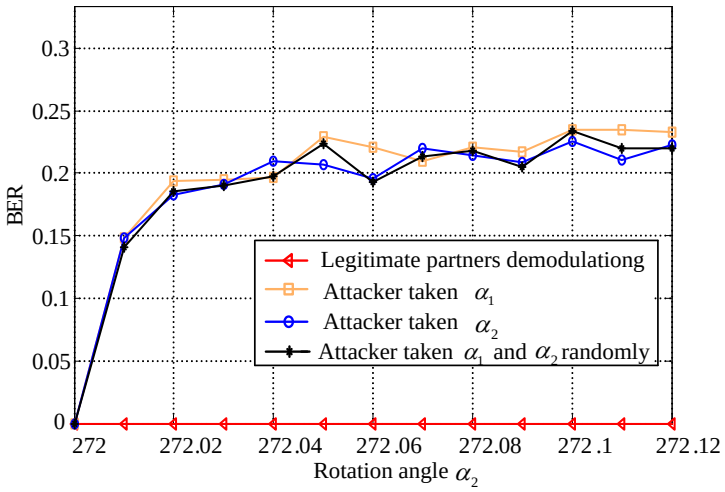


Figure 5.4: Received results of legitimate partners and attackers under $\alpha_1 = 272^o$.

5.4 Security System Model

Obviously, the scheme described in the previous section goes only half-way to providing a strong security communication. After DFRFT randomly flip-flopping transmission, the legitimate partners have better receiving results than that of the attackers. Our motivation is to let error probability of the legitimate receiver approach to zero and error probability of attackers close to 0.5, which meet the reliability and security condition Eqs. (2.3) and (2.4). To achieve this goal, we need the security codes (SC) that developed in the chapter 4 to degrade the information received by attackers without impairing the legitimate users. The secure communications model targeted in this study is shown in Figure 5.5, where the source intends to send m bits message $\mathbf{S} = (s_1, s_2, ..., s_m)$ to the destination. Firstly, the source encodes the message such that

$$\mathbf{X} = \chi_1(\mathbf{S}) \tag{5.12}$$

where χ_1 is the security encoder function. Alice continues to encode $\mathbf{X}$ such that

$$\mathbf{C} = \chi_2(\mathbf{X}) \tag{5.13}$$

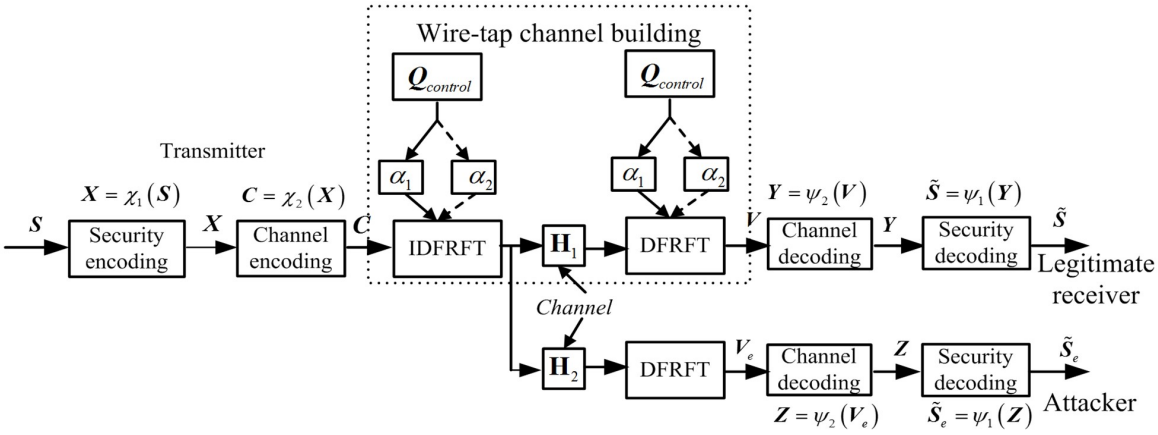


Figure 5.5: Security system model.

where χ_2 is the channel encoder function. Then IDFRFT is performed under the control sequence $\mathbf{Q}_{control}$. The sequence $\mathbf{V}$ received by the legitimate receiver is the noisy version of sequence $\mathbf{C}$. Meanwhile, an attacker can also observe the noisy sequence $\mathbf{V}_e$. The legitimate receiver performs DFRFT under the control sequence $\mathbf{Q}_{control}$. The attacker performs DFRFT without the control sequence $\mathbf{Q}_{control}$. Both the legitimate receiver and the attacker perform channel decoding as:

$$\mathbf{Y} = \Psi_2(\mathbf{V}) \tag{5.14}$$

$$\mathbf{Z} = \Psi_2(\mathbf{V}_e) \tag{5.15}$$

where Ψ_2 is channel decoding function, which is an invertible function of the channel encoding function χ_2. Then security decoding is performed as following:

$$\tilde{\mathbf{S}} = \Psi_1(\mathbf{Y}) \tag{5.16}$$

$$\tilde{\mathbf{S}}_e = \Psi_1(\mathbf{Z}) \tag{5.17}$$

where Ψ_1 is security decoding function, which is an invertible function of security encoding function χ_1.

5.5 Simulation Results

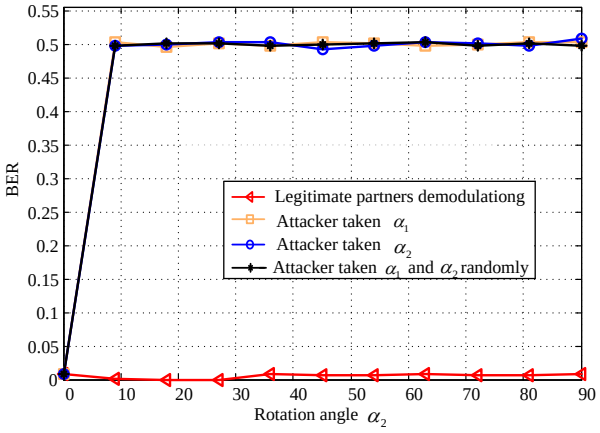


Figure 5.6: Received results of legitimate partners and attackers that put the security code on the top of the IDFRFT under $\alpha_1 = 0^o$ with α_2 changing from α_1 to $\alpha_1 + 90^o$.

The proposed **Construction 4.1** is based on binary resilient functions $(n, m, d-1)$, which can be generated by a corresponding linear code (n, m, d). In the experiment we implemented simplex codes $(2^m - 1, m, 2^{m-1})$, which are the dual of Hamming codes, so as to yield a $(2^m - 1, m, 2^{m-1} - 1)$ linear resilient function. Figure 4.3 shows the BER after applying the security codes versus the crossover probability p of the BSC before applying the security codes.

