Polar Codes Combined with Physical Layer Security on Impulsive Noise Channels

Huan Cao

School of Engineering

Newcastle University

A thesis submitted for the degree of

Doctor of Philosophy

April 2020

To my loving parents.

Acknowledgements

I would like to express my deeply gratitude to my supervisor Dr. Martin Johnston, for his support and advice during my master and PhD period at Newcastle University. His experience and enthusiasm inspired me to work on error-correcting codes and physical layer security, which is the focus of this thesis. I am very grateful to him for his excellent suggestions and times spent on discussing my research work and proofreading my papers regardless of his busy schedule. I would also like to thank my second supervisor Dr. Stéphane Le Goff for his constant encouragement during my PhD study.

In addition, I am very grateful to Dr. Zhen Mei for his valuable input towards my research. I would also like to acknowledge all my friends and colleagues in Intelligent Sensing and Communications (ISC) Group for their being with me in all my times and helping me to cope up with my research. Especially, I am grateful to my friends in China, Yao Bai, Xulong Cao, Yu Zhang. They were always ready to listen to me and motivated me to achieve the best while doing my PhD here in the UK.

Finally, I would like to express my deepest love and appreciation to my family. I really would like to thank my parents and my sister from the bottom of my heart for their continuous encouragement and support throughout my studies at the Newcastle University. And lastly my love to my 4 years old nephew as he was the one who made me laugh in my tough times. Compared with their love all words are eclipsed. Their great love and trust inspired me to work harder and finish this thesis.

Abstract

The need for secure communications is becoming more and more important in modern society as wired and wireless connectivity becomes more ubiquitous. Currently, security is achieved by using well established encryption techniques in the upper layers that rely on computational complexity to ensure security. However, processing power is continually increasing and well-known encryption schemes are more likely to be cracked. An alternative approach to achieving secure communication is to exploit the properties of the communication channel. This is known as physical layer security and is mathematically proven to be secure. Physical layer security is an active research area, with a significant amount of literature covering many different aspects. However, one issue that does not appear to have been investigated in the literature is the effect on physical layer security when the noise in the communication channel is impulsive. Impulsive noise adds large spikes to the transmitted signal for very short durations that can significantly degrade the signal. The main source of impulsive noise in wireless communications is electromagnetic interference generated by machinery. Therefore, this project will investigate the effect of impulsive noise on physical layer security.

To ensure a high level of performance, advanced error-correcting codes are needed to correct the multiple errors due to this harsh channel. Turbo and Low-Density Parity-Check (LDPC) codes are capacity-approaching codes commonly used in current wireless communication standards, but their complexity and latency can be quite high and can be a limiting factor when required very high data rates. An alternative error-correcting code is the polar code, which can actually achieve the Shannon capacity on any symmetric binary input discrete memoryless channel (B-DMC). Furthermore, the complexity of polar codes is low and this makes them an attractive error-correcting code for high data rate wireless communications. In this project, polar codes are combined with physical layer

security and the performance and security of the system is evaluated on impulsive noise channels for the first time.

This project has three contributions:

- Polar codes designed for impulsive noise channels using density evolution are combined with physical layer security on a wire-tap channel experiencing impulsive noise.
- The secrecy rate of polar codes is maximised. In the decoding of polar codes, the frozen bits play an important part. The positions of the frozen bits has a significant impact on performance and therefore, the selection of optimal frozen bits is presented to optimise the performance while maintaining secure communications on impulsive noise wire-tap channels.
- Optimal puncturing patterns are investigated to obtain polar codes with arbitrary block lengths and can be applied to different modulation schemes, such as binary phase shift keying (BPSK) and M-ary Quadrature Amplitude Modulation (QAM), that can be rate compatible with practical communication systems. The punctured polar codes are combined with physical layer security, allowing the construction of a variety of different code rates while maintaining good performance and security on impulsive noise wire-tap channels.

The results from this work have demonstrated that polar codes are robust to the effects of impulsive noise channel and can achieve secure communications. The work also addresses the issue of security on impulsive noise channels and has provided important insight into scenarios where the main channel between authorised users has varying levels of impulsiveness compared with the eavesdropper's channel. One of the most interesting results from this thesis is the observation that polar codes combined with physical layer security can achieve good performance and security even when the main channel is more impulsive than the eavesdropper's channel, which was unexpected. Therefore, this thesis concludes that the low-complexity polar codes are an excellent candidate

for the error-correcting codes when combined with physical layer security in more harsh impulsive wireless communication channels.

Contents

List of Figures

List of Tables

List of Acronyms & Symbols

Symbols

α	Characteristic exponent of α-stable process
β	Skewness of α-stable pdf
δ	Location parameter of α-stable process
ϵ	The erasure probability
Γ	The ratio of Gaussian to impulsive noise power
γ	Dispersion of α-stable process
$\star$	Convolution operations in the variable node domain
$\circledast$	Convolution operations in the check node domain
σ^2	The variance of the Gaussian noise
SNR_K	Geometric signal-to-noise ratio
C_s	Secrecy capacity
C_k	The exponential of the Euler constant
E_b	The energy per bit
N_0	Noise power
R	Code rate
R_s	Secrecy code rate
$I(W)$	Symmetric capacity
$Z(W)$	Bhattacharyya parameter

Acronyms/Abbreviations

AQR	Automatic Repeat Request
AWAN	Additive White Class A noise
AWGN	Additive White Gaussian Noise
B-DMC	Binary Discrete Memoryless Channel
BEC	Binary Erasure Channel
BEP	Bit Error Probability
BER	Bit Error Rate
BI-AWGN	Binary Input-Additive White Gaussian Noise
BLEP	Block Error Probability
BP	Belief Propagation
BPSK	Binary Phase-Shift Keying
BSC	Binary Symmetric Channel
CA-SCL	Cyclic Redundancy Check Aided Successive Cancellation List
CA-SCS	Cyclic Redundancy Check Aided Successive Cancellation Stack
CRC	Cyclic Redundancy Check
DE	Density Evolution
DMC	Discrete Memoryless Channel
EMI	Electromagnetic Interference
ECC	Error-correcting Codes
GA	Gaussian Approximation
GMM	Gaussian Mixture Model
HARQ	Hybrid Automatic Repeat Request
ISIT	International Symposium on Information Theory

IFT	Inverse Fourier Transform
LDPC	Low-density Parity-Check
LLR	Log-Likelihood Ratio
MAI	Multiple Access Interference
QAM	Quadrature Amplitude Modulation
M-QAM	M-ary Quadrature Amplitude Modulation
MIMO	Multiple-Input Multiple-Output
ML	Maximum Likelihood
OFDM	Orthogonal Frequency-Division Multiplexing
PDF	Probability Density Function
PLC	Power Line Channel
QC-LDPC	Quasi-cyclic Low-density Parity-Check
RC-LDPC	Rate Compatible Low-density Parity-Check
RCPP	Rate-compatible Punctured Polar
RM	Reed-Muller
SαS	Symmetric α-Stable
SC	Successive Cancellation
SCL	Successive Cancellation List
SCS	Successive Cancellation Stack
SNR	Signal-to-Noise Ratio

Chapter 1

Introduction

1.1 Introduction

The increasing popularity of mobile devices has meant that the security of wireless communications has never been more important. Secure communications are currently achieved by encrypting data, a process that takes place in the upper layers of the communication system. This has proven to be very effective, although not infallible as encryption is built on the assumption that it is computationally too complex to break and is not mathematically provable to be absolutely secure. Finding the secret key in order to ensure communication security is becoming easier due to the improvements in computer processing ability. The number of attacks on wireless communications is increasing due to the open characteristic of the wireless network.

An alternative approach to achieving secure communications is to exploit the random nature of the physical layer itself. This is known as physical layer security and it employs an information theoretic approach that is mathematically provable to be secure. It also has the advantage of not requiring the users in a communication system to share keys and employ complicated encryption and decryption methods. For these reasons, physical layer security is an active research area that presents many interesting problems to address.

The main focus of this thesis is to optimise the performance of a wireless communication system employing physical layer security, by combining it with powerful error-correcting codes (ECC). ECC works by adding redundancy to messages. Allowing the receiver to detect and correct channel errors. In traditional error-correction coding, we only desire that authorized receiver receives the message error

free. This is known as a reliability constraint on the coding problem. Designing codes for the wiretap channel model must satisfy both reliability constraints and security constraints. ECC should provide as much structure for the legitimate receiver to correct errors, while supplying enough confusion to unauthorized receivers to achieve security. Capacity-approaching codes, such as turbo and low-density parity-check (LDPC) codes, are commonly employed due to their powerful error correction and popularity in many communication standards. However, a more recent coding scheme, known as polar codes has gained increasing interest in academia and industry and has several advantages over turbo and LDPC codes. Polar codes are the first proven capacity-achieving codes on binary discrete memoryless channels (B-DMC), but also have much lower encoding and decoding complexity. These characteristics have made polar codes very popular and they have now been adopted into the 5G standard. Hence, it is interesting to investigate polar codes in the context of a communication system employing physical layer security. In this work we assume the channel model is an impulsive noise channel that is generated by a symmetric alpha-stable (SαS) distribution. We also assume an eavesdropper always has a Signal-to-Noise Ratio (SNR) equal to or less than the intended recipient.

1.2 Motivation and Challenges

Combining polar codes with physical layer security has been proposed in the literature, but there are several areas of novelty in this area that do not appear to have been considered. Previous research has focused on the well-known wiretap channel, where two legitimate users (Alice and Bob) are communicating with each other, but there is also a third unauthorised user (Eve) who is attempting to intercept the communication between Alice and Bob. The noise added at the receivers on the wiretap channel is always assumed to have a Gaussian distribution, but a scenario where impulsive noise is present has not been considered. This type of noise has a non-Gaussian distribution with heavy tails and will result in all users experiencing large amplitude random pulses that occur for an extremely short duration. Therefore, this thesis investigates the effect of impulsive noise on a polar-coded physical layer security system on the wiretap channel. This opens up a number of scenarios, such as varying the level of impulsiveness at Bob's and Eve's receiver and investigating if security can still be achieved using polar codes. Furthermore, both Bob and

Eve could experience different levels of impulsiveness, where Bob's channel could be more impulsive than Eve's channel.

This project presents several challenges that must be overcome to achieve the implementation of polar-coded physical layer security system. First, the design of polar codes that are optimised for impulsive noise channels must be investigated. Existing methodologies, such as density evolution (DE), must be modified to use the statistics of the impulsive channel model and allow the construction of good polar codes. Second, we must ensure that the designed polar codes can achieve good performance, but also guarantee security for Alice and Bob, which is a significant challenge. Finally, the block length of polar codes is limited to be 2^n, where n is a positive integer, and this limits the usability of these codes in practical applications where arbitrary block lengths are required. Therefore, puncturing methods will be investigated to shorten polar codes to arbitrary lengths and produce rate-compatible polar codes.

1.3 Aims and Objectives

The aim of this thesis is to design and evaluate the performance and security of polar codes in a wireless communication system employing physical layer security and subject to impulsive noise. Performance will be evaluated by simulating polar codes and physical layer security on a wiretap channel with impulsive noise modelled by a symmetric alpha-stable distribution. The bit-error rate (BER) of different polar codes will be obtained at Bob's receiver to evaluate performance and security will be achieved if the BER at Eve's receiver is as close to 0.5 as possible for all signal-to-noise ratios. The objectives of the thesis are:

- To design polar codes optimised for impulsive noise channels using density evolution.
- To investigate the performance and security of polar codes combined with physical layer security on impulsive noise channels with different levels of impulsiveness.
- To design polar codes that have maximal secrecy codes rates when combined with physical layer security, so that security is achieved while the redundancy in the polar codeword is minimised.

- To design an optimal puncturing method to obtain polar codes with arbitrary block lengths and can be applied to different modulation schemes, such as binary phase shift keying (BPSK) and M-ary Quadrature Amplitude Modulation (M-QAM), that can be rate compatible with practical communication systems.

1.4 Statement of Originality

This thesis comprises novel work focusing on the design of good polar codes that have excellent performance and security, with different block lengths and code rates. New polar codes have been designed that are shown to achieve excellent BER performance at Bob's receiver for varying levels of impulsiveness, while ensuring that the BER at Eve's receiver is high and does not obtain information about Alice and Bob's communication. The results from this part of the thesis have been published in "Construction of Polar Codes Combined with Physical Layer Security on Impulsive Noise Channels". However, these polar codes when combined with physical layer security suffered from low secrecy code rates, so the design of the polar codes was improved to ensure the secrecy code rates were significantly increased, while still guaranteeing very good performance and security. The results of this work were published in "Frozen Bit Selection Scheme for Polar Coding Combined with Physical Layer Security". The block lengths of both types of polar codes were limited to 2^n, so a puncturing method was proposed that shortens the block length to any arbitrary length and can be applied to different modulation schemes. A journal paper is currently in preparation to present these results.

1.5 Organization of the Thesis

This thesis is organized as follows:

Chapter two presents a literature survey on research related to physical layer security, error-correcting codes (LDPC codes, turbo codes and polar codes) combined with physical layer security and error-correcting codes designed for impulsive noise channels.

Chapter three provides an extensive theoretical background on polar codes, physical layer security and impulsive noise modelling, which is prerequisite knowledge

for the succeeding chapters comprising the novelty of this thesis.

Chapter four describes the design of good polar codes for impulsive noise channels with symmetric alpha-stable distribution, which are then combined with physical layer security. The performance and security of the polar-coded system is evaluated on the wiretap channel with different levels of impulsiveness.

Chapter five addresses the issue of low secrecy code rates due to the combination of polar codes with physical layer security. New polar coding scheme are designed with significantly increased secrecy code rates and performance and security and evaluated on the wiretap channel with different levels of impulsiveness.

Chapter six addresses the issue of limited block lengths by proposing a puncturing method to produce arbitrary block lengths and the performance and security of these punctured polar codes are evaluated for BPSK and M-QAM schemes on the wiretap channel with different levels of impulsiveness.

1.6 Publications Related to the Thesis

1. **H. Cao**, Z. Mei, M. Johnston, and S. Le Goff, "Construction of Polar Codes Combined with Physical Layer Security on Impulsive Noise Channels", *in Proc. IEEE 18th International Conference on Communication Technology (ICCT)*, Chongqing, China, 2018.

2. **H. Cao**, M. Johnston, and S. Le Goff, "Frozen Bit Selection Scheme for Polar Coding Combined with Physical Layer Security", *in Proc. IEEE 4th International Conference on UK - China Emerging Technologies (UCET)*, Glasgow, UK, 2019.

Chapter 2

Literature Survey

2.1 Introduction

In this chapter, the literature on physical layer security techniques, error-correction codes and impulsive noise will be reviewed. First, we give an overview of physical layer security on wireless communication that is modelled using wiretap channel. Then Low-Density Parity-Check (LDPC) codes, turbo codes and polar codes (conventional and punctured polar codes) are reviewed, with particular focus on their combination with physical layer security are reviewed. In addition, examples of common communication systems with impulsive noise are given. Finally, the performance of error-correcting codes in the presence of impulsive noise channel is presented.

2.2 Physical Layer Security

Physical layer security technology is based on the absolute security model proposed by Shannon [2] in 1949. In the classic encrypted system proposed by Shannon, the legitimate users share a key that the eavesdropper cannot obtain, and use this key to encrypt and decrypt the data. Under the condition that the the eavesdropper's receiving sequence is independent of the transmission sequence, the mutual information is 0. However this has issues, such as key distribution and computational complexity. More importantly, all encryption measures are based on the premise that it is computationally infeasible for eavesdroppers to be decrypted without the knowledge of the secret key, which remains mathematically unproven. A breakthrough in

communications security was physical layer security, which achieves secure transmissions without the need of any form of pre-shared secret keys between the legitimate users. Security can be achieved through the physical layer, by only exploiting the difference between the channels of intended receivers and those of eavesdroppers. This is well represented by Wyner's [3] wiretap channel model, in which there is a transmitter (Alice) sending confidential information to a legitimate receiver (Bob), in the presence of an eavesdropper (Eve). Since then, Wyner's wiretap channel has been extended to a variety of channels, such as broadcast channels with confidential messages [4] proposed by Csiszar and Korner, the Gaussian wiretap channel [5], and fading wiretap channels [6–8].

2.3 Coding Schemes Combined with Physical Layer Security

Error correction codes play an extremely important role in building real-world secure communication systems. The most popular types of error correction codes are LDPC codes, turbo codes and polar codes, which have all been considered with physical layer security.

2.3.1 LDPC Coding Scheme Combined with Physical Layer Security

Robert Gallager proposed LDPC codes in his doctoral thesis in 1960 and then published in [9]. However, LDPC codes were overlooked for a long period due to the computational limitation of hardware and the development of Reed-Solomon (RS) codes at that time. In 1996, David Mackay rediscovered LDPC codes and showed they can achieve near Shannon limit performance [10].

With good error correction performance, LDPC codes have been combined with physical layer security techniques to ensure secure communication. Thangaraj et al. [11] applied LDPC codes on a binary erasure wiretap channel system, where the main channel is noiseless, and proved that both reliability and Wyner's weak secrecy criterion could be satisfied simultaneously. LDPC codes and multi-level coding for the information reconciliation phase of a practical secret key agreement protocol was proposed by Bloch et al. in [12]. For Gaussian wiretap channels, in [13], the

authors proved that a 'security gap' was achievable by employing punctured LDPC codes and showed that their proposed coding scheme can be used in linear time and can be effectively applied to practical, finite-block length systems. The security gap was first introduced in [5] and is defined as the quality ratio between Bob's and Eve's channels that is required to achieve a sufficient level of physical layer security, while ensuring that Bob reliably receives the transmitted information. Taieb and Chouinard [14] applied rate compatible Low-density Parity-Check (RC-LDPC) channel coding with a Hybrid Automatic Repeat Request (HARQ) protocol using a feedback channel to ensure reliable and secure transmission between Alice and Bob and by increasing errors to prevent eavesdroppers obtaining information from Alice. Simulation results showed that by using the proposed RC-LDPC with HARQ secure coding scheme, secure transmission for the main channel can be achieved even when the main channel conditions are degraded compared to the wiretap channel.

2.3.2 Turbo Coding Scheme Combined with Physical Layer Security

Turbo codes invented in 1993 have raised great interest in the coding community due becoming the first practical codes to approach the channel capacity. In [15], adaptive secure channel coding based on punctured turbo codes was proposed to achieve reliability and security by applying the pseudo-random puncturing strategy to the eligible noisy channel. A secure turbo coding scheme based on random-puncturing was proposed in [16], with the puncturing pattern which is kept secret from the eavesdropper high equivocation-rates can achieve.

2.3.3 Polar Coding Scheme Combined with Physical Layer Security

2.3.3.1 Polar Codes

After more than half a century of unremitting research, a new generation of encoding and decoding schemes such as turbo codes and LDPC codes achieved a performance very close to the Shannon limit. However, no matter how close its performance is to the Shannon limitation, it never achieves it. For example, at present, the best known LDPC code has a theoretical performance distance of 0.0045 dB when the

block length is extremely long. Moreover, both turbo codes and LDPC codes have a certain randomness in construction, due to the interleaver construction of the turbo code and the design of the LDPC code node distribution, so that it is necessary to design a coding scheme according to the design parameters. This random configuration makes it difficult to achieve the theoretical optimal performance of the code with finite code length; on the other hand, the complexity is also quite high when constructing a finite code length turbo code or LDPC code with better performance using a searching method.

The concept of channel polarization was first proposed by Erdal Arikan in 2008 at the International Symposium on Information Theory (ISIT) Conference [17]. In 2009, [18] was published, in which channel polarization was elaborated in more detail, and a new encoding method named polar code was presented. Polar codes have a deterministic construction method and are the only known channel coding method that can be proven to achieve the channel capacity, and also have much lower encoding and decoding complexity.

When discussing channel polarization, Arikan assumes the binary discrete memoryless channel (B-DMC) W. However, the applicable range of the Bhattacharyya parameter $Z(W)$ which is mainly used to measure the reliability of channel, needs to be calculated when constructing the polar code on the binary erase channel (BEC). Therefore, this method could only be applied on the BEC. Then a heuristic method in [19] was proposed by considering other channels as an equivalent BEC with the same channel capacity. Mori et al. [20] proposed a construction method named density evolution (DE) which is applicable to all types of B-DMC. Due to the high complexity of DE, a simplification of the DE algorithm called Gaussian Approximation (GA) [21] for a Gaussian channel was proposed, where the probability density function (pdf) of the log-likelihood ratio (LLR) in the DE algorithm can be approximated by a Gaussian distribution, which can greatly reduce the computational complexity. Arikan proved polar codes can achieve the symmetric capacity of the binary-input discrete memoryless channels (B-DMCs) under a successive cancellation (SC) decoder. The SC decoder is a basic decoding algorithm for polar codes, which can decode bit-by-bit based on a recursive function in the butterfly diagram with low complexity. However, the finite-length performance of polar codes under SC is not competitive. Belief propagation (BP) was employed in [19] to evaluate the performance of polar codes compared with Arikan's rule and Reed-Muller (RM)

rule and was shown to have a significant improvement over SC, but its performance was still worse than the optimal maximum likelihood (ML) decoder. Later, successive cancellation list (SCL) [22], [23] decoding and successive cancellation stack (SCS) [24] decoding were proposed to achieve performance approaching the ML decoder with an acceptable complexity. Recently, cyclic redundancy check (CRC) concatenated polar codes with SCL decoding [22] and CRC-aided SCL/SCS (CA-SCL/SCS) decoders [25] showed polar codes outperforming the previous channel codes.

Compared with LDPC codes and turbo codes, polar codes have low complexity encoding and decoding algorithms, and have been proven to be capacity-achieving codes for the Binary Symmetric Channel (BSC), and extended to arbitrary binary-input discrete memoryless channels (DMCs) [18], [26]. These characteristics have made polar codes very popular and they have been studied extensively for a communication system employing physical layer security [26–30]. In 2010, Hof and Shamai [30] considered the use of secrecy polar codes for the binary-input memoryless symmetric and degraded wire-tap channel. This coding scheme was shown to achieve the secrecy capacity and the entire rate-equivocation region. Meanwhile, Mahdavifar and Vardy presented the construction from the strong security condition and weak security condition [31]. The polar coding scheme proposed by Mahdavifar and Vardy [31] divided the polarized channels into different parts to transmit information bits with bit-channels good for Bob but bad for Eve, random bits on bit-channels good for both Bob and Eve and zeros on the remaining bit-channels. This method can achieve the secrecy capacity but with a trade-off in secrecy rate. In this scheme, the polar codeword is split into three parts: information bits, random bits and frozen bits. The secrecy rate is defined as the message length divided by the codeword length, but this was very low due to large number of random bits required. Ideally we would like the secrecy rate to be equal to the code rate of a conventional polar code. Huiqing et al. [32] improved the secrecy rate by adding artificial noise, but this still could not increase the secrecy rate to 0.5 or higher. Recently, Liang et al [33] obtained a secrecy rate equal to 0.5 by using secure polar coding scheme with aided Automatic Repeat Request (ARQ), in which the frozen bits are obtained from the feedback of the legitimate receiver, for the wiretap channel system.

In addition, [34–40] focued on the design of secure polar coding schemes to achieve secrecy, where strong security is studied in [34,36,39,40], key agreement and

key generation were proposed in [35, 36, 40, 41], and other channel models that are different from discrete memoryless wiretap channel are considered in [38], [40] and [42]. Polar coding schemes for fading wiretap channels in multiple-antenna systems were first studied in [40], and results showed that the proposed scheme can provide both reliable and secure communication with low encoding and decoding complexity. A polar coding scheme for fading wiretap channels that achieves both reliability and security without the knowledge of instantaneous channel state information at the transmitter is proposed in [43]. Unlike the previous approaches using 1-D polar coding, a 2-D polar coding over block fading wiretap channels to achieve secrecy transmission is presented in [44].

2.3.3.2 Punctured Polar Codes

As proved by Ankan [18], polar codes can achieve channel capacity by using a SC decoder, however there is a constraint that the code length is limited to $N = 2^n, n = 1, 2, \cdots$. By adding or deleting information bit channels we can achieve various code rates, but the code length N is still limited to a power of two, which reduces the practical application of polar codes. As discussed in [45–47] puncturing is an effective method to design rate-compatible codes. Hence in order to create arbitrary code lengths, a method that punctured some coded bits to obtain rate-compatible punctured polar codes was first proposed in [48]. In that paper, the performance of random puncturing of polar codes is investigated and puncturing is also used for polar codes to improve the performance. Indeed, the results achieve good performance using the stopping-tree puncturing method with the BP decoding algorithm, but it is not as optimal as other decoding algorithms, such as SC [18], SCL [22], [23] and SCS [24] decoders. In [49], a universal coding scheme for rate-compatible punctured polar (RCPP) codes was proposed. According to the CRC concatenated polar encoder and CRC-aided SCL/SCS (CA-SCL/SCS) decoders, practical RCPP codes are generated which can satisfy both different block lengths and different code rates without changing their basic structure. Their simulation results proved the RCPP codes have the same performance or even better performance than turbo codes of the same code length on the binary input additive white Gaussian noise (BI-AWGN) channel. In [1], a novel puncturing scheme for polar codes was provided where the shortening pattern was given by the last bits of the mother polar code, and it

showed better performance than conventional punctured polar codes [49], [50]. Normally there is no a priori information fed to the decoder about the punctured bits and the initial corresponding log-likelihood ratios (LLRs) are set to zero. In terms of the conventional polar code, both the encoder and decoder have the same knowledge of the frozen bits. However, in that paper, the authors proposed a method that obtained the punctured bits only from the frozen bits. In that case their values can be known to the decoder and the initialized LLRs of the punctured bits are set to infinity.

Although previous methods can achieve any code length with polar codes, the complexity is high due to the DE algorithm which is used to find the puncturing [49] or shortening [1] set. In terms of attractiveness for hardware implementation, alternative approaches were proposed in [51–54].

As discussed, punctured or shortened polar codes can be designed with arbitrary code rates without the limitation of the code length being equal to a power of two. Based on this advantage a physical layer secrecy coding scheme based on punctured polar codes under Gaussian wiretap channel is proposed in [55], where the punctured position is calculated by the reliability of the coded-bit. This proposed coding scheme can reduces the security gap efficiently.

As shown in the literature, polar codes show good performance to achieve both weak and strong security, as well as reduce the security gap. However, there is still scope to design secure polar codes for physical layer security systems in the presence of no-Gaussian noise.

2.4 Error-correcting Codes in the Presence of Impulsive Noise

In conventional communication systems, noise is usually modelled as additive white Gaussian noise (AWGN). Noise that has a non-Gaussian distribution is called impulsive noise and plays an important role in modern communication systems. It occurs in wireless networks [56], [57], as well as in power line communications, underwater and molecular communication systems, multiple access interference (MAI) in ultra-wideband systems and electromagnetic interference (EMI) [58–63].

A main characteristic of impulsive noise is the heavier tails of the noise probabil-

ity density function causing a higher probability of large amplitude noise, which will severely degrade the communication system. Therefore several statistical-physical models, such as the Gaussian mixture model (GMM), Middleton Class A model and symmetric alpha stable (SαS) distributions [63–65], have been proposed to describe the behavior of impulsive noise.

2.4.1 LDPC Codes in the Presence of Impulsive Noise

Power line communication suffers from impulsive interference. Therefore, LDPC codes were applied to mitigate the noise. LDPC codes with a sum-product decoder for additive white class A noise (AWAN) channels was proposed in [66]. In [67], impulsive noise effects on the power line channel (PLC) with quasicyclic Low-density Parity-check (QC-LDPC) codes as the outer coding scheme was proposed. In addition, a practical noise model on an orthogonal frequency-division multiplexing (OFDM) power line communications system was investigated. Recently, the class of SαS distributions was shown to be an accurate model for impulsive noise, thus the performance of polar codes were investigated in the presence of SαS noise [68–71]. In [68] the theoretical performance of communication channels with SαS noise was derived. In order to reduce the complexity, the authors investigated a sub-optimal receiver for the LDPC-coded channels with SαS noise. Then a analysis of the theoretical bit error probability (BEP) of M-ary quadrature amplitude modulation on Rayleigh fading channels modelled by alpha stable distribution was analysed by [69]. LDPC codes with extremely long block lengths are well known for their powerful error correction, but it is not always applicable in communication systems, thus [70] analysed the performance of finite length LDPC codes on impulsive noise channels. Finally, in [71] LDPC codes with different linear combining techniques on Rayleigh fading channels with SαS impulsive noise were examined.

2.4.2 Turbo Codes in the Presence of Impulsive Noise

Middleton's class A noise model is frequently utilized for the modeling of impulsive noise environments, and a turbo decoding algorithm was proposed for an additive white class A noise (AWAN) channel [72]. As we know, non-binary codes are more effective in correcting burst errors, thus the coding scheme of non-binary turbo codes on additive impulsive noise channels was first proposed in [73]. After that,

the authors [74] applied non-binary turbo codes on OFDM-PLC system which are modelled by impulsive noise.

2.4.3 Polar Codes in the Presence of Impulsive Noise

Recently, polar codes have been adopted for impulsive noise channels due to them being the first proven capacity achieving codes for a wide range of channels with low encoding and decoding complexity. The bit error rate (BER) performance of polar codes with SC decoding over the impulsive noise channel modeled by Middleton's Class A noise was analysed in [75]. Later, to reduce the effect of impulsive noise, polar codes with different codeword lengths and noise scenarios in OFDM systems were investigated in [76]. In this paper,simulation results showed that polar codes achieved better performance on PLC systems than LDPC codes. In addition, the performance of polar codes constructed by DE on impulsive noise channels for single-carrier and multi-carrier systems were proposed and evaluated [77]. However, there seem to be no publications that have examined the performance of polar codes on impulsive noise channels with SαS distributions. In this thesis, we will focus on the noise with SαS distribution and investigate polar-coded performance and polar code combined with physical layer security in the presence of SαS noise.

2.5 Conclusion

In conventional communication systems, noise is normally modeled using a Gaussian distribution. However, in some scenarios, the system has a non-Gaussian distribution which contains a significant interference component, such as impulsive noise. In addition, for the communication security problem, different coding scheme have been proposed to achieve secrecy capacity, reduce the security gap and increase the secrecy code rate at the same time to ensure illegal receivers cannot extract any useful information. Compared with LDPC codes and turbo codes, polar codes are the first proven capacity-achieving codes on B-DMCs, and also have much lower encoding and decoding complexity. To the best of our knowledge, the security performance of polar codes is only investigated on the BEC, BSC and BI-AWGN channel, but not impulsive noise channels. Finally, to construct rate-compatible punctured polar codes, puncturing methods are investigated for Gaussian wiretap channel system in

the literature. Therefore, based on the literature, we will investigate polar coded physical layer security on impulsive noise channels and assess if security can still be achieved.

Chapter 3

Theoretical Background

In this chapter, the background theory on symmetric alpha-stable (SαS) noise is first explained. Second, different types of wiretap channel models which are an important part of physical layer security are reviewed. Finally, the chapter concludes with detailed explanations on polar codes, which includes channel polarization, the construction of polar codes by a heuristic method, GA method and DE method, and performance of polar codes with SC and SCL decoding on AWGN channel with different code lengths. These are the essential theoretical background information for the novel work presented in chapters four, five and six.

3.1 Symmetric Alpha-stable (SαS) Distribution

There are several well known methods for modeling impulsive noise, including the Gaussian mixture model (GMM), Middleton Class A model and α-stable model. In this chapter we describe SαS distributions which are widely used to generate impulsive noise. With the advantages of flexibility and accuracy over other models, the α-stable distribution is applied in many areas, such as, signal processing, underwater acoustic communications and power line communications [78,79]. The characteristic function of α-stable distributions is given as

$$\varphi(t) = \exp\left\{j\delta t - \mid \gamma t \mid^{\alpha} (1 - j\beta \text{sign}(t)\omega(t,\alpha))\right\}, \tag{3.1}$$

where

$$\omega(t,\alpha) = \begin{cases} \tan(\pi\alpha/2), & \alpha \neq 1, \\ -2/\pi \log|t|, & \alpha = 1. \end{cases}$$

The alpha-stable distribution $S(\alpha, \beta, \gamma, \delta)$ has four parameters, α, β, γ and δ. The characteristic exponent α ($\alpha \in (0, 2]$) represents the tail-heaviness of the pdf. When $\alpha = 2$, the pdf is Gaussian and when α decreases, the noise becomes more impulsive. The skewness is denoted by β, the dispersion is denoted by γ^α, which is a measure of the spread of the noise and the location parameter is denoted as δ [65]. The alpha-stable distribution is called symmetric if β is 0. Then the characteristic function is

$$\varphi(t) = \exp\left(j\delta t - \gamma^\alpha \mid t \mid^\alpha\right). \tag{3.2}$$

By performing the inverse Fourier transform (IFT) of the characteristic function we can obtain the pdf of a SαS random variable, $x \sim S(\alpha, 0, 0, \gamma)$ is

$$f_\alpha(x; \delta, \gamma) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp(-\gamma^\alpha |t|^\alpha) e^{-jtx} dt. \tag{3.3}$$

There are two special SαS distributions that have closed form expressions. When $\alpha = 1$, the noise is Cauchy and the pdf is given as

$$f_1(x; \delta, \gamma) = \frac{1}{\pi} \frac{\gamma}{\gamma^2 + (x - \delta)^2}, \tag{3.4}$$

when $\alpha = 2$, the distribution is Gaussian and the standard pdf is

$$f_2(x; \delta, \gamma) = \frac{1}{2\sqrt{\pi}\gamma} \exp\left[-\frac{(x - \delta)^2}{4\gamma^2}\right]. \tag{3.5}$$

For $\alpha = 2$, the noise is Gaussian and has a finite variance σ^2 defined as $\sigma^2 = 2\gamma^2$. As α decreases, the tail of the pdf becomes thicker and can be observed in Fig. 3.1, which shows the pdf of standard SαS distributions with different α.

Since almost all SαS distributions have infinite variance, the conventional definition of the signal-to-noise ratio (SNR) based on second-order statistics is no longer applicable. Therefore, we use the geometric SNR (SNR_K) instead [80]. The geometric power N_0 is defined as

$$N_0 = \frac{(C_k)^{1/\alpha}\gamma}{C_k}, \tag{3.6}$$

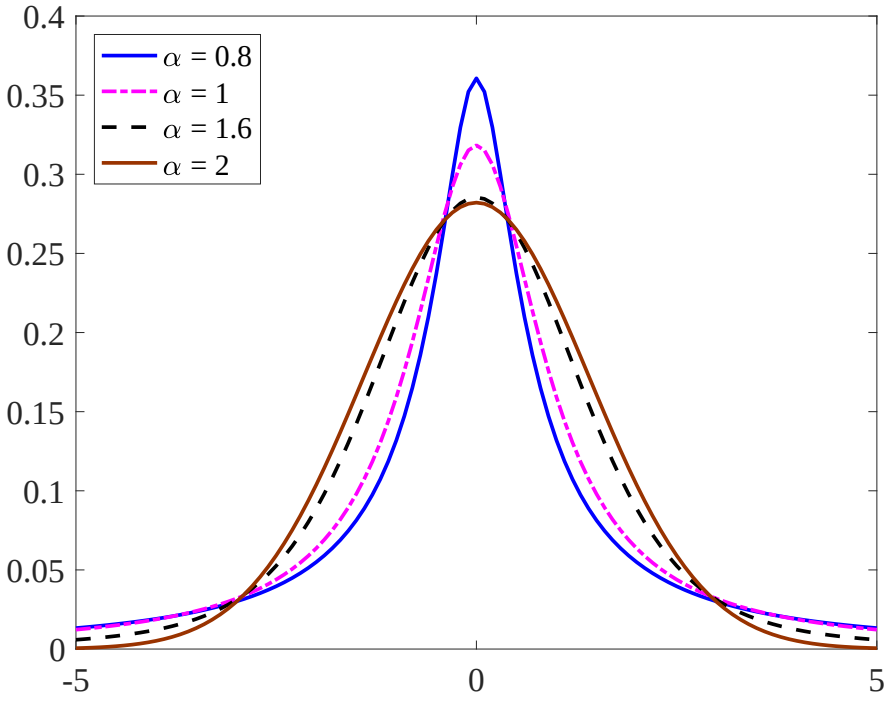

Figure 3.1: Standard SαS distributions($\gamma = 1, \delta = 0$).

where C_k is the exponent of the Euler constant and $C_k \approx 1.78$. $\mathrm{SNR_K}$ is defined as

$$\mathrm{SNR_K} = \frac{1}{2C_k}\left(\frac{B}{N_0}\right)^2, \tag{3.7}$$

where B^2 is the transmitted energy of the modulated signal and the constant $\frac{1}{2C_k}$ ensures $\mathrm{SNR_K}$ remains valid when the noise is Gaussian (i.e. when $\alpha = 2$). In this thesis we set $B = 1$ and $\frac{E_b}{N_0}$ for BPSK is given as

$$\frac{E_b}{N_0} = \frac{\mathrm{SNR_K}}{2R} = \frac{1}{4RC_k^{(\frac{2}{\alpha}-1)}\gamma^2}, \tag{3.8}$$

where R is the code rate.

Here we list several important properties of SαS distribution, which are explained in [65, 81].

Property 1. A random variable X is stable if and only if

$$a_1X_1 + a_2X_2 \overset{d}{=} aX + b, \tag{3.9}$$

where a_1, a_2, a and b are arbitrary constants and X_1 and X_2 are independent ran-

dom variables having the same distribution as X. $X \overset{d}{=} Y$ denotes that X and Y have the same distribution.

Property 2. The generalized central limit theorem shows that the sum of a number of SαS distributed random variables will tend to a stable distribution.

Property 3. For a SαS random variable v_α with dispersion γ, we have

$$\lim_{x\to\infty} P(v_\alpha > x) = \frac{\gamma^\alpha C_\alpha}{x^\alpha}, \tag{3.10}$$

where $C_\alpha = \frac{1}{\pi}\Gamma(\alpha)\sin\left(\frac{\pi\alpha}{2}\right)$.

Property 4. If $v_i \sim S(\alpha, 0, 0, \gamma_i)$, $i = 1, 2, \cdots, N$, then $\sum_{i=1}^{N} v_i \sim S(\alpha, 0, 0, \gamma)$, where $\gamma = \left(\sum_{i=1}^{N} \gamma_i^\alpha\right)^{\frac{1}{\alpha}}$.

Property 5. With a constant c, if $v \sim S(\alpha, 0, 0, \gamma)$, then $cv \sim S(\alpha, 0, 0, |c|\gamma)$.

Property 6. Any SαS random variable $v \sim S(\alpha, 0, 0, \gamma)$ can be classified as α-sub-Gaussian, which can be expressed as

$$Z = \sqrt{A}G, \tag{3.11}$$

where A and G are independent. $A \sim S(\alpha/2, 1, 0, [\cos(\pi\alpha/4)]^{2/\alpha})$ is a skewed α-stable random variable and $G \sim \mathcal{N}(0, 2\gamma^2)$ is a Gaussian random variable.

3.2 Physical Layer Security

To illustrate the general concept of physical layer security, a three-node wireless network system model is shown as an example in Fig. 3.2, where the communication between terminals T_1 and T_2 is being intercepted by an unauthorized receiver T_3. The communication channel between the legitimate users is called the main channel and the communication channel between T_1 and T_3 is the eavesdropper's channel.

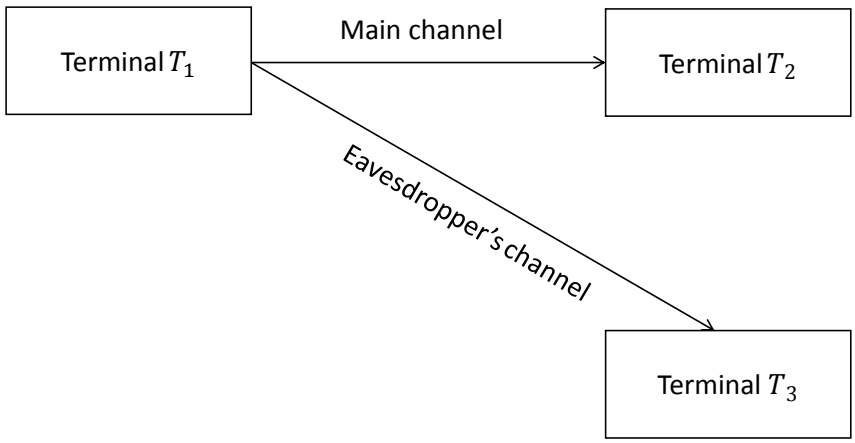

Figure 3.2: Eavesdropping in wireless communication.

3.2.1 Wiretap Channel Model

As a breakthrough in communications security, physical layer security achieves secure transmissions without the need of any form of pre-shared secret within the group of legitimate users. Security can be achieved through the physical layer, by only exploiting the difference between the channels of legitimate receivers and those of potential eavesdroppers. This is well represented by Wyner's [3] wiretap channel model, as shown in Fig.3.3. Wyner presented the wiretap channel [3] in 1975, in which there is a transmitter (Alice) sending confidential information to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). S^K denotes a K-bit message that Alice wishes to send to Bob. It is assumed that S is a uniformly distributed random variable that takes values in $\{0,1\}^K$. This sequence is transmitted across the main channel, which is modeled as a discrete memoryless channel and the wiretap channel resulting in the corresponding channel outputs Y^N and Z^N.Finally, the decoder maps Y^N and Z^N into estimate $\hat{S_B^K}$ and $\hat{S_E^K}$.

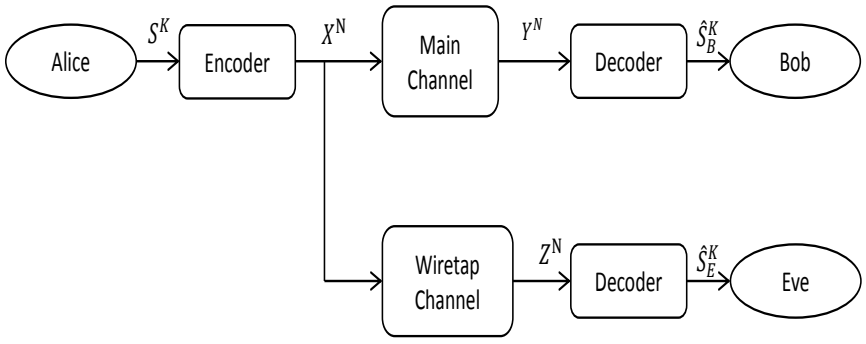

Figure 3.3: The wiretap channel of Wyner, where the eavesdropper's channel is degraded compared to the main channel.

3.2.2 Secure Coding Measurement

The purpose of designing a coding scheme with physical layer security is to ensure reliable and secure communication when the message length K tends to infinity. The error probability P_r for the original message U is a measurement of reliability, which is shown in (3.12)

$$\lim_{k\to\infty} P_r\left\{\hat{U} \neq U\right\} = 0. \tag{3.12}$$

Security is usually measured using the normalized mutual information $I(\boldsymbol{U};\boldsymbol{Z})$ between the original message $\boldsymbol{U}$ and the observations $\boldsymbol{Z}$ by the eavesdropper, which is a measurement of Eve's uncertainty and can be represented by:

$$\lim_{k\to\infty} I(\boldsymbol{U};\boldsymbol{Z}) = 0. \tag{3.13}$$

In Fig. 3.3, Wyner [3] assumes both the main channel C_M and wiretap channel C_W are DMCs, and C_W is less than C_M. He proved that this kind of system is characterized by a constant secrecy capacity C_s and there exists a coding scheme that achieves secrecy capacity. For the degraded wiretap channel [5] with additive Gaussian noise, secrecy capacity C_s is the difference between the Shannon capacity of the main channel C_M and wiretap channels C_W

$$C_s = C_M - C_W. \tag{3.14}$$

Furthermore, [4] studied the general wiretap channel and gave the definition of secrecy capacity as:

$$C_s = \max_U \left\{I(\boldsymbol{U};\boldsymbol{Y}) - I(\boldsymbol{U};\boldsymbol{Z}), 0\right\}. \tag{3.15}$$

Secrecy capacity of the classical wiretap channel model is shown in Fig. 3.4. It is the theoretical secrecy capacity for an infinite size constellation and mapping technologies are not involved with the capacity. Also, it is assumed the BER performances are optimal, using a Shannon limit code. Clearly, secrecy capacity is proportional to the difference in the signal to noise ratio between the main channel and the eavedropper's channel.