Corresponding to Figure 5.2-Figure 5.4, the security codes in Figure 4.3 are put onto the cross-layer model under AWGN channel and Rayleigh channel. The WG stream ciphers [115] are employed to generate the control sequences. The security codes $(7, 3, 2/7)$, $(15, 4, 4/15)$ and $(31, 5, 8/31)$ are put on the top of the cross model in Figure 5.6 to Figure 5.8, respectively.

Figure 5.6, Figure 5.7 and Figure 5.8 illustrate the received results when the rotation angle α_1 and α_2 taken different value after combining with security codes. In Figure 5.6, the rotation angle α_1 taken 0^o and the rotation angle α_2 will change from α_1 to $\alpha_1 + 90^o$.

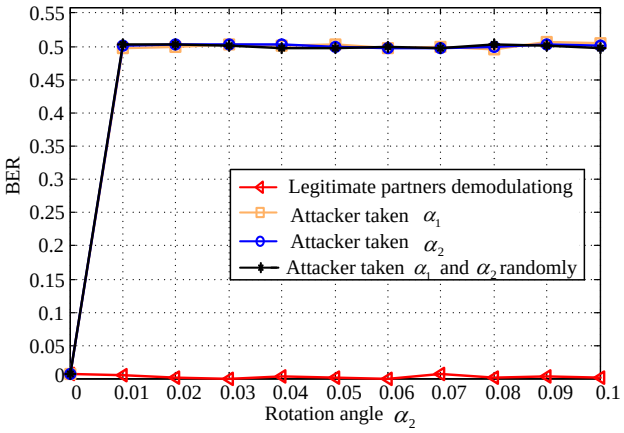


Figure 5.7: Received results of legitimate partners and attackers that put the security code on the top of the IDFRFT under $\alpha_1 = 0^o$ with α_2 changing from α_1 to $\alpha_1 + 0.1^o$.

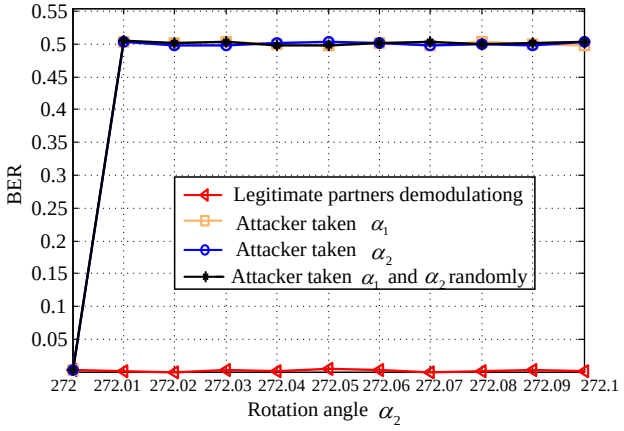


Figure 5.8: Received results of legitimate partners and attackers that put the security code on the top of the IDFRFT under $\alpha_1 = 272^o$.

In Figure 5.7 and Figure 5.8 the rotation angle α_1 taken 0^o and 272^o, respectively while the rotation angle α_2 will change from α_1 to $\alpha_1 + 0.1^o$. In Figure 5.6 and Figure 5.8, we can know that the BER of legitimate receivers are 0.007 to 2.016×10^{-4} when BER of attackers is approaching to 0.5, which means that the security system achieves almost error-free transmissions for the legitimate partners while zero information obtained by the attackers.

Chapter 6

Testbed for Unconditionally Secure Communications

In this chapter, a USRP testbed is presented, under which the physical layer security transmission system is built. Security communication between users are successfully established and performance of this USRP platform shows that the security condition Eq. (2.3) and reliability Eq. (2.4) can be realized in the actual environment.

6.1 Security Communication System Platform

The security communication system platform is designed as an universal platform, on which MIMO and single antenna systems all can be run. Here we mainly introduce the performance of the single antenna system associated with the security codes to build the unconditional communication security system, in which one to three Eves are presented in the system. The system scenario is shown in Figure 6.1. Because the platform adopt the broadband transmission, the Orthogonal Frequency Division Multiplexing (OFDM)

technology is used. Even if the platform can provide multiple antennas, here we only use single antenna of the system in Figure 6.1.

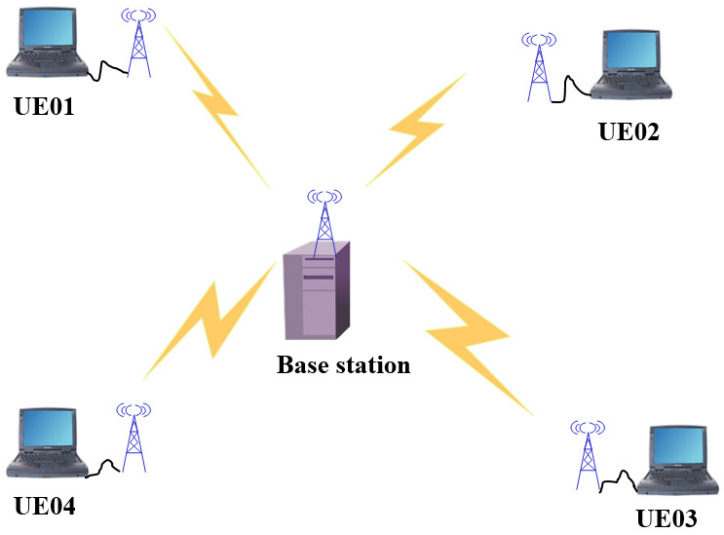


Figure 6.1: The security system scenario with one to three Eves

An USRP device is an open source software defined radio platform, which consist of a motherboard and two UBX160 daughter boards and vert2450 antennas are used. Motherboard is equipped with a dual 14-bit Analog to Digital Converter (ADC) operating at 100MHz and dual 16-dit Digital to Analog Converter(DAC)operating at 400MHz, and UBX160 transceiver daughter boards that act as a front end and have a frequency range from 10MHz to 6GHz [118]. Each USRP installed two transmit antennas and two receive antennas. Twelve USRP devices are used to build this security communication platform, whose is shown in Figure 6.2. The platform consists of five groups of wireless communication devices, called base stations, UE01, UE02, UE03 and UE04. The number of base stations and UE01 antennas is eight, the number of UE02 antennas is four, and the number of antennas for UE03 and UE04 is two. The four users—UE01, UE02, UE03 and UE04 can be the receiver or sender, and UE01, UE02, UE03 and UE04 can be either legitimate receiver or transmitter, or can be eavesdropper or attacking end. The

four users can establish a communication link with the base station at the same time. But only one user can establish a trust connection with the base station, that is, as a legitimate user, the other three users are regarded as eavesdroppers.