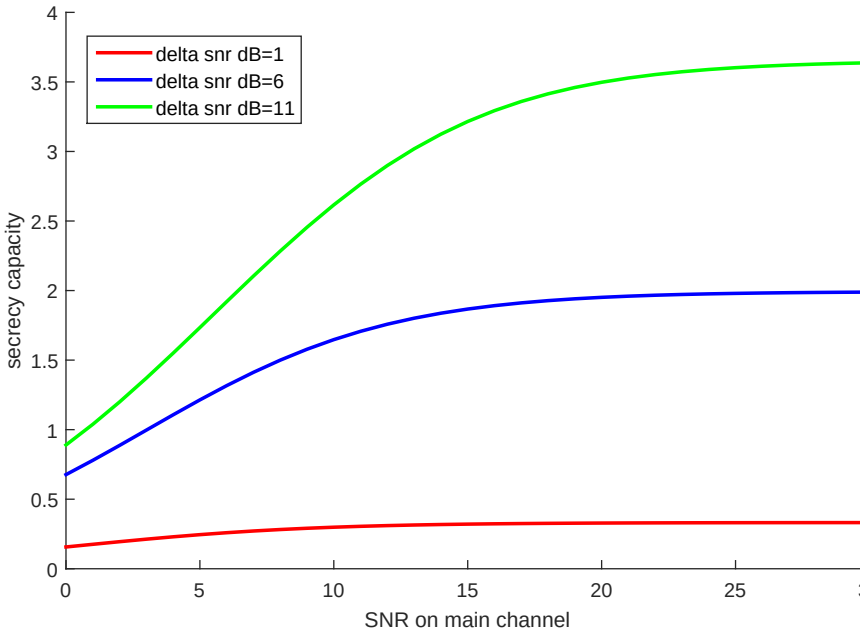

Figure 3.4: Secrecy capacity of classical wiretap channel model.

3.3 Polar Codes

Polar codes were proposed by Arikan [18] based on the novel concept named channel polarization [17] and have been proved to achieve channel capacity for any symmetric B-DMC. With their low encoding and decoding complexity, polar codes have excellent performance and have now been included in the 5G standard by 3GPP. In this section, we introduce the basic theoretical background, encoding and decoding algorithms of polar codes. Moreover, the performance of polar codes on AWGN is presented.

3.3.1 Overview

From the perspective of algebraic coding and probability, polar codes have their own characteristics. First, as long as the block length is given, the code structure of the polarization code is uniquely determined, and the coding process can be completed by generating a matrix, which is consistent with the common thinking of algebraic coding. Secondly, the polar code does not consider the minimum distance in the design, but uses the process of channel combination and channel splitting to select a specific coding scheme, and a probabilistic algorithm is also used in the decoding.

For a $N = 2^n, n = 1, 2, \ldots$ length polar codes, N independent channels W are used for channel combination and channel splitting to obtain N new polarized channels $\left\{W_N^{(1)}, W_N^{(2)}, \cdots, W_N^{(N)}\right\}$. As the code length N increases, the split channel will tend to two extremes: some of the split channels will approach a perfect channel, that is, a noiseless channel with a channel capacity approaching 1; the other part of the split channels will converge to nearly noisy channels, that is, the channel capacity approaches zero. Assuming that the binary input symmetric capacity of the original channel W is denoted as $I(W)$, when the code length N approaches infinity, the split channel ratio whose channel capacity approaches 1 is approximately $K = N \times I(W)$, and the ratio of channels' capacity approaching zero is approximately $N \times (1 - I(W))$. For a reliable bit channel with a channel capacity of 1, the information bits can be transmitted directly without any coding; and for an unreliable bit channel with a channel capacity of 0, a frozen bit can be placed which are known in advance to both the transmitting point and the receiving point. Then, when the code length $N \to \infty$, the reachable coding rate of a polar code is $R = N \times I(W)/N = I(W)$, that is, in theory, polar codes can be proved to achieve channel capacity.

In the process of polar code encoding, first we must distinguish the reliability of N split bit channels, ie, which belong to the reliable channel and which belong to the unreliable channel. There are three methods commonly used to measure the reliability of polarization channels: the Bhattacharyya Parameter method, the DE method, and the GA method.

- Initially, polar codes use the Bhattacharyya parameter $Z(W)$ as the reliability metric for each split channel, and the larger $Z(W)$ is the lower the reliability of the channel. When the channel W is a Binary Erasure Channel, each $Z(W_N^{(i)})$ can be calculated recursively with a complexity of $O(N \log N)$. However, for other channels, such as binary-input symmetric channel or binary-input Additive White Gaussian channel (BAWGNC), there is no accurate calculation method for $Z(W_N^{(i)})$.

- In order to estimate the error probability of each bit channel, Mori et al. proposed a method of using the density evolution to track each bit channel's probability density function (pdf). This method is applicable to any binary-input discrete memoryless channel.

- In most research scenarios, the channel coding model is the BAWGNC chan-

nel. Under the BAWGNC channel, the pdf of LLR in density evolution can be approximated by a Gaussian distribution with variance is two times the mean, which simplifies the calculation of the one-dimensional mean and greatly reduces the amount of calculation. This simplified calculation for DE is called Gaussian approximation.

3.3.2 Preliminaries

Polar codes were first proposed for an arbitrary B-DMC. A generic B-DMC can be wrote as $W : \mathcal{X} \to \mathcal{Y}$ includes input alphabet $\mathcal{X}$, output alphabet $\mathcal{Y}$, and transition probabilities $W(y|x)$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$. The input alphabet $\mathcal{X} = \{0, 1\}$, the output alphabet and the transition probabilities can be arbitrary. Here W^N is applied to denote the channel corresponding to N uses of W; thus, $W^N : \mathcal{X}^N \to \mathcal{Y}^N$ with $W^N\left(y_1^N|x_1^N\right) = \prod_{i=1}^N W\left(y_i|x_i\right)$.

Given a B-DMC W, there are two important channel parameters: the symmetric capacity

$$I\left(W\right) = \sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} \frac{1}{2} W\left(y|x\right) \log \frac{W\left(y|x\right)}{\frac{1}{2}W\left(y|0\right) + \frac{1}{2}W\left(y|1\right)}, \tag{3.16}$$

and the Bhattacharyya parameter

$$Z\left(W\right) = \sum_{y\in\mathcal{Y}} \sqrt{W\left(y|0\right) W\left(y|1\right)}. \tag{3.17}$$

$I\left(W\right)$ is used as measure of rate and is the highest rate at which reliable communication is possible across W when the inputs of W have equal probability. $Z\left(W\right)$ is an upper bound on the probability of the ML decision error when W is used only once to transmit a 0 or 1, which is the measurement of reliability.

The range of $I(W)$ and $Z(W)$ is $[0, 1]$. Since the logarithm is base 2, the unit of code rate and channel capacity is 'bit'. $I(W)$ and $Z(W)$ satisfy such a relationship: $I(W) \approx 1$ iff $Z(W) \approx 0$, and $I(W) \approx 0$ iff $Z(W) \approx 1$.

Proposition 1 [18]:

$$I\left(W\right) \geq \log \frac{2}{1 + Z\left(W\right)}, \tag{3.18}$$

$$I(W) \leq \sqrt{1 - Z(W)^2}. \tag{3.19}$$

3.3.3 Channel Polarization

The process of channel polarization consists of channel combining and channel splitting. N mutually independent B-DMC channels are combined into W_N by a linear transformation, and then W_N is split into certain correlation channel $\left\{W_N^{(i)}, 1 \leqslant i \leqslant N\right\}$, which are the concrete realization process of channel polarization.

3.3.3.1 Channel Combining

At this stage, after combining with N independent copies of B-DMC W, a vector channel $W_N : \mathcal{X}^N \to \mathcal{Y}^N$ is generated recursively, where N is a power of 2 $N = 2^n, n \geq 0$. During this process the total channel capacity is constant. The detailed process of channel combing is shown in Fig. 3.5 and obtains the channel W_N with the transition probabilities

$$W_N\left(\mathbf{y}_1^N|\mathbf{u}_1^N\right) = W^N\left(\mathbf{y}_1^N|\mathbf{u}_1^N\mathbf{G}_N\right), \tag{3.20}$$

where $\mathbf{G}_N$ is the generator matrix of polar codes, $\mathbf{u}_1^N$ is a vector of all output variables, $\mathbf{x}_1^N = \mathbf{u}_1^N\mathbf{G}_N$.

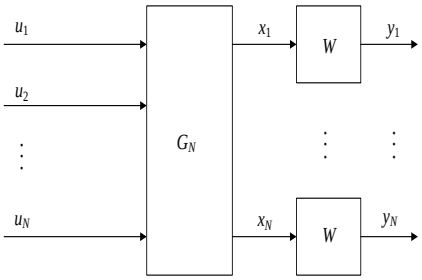

Figure 3.5: The channel combining and splitting.

A recursive manner starts at level 0 (n=0), using only 1 copy of W and defining $W_1 \triangleq W$. Level 1 (n=1) recursively combines two independent copies of W. As shown in Fig. 3.6, the vector channel $W_2 : \mathcal{X}^2 \to \mathcal{Y}^2$ is produced, and the transition

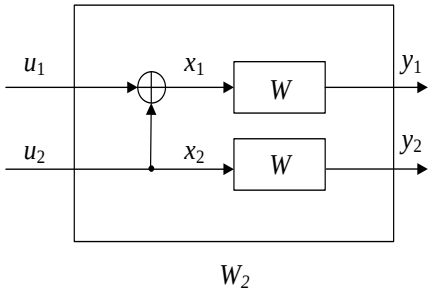

Figure 3.6: The channel W_2.

probability is

$$\begin{aligned} W_2\left(y_1, y_2 | u_1, u_2\right) &= W\left(y_1 | u_1 \oplus u_2\right) W\left(y_2 | u_2\right) \\ &= W^2\left(\left[y_1, y_2\right] | \left[u_1 \oplus u_2, u_2\right]\right) \\ &= W^2\left(y_1^2 | u_1 G_2\right). \end{aligned} \tag{3.21}$$

In Fig. 3.6, the input variable $\mathbf{u}_1^2$ of channel W_2 maps to the input variable $\mathbf{x}_1^2$ of channel W^2 can be represent as:

$$\left[\mathbf{x}_1, \mathbf{x}_2\right] = \left[\mathbf{u}_1, \mathbf{u}_2\right] \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \left[\mathbf{u}_1, \mathbf{u}_2\right] \mathbf{G}_2, \tag{3.22}$$

where $\mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

The second level ($n = 2$) of the recursion combines two independent copies of W_2 as shown in Fig. 3.7 and obtains the channel $W_4 : \mathcal{X}^4 \to \mathcal{Y}^4$ with the transition probabilities:

$$\begin{aligned} W_4\left(y_1^4 | u_1^4\right) &= W_2\left(y_1^2 | u_1 \oplus u_2, u_3 \oplus u_4\right) W_2\left(y_3^4 | u_2, u_4\right) \\ &= W\left(y_1 | u_1 \oplus u_2, u_3 \oplus u_4\right) W\left(y_2 | u_3 \oplus u_4\right) W\left(y_4 | u_4\right) \\ &= W_4\left(y_1^4 | u_1 G_4\right). \end{aligned} \tag{3.23}$$

The operator R_4 in Fig. 3.7 is a permutation, known as the reverse shuffle operation, which maps (s_1, s_2, s_3, s_4) into $v_1^4 = (s_1, s_3, s_2, s_4)$.The input variable $\mathbf{u}_1^4$ of channel W_4 maps to the input variable $\mathbf{x}_1^4$ of channel W^4 and can be represented

as:

$$[\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4] = [\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4] \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} = [\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4]\, \mathbf{G}_4, \tag{3.24}$$

where $\mathbf{G}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$.

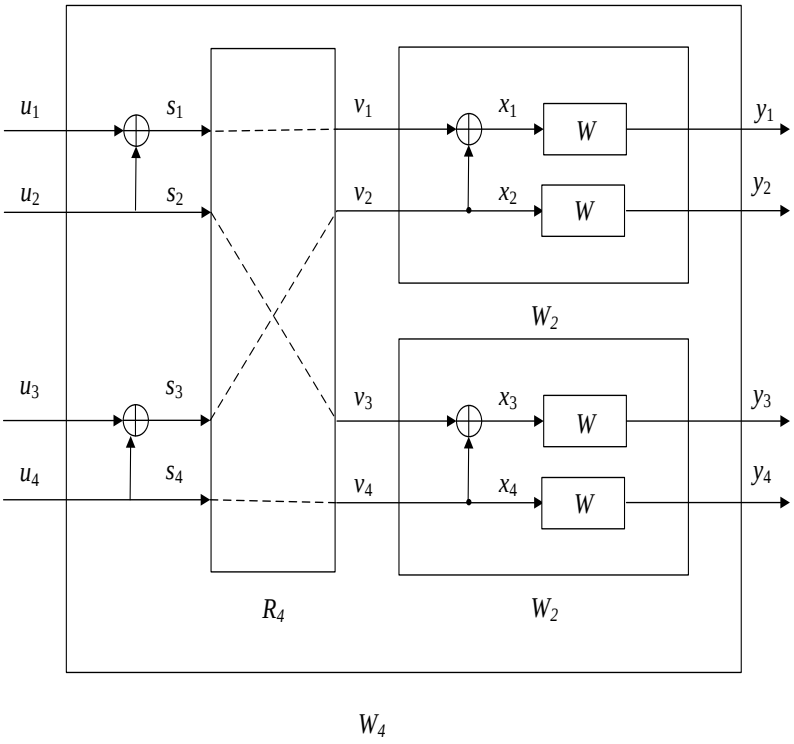

Figure 3.7: The channel W_4 and its relation to W_2 and W.

The general form of the recursion is shown in Fig. 3.8 where two independent copies of $W_{N/2}$ are combined to generate the channel $W_N : \mathcal{X}^N \to \mathcal{Y}^N$. The input vector u_1^N to W_N is first transformed into s_1^N so that $s_{2i-1} = u_{2i-1} \oplus u_{2i}$ and $s_{2i} = u_{2i}$ for $1 \leqslant i \leqslant N/2$. The operator R_N in Fig. 3.8 is a permutation, known as the reverse shuffle operation, and acts on its input s_1^N to produce $v_1^N = (s_1, s_3, \cdots s_{N-1}, s_2, s_4, \cdots s_N)$, which becomes the input to the two copies of $W_{N/2}$ as shown in the Fig. 3.8.

Finally, it can be inferred that for any polar code with a code length of N, $(N = 2^n, n \geq 0)$, the generator matrix $\mathbf{G}_N = \mathbf{B}_N \mathbf{F}_2^{\otimes n}$, $\mathbf{B}_N$ is the bit-reversal permutation matrix, which acts as an exchange of the following matrix. For example when $N = 8$, then the row numbers of $\mathbf{F}_2^{\otimes 3}$ are $(0, 1, 2, 3, 4, 5, 6, 7)$, the corresponding binary representation is $(000, 001, 010, 011, 100, 101, 110, 111)$ and after the bit inversion conversion is $(000, 100, 010, 110, 001, 101, 011, 111)$, the corresponding decimal representation is $(0, 4, 2, 6, 1, 3, 5, 7)$. $\mathbf{F}_2^{\otimes n}$ is the n-th Kronecker power of $\mathbf{F}_2$ and $\mathbf{F}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, $\mathbf{F}_2^{\otimes 2} = \begin{bmatrix} \mathbf{F} & 0 \\ \mathbf{F} & \mathbf{F} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$, $\mathbf{F}_2^{\otimes n} = \begin{bmatrix} \mathbf{F}_2^{\otimes n-1} & 0 \\ \mathbf{F}_2^{\otimes n-1} & \mathbf{F}_2^{\otimes n-1} \end{bmatrix}$.

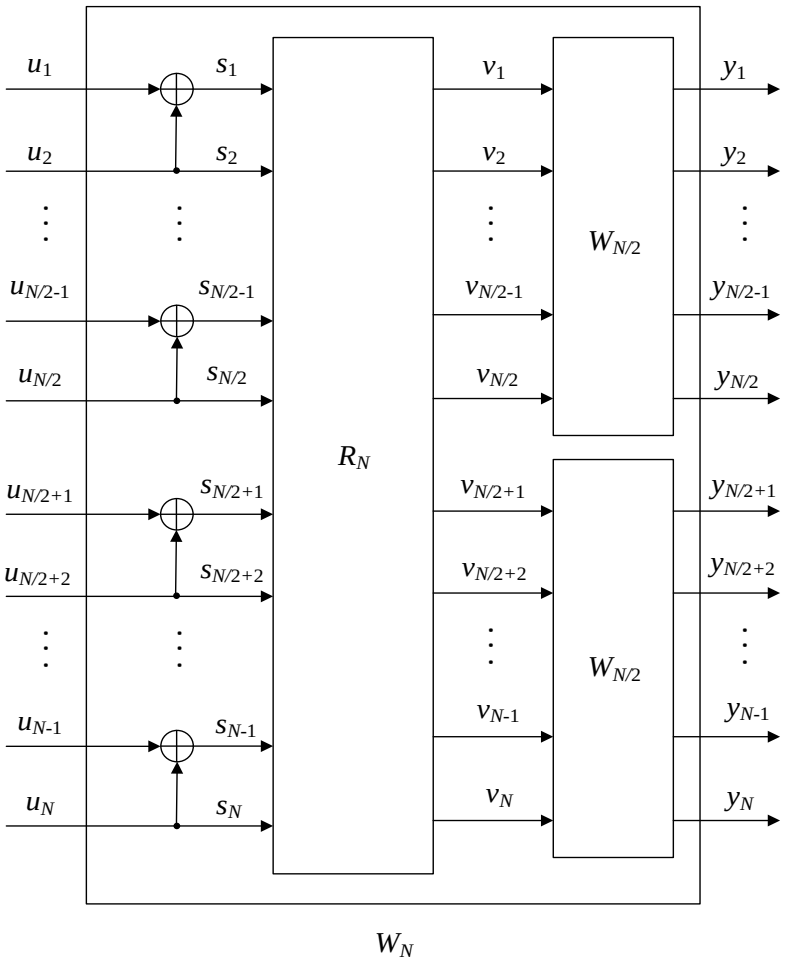

Figure 3.8: Construction of W_N from two copies of $W_{N/2}$.

3.3.3.2 Channel Splitting

This is the second phase of channel polarization. The composite channel W_N formed by combining the channels is split into N binary input coordinate channels W_N^i

$W_N^i : \mathcal{X} \to \mathcal{Y}^N \times \mathcal{X}^{i-1}, 1 \le i \le N$, and the transition probability is defined as

$$W_N^i \left(y_1^N, u_1^{i-1} | u_i\right) \triangleq \sum_{u_{i+1}^N \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N \left(y_1^N | u_1^N\right), \tag{3.25}$$

where $\left(y_1^N, u_1^{i-1}\right)$ denotes the output of $W_N^{(i)}$ and u_i its input. The transition probabilities of the odd-sequence splitbit channel and the even-order split bit channel are obtained by two recursive equations. For any $n \ge 0, N = 2n, 1 \le i \le N$, there is [18]

$$W_{2N}^{(2i-1)} \left(y_1^{2N}, u_1^{2i-2} | u_{2i-1}\right) = \sum_{u_{2i}} \frac{1}{2} W_N^{(i)} \left(y_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i}\right) \cdot W_N^{(i)} \left(y_{N+1}^{2N}, u_{1,e}^{2i-2} | u_{2i}\right), \tag{3.26}$$

$$W_{2N}^{(2i)} \left(y_1^{2N}, u_1^{2i-1} | u_{2i}\right) = \frac{1}{2} W_N^{(i)} \left(y_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i}\right) \cdot W_N^{(i)} \left(y_{N+1}^{2N}, u_{1,e}^{2i-2} | u_{2i}\right). \tag{3.27}$$

3.3.3.3 Channel Polarization

Here we list two important theorems of channel polarization, which are proposed in [18].

Theorem 1: For any B-DMC W, the channels $W_N^{(i)}$ polarize in the sense that, for any fixed $\delta \in (0, 1)$, as N goes to infinity through powers of two, the fraction of indices $i \in \{i, \cdots, N\}$ for which $I(W_N^{(i)}) \in (1 - \delta, 1]$ goes to $I(W)$ and the fraction for which $I(W_N^{(i)}) \in [0, \delta)$ goes to $1 - I(W)$.

We assume W is a BEC with erasure probability $\epsilon = 0.5$ to show the polarization effect in Fig. 3.9. The numbers of $I(W_N^{(i)})$ have been calculated by the following recursive relations with $I(W_1^{(1)}) = 1 - \epsilon$.

$$\begin{aligned} I(W_N^{(2i-1)}) &= I(W_{N/2}^{(i)}), \\ I(W_N^{(2i)}) &= 2I(W_{N/2}^{(i)}) - I(W_{N/2}^{(i)})^2. \end{aligned} \tag{3.28}$$

Fig. 3.9 shows that $I(W^{(i)})$ approaches to for small i and near 1 for large i.

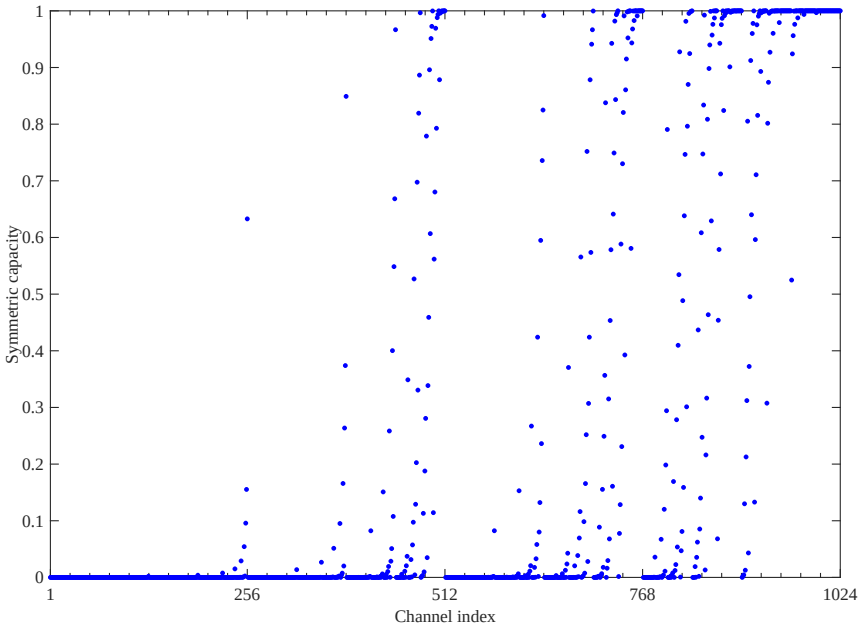

Figure 3.9: Plot of $I(W_N^{(i)})$, where $i = 1, \cdots, N = 2^1 1$ for a BEC with $\epsilon = 0.5$.

Theorem 2: For any B-DMC W with $I(W) > 0$, and any fixed $R < I(W)$, there exists a sequence of sets $\mathcal{A}_N \subset \{1, \cdots, N\}, N \in \{1, 2, \cdots, 2^N, \cdots\}$, such that $\mathcal{A}_N \geq NR$ and $Z\left(W_N^{(i)}\right) \leq O\left(N^{-5/4}\right)$ for all $i \in \mathcal{A}_N$.

3.3.4 Codes Construction

In the construction of a polar code, the probability of error during channel transmission is more normally applied, that is, the unreliable $Z(W)$ of the channel W described in (3.17). The larger the $Z(W)$, the worse the reliability of the channel. After channel polarization is performed on N arbitrary B-DMC channels W to obtain a polarized channel W_N^i $(i = 1, 2, \cdots, N)$. Let event A_i denote "the information bits transmitted by the i-th polarized channel W_N^i are erroneous at the receive end", that is

$$A_i = u_1^N, y_1^N : W_N^i(y_1^N, u_1^{i-1}|u_i) < W_N^i(y_1^N, u_1^{i-1}|u_i \oplus 1). \tag{3.29}$$

Let $P(A_i)$ denote the error probability of the polarized channel W_N^i. Next we will explain the polar method used for constructing polar codes: Bhattacharyya parameter method, DE and GA.

3.3.4.1 Bhattacharyya Parameter Method

$Z(W)$ is an upper bound when channel W uses maximum-liklihood (ML) to decide the error probability, and is mainly used to measure the reliability of channel W. When discussing the channel polarization, Arikan focuses on the binary discrete memoryless channel (B-DMC). However, the applicable range of the Bhattacharyya parameter $Z(W)$ that needs to be calculated when constructing the polar code is the binary erase channel (BEC). BEC is a subset of B-DMC. Therefore, this method can only be applied on the BEC.

Proposition 2: Assume $(W, W) \leftrightarrow (W', W'')$ for any binary-input channels. Then

$$Z(W'') = Z(W)^2, \tag{3.30}$$

$$Z(W') \leq 2Z(W) - Z(W)^2, \tag{3.31}$$

$$Z(W') \geq Z(W) \geq Z(W'). \tag{3.32}$$

If the channel W is BEC, the (3.31) is an equality.

When $N = 2^n$, the parameters $Z(W_N^{(i)})$ can be computed through the recursion (3.30) and (3.31):

$$Z(W_N^{(2i-1)}) \leqslant 2Z(W_N^{(i)}) - Z(W_N^{(i)})^2, \tag{3.33}$$

$$Z(W_{2N}^{(2i)}) = Z(W_N^{(i)})^2. \tag{3.34}$$

If the channel W is BEC, (3.33) is an equality. For the special case that W is a BEC with an erasure probability ϵ the error probability of each polarized bit channel W_N^i is

$$P(A_i) = 0.5Z(W_N^{(i)}). \tag{3.35}$$

Since the Bhattacharyya parameter can only be exactly calculated under the BEC, Arikan proposed a heuristic method in [19] by considering other channels as an equivalent BEC with the same channel capacity.

3.3.4.2 Density Evolution

When the channel is not a BEC channel, such as a BSC or a BAWGNC, it is beyond the applicable range of $Z(W)$, and $Z\left(W_N^{(i)}\right)$ of each split bit channel cannot be accurately obtained. In order to more accurately estimate the reliability of each split bit channel in channel polarization, Mori et al. [20] proposed a construction method named DE. This method is applicable to all types of B-DMC. The algorithm of DE is performed on the Tanner graph.

Since the bit values of the variable nodes only have two values zero or one, the messages stored in the variable nodes are often represented by the LLR,

$$L_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1}\right) = \ln \frac{W_N^i\left(y_1^N, \hat{u}_1^{i-1}|0\right)}{W_N^i\left(y_1^N, \hat{u}_1^{i-1}|1\right)}. \tag{3.36}$$

Using recursive expressions (3.33) and (3.34), we can obtain the recursive formula for LLR of each variable node,

$$\begin{aligned} &L_{2N}^{(2i-2)}(y_1^{2N}, \hat{u}_1^{2i-1}) \\ &= 2\ \tanh^{-1}(\tanh(\frac{(L_N^{(i)}(y_1^N, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1.e}^{2i-2})}{2}) \tanh(\frac{(L_N^{(i)}(y_{N+1}^{2N}, \hat{u}_{1.e}^{2i-2})}{2})), \end{aligned} \tag{3.37}$$

$$\begin{aligned} &L_{2N}^{(2i)}(y_1^{2N}, \hat{u}_1^{2i-1}) \\ &= L_N^{(i)}(y_1^N, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1.e}^{2i-2}(-1)^{\hat{u}_{2i-1}} + L_N^{(i)}(y_{N+1}^{2N}, \hat{u}_{1,e}^{2i-2}). \end{aligned} \tag{3.38}$$

Then the estimate of u_i is

$$\hat{u}_i = \begin{cases} 0, & L_N^i(y_1^N, \hat{u}_1^{i-1}) > 0, \\ 1, & \text{otherwise.} \end{cases} \tag{3.39}$$

Consider the LLR of a variable node as a random variable with a pdf represented by $a(z)$. Assume channel W is symmetric when the all-zero codeword is transmitted, then the probability that the variable node misjudgment is P_e,

$$P_e = \int_{-\infty}^{0} a(z)dz. \tag{3.40}$$

Let us denote $a_N^{(i)}(y)$ as the pdf of $L_N^{(i)}(y_1^N,\ \hat{u}_1^{i-1})$. The pdf of the i-th polarized

bit channel's LLR can be calculated by (3.37) and (3.38),

$$\begin{aligned} a_{2N}^{(2i)} &= a_N^{(i)} \star a_N^{(i)}, \\ a_{2N}^{(2i-1)} &= a_N^{(i)} \circledast a_N^{(i)}, \\ a_1^{(1)} &= a_w, \end{aligned} \tag{3.41}$$

where a_w is pdf of LLR of the original channel W when sending an all-zero sequence, $\star$ and $\circledast$ are the convolution operations in the variable node domain and check node domain, respectively [82]. The error probability of each polarized bit channel is shown as follows:

$$P(A_i) = P_e(W_N^i) = \int_{-\infty}^{0} a_N^i(z)dz. \tag{3.42}$$

3.3.4.3 Gaussian Approximation

For a Gaussian channel, the pdf of the LLR in the DE algorithm can be approximated by a Gaussian distribution, where the variance is twice the mean, which can greatly reduce the computational complexity. This simplification of the DE algorithm is called Gaussian Approximation (GA).

If we assume the channel is Gaussian, the initial message can be calculated as

$$L(y) = \ln \frac{W(y|x=0)}{P(y|x=2)} = \frac{-2y}{\sigma^2}. \tag{3.43}$$

Assuming that an all zeros codeword with length N is transmitted and a BPSK modulation is used. Denote the LLRs of x_1^N as L_1^N , which are Gaussian random variables with mean $\frac{2}{\sigma^2}$ and variance $\frac{4}{\sigma^2}$. Denote the pdf of the LLRs as $N\left(\frac{2}{\sigma^2}, \frac{4}{\sigma^2}\right)$. For a Gaussian distribution with a mean of m and variance of σ^2, $\sigma^2 = 2m$. Let us denote $a_N^{(i)}$ as the pdf of $L_N^{(i)}(y_1^N, \hat{u}_1^{i-1})$, $a_N^{(i)}$ can be expressed as $N\left(m_N^{(i)}, 2m_N^{(i)}\right)$. The pdf of the i-th polarized bit channel's LLR can be calculated by

$$\begin{aligned} m_{2N}^{(2i)} &= 2m_N^i, \\ m_{2N}^{(2i-1)} &= \phi^{-1}(1-(1-\phi(m_N^i)))^2), \\ m_1^{(1)} &= 2/\sigma^2, \end{aligned} \tag{3.44}$$

where

$$\phi(x) = \begin{cases} \exp(-0.4527x^{0.86} + 0.0218), & 0 < x < 10, \\ \frac{1}{2}(\sqrt{\frac{\pi}{x}e^{-\frac{x}{4}}(1-\frac{3}{x}) + \frac{\pi}{x}e^{-\frac{x}{4}}(1=\frac{3}{7x})}), & x \geq 10. \end{cases}$$

The error probability of the i-th bit channel is shown as follows:

$$p\left(A_i\right) = \int_{-\infty}^{0} \frac{1}{2\sqrt{\pi m_N^{(i)}}} \exp\left(\frac{-\left(x - m_N^{(i)}\right)^2}{4m_N^{(i)}}\right) dx. \tag{3.45}$$

Table 3.1 shows the complexity of polar codes constructed using different methods.

Table 3.1: a complexity comparison of polar codes constructed using different methods

Design and construction	
Methods	Complexity
Heuristic [19]	Medium
DE [20]	High
GA [21]	Low

3.3.5 Polar Encoding

Arikan [18], takes advantage of the polarization effect to construct codes that achieve the symmetric channel capacity $I(W)$ by a method called polar coding. The complexity of recursive encoder is only $O(N \log N)$. The basic idea of polar coding is to create a coding system where one can access each $W_N^{(i)}$ coordinate bit-channel individually and send information bits only through those for which $Z\left(W_N^{(i)}\right)$ is near 0. That is, the information bits are assigned to the polarized channels which are almost noiseless, while the frozen bits are assigned to noisy channels.

Polar codes have a codeword length of $N = 2^n, n = 1, 2, \ldots$, and information

length K. The information source $\mathbf{u} = (u_1, u_2, ..., u_n)$ includes K information bits and $N - K$ frozen bits which are given fixed values of 0. The codeword $\mathbf{x}$ with code rate $R = K/N$ can be obtained as $\mathbf{x} = \mathbf{u}\mathbf{G}_N$, where $\mathbf{G}_N = \mathbf{B}_N\mathbf{F}_2^{\otimes n}$ is the generator matrix, $\mathbf{B}_N$ is the bit-reversal permutation matrix and $\mathbf{F}_2^{\otimes n}$ is the n-th Kronecker power of $\mathbf{F}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

In order to better explain the encoding process, this section will give an example of coding process of a (8,4) polar code on BEC, with $\epsilon = 0.5$. First calculate $\mathbf{B}_8$:

$$\mathbf{B}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$\mathbf{I}_2 \otimes \mathbf{B}_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

$\mathbf{R}_4$ is transformed from $\mathbf{I}_4$, first arrange the odd columns of $\mathbf{I}_4$, then the even columns:

$$\mathbf{I}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \Rightarrow \mathbf{R}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\mathbf{B}_4 = \mathbf{R}_4(\mathbf{I}_2 \otimes \mathbf{B}_2) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\mathbf{I}_2 \otimes \mathbf{B}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

$\mathbf{R}_8$ is transformed from $\mathbf{I}_8$, first arrange the odd columns of $\mathbf{I}_4$, then the even columns:

$$\mathbf{I}_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \Rightarrow \mathbf{R}_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\mathbf{B}_8 = \mathbf{R}_8(\mathbf{I}_2 \otimes \mathbf{B}_4) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Now calculating $\mathbf{F}_2^{\otimes 3}$

$$\mathbf{F}_2^{\otimes 1} = \mathbf{F}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

$$\mathbf{F}_2^{\otimes 2} = \mathbf{F}_2 \otimes \mathbf{F}_2^{\otimes 1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \mathbf{F}_2^{\otimes 1} = \begin{bmatrix} \mathbf{F}_2^{\otimes 1} & 0 \\ \mathbf{F}_2^{\otimes 1} & \mathbf{F}_2^{\otimes 1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix},$$

$$\mathbf{F}_2^{\otimes 3} = \mathbf{F}_2 \otimes \mathbf{F}_2^{\otimes 2} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \mathbf{F}_2^{\otimes 2} = \begin{bmatrix} \mathbf{F}_2^{\otimes 2} & 0 \\ \mathbf{F}_2^{\otimes 2} & \mathbf{F}_2^{\otimes 2} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Then constructing the generator matrix $\mathbf{G}_8$:

$$\mathbf{G}_8 = \mathbf{B}_8\mathbf{F}_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

For a BEC channel with $\epsilon = 0.5$, we have $Z(W) = 1 - \epsilon = .5$, using (3.33) and

(3.34) to calculate $\{Z(W_8^i)\}, i = 1, 2, \cdots, 8$. Arrange $Z(W_8^i)$ in descending order, selects the smallest four-bit channel numbers to form the information bits index set $\{4, 6, 7, 8\}$. Let the information bits be $\{1, 1, 1, 1\}$ then $\mathbf{u}_1^8 = \{0, 0, 0, 1, 0, 1, 1, 1\}$

Finally polar code word can be produced

$$\mathbf{x}_1^8 = \mathbf{u}_1^8 \mathbf{G}_8 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{3.46}$$

3.3.6 Polar Decoding

3.3.6.1 Successive Cancellation Decoding

The successive cancellation (SC) decoding algorithm is employed to decode polar codes and can achieve channel capacity [18]. Let A and A^c denote the index sets of information bits and frozen bits, respectively. The information source u_1^N contains information bits u_A and frozen bits u_{A^c}. In the decoding process, the estimated value $\hat{u}_i$ of bit u_i is decided bit-by-bit, based on the output of the received signal y_1^N and the previous detected estimates $\hat{u}_1^{i-1}$. This is achieved by computing the transfer probability $p(y_i|x_i)$ of the polarized channel W_N^i when $\hat{u}_i = 0$ and $\hat{u}_i = 1$. The decision of u_i is made as follows [18]:

$$\hat{u}_i = \begin{cases} u_i, & i \in A^c, \\ h_i(y_1^N, \hat{u}_1^{i-1}), & i \in A. \end{cases} \tag{3.47}$$

When $i \in A^c$, it is frozen bit, directly giving the decision $\hat{u}_i = u_i$; when $i \in A$, u_i is information bit, and

$$h_i(y_1^N, \hat{u}_1^{i-1}) = \begin{cases} 0, & \frac{p(y_1^N, \hat{u}_1^N|0)}{p(y_1^N, \hat{u}_1^N|1)} > 1, \\ 1, & \text{otherwise.} \end{cases} \tag{3.48}$$

The log-likelihood ratio (LLR) is defined as

$$L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) = \log \frac{p(y_1^N, \hat{u}_1^N|0)}{p(y_1^N, \hat{u}_1^N|1)}. \tag{3.49}$$

Then (3.47) is changed to

$$\hat{u}_i = \begin{cases} 0, & L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) > 0, \\ 1, & \text{otherwise.} \end{cases} \tag{3.50}$$

The calculation of the LLR can be done by recursion. Now define the functions f and g as follows:

$$f(a, b, u_s) = (-1)^{u_3} a + b \tag{3.51}$$

$$f(a, b) = \ln(\frac{1 + e^{a+b}}{e^a + e^b}) \tag{3.52}$$

where, $a, b \in \mathbf{R}, u_s \in \{0, 1\}$. The recursive operation of the LLR is represented by the functions f and g as follows:

$$\begin{aligned} &L_N^{(2i-1)}(y_1^N, \hat{u}_1^{2i-2}) \\ &= f(L_{N/2}^{(i)}(y_1^{N/2}, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1.e}^{2i-2}), L_{N/2}^{(i)}(y_{N/2+1}^N, \hat{u}_{1,e}^{2i-2}) \end{aligned} \tag{3.53}$$

$$\begin{aligned} &L_N^{(2i)}(y_1^N, \hat{u}_1^{2i-1}) \\ &= g(L_{N/2}^{(i)}(y_1^{N/2}, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1.e}^{2i-2}), L_{N/2}^{(i)}(y_{N/2+1}^N, \hat{u}_{1,e}^{2i-2}, \hat{u}_{2i-1}) \end{aligned} \tag{3.54}$$

$$L_1^{(i)}(y_i) = \log \frac{p(y_i|0)}{p(y_i|1)} \tag{3.55}$$

Thus, according to (3.53), (3.54) and (3.55) all the $L_N^{(i)}(y_1^N, \hat{u}_1^{i-1})$ of the polarized bit channels can be calculated, then use (3.47) and (3.48) to obtain the estimate $\hat{u}_i$ of u_i.

Fig. 3.10 shows a diagram of an SC decoding algorithm for a polar code with code

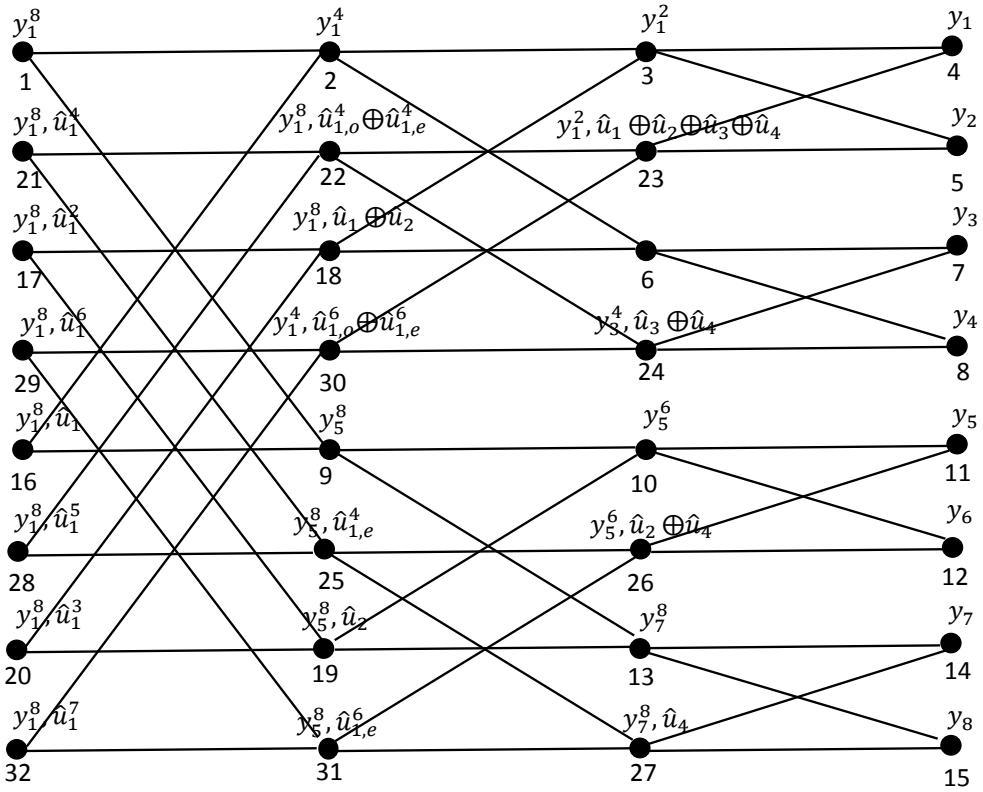

Figure 3.10: SC decoding process for polar code with $N = 8$.

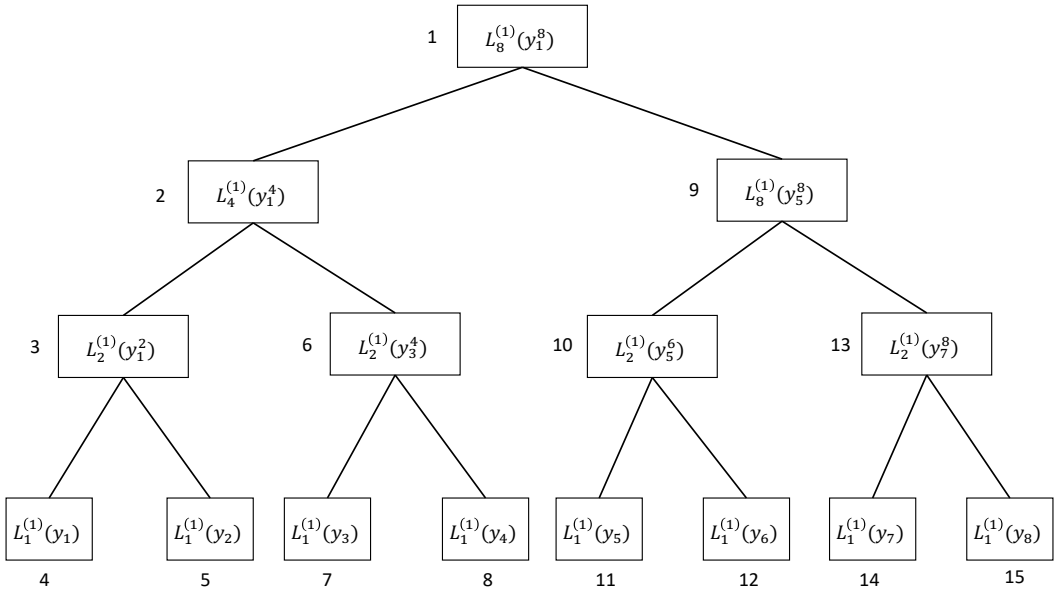

Figure 3.11: Calculation phase of the estimated value $\hat{u}_1$ of the first input bit u_1.

length $N = 8$. Since the SC decoding algorithm is a bit-by-bit decoding process, the known condition required for decoding the i-th bit u_i is the estimation of the received signal y_i^N and the estimate of the previous $i-1$ bits, so that the estimated value $\hat{u}_1$ of u_1 should be calculated first in Fig. 3.10. According to (3.47), we first determine whether the bit is a frozen bit, and if so, directly determine $\hat{u}_1 = u_1 = 0$; if not, perform the decoding process according to Fig. 3.10. In Fig. 3.10, SC decoding starts form the left node 1 and we should calculate $L_8^{(1)}(y_1^8)$. From (3.53) we can observe $L_4^{(1)}(y_1^4)$ of node 2 and $L_4^{(1)}(y_5^8)$ of node 9 need to be calculated. Also $L_4^{(1)}(y_1^4)$ of node 2 based on the calculation of $L_2^{(1)}(y_1^2)$ of node 3 and $L_2^{(1)}(y_3^4)$ of note 6. Node 3 needs node 4 and 5 LLRs $L_1^{(1)}(y_1)$ and $L_1^{(1)}(y_2)$. Similar to the previous process, the LLRs of node 9 to node 15 are calculated, and the LLR of the upper node can be calculated to obtain the LLR $L_8^{(1)}(y_1^8)$ of u_1, and then the estimated value $\hat{u}_1$ of u_1 can be determined according to (3.48).