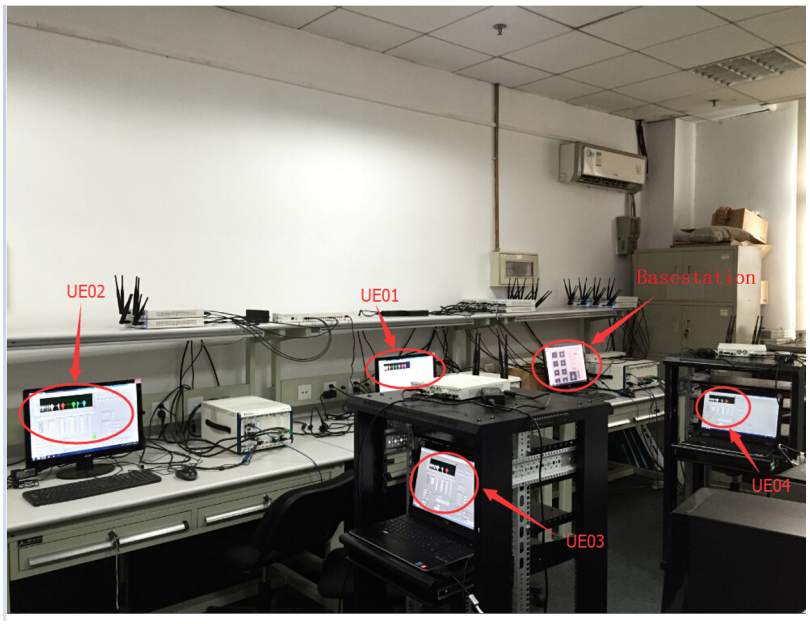


Figure 6.2: The security communication platform

6.2 The Communication Link of the Security Communication Platform

In the test, the base station transmits the signals and the other four users receive the signals and process the data to output results. Four users also will send pilot signals to the base station while the base station will choose one as a legitimate partner and perform handshaking with it and build trust connect with the channel estimation.

6.2.1 The signal processing at the transmitter

The base station as the transmitter, the signal processing flow chart in the transmitter is shown in Figure 6.3, in which the dashed line frame represents the signal process of the DFRFT transmitter system. It is assumed that the base station has discussed with all other four users, and has determined who is legitimate partner and pre-shares the control sequence $Q_{control}$ in Eq. (5.11) with its partner. The signal processing flow chart in the

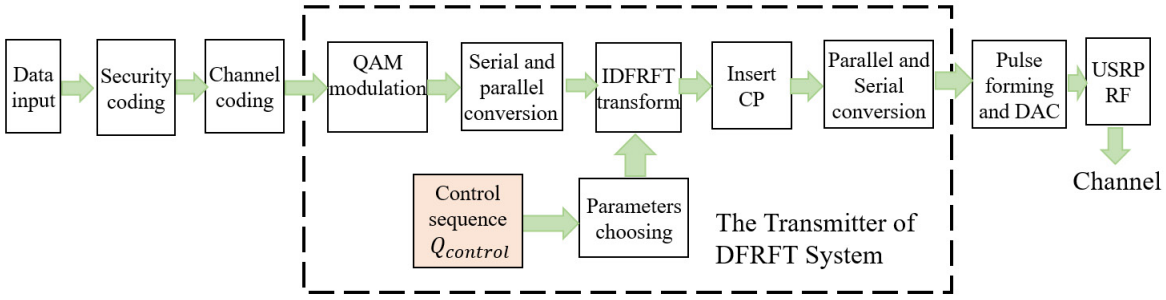


Figure 6.3: Signal processing flow chart of the DFRFT security system in the USRP transmitter

transmitter as following. firstly, enter the information messages that need to be sent and they will go through security encoding, channel encoding, QAM (Quadarature Amplitude Modulation) modulation, serial and parallel conversion. Then IDFRFT is performed, in which the parameters of DFRFT is chosen by Eq. (5.11) according to the pre-shared the control sequence $Q_{control}$. Thirdly, Cyclic Prefix (CP) is inserted. Finally, pulse shaping is made and Digital-Analog Conversion (DAC) is launched, which is transmitted through USRPs RF.

6.2.2 The signal processing at the receiver

The implementation flow of the received signal is shown in Figure 6.4, in which the dashed box represents the signal processing of the DFRFT system in the receiving end. Firstly, the signals that are received by the Radio Frequency (RF) performs Analog-to-Digital Conversion (ADC) and matched filtering to pass the signal to the host for core algorithm processing. Then serial and parallel conversion is performed. Then the CP is removed and the channel estimation is performed. Thirdly, verify the identity information (legal or illegal) is performed, DFRFT is carried out, in which the legitimate partner chooses the parameters of DFRFT by Eq. (5.11) according to the pre-shared the control sequence $Q_{control}$ while the Eve only can use the guessed control sequence $Q^{g}_{control}$ to determine the parameters of DFRFT. Finally, QAM demodulation, the secure decoding and channel decoding are carried to get the recovered security information and output. The BERs are calculated from the input signal and displayed on the front panel.

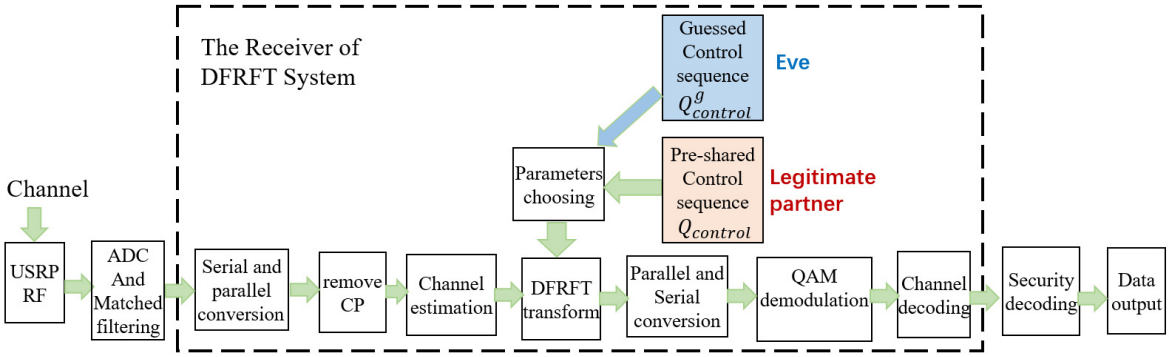


Figure 6.4: Signal processing flow chart of the DFRFT security system in the USRP receiver

6.3 Experimental Results

The system parameters are listed in Table 6.1 and the parameters of USRP devices are listed in Table 6.2.