Fig. 3.11 describes the calculation phase of the estimated value $\hat{u}_1$ of the first input bit u_1, which corresponds to Fig. 3.10. When the estimate $\hat{u}_1$ of the first input bit u_1 is determined the second input bit can be determined. The process is similar to the previous bit, but the resulting estimate $\hat{u}_1$ is added until the 8-th input bit gets the estimated value and the decoding process finish.

We give the BER and frame error rate (FER) performances of different length polar code with SC decoder on AWGN channel in Fig. 3.12 and Fig. 3.13. In simulations, polar codes have a code rate $R_c = 0.5$ and are constructed using a heuristic method, with the maximum number of frames set to 10000. We can observe that, with a fixed value of code rate, the bit error rate and frame error rate get lower with the increasing code length of the polar code, which means the decoding performance increases. The main reason of this is with the increase of code length N the phenomenon of channel polarization is becoming more and more obvious.

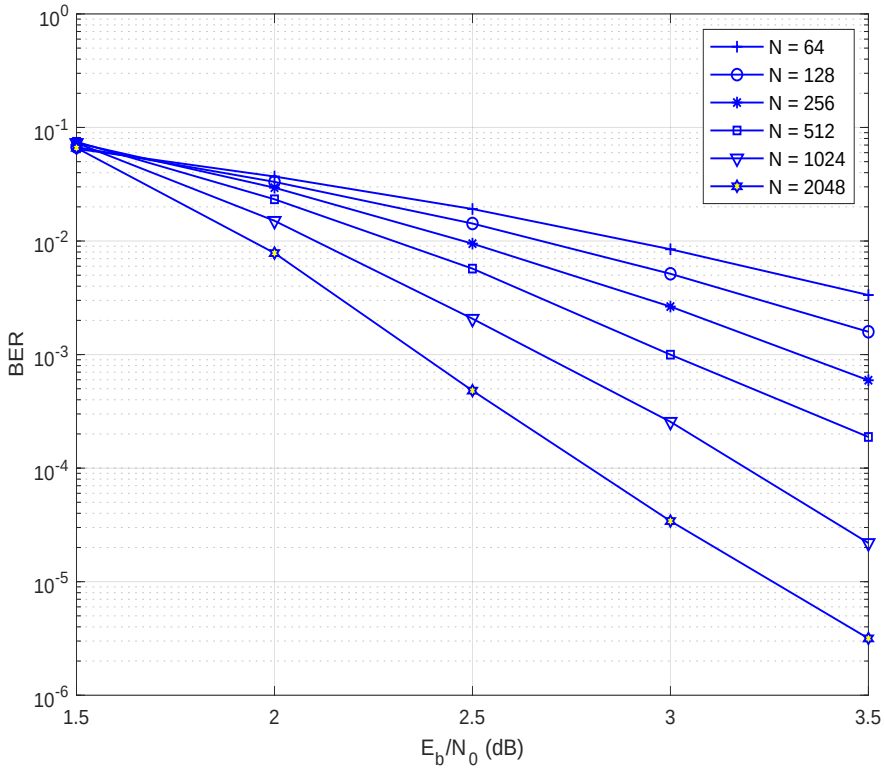

Figure 3.12: BER performances of different length polar code with SC decoder on AWGN channel.

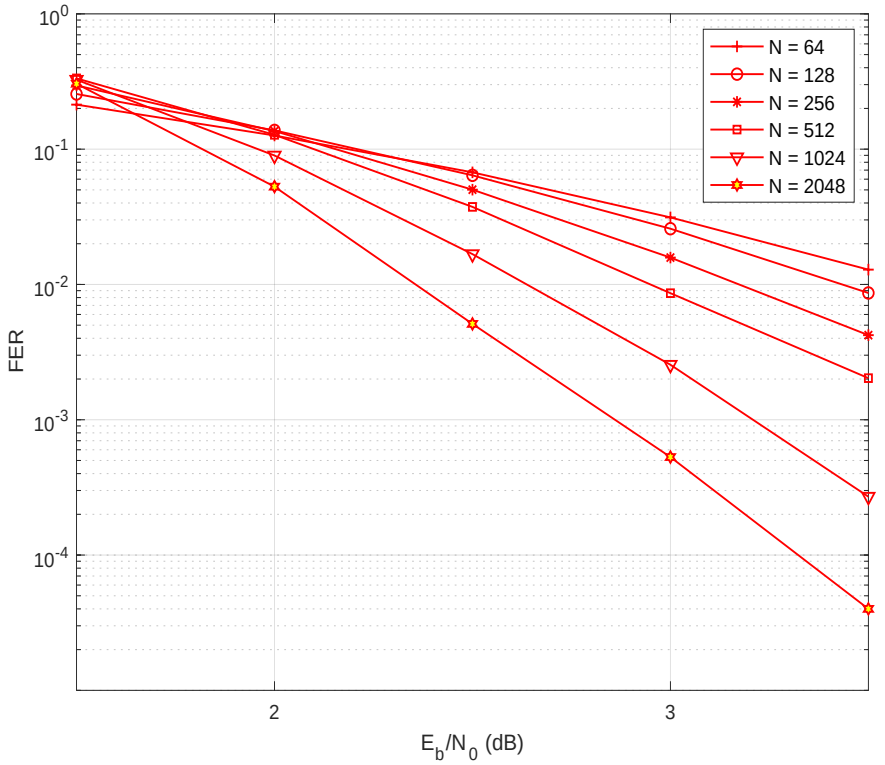

Figure 3.13: FER performances of different length polar code with SC decoder on AWGN channel.

3.3.6.2 Successive Cancellation List Decoding

For a polar code when the code length approaches infinity, the channel will polarize completely. However, with a limited code length, there are still some information bits that cannot be decoded correctly because the channel polarization is not complete. When an error occurs in the decoding of the previous $i-1$ information bits, due to the SC decoder needing the estimated value of the previous information bits when decoding the subsequent information bits, this will cause a more serious error transmission. The SC decoding algorithm is a greedy algorithm. For each layer of the code tree, only the optimal path is searched and the next layer is performed. Therefore, errors cannot be modified. The SCL decoding algorithm is an improvement on the SC algorithm. This thesis focuses on the security performance and all works based on SC decoding. Here we will show simulation results of polar codes with SCL decoding on AWGN channel and the specific explanation of SCL decoding can be found in [22, 23, 83].

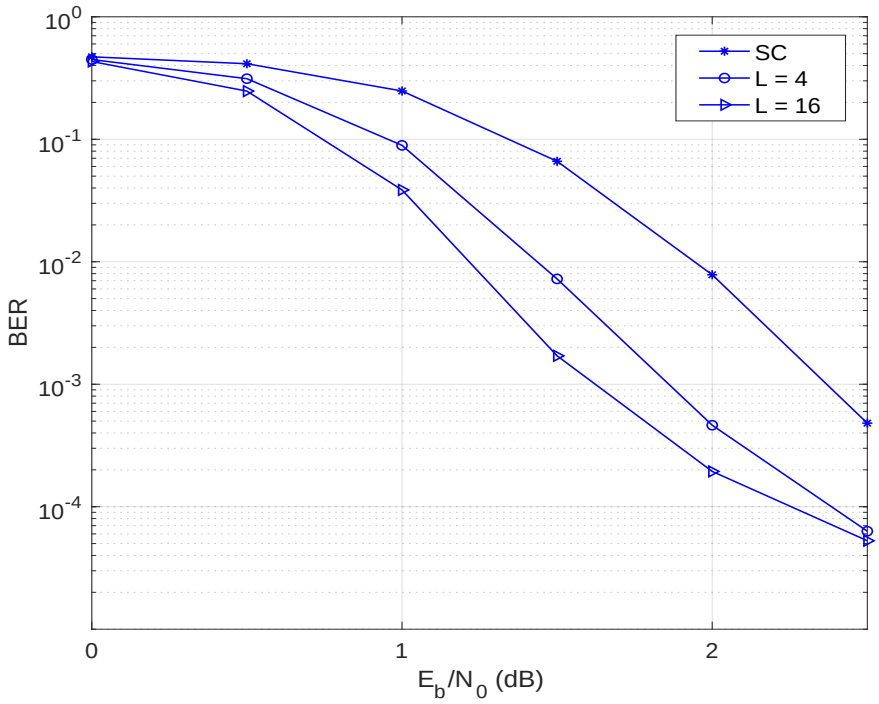

Figure 3.14: BER performance of heuristic-constructed polar codes on AWGN channel under SCL decoding with different list size.

The BER performance of a length $N = 2048$, rate 0.5 polar code constructed using the heuristic method for various list sizes can be seen in Fig. 3.14. When the list size is equal to 1 it is SC decoding. We observed with list size increasing the

BER performance is improving.

In Table 3.2 we give a complexity comparison of polar decoding methods.

Table 3.2: a complexity comparison decoding of polar codes

Decoding	
Algorithms	Complexity
SC [18]	$O(N \log N)$ low
SCL [22]	$O(LN \log N)$ medium

3.4 Conclusion

In this chapter, physical layer security technique has been explained in detail, which includes the wiretap channel model, security measurement. In addition, the SαS noise model has been explained in detail. This chapter has also given the details of the encoding and the decoding of polar codes. To analyze the asymptotic performance of polar codes, density evolution, Gaussian approximation and heuristic have been described in detail. To conclude, this chapter provides the essential background theory for the following novel chapters.

Chapter 4

Construction of Polar Codes Combined with Physical Layer Security on Impulsive Noise Channels

4.1 Introduction

Polar codes are the first proven capacity-achieving codes for any symmetric binary input discrete memoryless channel (B-DMC) and their has been recent interest in their combination with the popular area of physical layer security.

Current literature on polar codes combined with physical layer security assumes that noise added at the recipient's and eavesdropper's receiver has a Gaussian distribution. However, the distribution of noise in wireless communication systems is not always Gaussian due to other sources of noise, such as impulsive noise. Symmetric α-stable (SαS) distributions [84] are commonly used to accurately model impulsive noise channels, due to their heavy-tailed distributions, and are used in this work. We would like to explore polar codes' performance in the presence of impulsive noise, particular when combined with security, to assess whether it can still achieve high security and performance. In addition to evaluating the performance of polar codes on an impulsive wiretap channel, we are also interested in the scenario where the main channel is more impulsive than the eavesdropper's channel and whether secure communication is still possible.

Motivated by the above observations and the lack of published work on the analysis of polar codes on more general memoryless channels, we present the construction of polar codes combined with physical layer security, where each user experiences varying levels of impulsive noise. The polar codes are constructed using density evolution (DE), which has knowledge of the α-stable noise distribution, in order to construct optimal codes for this environment. To ensure secure communication, the bit-channels are divided into three sections within the polar codeword: information bits, random bits and frozen bits [31]. Therefore, the intended recipient will receive information bits on some of their good channels, while the eavesdropper will only receive random bits on their good channels, as explained later in this chapter. We expand the work of [31] to evaluate the performance of polar codes on wiretap channels where each user experiences varying levels of impulsive noise for the first time.

In this chapter, we first examine the security performance of polar codes constructed with different values of design-SNR on Gaussian wiretap channels. In addition, we evaluate the BER performance of polar codes constructed by density DE and heuristic methods on SαS channels for different values of α. Finally, the construction of polar codes combined with physical layer security on additive impulsive noise has been derived. Simulation results confirm that the BER at the eavesdropper is always 0.5 for all signal-to-noise ratios, thus always ensuring secure communication, and we present the very interesting result where this is still achieved when the main channel is more impulsive than the eavesdropper's channel.

4.2 System Model

In this section, we first explain the system model in detail. As shown in Fig. 4.1, in which there is a transmitter (Alice) sending confidential information to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). $\mathbf{U}$ denotes a K-bit secret information that Alice intends to send to Bob. It is assumed that $\mathbf{U}$ is a uniformly distributed random vector that takes values in $\{0,1\}^K$. The outputs of the polar encoder $\mathbf{X}$ are transmitted across the main channel and eavesdropped by Eve, resulting in the corresponding channel outputs $\mathbf{Y}$ and $\mathbf{Z}$. Finally, the polar decoder maps $\mathbf{Y}$ and $\mathbf{Z}$ into the estimate $\hat{\mathbf{U}}_B$ and $\hat{\mathbf{U}}_E$ of the original message detected by Bob and Eve.

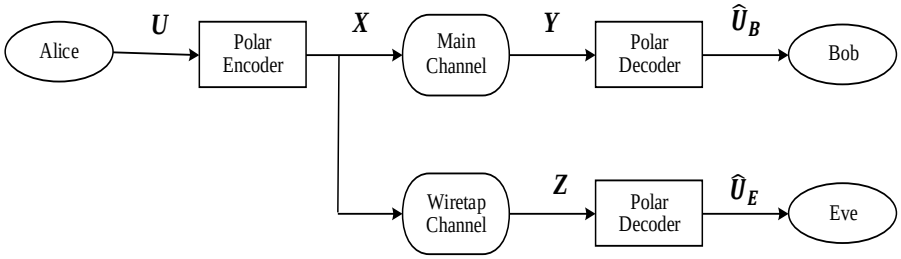

Figure 4.1: Block diagram of a polar coded wiretap channel system.

4.3 Design of Polar Codes on Gaussian Wiretap Channel

For the Gaussian wiretap channel model, it assume that the noise of main channel and eavesdropper channel are Additive White Gaussian Noise (AWGN). We assume that the AWGN channel is a binary input channel so polar codes constructed by a heuristic method can be used on the Gaussian wiretap channel to ensure security.

The design of polar codes combined with physical layer security is shown in Fig. 4.2. The basic idea of this proposed coding scheme is to transmit information over those bit-channels that are only noiseless for Bob but noisy for Eve, while filling bit channels that are noiseless for both Bob and Eve with random bits and sending zeros on the remaining bit channels. The most important part of secure polar coding is the selection of the bit channels of the information bits for the main channel and the wiretap channel. For the Gaussian wiretap channel we use a heuristic method to construct polar codes and the Successive Cancellation decoder is employed for the decoding process.

4.3.1 Design-SNR of Polar Codes

Different from most codes in coding theory, polar codes have an important characteristic which is their non-universality. That is, the definition of polar codes depends on a specified value of SNR, known as design-SNR. Arikan gives the set $\mathcal{F}$ of polar codes in the sense that the block error rate (BLER) of polar codes is minimum under SC decoding. As BLER is a function of SNR, the polar code will change with different given design-SNRs.

In Fig. 4.3 we plot the BERs performance of different design-SNRs of polar codes constructed by a heuristic method with a SC decoder on the AWGN channel, where

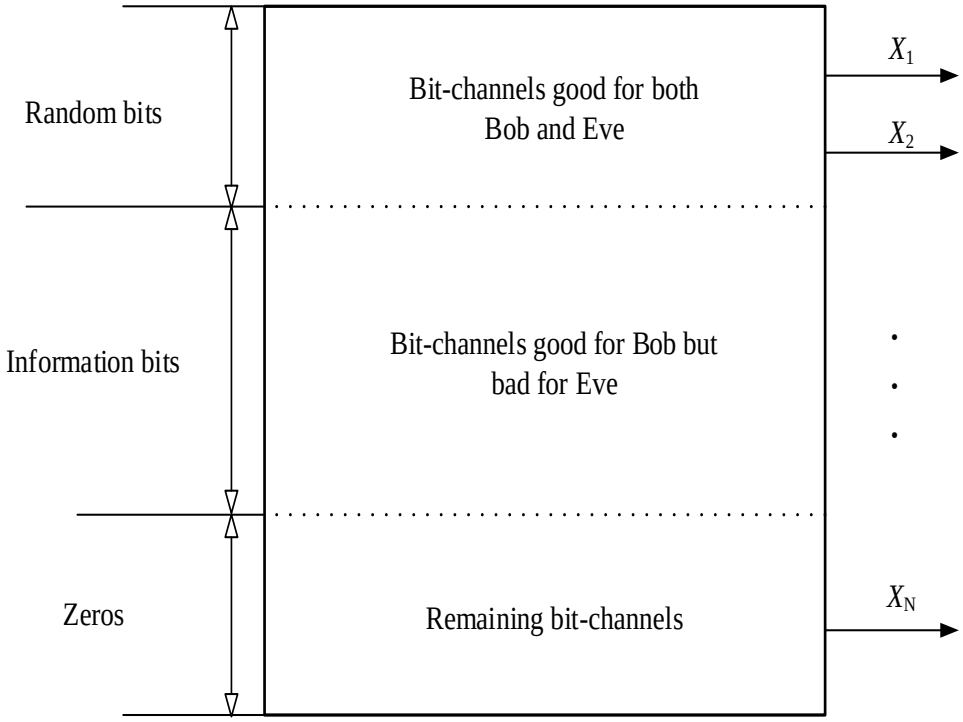

Figure 4.2: Row-permuted version of $\mathbf{F}_2^{\otimes n}$.

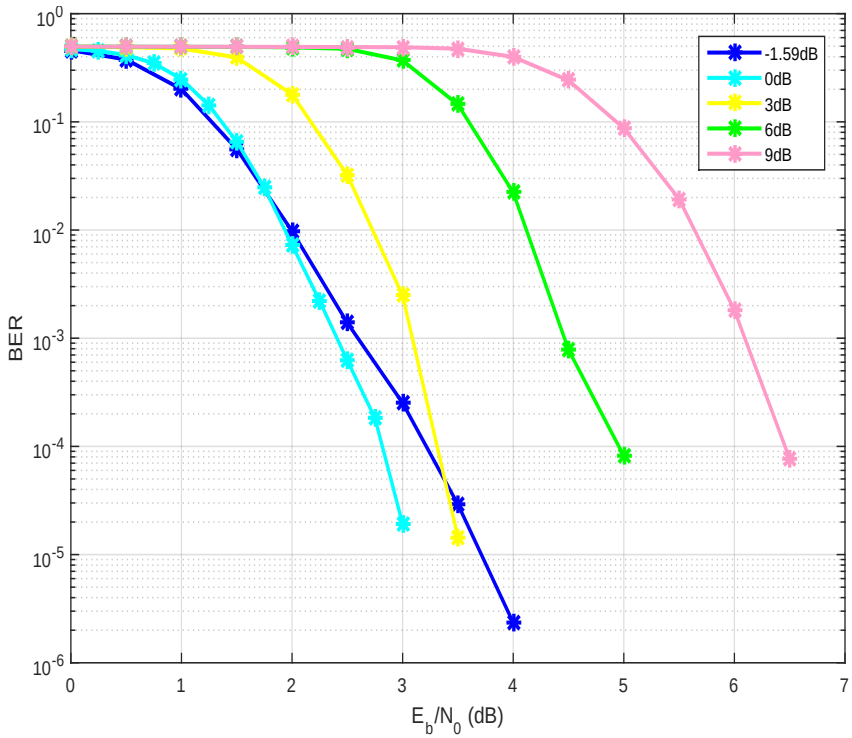

Figure 4.3: The effect of design-SNR of polar code with code length $N = 2048$ and code rate $R = 0.5$.

the code length is $N = 2048$ and code rate is $R = 0.5$. We can observe that the change of design-SNR is significant in terms of the BER performance of polar codes. This difference is the main point of our secure polar coding scheme for Gaussian wiretap channels.

4.3.2 Degraded Gaussian Wiretap Channel

The noise in the main channel and wiretap channel are denotes N_1 and N_2, when $N_1 \sim \mathcal{N}(0, \sigma_1^2)$, $N_2 \sim \mathcal{N}(0, \sigma_2^2)$, and N_1 and N_2 are independent. If the variances of noise satisfy $\sigma_1^2 < \sigma_1^2$, that is, the noise of the main channel is smaller than the noise of the eavesdropping channel, it is considered that the eavesdropper channel is worse than the main channel and the wiretap channel is called the degraded wiretap channel.

In this section we first show the performance of conventional polar codes without any secure design on the degraded wiretap channel. First a polar code with code length $N = 2048$ and code rate $R = K/N = 0.5$ is constructed by a heuristic method explained in chapter 3. After the polar encoder, the codeword is transmitted to Bob through an AWGN channel, without secure encoding so Eve can receive the same codeword. In order to prevent Eve from receiving useful information we assume Eve's channel is worse than Bob's channel, and this can be achieve by the difference between the SNRs of Bob and Eve, called the Signal-to-Noise Ratio gap $SNR_g = SNR_M - SNR_W$, where SNR_M and SNR_W represent the SNR of main channel between Alice and Bob and eavesdropper channel between Alice and Eve, respectively. If SNR_g is positive the wiretap channel is non-degraded, and the smaller SNR_g is, the more capable Eve's channel is. Finally, the original information detected by Bob and Eve will be obtained by the SC decoder. Fig. 4.4 gives the BER performance of this method. The simulation results show that as the SNR_g increases the secure and reliable zone becomes larger, while secure and reliable communication cannot achieved in higher SNRs. In that case we apply secure polar codes to achieve secure communication.

The most important part of secure polar coding is the selection of the index set $\mathcal{A}^s$ of the secure information bits for the main channel and the eavesdropper channel. As describe in the previous section, the change of design-SNR will influence polar codes, thus we use design-SNR to select $\mathcal{A}^s$. First, we give two different design-SNRs,

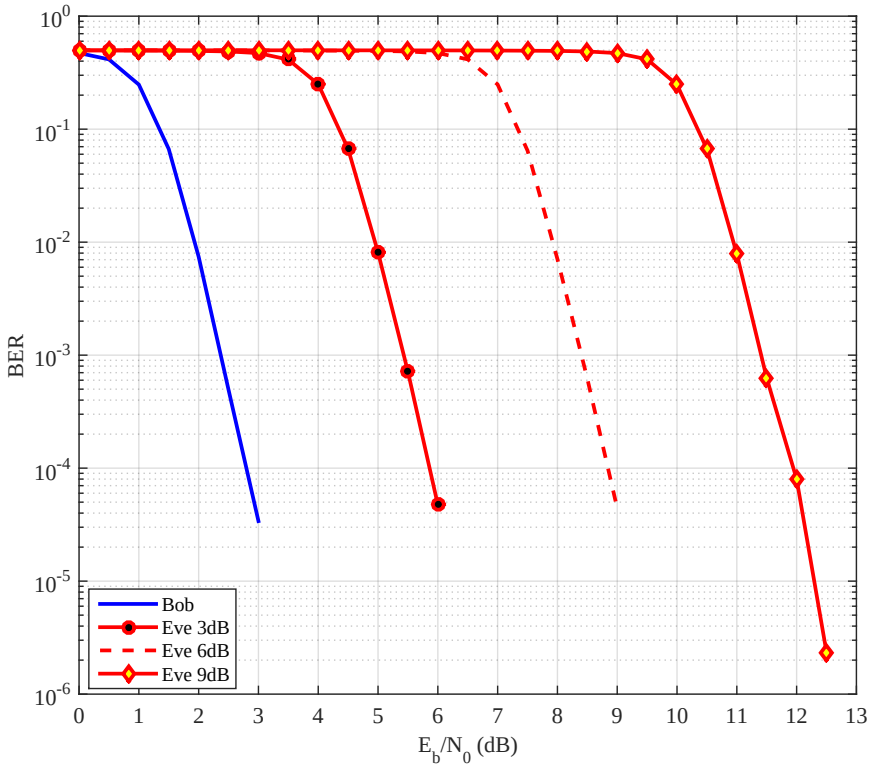

Figure 4.4: BER performance of heuristic-constructed polar codes for the degraded Gaussian wiretap channel, where SNR_g = 3dB, 6dB and 9dB.

then apply them separately with the heuristic method to construct polar codes with the same code length N and code rate $R = 0.5$ to produce two different sets of error probability $P(A_i)$ of each polarized bit channel. Then order them separately and save the bit index. Define the information index set $\mathcal{A}^{i1}$ and $\mathcal{A}^{i2}$ and frozen index set $\mathcal{A}^{f1}$ and set $\mathcal{A}^{f2}$. The intersection of $\mathcal{A}^{i1}$ and $\mathcal{A}^{f2}$ is $\mathcal{A}^s$; the intersection of $\mathcal{A}^{i1}$ and $\mathcal{A}^{i2}$ is $\mathcal{B}$, which is the index set for random bits; and others are set as frozen bits index.

Encoding Algorithm: The message $\boldsymbol{u} \in \{0,1\}^s$ and a vector $\boldsymbol{e} \in \{0,1\}^r$ are the inputs of the encoder with the function $\varepsilon : \{0,1\}^s \times \{0,1\}^r \to \{0,1\}^n$, where s and r are the length of information bits and random bits and n is the length of the codeword. First, the encoder generates a vector $\boldsymbol{v} \in \{0,1\}^n$, by letting $\boldsymbol{v}_{\mathcal{R}} = \boldsymbol{e}$, $\boldsymbol{v}_{\mathcal{A}^s} = \boldsymbol{u}$, and $\boldsymbol{v}_{\mathcal{B}} = \boldsymbol{0}$, where $\mathcal{R}$, $\mathcal{A}^s$ and $\mathcal{B}$ are the set of random bits, information bits and zeros. The output of the encoder is $\mathbf{x} = \mathbf{v}\mathbf{G}_N = \mathbf{v}\mathbf{B}_N\mathbf{F}_2^{\otimes n}$. The secrecy code rate is $R_s = r/n$.

Decoding Algorithm: The input of the decoder is a vector $\boldsymbol{y} \in y^n$ which is the output of the channel. It then applies the SC decoding algorithm and the decoder output is $\hat{\boldsymbol{v}}_{\mathcal{A}^s}$.

Table 4.1: the secrecy code rate for the different design-SNR in dB

N	K	design-SNR_B	design-SNR_E	R	R_s
2048	1024	-1.59	0	0.5	0.0078
2048	1024	-1.59	3	0.5	0.0400
2048	1024	-1.59	6	0.5	0.0767
2048	1024	-1.59	9	0.5	0.0869
2048	1024	0	3	0.5	0.0322
2048	1024	0	6	0.5	0.0688
2048	1024	0	9	0.5	0.0791

The most important part of secure polar coding is the selection of the index set $\mathcal{A}^s$ of the information bits for the main channel and the wiretap channel. For polar codes constructed by the heuristic method on degraded Gaussian wiretap channel, the information bits can be selected differently for Bob and Eve by different design-SNRs. Table 4.1 shows the secrecy code rate for the different design-SNR in dB.

4.4 Construction and Secure Transmission of Polar Codes on Impulsive Noise Channels

4.4.1 Design of Polar Codes on SαS Channels

As stated in the literature review, polar codes show good performance on channels with Gaussian noise, but in this section we are interested in their performance on impulsive noise channels with SαS distributions.

4.4.1.1 Channel Model

We consider a polar-coded system with a codeword of length N bits. In order to generate the transmitted signal the codeword is mapped on to a binary phase shift keying (BPSK) constellation. The received signal is impaired by additive impulsive noise with a SαS distribution which is defined as

$$y_k = x_k + \eta_k, \tag{4.1}$$

where y_k is the k-th received signal, $x_k \in \{-1, +1\}$ is the BPSK symbol, η_j is an SαS distributed noise sample and $k = 1, 2, \ldots, n$.

4.4.1.2 Density Evolution of Polar Codes on SαS Channels

Polar codes can be constructed by several methods, such as the heuristic method, DE and GA. As introduced in Chapter 3 the heuristic method and GA are construction methods for channels with Gaussian noise, which is not of interest in our wok. However, DE can be applied to any binary memoryless symmetric channels (BMSC). As impulsive noise we interest in has a SαS distribution, which is non-Gaussian distribution. Therefore, DE can be employed to design optimal polar codes for impulsive noise channels and we examine the performance of the polar codes with impulsive noise.

According to [70], the channel output of SαS noise and the LLR is symmetric, hence DE can be performed. Let us denote $d_N^{(i)}(y)$ as the pdf of $L_N^{(i)}$ (y_1^N and $\hat{u}_1^{i-1}$) when the all-zero codeword is transmitted. The DE of the updated LLRs in the SC decoder is

$$d_{2N}^{(2i)} = d_N^{(i)} \star d_N^{(i)}, \quad d_{2N}^{(2i-1)} = d_N^{(i)} \circledast d_N^{(i)}, \tag{4.2}$$

where $\star$ and $\circledast$ are the convolution operations in the variable node domain and check node domain, respectively [82]. The error probability of the i-th bit channel is shown as $P_e^{(i)} = \lim_{\epsilon \to +0} \left(\int_{-\infty}^{-\epsilon} d_N^{(i)}(x)dx + \frac{1}{2} \int_{-\epsilon}^{+\epsilon} d_N^{(i)}(x)dx \right)$, where $d_1^1(y)$ is the pdf of the initial LLRs. For DE, it starts with the calculation of the pdf of the initial LLR. The optimal LLR of the i-th variable node is expressed as

$$L = \log \left(\frac{\Pr(y|x=1)}{\Pr(y|x=-1)} \right) = \log \left(\frac{f_\alpha(y-1;\gamma)}{f_\alpha(y+1;\gamma)} \right). \tag{4.3}$$

However, the pdf of (4.3) can only be evaluated numerically. After obtaining $P_e^{(i)}$ for the i-th bit channel, the DE construction method chooses the K bit channels with the smallest $P_e^{(i)}$ for the information bits and the remaining $N-K$ bit channels for frozen bits.

4.4.2 Polar Coding on Wiretap Channels with SαS Noise

In this section we extend the work of [31] to the wiretap channel with SαS impulsive noise. The secure polar coding scheme is illustrated in Fig. 4.2. For polar codes constructed by the heuristic method on SαS channels, the information bits can be selected differently for Bob and Eve by different design-SNRs. In our simulation, the design-SNRs are 0dB and 6dB for Bob's channel and Eve's channel, respectively. When polar codes are constructed by the DE method, the error probability of polarized channels will be different for different α. Thus, the design-SNR is 0dB for both Bob and Eve's channels for DE-constructed polar codes.

For DE-constructed polar codes the selection of the index set $\mathcal{A}^s$ of the secure information bits for the main channel and the wiretap channel is similar to the heuristic method. As DE is based on SαS noise, we choose two different values of α, then apply them separately with the DE method to construct polar codes with the same code length N and code rate $R = 0.5$ to produce two different sets of error probability $P(A_i)$ of each polarized bit channel.

4.5 Results and Discussion

In our work, we use the BER to measure the performance of polar code combined with physical layer security on wiretap channels. In order to make sure Eve cannot extract any useful information from Alice, we require that the BER of Bob approaches 0 while at the same time the BER of Eve is as close to 0.5 as possible. We use P_r^B and P_r^E to denote the bit-error probability of Bob and Eve respectively, which are related by:

$$P_r^B \cong 0, \quad P_r^E \cong 0.5. \tag{4.4}$$

4.5.1 Performance of Polar Codes on Gaussian Wiretap Channels

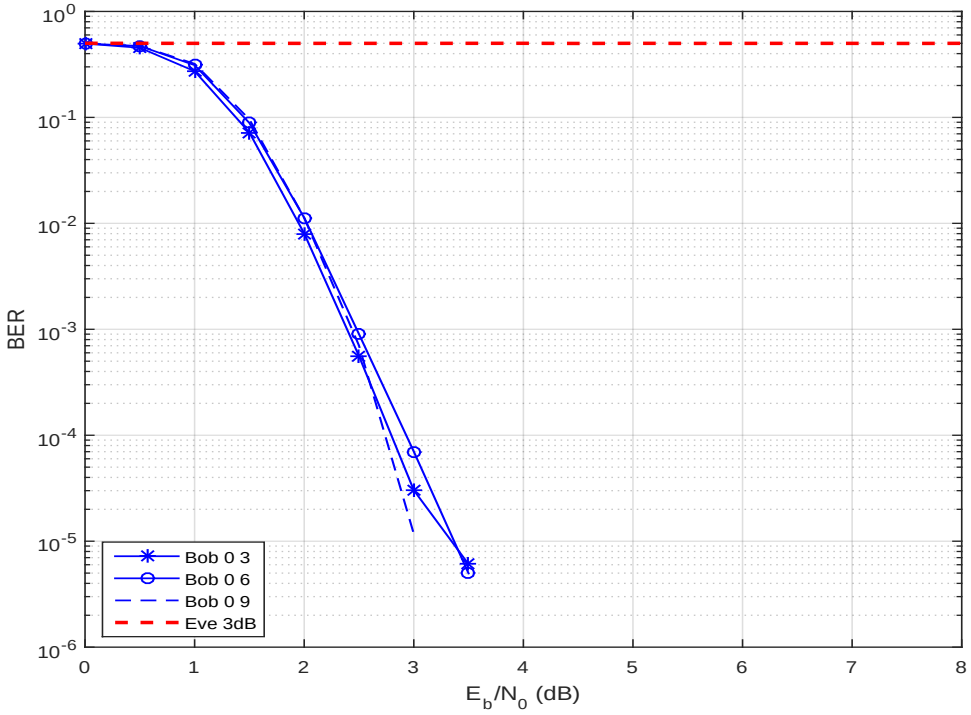

Figure 4.5: BER performance of heuristic-constructed polar codes with design-SNR of the main channel is 0dB and the eavesdropper channel is 3dB, 6dB and 9dB on Gaussian wiretap channel, where the $SNR_g = 3$dB.

Fig. 4.5 presents the BER performance of heuristic-constructed polar codes with the design-SNR of the main channel being 0dB and the eavesdropper channel being 3dB, 6dB and 9dB on the Gaussian wiretap channel, where the main channel is better than the eavesdropper channel by 3dB. Fig. 4.6 presents the BER performance of heuristic-constructed polar codes when the design-SNR of the main channel is 0dB and the eavesdropper channel is 3dB, 6dB and 9dB on the Gaussian wiretap channel and when the main channel is same as the eavesdropper channel. Fig. 4.7 gives BER performance of heuristic-constructed polar codes when the design-SNR of the main channel is -1.59dB and the eavesdropper channel is 0dB, 3dB, 6dB and 9dB on Gaussian wiretap channel, and the main channel is same as the eavesdropper channel. Fig. 4.8 illustrates the BER performance of heuristic-constructed polar codes when the design-SNR of the main channel is 0dB and the eavesdropper channel is 6dB on Gaussian wiretap channel and the main channel is worse than the eavesdropper channel with 3dB, 6dB and 9dB difference. It was shown that with proposed polar coding scheme a secure channel between Alice and Bob can be

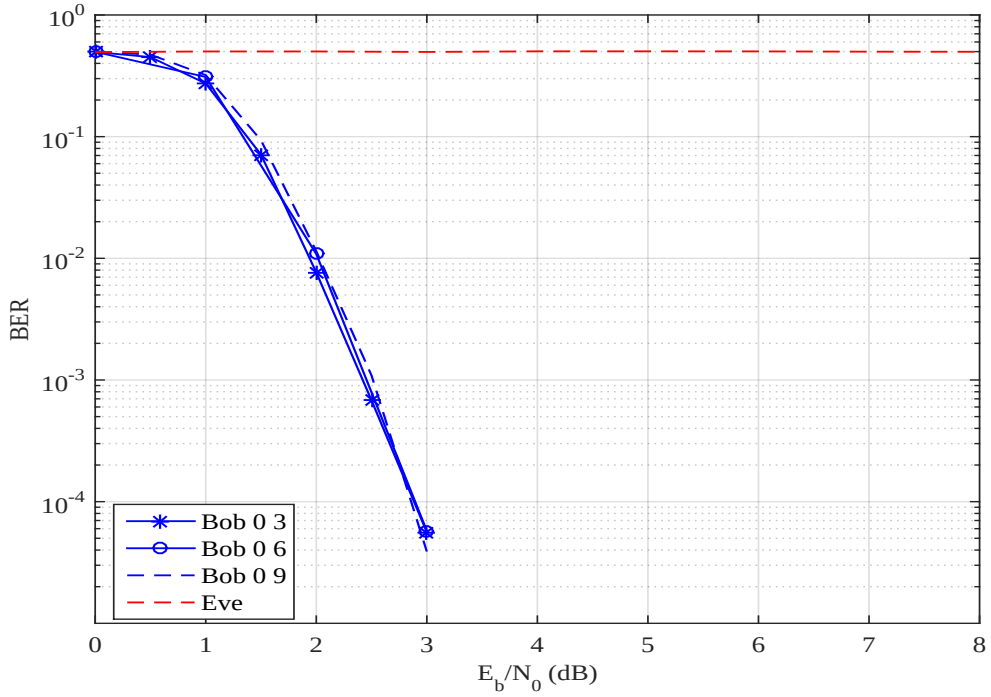

Figure 4.6: BER performance of heuristic-constructed polar codes with design-SNR of the main channel is 0dB and the eavesdropper channel is 3dB, 6dB and 9dB on Gaussian wiretap channel, where the main channel is same as the eavesdropper channel.

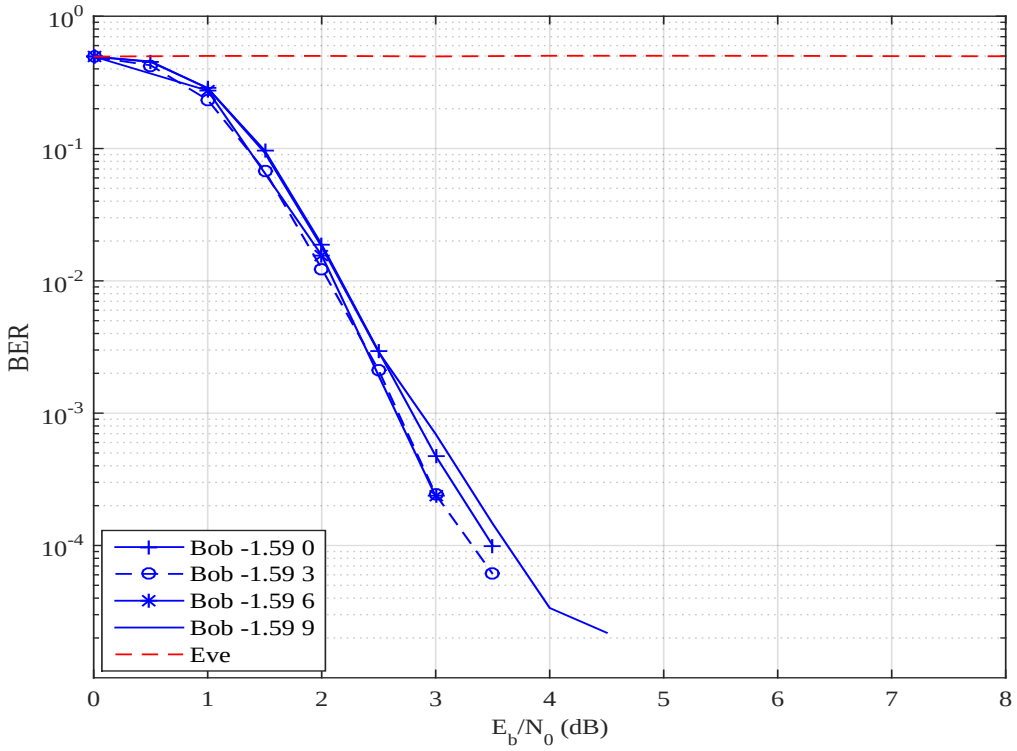

Figure 4.7: BER performance of heuristic-constructed polar codes with design-SNR of the main channel is -1.59dB and the eavesdropper channel is 0dB, 3dB, 6dB and 9dB on Gaussian wiretap channel, where the $SNR_g = 0$dB.

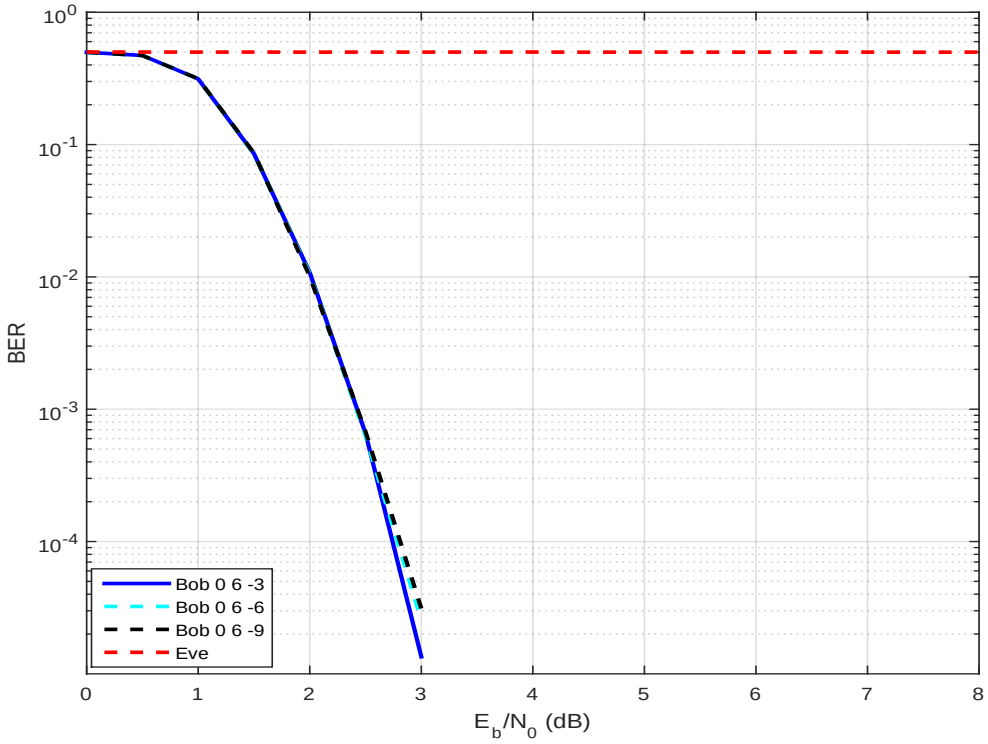

Figure 4.8: BER performance of heuristic-constructed polar codes with design-SNR of the main channel is 0dB and the eavesdropper channel is 6dB on Gaussian wiretap channel, where the SNR_g = -3dB, -6dB and -9dB.

achieved at all SNRs, no matter if the main channel is better, same or worse than the eavesdropper's channel.

4.5.2 Performance of Polar Codes on Impulsive Noise Channels

4.5.2.1 Performance of Polar Codes on SαS Channels

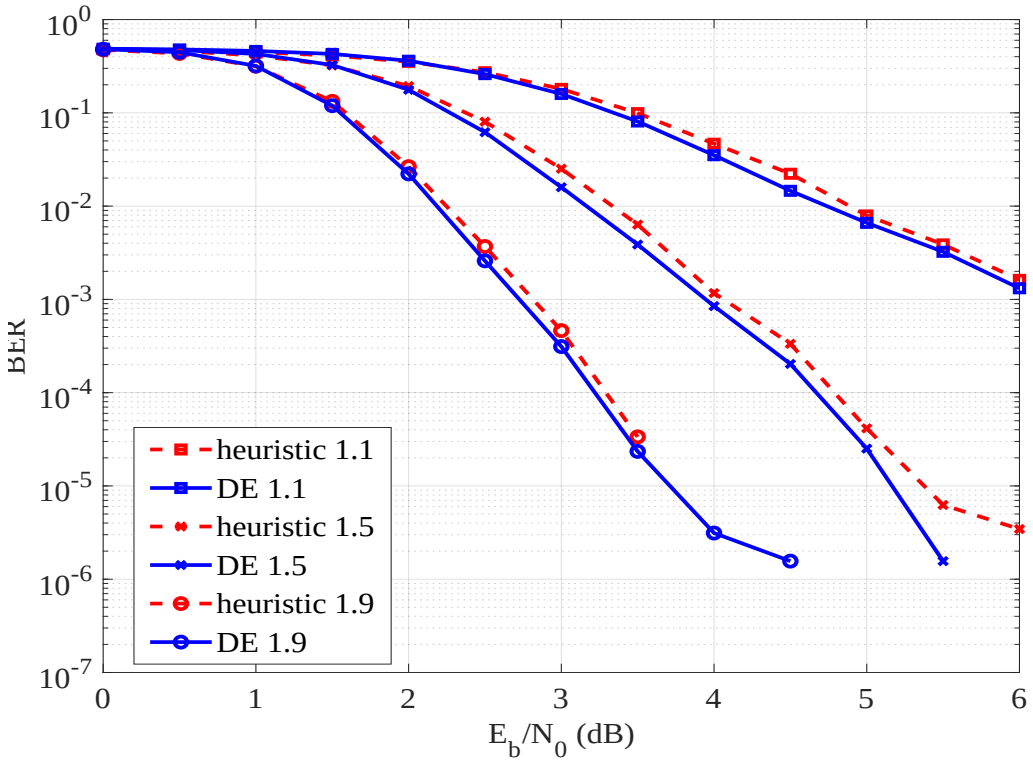

Figure 4.9: BER performance of polar codes on SαS impulsive channels with different values of α.