Table 6.1: System parameters

Parameters	Values
The number of subcarriers	128
The number of tested frames	100000
The number of OFDM symbols	30
The number of cyclic prefix samples	32
The training symbols for synchronization	8

Table 6.2: USRP settings

Parameters	Values
The center frequency	3.5 GHz
The subcarrier interval	15 KHZ
The rate of I/Q	1M bit/s
The maximum transmit power	15 dBm
The channel gain	20 dB
The number of taps for multipath channel	16
The type of modulation	QAM

In the performance, four users—UE01, UE02, UE03 and UE04 randomly act as the legitimate user or eavesdroppers. Lets take an example, in which user UE01 acts as legitimate user and other users as illegal users. the following results are displayed and analyzed.

As shown in Figure 6.5, the base station randomly selects UE01 as the legitimate user and sends out the security messages. Therefore, the first lamp of four user identification lamps is green and other three lamps are red. The waveform of the transmitting signal is shown on the front panel. The front panel of the legal user UE01 is shonw in Figure 6.6, in which the lamp of "user status" is green. The eight waveform boxes on the left represent the waveform of the received signals of the eight slots. The constellation on the right shows the constellation of the data recovered by the user UE01. The constellation of the decoder is highly convergent from the diagram. The average error rate of 1000 frames is 2.41×10^{-6}.

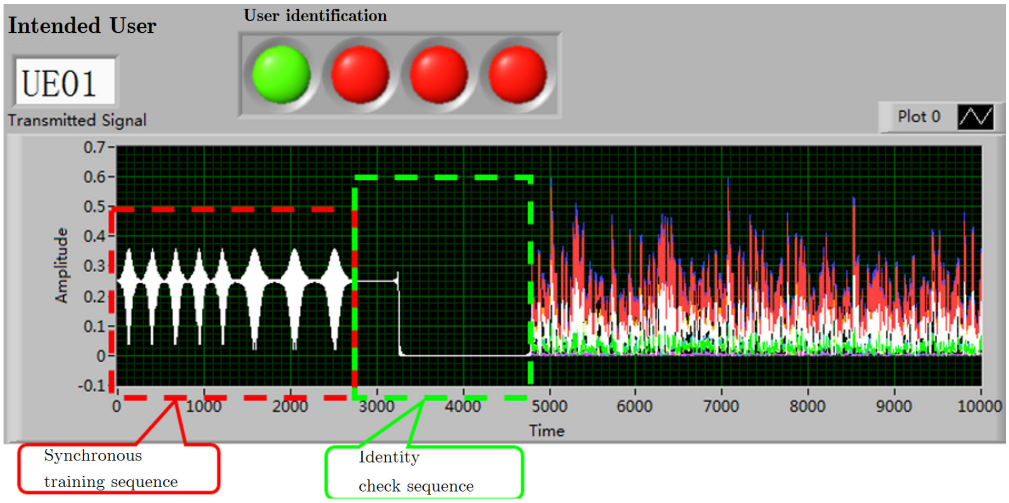


Figure 6.5: The front panel of the base station

Figure 6.7 is the front panel of UE02 who acts as illegal user. Therefore, the lamp of "user status" is red. The constellation of UE02 is scattered and disorganized at random, and the average error rate of 1000 frames is 0.499768. Figure 6.8 is the front panel of UE03 who also acts as illegal user and the lamp of "user status" is red. Same as that of UE02, the constellation of UE03 is scattered and disorganized at random.

In every test, the base station randomly select one of four users as the legitimate user

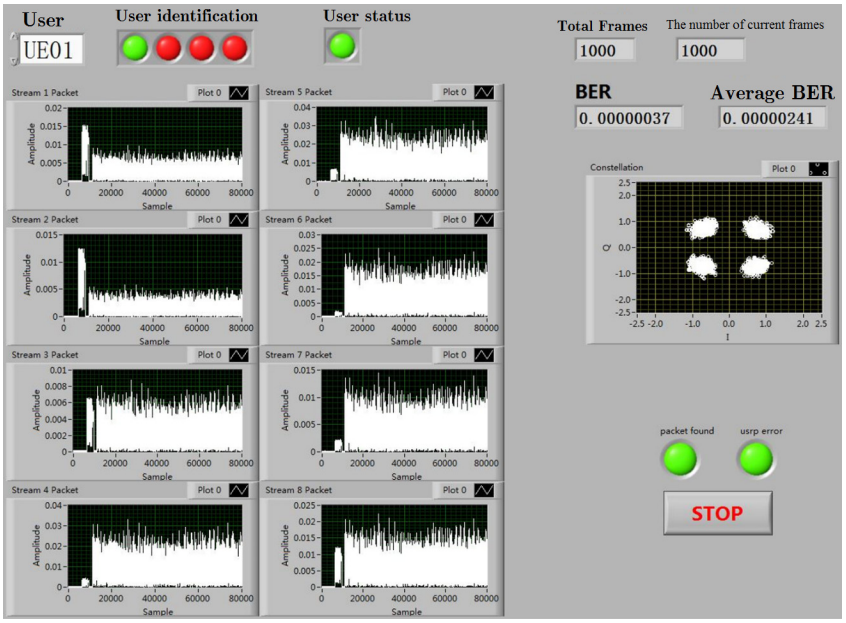


Figure 6.6: The front panel of UE01

and the total 1000 frames will be sent and the length of one frame is 1024 bits. Four users will alternately act as legal and illegal user and they received signals and try to recover the security messages. Every user will calculate its BERs in every frame and counts the average BERs at the end of 1000 received frames. Average BER of every user is shown in Table 6.3, in which 100 times tests are repeated and the total number of tested frames are 10^5.

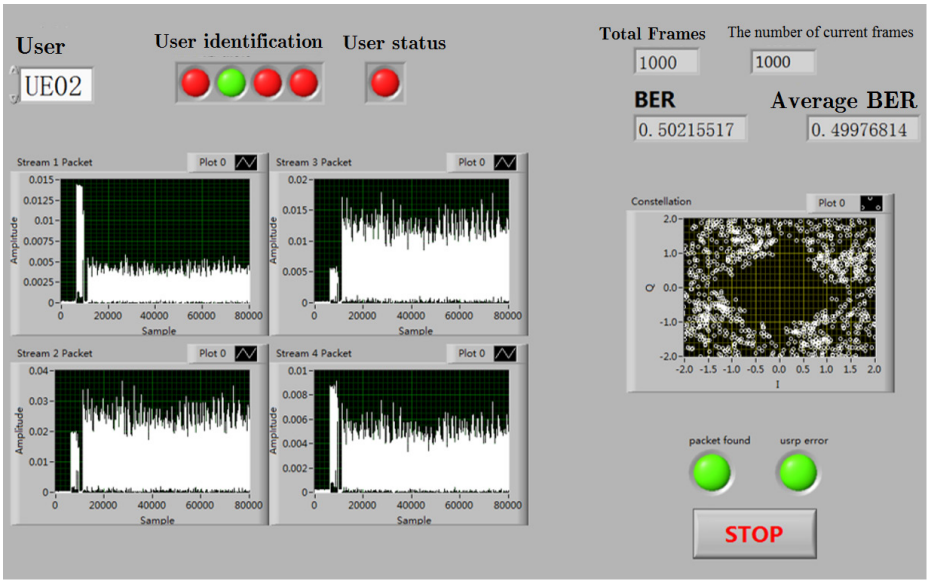


Figure 6.7: The front panel of UE02

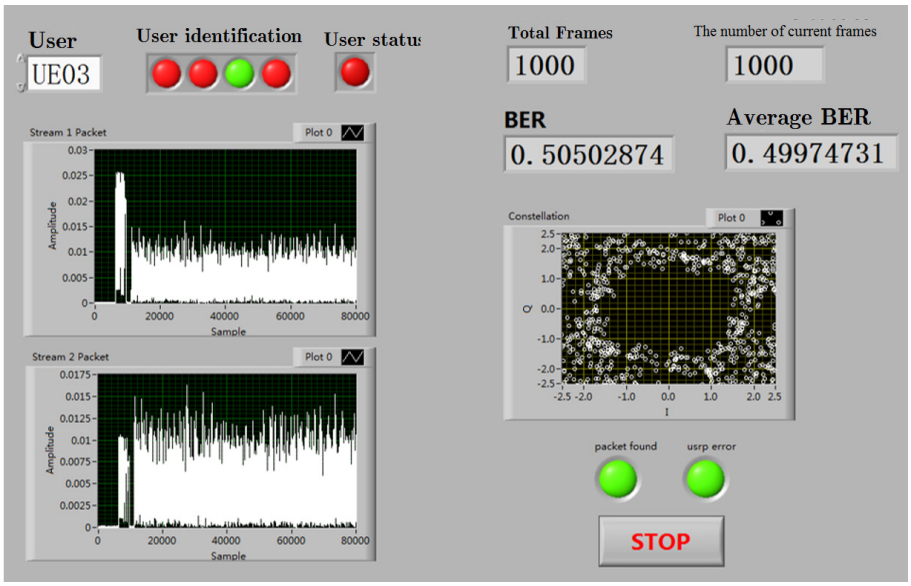


Figure 6.8: The front panel of UE03

Table 6.3: Average BER of every user

Received BER of legitimate users				
	UE01	UE02	UE03	UE04
UE01	2.41×10^{-6}	0.49900790	0.49938789	0.49956789
UE02	0.49976814	4.72×10^{-6}	0.49947343	0.49975389
UE03	0.49974731	0.49912165	8.91×10^{-6}	0.49988674
UE04	0.49974749	0.49912645	0.49929985	8.36×10^{-6}

Chapter 7

Conclusions and Further Work

7.1 Conclusions

In this thesis, we have

- Under the theory of Shannon and Wyner, a two-step unconditional model is given, in which the first step is build the advanced main channel and followed step is to choose a suitable security codes. Following this model, a novel wiretap channel built method called MRTWC is proposed, in which manipulating feedback mechanisms adds randomness to the feedback signals from the destination for keeping the eavesdropper ignorant and the redundancy is added and encoded by the LDPC codes such that a legitimate receiver can correctly receive and decode the signals. BERs of the proposed method are derived according to the crossover probability in the case of BSC, or the Signal to Noise Ratio (SNR) in the case of AWGN and Rayleigh channels. The representation of bit Log-likelihood Ratios (LLR) for optimal soft information decoding and demodulation is extracted.

- As effort of the second step, a low complexity encoding method of security codes is developed by taking advantage of a matrix general inverse algorithm, which is suitable to all kinds of coset security codes. Several families of binary and non-binary security codes with low complexity are constructed by the resilient functions. The threshold probabilities of novel security codes are derived, which provides the strong security proof for the proposed security codes.

- A scheme to build the secure communications via a cross-layer method based on DFRFT is proposed. By combining cryptographic techniques implemented in the higher layer with the physical layer security scheme using random parameters flipping of DFRFT, where the channel advantage of the intended receiver is ensured first by DFRFT and IDFRFT processing controlled by higher layer cryptography. The advantages of the legitimate partners are continuously extended by developing the security codes on top of our cross-layer DFRFT security communication model. A strong secure model for mobile communications is built. The extensive experiments are illustrated to verify the proposed security systems and demonstrate its feasibility and implement ability.

7.2 Further Research

The following issues could be further investigated:

- LLR extraction model for MRTWC under Rayleigh channel still left for opening. In the two-step joint scheme, experiments only can perform under bit-flipping decoding method under Rayleigh channel, which is not the optimal decoding method. The security capacity can not exactly evaluated. Therefore, LLR extraction under Rayleigh channel is necessary to develop in the future.

- The binary and non-binary resilient functions are a big family of cryptographic function, which provides a good way to construct provable secure and optimal security codes. It is deserve to explore the method to construct novel binary or non-binary security codes by other cryptographic functions. Particularly, the proposed non-binary security codes have better performance than that of binary security codes. Therefore, the future research can pay more attention to construct novel non-binary security codes.

- Although mobility is an intrinsic property of wireless networks, the impact of mobility on wireless physical layer security is not well understood. The physical layer security in the scenario with a random mobile receiver is deserve to investigate in the futuer.

- This thesis considers the framework of associating advantages build of the main channel with secure code to achieve unconditional secure communications under the single antenna system. More scenarios that joint advanced channel building and security codes could be considered. Such as, in cooperative security system how to build the advantages of the main channel by cooperative partners and associates with the security codes to satisfy the security and reliability conditions are the future research topic.

- The most results of the cross-layer security technologies are based on the simulation study. It is deserve to do more deep research work about the theoretical development in the cross-layer approach.

- The physical layer security schemes are at the expense of bandwidth. In the practical communication scenarios, it is suitable to use the physical layer security scheme to enhance the wireless system security when the bandwidth is rich. Therefore, a physical layer transmission method based on the channel prediction and users

Quality-of-Service (QoS) is deserved to study in the future, in which the system capacity is calculated and the judgement whether the extra capacity can be provided for the physical layer security scheme by the channel prediction.

Bibliography

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

[2] M. Agiwal, A. Roy and N. Saxena, "Next generation 5G wireless networks: a comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 18, 2016.

[3] Y. Zou, J. Zhu, X. Wang, et al., "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp.1727-1765, 2016.

[4] X. Chen, D. W. Kwan, W. H. Gerstacker, H, Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027 - 1053, 2017.

[5] M. Kamel, W. Hamouda, A. Youssef, " Physical layer security in ultra-dense networks," *IEEE Wireless Communications Letters*, 2017.