Fig. 4.9 presents the BER performance of DE-constructed polar codes with code length $N = 2048$ and code rate $R_c = 0.5$ on SαS impulsive channels with different values of α and we also provide a performance comparison of the heuristic and DE-based construction of polar codes. The BER performance is evaluated for SαS channels with $\alpha = 1.1$, $\alpha = 1.5$ and $\alpha = 1.9$ which represent extremely impulsive, moderately impulsive and lightly impulsive noise, respectively. We note that the design-SNR of the heuristic method has already been optimized by experiments. From the simulation results we can observe that under the same channel conditions, DE-based construction of polar codes has 0.1 dB gain over polar codes constructed using heuristic methods for N = 2048 at BER = 10^{-4} on SαS channels with $\alpha = 1.5$ and $\alpha = 1.9$. When the channel is extremely impulsive ($\alpha = 1.1$), the BER performance of polar codes constructed by the DE method is still slightly better than the heuristic method. It proves that DE is a better option for design polar codes in the presence of impulsive noise.

4.5.2.2 Performance of Polar Codes on Wiretap Channels with SαS Noise

To examine the simulated performance of polar codes on wiretap channels with SαS noise we use a polar code with code length $N = 2048$ and code rate $R_c = 0.5$. The polar code is constructed by heuristic and DE method and the maximum frames number is set to 10000.

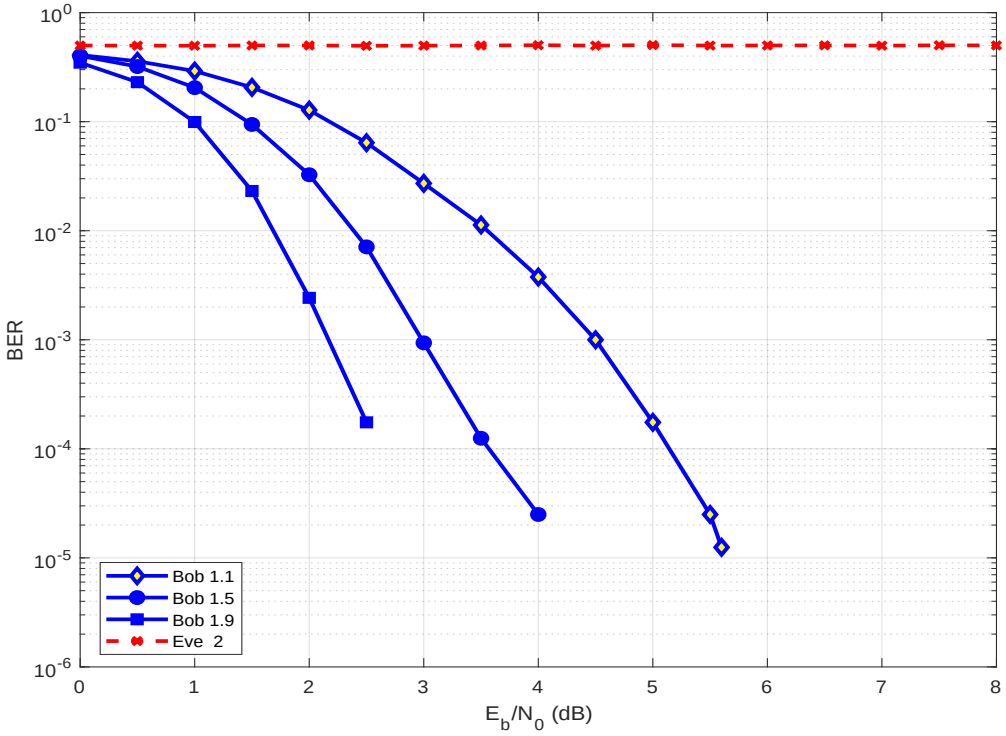

Figure 4.10: BER performance of DE-constructed polar codes on wiretap channel, where the main channel is impulsive with different values of α (1.1, 1.5 and 1.9) and the eavesdropper channel is Gaussian.

In Fig. 4.10, the polar code constructed using DE is transmitted over an AWGN channel to Eve while Bob's channel has varying levels of impulsiveness, with $\alpha = 1.1$, $\alpha = 1.5$ and $\alpha = 1.9$. In Fig. 4.11 we considered both main channel ($\alpha = 1$ and $\alpha = 1.5$) and eavesdropper channel ($\alpha = 1.9$) as impulsive noise channels, where the former is more impulsive than the latter. This means that in both figures the main channel is more impulsive than the eavesdropper's channel. Figs. 4.10 and 4.11 show the simulated performance of Bob and Eve for different wiretap channels. We observe that with different values of α, the BER of Bob approaches zero with increasing SNR, however most importantly the BER of Eve is very close to 0.5 at all SNRs. This shows that the proposed physical layer security scheme

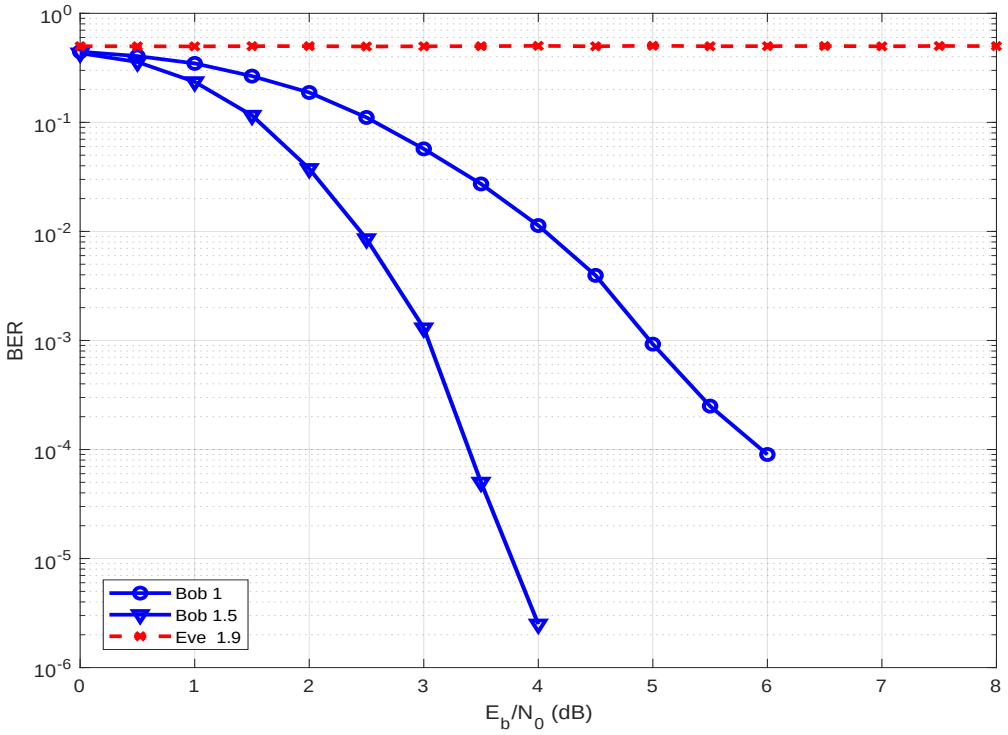

Figure 4.11: BER performance of DE-constructed polar codes on wiretap channel, where the main channel is impulsive with different values of α (1, 1.5) and the eavesdropper channel is slightly impulsive with α=1.9.

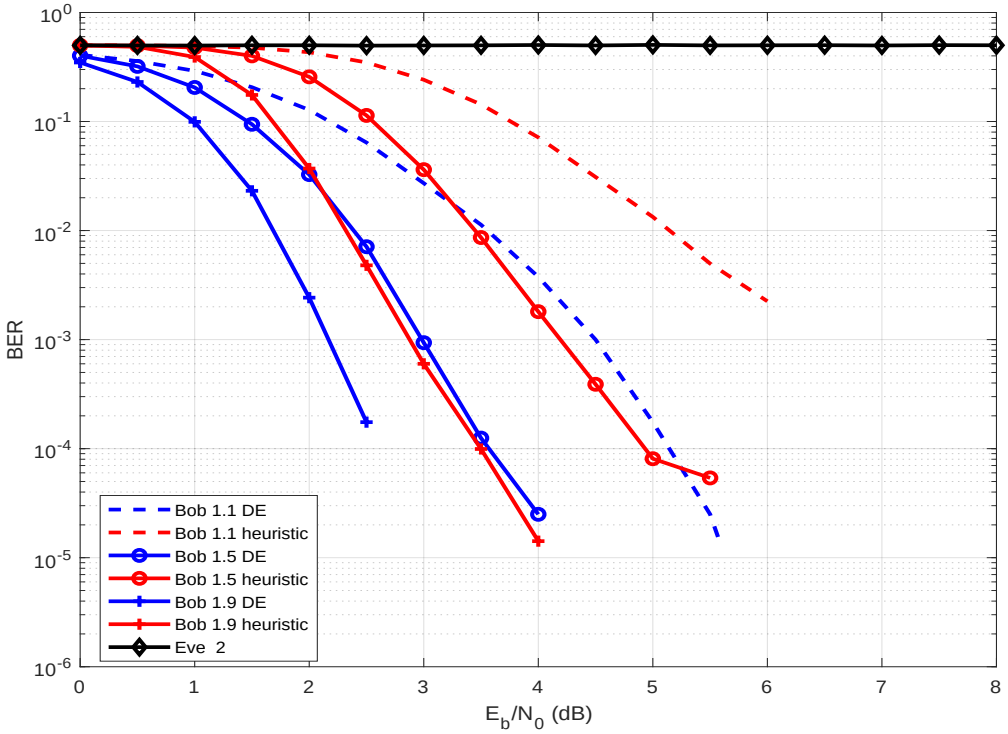

Figure 4.12: BER performance of heuristic-constructed and DE-constructed polar codes on wiretap channel, where the main channel is impulsive with different values of α (1.1, 1.5 and 1.9) and the eavesdropper channel is Gaussian.

using DE-constructed polar codes can still achieve excellent performance and secure communication, even when the main channel is more impulsive than the wiretap channel. As shown in Fig. 4.12, we also compare the performance of DE and heuristic construction methods for different values of α on wiretap channel, where the main channel is impulsive with different values of α (1.1, 1.5 and 1.9) and the eavesdropper channel is Gaussian. Compared with Fig. 4.9, the performance of the DE-based construction is much better than the heuristic method due to the smaller R_s of the DE-based construction polar codes.

After reviewing the literature, we observed that previous work on error-correcting codes and physical layer security has assumed a wiretap channel where each user experiences Gaussian noise, but this chapter presents the first results evaluating the performance of polar codes on wiretap channels where both the intended recipient and eavesdropper experience varying levels of impulsive noise. Simulation results show that DE-based construction of polar codes combined with physical layer security still achieve high security and performance in the present of impulsive noise.

4.6 Conclusion

In this chapter, we have examined the performance of polar codes combined with physical layer security on different type of wiretap channels. A secure construction of polar codes has been proposed that provides a good performance and security, even when the eavesdropper channel is better than the main channel. In addition, a DE design of the polar codes on SαS channels was presented. Moreover, simulation results of construction of polar codes combined with physical layer security on impulsive noise channels have been presented to validate the DE analysis.

The simulated results show that the proposed polar coding scheme can achieve near-optimal performance with only the knowledge of the design-SNR values on degraded Gaussian and non-degraded Gaussian wiretap channels. We also observe that without constructed polar codes, security and reliability can only be achieved within a limited values of SNRs when Bob's channel condition is better than Eve's channel. However, in real communication we cannot guarantee that, and Eve could have a better channel than Bob. We can conclude that the proposed polar construction is a good choice for Gaussian wiretap channels.

In order to better examine the secure performance of polar codes in more gen-

eral memoryless channels which we are focus on in our work we have shown the BER performance of polar codes constructed by DE and heuristic methods on SαS channels for various values of α. We observed that DE constructed polar codes have better performance than heuristic constructed polar codes on impulsive channels. That means DE can be used to design optimal polar codes in the present of SαS noise. We also presented the construction of polar codes using DE on a wiretap channel with varying levels of impulsive noise and provided simulation results from Fig. 4.10 to Fig. 4.12 showing the BER performance and security of the system. These appear to be the first results evaluating the performance of polar codes combined with physical layer security when the noise is impulsive. Most importantly, it was shown that polar codes can still ensure a secure channel between Alice and Bob at all SNRs, even when the main channel is more impulsive than the eavesdropper's channel. This was a surprising result and shows that polar codes are a good candidate for achieving secure communication systems in more harsh environments where impulsive noise is present.

Chapter 5

Frozen Bit Selection Scheme for Polar Coding Combined with Physical Layer Security in the Presence of Impulsive Noise

5.1 Introduction

In chapter four, the BER performance of polar codes constructed by DE and heuristic methods on additive impulsive noise channels was presented. The simulation result showed that when the impulsive noise is modelled by SαS distributions the performance of DE-constructed polar codes perform better than polar codes constructed by the heuristic method. Also the security performance of polar codes constructed by DE and heuristic method on a wiretap channel with varying levels of SαS noise was presented. All the simulation results show our proposed polar coding scheme can achieve secure and reliable communication. However, there is a trade-off between secrecy code rate and system security performance.

In this chapter, in order to increase the secrecy code rate we consider the effect of frozen bits on polar coding performance. Here, we propose a secure polar coding scheme with aided Automatic Repeat Request (ARQ), in which the frozen bits are obtained from the feedback of the legitimate receiver. First we evaluate the BER performance of polar codes constructed by the heuristic method on Gaussian noise channels and polar codes constructed by DE on impulsive noise channels with one

bit error in the frozen bits. Based on the polar codes BER performance with one bit error in a frozen bit we select the "optimal" frozen bits to reduce the computational cost of ARQ between Bob and Alice, and evaluate the performance of the security on channels with AWGN and symmetric α-stable noise.

5.2 System Model

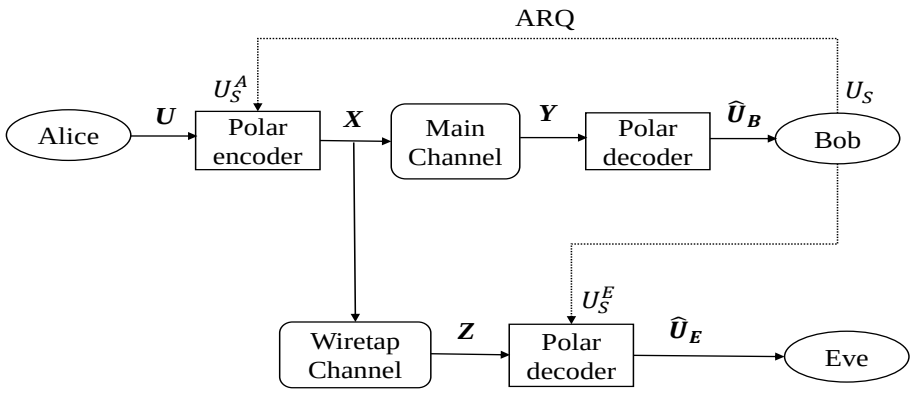

Figure 5.1: Diagram of the proposed polar coding structure.

In Fig. 5.1, a diagram of the proposed polar coding structure is illustrated, where legitimate users Alice and Bob communicate with each other. Alice sends a K-bit secret message $\mathbf{U}$ to a legitimate receiver Bob through the forward main channel in the presence of an eavesdropper Eve. The codeword $\mathbf{X}$ after polar encoding is transmitted across the main channel and eavesdropped by Eve, resulting in the corresponding received signals $\mathbf{Y}$ and $\mathbf{Z}$ which decode into the estimates $\hat{\mathbf{U}}_B$ and $\hat{\mathbf{U}}_E$ of the original message detected by Bob and Eve. In addition, before Alice sends $\mathbf{U}$ to Bob, Bob send $\mathbf{U}_S$ which contains $N-K$ random bits to Alice which are used as frozen bits for Alice. Thus there is a feedback channel between Bob and Eve and an ARQ protocol is used to enhance communication security, by Cyclic Redundancy Check (CRC) and retransmissions. However, because of the openness of the wireless channel, Eve can also eavesdrop information $\mathbf{U}_S^E$ from the feedback channel and set it as the frozen bits for her decoder.

ARQ is a simple error-control method for data transmission, widely used due to the advantage of providing high system reliability [85,86]. In the ARQ scheme, only the intended recipient can request retransmission. Thus, when Bob sends information to Alice, if there are errors in the received signals, they can be detected by

CRC, Alice will ask for retransmission until there are no errors. However, Eve does not have the access to require retransmission, so we can assume beaming forming and artificial noise [87], [88] to increase the errors for Eve. Here we need to explain that additional CRC and ARQ will increase the complexity.

5.3 Proposed Coding Method

As mentioned in chapter 4, the polar coding scheme proposed by Mahdavifar and Vardy [31] divided the polarized channels into different parts to transmit information bits with bit-channels good for Bob but bad for Eve, random bits on bit-channels good for both Bob and Eve and zeros on the remaining bit-channels. This method can achieve the secrecy capacity but with a trade-off in secrecy rate. In this scheme, the polar codeword with code length N is split into three parts: information bits with length S, random bits with length L and frozen bits length M, where $S+L+M = N$. The secrecy rate is defined as the message length divided by the codeword length: $R_s = S/N$, but this was very low due to large number of random bits required. Ideally we would like the secrecy rate to be equal to the code rate of a conventional polar code with code rate $R_c = K/N = 0.5$. Hence, in this chapter we consider the polar coding scheme from the aspect of the decoding process instead of polar codes construction or encoding process. By applying this method we use all the $K = N/2$ bit channels to transmit information to increase the secrecy code rate $R_s = R_c = 0.5$.

We observe that in the process of polar codes decoding, the information bits are decoded sequentially and the frozen bits play an important role when decoding the information bits. If the previous detected estimates $\hat{u}_1^{i-1}$ have errors in the frozen bits then the $L_N^{(i)}(y_1^N, \hat{u}_1^{i-1})$ in (3.49) is unreliable, which will lead to the incorrect decoding of the information bits. In [33], the authors use this idea to design an ARQ-aided polar coding scheme. Inspired by their works we propose a more efficient ARQ-aided polar coding scheme combined with physical layer security on impulsive noise channels. In [33], all random frozen bits are fed back to Alice, which reduces the efficiency of this scheme. However, we will show that the same level of security can still be achieved if only a small proportion of the random frozen bits is fed back, which increases efficiency.

5.3.1 Coding Scheme on AWGN Wiretap Channel System

In this section we will first evaluate the BER performance of the polar codes with a single error in the frozen bits on the AWGN channel in Fig. 5.2, where the SNR is 3dB. In addition, in order to compare with the original work we use a binary polar code with code length $N = 512$, code rate $R_c = 0.5$ and SC decoder is for the process of decoding. From the simulation result we can observe that a signal error in frozen bits has a serious effect on polar decoding.

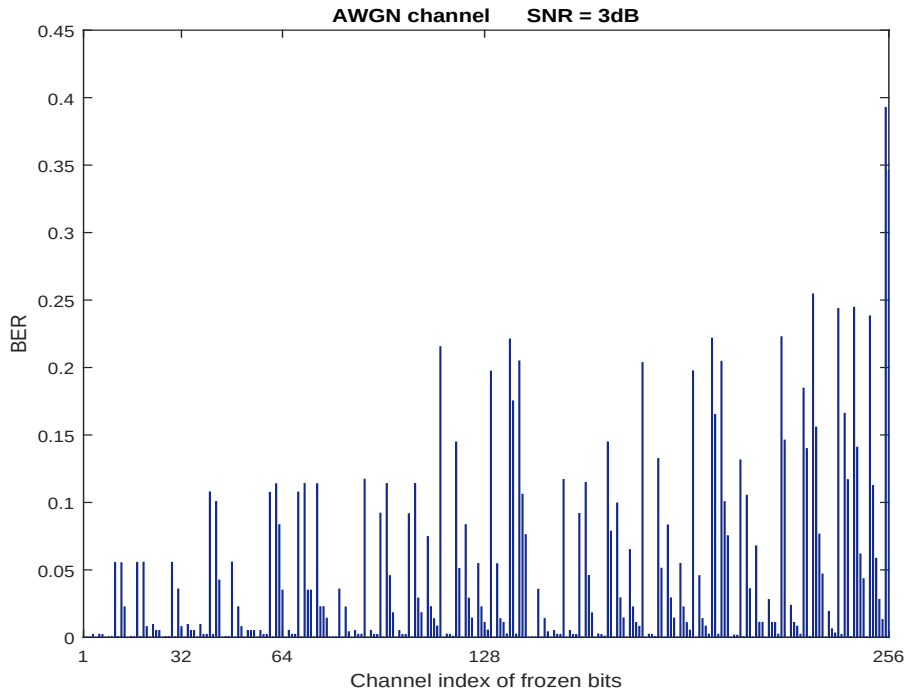

Figure 5.2: BER performance of polar codes with one bit error in frozen bits with AWGN.

According to the BER results in Fig. 5.2 and previous discussion our ARQ-aided polar coding scheme to achieve the reliable and secure communication between legitimate users Alice and Bob can be described as follows.

ARQ Channel: Before Alice sends confidential information, Bob transmits a S-bit ($S = 32$) random sequence U_s to Alice. However, due to the openness of wireless communications Eve can also access this, resulting in the random sequences U_S^A and U_S^E received by Alice and Eve respectively. By applying a CRC code and retransmission on the ARQ channel we can make sure U_S^A is the same as U_S. Although Eve may know the indices of frozen bits, we can assume beaming forming and artificial noise [87], [88] to increase the errors in U_S^E for Eve, i. e. $P_r\left\{U_s^E \neq U_s\right\} \rightarrow 1$.

Selection of frozen bit channels for U_s^A:

- For a N length polar code, set the $N-K$ frozen bits as random bits (0,1).
- Flip each of the $N-K$ frozen bits individually and evaluate the BER performance of each of the $N-K$ scenarios on the AWGN channel.
- Choose the largest $S \leq (N-K)$ BERs, and save the corresponding frozen bit channels P.
- Assign the random bits which Bob sent to Alice to the set of P frozen bits and set the others to 0.

Encoding: Alice uses the K information bit channels to send secure messages, takes the U_s^A as a part of the frozen bits to encode at the polar encoder and other frozen bits are set as zeros. After polar encoding, the codeword is transmitted to Bob via the AWGN channel, but it also can be received by Eve through the AWGN eavesdropper channel.