[6] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016 - 3025, 2016.

[7] F. Zhu, F. Gao, T. Zhang, K. Sun, M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 329 - 340, 2016.

[8] Z. Qin, Y. Liu, Z. Ding, Y. Gao, M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," *2016 IEEE International Conference on Communications (ICC)*, pp. 1-6, 2016.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[10] L. H. Ozarow and A. D. Wyner, "Wire tap channel II,", *AT&T Bell Labs. Tech. J.*, vol. 63, no. 10, pp. 2135-2157, Dec. 1984.

[11] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *in Proc. EUROCRYPT 84 workshop on Advances in cryptology: theory andapplication of cryptographic techniques. New York, NY, USA: Springer-Verlag New York, Inc.*,pp.33-51. 1985.

[12] A.O. Hero, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[13] F. Zhou, Z. Li, J. Cheng, et. al, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive Radio With SWIPT," *IEEE Transactions on Wireless Communications*, vol.16, no. 4, pp.2450 - 2464, 2017.

[14] T. R. Dean, A. J. Goldsmith, "Physical-Layer Cryptography Through Massive MIMO," *IEEE Transactions on Information Theory*, vol.63, no. 8, pp.5419 - 5436, 2017.

[15] W. Wu, S. Wu, B. Wang Robust, "Multi-objective beamforming design for power efficient and secure communication in MU-MISO networks," *IEEE Access*, vol. 5, pp. 13277 - 13285, 2017.

[16] M. Zhao, X. Wang, Suili Feng, "Joint power splitting and secure beamforming design in the multiple non-regenerative wireless-powered relay networks," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1540 - 1543, 2015.

[17] H. M. Wang, M. Luo, X. Xia, et. al "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdroppers CSI," *IEEE transactions on signal processing Letter*, vol. 20, no. 1, pp. 39-42, 2013.

[18] A. Mukherjee, A. L. Swindlehurst, , "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IIEEE transactions on signal processing*, vol. 59, no. 1, pp. 351-361, 2011.

[19] S. Goel, R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE transactions on wireless communications*, vol. 7, no. 7, pp. 2180-2189, Jun. 2008.

[20] A. Khisti, G. W. Wornell, "Secure transmission with multiple antennas I: the MIMOME wiretap channel," in *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088-3104, 2010.

[21] A. Khisti, G. W. Wornell, "Secure transmission with multiple antennas II: the MISOME wiretap channel," in *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 5515-5532, 2010.

[22] X. He, A. Khisti, A. Yener, "MIMO broadcast channel with an unknown eavesdropper: secrecy degrees of freedom," *IEEE Transactions on Communication*, vol. 62, pp. 246-255, 2014.

[23] L. Dong, Z. Han, A. P. Petropulu, et. al, "Improving wireless physical layer security via cooperating relays," *IEEE transactions on signal processing*, vol. 58, no. 3, pp. 1875-1888, 2010.

[24] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 524-527, 2017.

[25] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive base station cooperation for physical layer security in two-cell wireless networks," *IEEE Access*,vol. 4, pp.5607-5623, 2016.

[26] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," *IEEE ICC*, Kuala Lumpur, 1-5, 2016.

[27] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, Z. Zhang, Y. Jiang, and A. Xu, "Cooperative jamming aided secrecy enhancement in wireless networks with multiple eavesdroppers," *IEEE VTC Fall*, Toronto, accepted for publication, 2017.

[28] L. Hu, H. Wen, J. Tang, Z.-Q. He, and J. Su, "Joint cooperative jamming and beamforming for secure transmission in two-cell networks," *IEEE/CIC ICCC Wksps.*, Shenzhen, pp.1-5, 2015.

[29] M. L. Ammari, P. Fortier, "Physical layer security of multiple-input-multiple-output systems with transmit beamforming in Rayleigh fading," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1096-1103, 2015.

[30] W. C. Liao,, T. J. Chang, W. K. Ma, et. al, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE transactions on signal processing*, vol. 59, no. 3, pp. 1202-1215, 2011.

[31] G. Cohen and G. Zmor, Syndrome-coding for the wiretap channel revisited, in Proc. *IEEE Information Theory Workshop*, pp. 33C36, Chengdu, China, Oct. 2006.

[32] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communications Letters*, vol. 14, pp. 752-754, June 2010.

[33] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channels," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2933-2945, Aug. 2007.

[34] A. Subramanian, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth ldpc codes," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 585 -594, Sept. 2011.

[35] S. El Rouayheb, E. Soljanin, A. Sprintson, "Secure network coding for wiretap networks of Type II," *IEEE Trans. Inf. Theory*, vol.58, no.3, pp. 1361-1371, 2012.

[36] G. J. Foschini, M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Commun.*, Kluwer Academic Press, no. 6, pp. 311-335, 1998.

[37] Yanbing Zhang and Huaiyu Dai, "A unitary space-time coding scheme for UWB systems and its application in wireless secure communications", in Proc. *2006 IEEE International Conference on Acoustics, Speech and Signal*, vol. 4, pp.4-10, 14-19 May 2006.

[38] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, May 2007.

[39] H. Kim and J. D. Villasenor, "Secure MIMO communcications in a system with equal numbers of transmit and receive antennas," *IEEE Communications Letters*, vol. 12, no. 5, pp. 386–388, May 2008.

[40] Lifeng Lai, Praveen K. Gopala and Hesham El Gamal, "Secure communications over wireless channels," in Proc. *ITA 2007*, pp.1-5, Jan. 2007.

[41] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2735-2751, June, 2008.

[42] S. Ali. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Transactions on Signal Processing*, vol. 59, no.10, pp. 5013-5022, 2011.

[43] F. Renna, N. Laurenti and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol.7, no.4, pp. 1354-1367, 2012.

[44] Lifeng Lai, Yingbin Liang and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, pp.480-490, 2012.

[45] C. Wang, H.-M. Wang, X.-G. Xia, et al., "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, 2015, 14(5): 2596-2612.

[46] J. Tang, H. Wen, L. Hu, et al., "Associating MIMO beamforming with security codes to achieve unconditional communication security," *IET Commun.*, vol.10, no. 12, pp.1522-1531, 2016.

[47] R. Zhao, Y. Huang, W. Wang, et al., "Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2537-2551, 2016.

[48] X. Hu, P. Mu, B. Wang, et al., "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Trans. Veh. Technol.*, 2016, [DOI]: 10.1109/TVT.2016.2599223.

[49] D. Wang, B. Bai, W. Chen, et al., "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861-1874, 2016.

[50] M. Haus, M. Waqas, A. Y. Ding, et al., "Security and privacy in Device-to-Device (D2D) communication: A review," *IEEE Commun. Surveys Tut.*, 2017. [DOI]: 10.1109/COMST.2017.2649687.

[51] M. Alam, D. Yang, J. Rodriguez, et al., "Secure device-to-device communication in LTE-A," *IEEE Commun Mag.*, pp.66-73, vol. 52, no. 4, 2014.

[52] G. Fodor, S. Parkvall, S. Sorrentino, et al., "Device-to-device communications for national security and public safety," *IEEE Access*, vol.2, pp.1510-1520, 2014.

[53] H. Zhang, T. Wang, L. Song, et al., "Radio resource allocation for physical-layer security in D2D underlay communications," *IEEE ICC*, pp.2319-2324, Sydney, Australia,, 2014.

[54] D. Zhu, A. L. Swindlehurst, S. A. A. Fakoorian, et al., "Device-to-device communications: The physical layer security advantage," *IEEE ICASSP, Florence*, Italy, pp. 1606-1610, 2014.

[55] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733-742, 1993.

[56] C. Candan, M. A. Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *IEEE Trans. Signal Process.*, vol. 48, no. 5, pp. 1329-1337, May 2000.

[57] E. H. Elshazly, M. A. Ashour, E. M. Elrabaie, and A. M. Abbas, "An efficient fractional Fourier transform approach for digital image watermarking," in *Proc. 29th Nat. Radio Sci. Conf. (NRSC)*, Apr. 2012, pp. 245-254.

[58] B. Chor, O. Goldreich, J. H. astad, J. Friedman, S. Rudich, and R. Smolensky, "The bit extraction problem or t-resilient functions," *in IEEE Symp. on Foundations of Computer Science*,vol. 26, pp. 396-407, 1985.

[59] C. H. Bennett, G. Brassard, and J. M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, pp. 210-229, 1988.

[60] Jrgen Bierbrauer, K. Gopalakrishnan, and D. R. Stinson, "Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds," *SIAM J. Discrete Math.* vol. 9, no. 3, pp. 424-452, 1996.

[61] Mahdavifar. H, Vardy. A, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428-6443, 2011.

[62] H. Wen, G. Gong, P. H. Ho, "Achieving secure communications over wiretap channels via security codes from resilient functions," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 273-276, 2014.

[63] S. Thangaraj, A. R. Calderbank, et. al, "Applications of LDPC codes to the wiretap channels," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933-2945, 2007.

[64] M. Yi, X. S. Ji, K. Z. Huang, et. al, "Achieving strong security based on fountain code with coset pre-coding," *IET Communication*, vol. 8, no. 9, pp. 2476-2483, 2014.

[65] H. Wen, G. Gong, P. H. Ho, "Build-in wiretap channel I with feedback and LDPC," *Journal of Communications and Networks*, vol. 11, no. 12, pp. 24-32, 2009.

[66] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no.3, pp. 339-348, May 1978.

[67] S. Leung-Yan-Cheong, "On a special class of wire-tap channels," *IEEE Trans. Inform. Theory*, vol. 23, no.5, pp. 625-627, Sept. 1977.

[68] M. van Dijk, "On a special class of broadcast channels with confidentail messages," *IEEE Trans. Inform. Theory*, vol. 43, no.3, pp. 733-742, May 1997.

[69] R.G.Gallager, "Low-density parity-check codes,"*IRE Trans. Inform. Theory*, vol. IT-8, no. 1, pp. 21-28, 1968.

[70] M.R.David, *Single parity check product codes and iterative decoding*, Phd Thesis, School of Electrical and Electronic Engineering at the University of Canterbury, New Zealand, 2001.

[71] G. Cohen and G. Zmor, The wire-tap channel applied to biometrics, in Proc. *Int. Symp. Information Theory and its Applications*, Parma, Italy, Oct. 2004.

[72] Hagenauer, J., Offer, E., Papke, L., "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 429-445, 1996.

[73] Baldi, M., Cancellieri, G., Carassai, A., et al., "LDPC codes based on serially concatenated multiple parity-check codes," *IEEE Commun. Lett.*, vol. 13, no. 2, pp. 142-144, 2009.

[74] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio telepathy: extracting a secret key from an unauthenticated wireless channel," *in MobiCom'08: Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, pp. 128-139, 2008.

[75] Kai Zeng and Daniel Wu, An (Jack) Chan and Prasant Mohapatra"Exploiting multiple-Antenna diversity for shared secret key generation in wireless networks," *IEEE INFOCOM 2010*, pp.1-9, 2010.

[76] Hadi Ahmadi and Reihaneh Safavi-Naini, "Secret keys from channel noise," *EUROCRYPT 2011*, pp.266-283, 2011.

[77] Hongsong Shi, Shaoquan Jiang, Reihaneh Safavi-Naini and Mohammed Ashraful Tuhin, "On optimal secure message transmission by public discussion," *IEEE Transactions on Information Theory*, vol. 57, no.1, pp.572-585, 2011.

[78] Bhavana Kanukurthi and Leonid Reyzin, "Key agreement from close secrets over unsecured channels," *EUROCRYPT2009,*. pp. 206-223.

[79] Q. Chai and G. Gong, "BUPLE: securing passive RFID communication through physical layer enhancements," *7th Annual Workshop on RFID Security and Privacy (RFIDsec'11)*, Amherst, MA, USA, June, 2011.

[80] S. L. Campbell and C. D. Meyer, Jr., "Generalized Inverses of Linear Transformations," Pitman, London, 1979.

[81] M.Z.Nashed, ed., "Generalized Inverses and Applications," *Academic Press, New York*,1976.

[82] G. H. Golub and C. F. Van Loan, Matrix Computations. Baltimore, MD, USA: The Johns Hopkins Univ. Press, 2012.

[83] H. Wen, P. Ho and X. Jiang, "On achieving unconditional secure communications over binary symmetric channels (BSC)," *IEEE Wireless Communications Letters*, vol.1, no. 2,pp.49-52, 2012.

[84] F. J. MacWilliams and N. J. A. Sloane, "The theory of error correcting codes," *Amsterdam: North-Holland*, 1977.

[85] K. Gopalakrishnan , D. R. Stinson, "Three characterizations of non-binary correlation-immune and resilient functions," vol.5, pp. 241-251, 1995.

[86] P. Camion and A. Canteaut, "Construction of t-resilient functions over a finite alphabet," *Proceedings of EUROCRYPT'96*, pp. 283-293, 1996.

[87] D. R. Stinson, "On some methods for unconditionally secure key distribution and broadcast encryption," *Designs, Codes and Cryptography*, vol. 12, pp.215-243, 1997.

[88] S. Afreen, N. Ikram, "Resilient function based sequence generator-RFSG," *Computer Science Journal*, vol.1, no. 1, pp.7-15, 2011.

[89] L. Xu and C. Huang, "Computation-efficient multicast key distribution," *IEEE Transactions on Parallel and Distributed Systems*, vol.19, no. 5, pp.577-587, 2008

[90] C. Ding, G. Xiao and W. Shan, "The stability theory of stream ciphers (Lecture notes in computer science)," *Berlin, Germany, Springer-Verlag*, vol. 561, 1991.

[91] K. Gopalakrishnan, "A study of correlation-immune, resilient and related cryptographic functions," *PhD. Thesis, University of Nebraska at Lincoln*, 1994.

[92] Irving S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics (SIAM)*, vol. 8, no. 2, pp.300-304, 1960.

[93] N. Suresh Babu, "Studies on rank distance codes," *Ph.D Dissertation, IIT Madras*, Feb. 1995.

[94] J. G. Proakis, "Digital Communications," *4th Ed., McGraw-Hill, New York*, 2001.

[95] C. Berrou, A. Glavieux and P. Thitimajshima, "Near shannon limit error correcting coding and decoding: turbo codes," *in Proc. IEEE Int. Conf. Commun.,* Geneva, Switzerland, pp. 1064-1070, 1993.

[96] H. Behairy and S.-C. Chang, "Parallel concatenated gallager codes," *Electron. Lett.*, vol.36, no.24, pp. 2025-2026, 2000.

[97] M. Bloch, J. Barros, M. R. D. Rodrigues, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515-2534, 2008.

[98] V. U. Prabhu, , M. R. D. Rodrigues, " On wireless channels with antenna eavesdroppers: characterization of the outage probability and outage secrecy capacity," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 9, pp. 853-860, 2011.

[99] S. Gerbracht, C. Scheunert, E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 704-716, 2012.

[100] M. L. S. Kundu, D. A. Pados, S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1864-1873, 2013.

[101] W. C. Liao,, T. J. Chang, W. K. Ma, et. al, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE transactions on signal processing*, vol. 59, no. 3, pp. 1202-1215, 2011.

[102] X. Li, "Blind channel estimation and equalization in wireless sensor networks based on correlations among sensors," in *IEEE transactions on signal processing*, vol. 53, no. 4, pp. 1511-1519, 2005.

[103] L. Liu, J. Liang, K. Z. Huang, "Eavesdropping against artificial noise: hyperplane clustering," in *Proc. ICIST,*, YangZhou, China, pp. 1571-1575, March. 2013,

[104] Y. Gu, N. A. Goodman, S. Hong, et. al "Robust adaptive beamforming based on interference covariance matrix sparse reconstruction," *Elsevier Signal Process*, vol. 96, no. 10, pp. 375-381, Jul. 2013.

[105] Y. Gu, A. Leshem, 'Robust adaptive beamforming based on interference covariance matrix reconstruction and steering vector estimation," *IEEE transactions on signal processing*, vol. 60, no. 7, pp. 3881-3885, 2012.

[106] Q.-W. Ran, H.-Y. Zhang, Z.-Z. Zhang, and X.-J. Sha, "The analysis of the discrete fractional Fourier transform algorithms," in *Proc. Can. Conf. Elect. Comput. Eng. (CCECE)*, May 2009, pp. 979-982.

[107] S.-C. Pei and W.-L. Hsue, "The multiple-parameter discrete frac- tional Fourier transform," *IEEE Signal Process. Lett.*, vol. 13, no. 6, pp. 329-332, Jun. 2006.

[108] A. Mostayed, K. Sikyung, and S. Z. K. Sajib, "Novel parameter estimation method for chirp signals using Bowtie Chirplet and discrete fractional Fourier transform," in *Proc. 2nd Int. Conf. Future Generat. Commun. Netw. Symp. (FGCNS)*, vol. 3. Dec. 2008, pp. 23-26.

[109] A. M. Youssef, "On the security of a cryptosystem based on multiple- parameters discrete fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 15, no. 1, pp. 77-78, Jan. 2008.

[110] R. Tao, X.-Y. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 734-738, Dec. 2010.

[111] N. Jindal and K. Singh, "Image encryption using discrete fractional transforms," in *Proc. Int. Conf. Adv. Recent Technol. Commun. Comput.*, 2010, pp. 165-167.

[112] N. Ghoshal and J. K. Mandal, "Discrete Fourier transform based multimedia colour image authentication for wireless communication (DFTMCIAWC)," in *Proc. Int. Conf. Wireless VITAE*, Feb./Mar. 2011, pp. 1-5.

[113] W. Yaqing and Z. Shangbo, "A novel image encryption algorithm based on fractional Fourier transform," in *Proc. Int. Conf. Comput. Sci. Service Syst. (CSSS)*, Jun. 2011, pp. 72-75.

[114] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915-1923, Nov. 1955.

[115] Y. Nawaz and G. Gong, "WG: A family of stream ciphers with designed randomness properties," *Inf. Sci.*, vol. 178, no. 7, pp. 1903-1916, 2008.

[116] M. H. Ozaktas, O. Arikan, M. A. Kutay, and G. Bozdagt, "Digital computation of the fractional Fourier transform," *IEEE Trans. Signal Process.*, vol. 44, no. 9, pp. 2141-2150, Sep. 1996.

[117] M. Martone, "A multicarrier system based on the fractional Fourier transform for time-frequency-selective channels," *IEEE Trans. Commun.*, vol. 49, no. 6, pp. 1011-1020, Jun. 2001.

[118] M. Ettus, Universal software radio peripheral, Ettus Research, Mountain View, CA, www.ettus.com, 2012.

Appendix A: Published Papers

- Hong Wen, Tang Jie, Jinsong Wu, Huanhuan Song, Pin-han Ho, A Cross-layer Secure Communication Model Based on Discrete Fractional Fourier Transform (D-FRFT), IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 1, pp.119-126, Mar. 2015.

- Hong Wen, Pin-han Ho, Bin Wu, Achieving Secure Communications over Wiretap Channels via Security Codes from Resilient Functions, IEEE Wireless Communication Letter, vol. 3, no. 3, pp. 273-276, 2014.

- Hong Wen, Pin-han Ho, Xiaohong Jiang, On Achieving Unconditional Secure Communications over Binary Symmetric Channels (BSC), IEEE Wireless Communications Letters, vol. 1, no. 2, pp.49-52, Apr. 2012.

- Hong Wen, Guang Gong, Shi-Chao Lv and Pin-han Ho, Framework for MIMO Cross-Layer Secure Communication Based on STBC, Telecommunication Systems, vol.47, no.3, pp. 1-9, Agu. 2013.

- Hong Wen, Pin-han Ho, A Novel Scheme of Detecting the Sybil Attack Based on Channel Identification, The First International Workshop on Security in Computers, Networking and Communications, Joint with ICC2012, Ottawa, Canada 10-11 June, 2012.