Decoding: For the process of SC decoding, Bob use the the sequence where U_s^A is a part of the frozen bits, but for Eve's decoder the received sequence contains U_s^E.

5.3.2 Coding Scheme on SαS Noise Wiretap Channel System

We first show the BER performance of the polar codes with single errors in the frozen bits on SαS noise (α=1.3) channel in Fig. 5.3. In order to get the optimal performance on impulsive noise channels, density evolution is applied to construct the polar codes which was proposed in [89]. From Fig. 5.3 we can observe the effect on the BER for each flipped frozen bit in the binary polar codewords, where code length $N = 512$, code rate $R = 0.5$. Our proposed coding scheme for wiretap channel system with SαS noise is shown as follows:

ARQ Channel: Before Alice sends confidential information, Bob transmits a S-bit random sequence U_s to Alice.

Selection of frozen bit channels for U_s^A:

- Construct a N length polar code by DE and set the $N-K$ frozen bits as random bits (0,1).

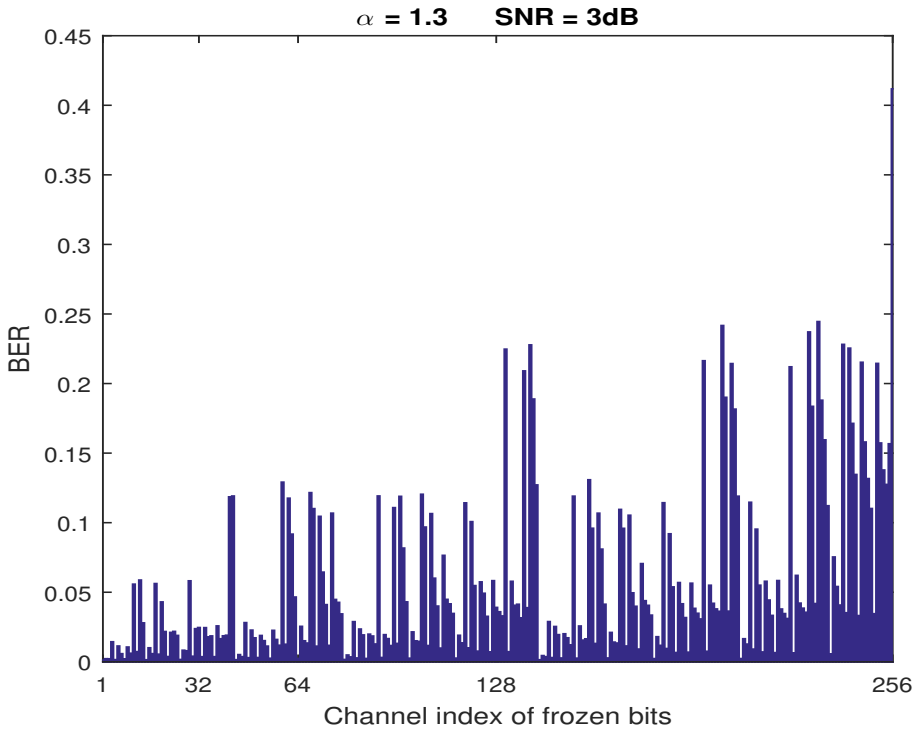

Figure 5.3: BER performance of polar codes with one bit error in frozen bits with SαS noise.

- Flip each of the $N-K$ frozen bits individually and evaluate the BER performance of each of the $N-K$ scenarios in the present of impulsive noise with SαS distribution.
- Choose the largest $S \leq (N-K)$ BERs, and save the corresponding frozen bit channels P.
- Assign the random bits U_s^A received by Alice from Bob which is free of errors to the set of P frozen bits and set the others to 0.

5.4 Analysis

5.4.1 Reliability

We assume that the communication between Alice and Bob is under the condition that the frozen bits are error-free. From [90] the following propositions of rate of polarization are presented:

Proposition 3: For a B-DMC channel W. For any constant rate $R < I(W)$

and positive fixed $\beta < 1/2$, there must exists a sequence of sets A_N with $A_N \subset 1, 2, \ldots, N$, $|A_N| \geq NR$, and

$$\sum_{i \in A_N} Z(W_N^{(i)}) = o(2^{-N^\beta}). \tag{5.1}$$

Contrary, if $R > 0$ and $\beta > 1/2$, a sequence of sets A_N, where $A_N \subset 1, 2, \ldots, N$, $|A_N| \geq NR$, we obtain:

$$\max \left\{ Z(W_N^{(i)}) : i \in A_N \right\} = w(2^{-N^\beta}). \tag{5.2}$$

As a corollary, Theorem 3 in [18] is strengthened to:

Proposition 4: For a B-DMC W with polar coding at any constant rate $R < I(W)$ and arbitrary fixed $\beta < 1/2$, we have

$$P_e(N, R) = o(2^{-N^\beta}), \tag{5.3}$$

where $P_e(N, R)$ is block error probability for polar coding which is under SC decoding. Then we have

$$P_e(\hat{U} \neq U) \leq Z(W_N^{(i)}) \leq o(2^{-N^\beta}). \tag{5.4}$$

It is easy to see that $\lim_{N \to \infty} P_e(\hat{U} \neq U) = 0$, such that the reliability condition required in (3.12) can be satisfied.

5.4.2 Security

In [91], the authors first apply iterations of the Bhattacharyya parameter to obtain the expression of the Bhattacharyya parameter bound. According to this, [33] proposed the following theorem

Theorem 3: For a bit-channel $W_N^{(i)}$ $(0 < i \leq N)$ and a fixed $\lambda \in [0, 1]$, if there exists a parameter group $\varrho_1^i, \varrho_2^i, \cdots, \varrho_N^i$, $(\varrho_j^i \in [0, 1], 0 < j \leq N)$ that satisfies at least two of $Z(W_1^{(1)}) \geq \varrho_1^i, Z(W_1^{(2)}) \geq \varrho_2^i, \cdots, Z(W_1^{(N)}) \geq \varrho_N^i$, then

$$I(W_N^{(i)}) \leq \lambda, \tag{5.5}$$

where the ith use of a physical channel is described by $W_1^{(i)}$ $(1 \leq i \leq N)$.

Proof: Let us define the function $f(\rho) = \sqrt{1-\rho^2}$, $\rho \in [0,1]$, where f is the monotonic decreasing function of ρ and $f(\rho) \in [0,1]$. Hence for a fixed $\lambda \in [0,1]$, there must exist $\rho = \vartheta \in [0,1]$ that satisfies $f(\vartheta) = \sqrt{1-\vartheta^2} = \lambda$. Let $Z^l(W_N^{(i)})$ denote the lower bound on $Z(W_N^{(i)})$ [91].

$$Z^l(W_N^{(i)}) = g^l_{(N,i)}(Z(W_1^{(i)}), \cdots Z(W_1^{(N)})). \tag{5.6}$$

As $Z(W_N^{(i)})$ is a monotonic increasing function of $Z(W_1^{(i)}), \cdots Z(W_1^{(N)})$, we can conclude that $Z(W_1^{(1)}) = \varrho_1^i, Z(W_1^{(2)}) = \varrho_2^i, \cdots, Z(W_1^{(N)}) = \varrho_N^i$, thus $Z^l(W_N^{(i)}) = \vartheta$. Due to the monotonic behaviour of $Z^l(W_N^{(i)})$, if $Z(W_1^{(1)}) \geq \varrho_1^i, Z(W_1^{(2)}) \geq \varrho_2^i, \cdots, Z(W_1^{(N)}) \geq \varrho_N^i$ we have $Z^l(W_N^{(i)}) \geq \varrho$. According to [18], $I(W_N^{(i)}) \leq \sqrt{1-Z(W_N^{(i)})^2}$, we can have $I(W_N^{(i)}) \leq \sqrt{1-Z^l(W_N^{(i)})^2}$. Then

$$I(W_N^{(i)}) \leq \sqrt{1-Z^l(W_N^{(i)})^2} \leq \sqrt{1-\vartheta^2} = \lambda. \tag{5.7}$$

For Eve, Theorem 3 shows that given λ, $I_E(W_N^i) \leq \lambda$ can be obtained by changing $Z(W_1^{E(1)}), Z(W_1^{E(2)}), \cdots, Z(W_1^{E(N)})$. For BSC, $Z(W_1^{E(i)}) = 2\sqrt{\varphi_E^i(1-\varphi_E^i)}$, φ_E^i is the crossover probability of the ith use of the channel [18]. To make the value $Z(W_1^{E(i)})$ increase, in the proposed coding scheme, more errors in frozen bits of Eve will make the channel between Bob and Eve become worse, which leads to φ_E^i having a larger value, and $Z(W_1^{E(i)})$ become larger. Hence we have

$$\begin{aligned} &I(u_1^K; z_1^N) = I(u_{\mathrm{A}}; z_1^N) \\ &\overset{(i)}{\leq} \sum_{i \in \mathrm{A}} C(W_N^{E(i)}) \overset{(ii)}{=} \sum_{i \in \mathrm{A}} I(W_N^{E(i)}) \overset{(iii)}{\leq} |\mathrm{A}|\lambda. \end{aligned} \tag{5.8}$$

The inequality (i) is obtained from Shannon's theory of channel capacity. The equality (ii) $C(W_N^{E(i)}) = I(W_N^{E(i)})$ is proven in [18], [31]. Inequality (iii) is obtained from Theorem 3. From (5.8), we have $|A| \leq N$, and when $\lambda = o\frac{1}{N}$, we have

$$\lim_{N\to\infty} I(u_1^K;\ z_1^N) \leq \lim_{N\to\infty} |\mathrm{A}|\lambda = 0, \tag{5.9}$$

which indicates that the proposed scheme can satisfy the security condition given in (3.13).

5.4.3 Secrecy Capacity

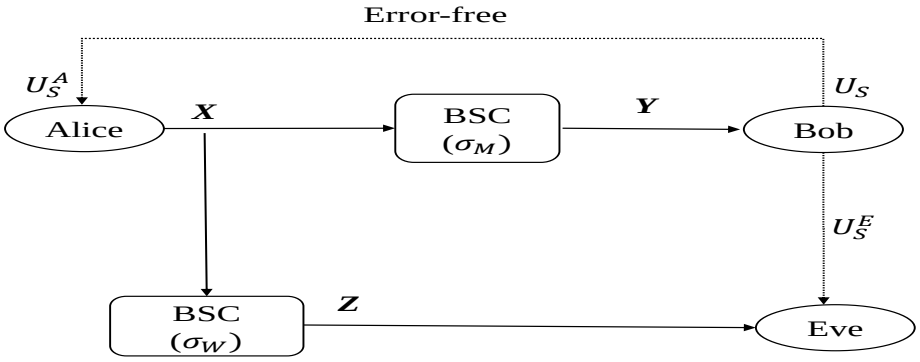

Figure 5.4: A simplified system model of the proposed polar coding scheme.

In order to analyze the achievable secrecy capacity of the proposed secure coding scheme, a simplified system model is shown in Fig. 5.4, in which both the main channel and eavesdropper channel are assumed as BSCs. Here, σ_M and σ_W represent the crossover probability of the main channel from Alice to Bob and the eavesdropper's channel Alice to Eve,respectively, and the crossover probability of the feedback channel from Bob to Alice and Bob to Eve are denoted by φ_M and φ_W, respectively. Variables σ and φ satisfy an increasing function $\phi(\sigma, \varphi)$, which describes the crossover probability of the channel combining the forward channel and feedback channel, and $\phi \in \left[0, \frac{1}{2}\right]$. Thus the channel condition of communication between Alice and Bob can be performed by $\phi(\sigma_M, \varphi_M)$, and $\phi(\sigma_W, \varphi_W)$ corresponds to Alice and Eve. Here, we assume the eavesdropper channel is the same condition as the main channel, such that $\sigma_M = \sigma_W$. The ARQ channel from Bob to Alice is able to obtain an channel that is error-free, which means $\varphi_M = 0$, while $\varphi_W > 0$. Based on the previous statement, it is clear that the channel condition between Alice and Bob is better than that between Alice and Eve, in such case $\phi(\sigma_M, 0) < \phi(\sigma_W, \varphi_W)$. For a BSC, the channel capacity can be represent as $C(W) = 1 - h(p_w)$, where $h(\cdot)$ is the binary entropy function and p_w is the crossover probability of channel W, $h(p_w = -p_w \log(p_w) - (1 - p_w) \log(1 - p_w)$, then we have

$$C_M(W) = 1 - h(\phi(\sigma_M, 0)), \tag{5.10}$$

$$C_W(W) = 1 - h(\phi(\sigma_M, \varphi_W)). \tag{5.11}$$

As $\phi(\sigma_M, 0) < \phi(\sigma_W, \varphi_W \leq \frac{1}{2}$ and $h(\cdot)$ is increasing from 0 to $\frac{1}{2}$, hence we obtain $C_M(W) > C_W(W)$. In addition, we suppose $U_S^A = U_S, U_S^E = \hat{U}_S$ and according to

(3.15), the secrecy capacity of our proposed polar coding scheme is:

$$\begin{aligned} C_s &= \max\{C_M(W) - C_W(W), 0\} \\ &= \max\left\{I(U;Y|U_S^A) - I(U;Y|U_S^E), 0\right\} \\ &= \max\left\{I(u_1^K;y_1^N|U_S) - I(u_1^K;Z_1^N|\hat{U}_S), 0\right\}. \end{aligned} \tag{5.12}$$

Although the main channel and eavesdropper channel have the same channel condition, Eve's feedback channel is worse than Bob's, thus it is obvious we can obtain $C_s > 0$. The error rate of U_S^E is defined as follow:

$$P_e^c = \frac{1}{m}\sum_{l=1}^{m} P_e\left\{u_{s,l}^e \neq u_{s,l}\right\}, \tag{5.13}$$

where $u_{s,l}^e$ and $u_{s,l}$ is the lth bit of U_s^E and U_S. It is clear that P_e^c has an effect on the secrecy capacity. Here we consider a special case, where we assume there is a P_e^c which make Eve's BER approach to 0.5 using frozen bits with errors, so $I(u_1^K;Z_1^N|\hat{U}_S) = 0$. In this case, the maximum secrecy capacity $C_s = C_M(W)$ can be achieved.

5.5 Results and Discussion

In this section, the BER performance of polar codes combined with physical layer security on the AWGN channel and the SαS impulsive noise channel is presented.

5.5.1 Performance of Proposed Coding Scheme on AWGN Wiretap Systems

Figs. 5.5 to 5.7 show the simulation performance of Bob and Eve on AWGN wiretap channel systems for different values of SNR gaps, SNR_g. The random bits Bob send to Alice have length $S = 32$. The polar codes employed have a code rate of 0.5, code length $N = 512$ and BPSK modulation. The polar codes are constructed by the heuristic method and SC decoders are applied to recover the information messages. In Fig. 5.5 we set $SNR_g = 0$, such that the main channel and the wiretap channel have the same level of noise. The probability that $U_S^E \neq U_S$, P_e^c can be interpreted as the average number of bit errors in the random sequence U_S^E obtained by Eve. We

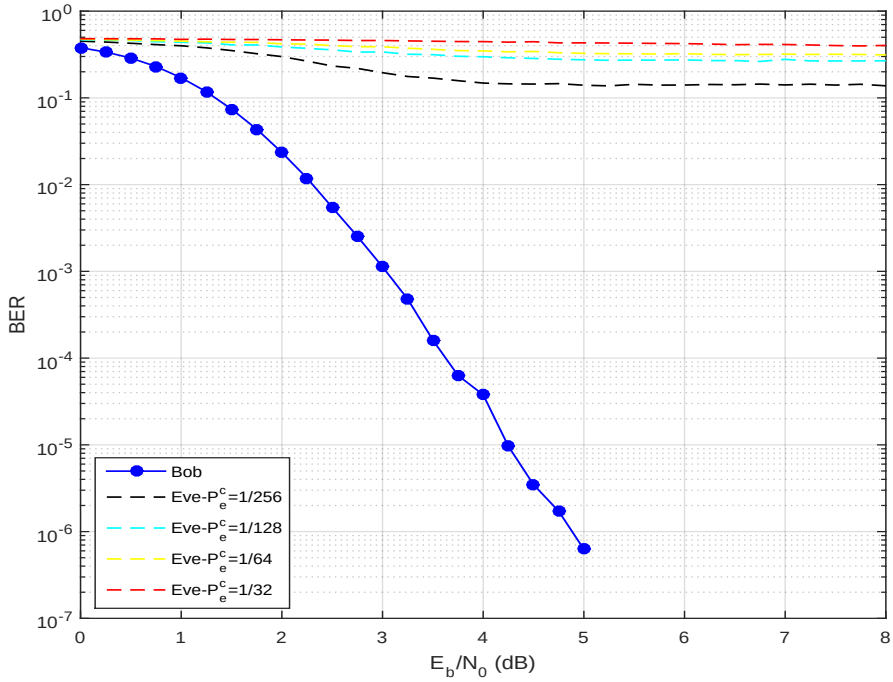

Figure 5.5: BER performance of proposed coding scheme, where the main channel and wiretap channel are both AWGN channels, where $SNR_d = 0dB$.

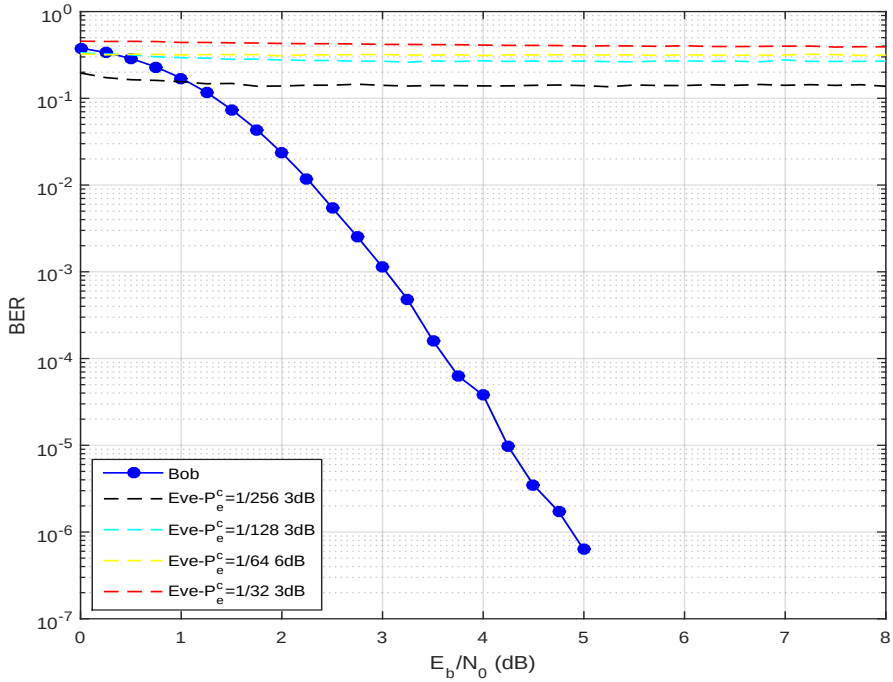

Figure 5.6: BER performance of proposed coding scheme, where the main channel and wiretap channel are both AWGN channels, where $SNR_g = -3dB$.

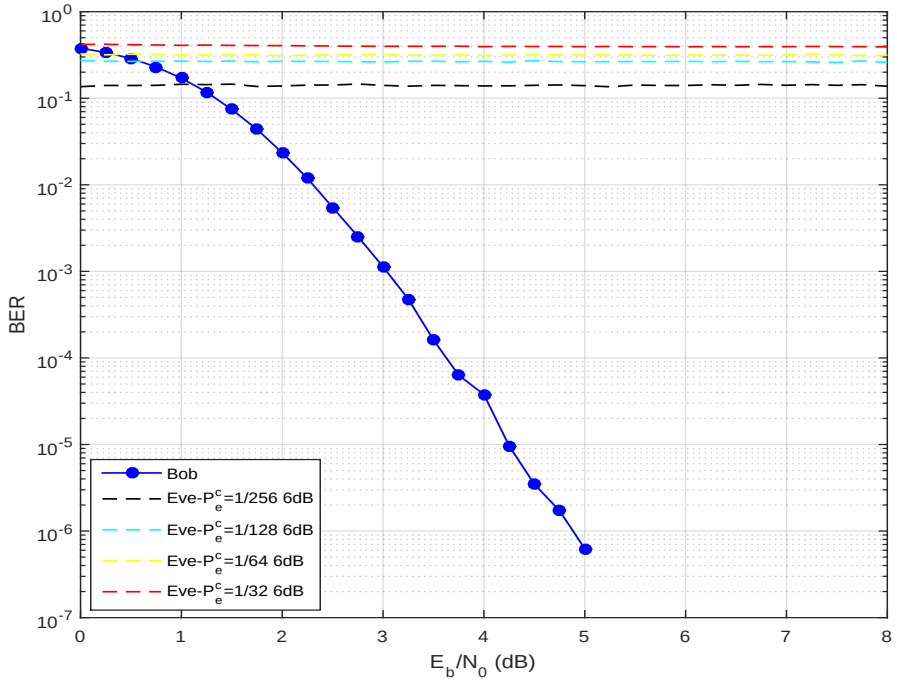

Figure 5.7: BER performance of proposed coding scheme, where the main channel and wiretap channel are both AWGN channels, where $SNR_g = -6dB$.

can see when $P_e^c = 1/256$, there is only one error in the frozen bits of Eve's decoder, however the BER is always higher than 0.13. In addition with P_e^c increased to 1/32 the BER of Eve approaches 0.5. As for Bob, as the SNR increases, the BER of Bob approaches zero. This means our proposed scheme can obtain secure and reliable communication between Alice and Bob. In Fig. 5.6 and 5.7 the SNR_gs are -3dB and -6dB respectively. In these case the wiretap channels are non-degraded. Hence, when the eavesdropper channel is better than the main channel, our proposed scheme still works. In [33], all random frozen bits are fed back to Alice, which reduces the efficiency of this scheme. However, we show that the same level of security can still be achieved if only a small proportion of the random frozen bits is fed back, which increases efficiency.

5.5.2 Performance of Proposed Coding Scheme on Wiretap Systems with SαS Noises

For Figs. 5.8 to 5.13 a polar code with block length $N = 512$ and code rate 0.5 is constructed using DE. The random bits length from the feedback channel is still $S = 32$.

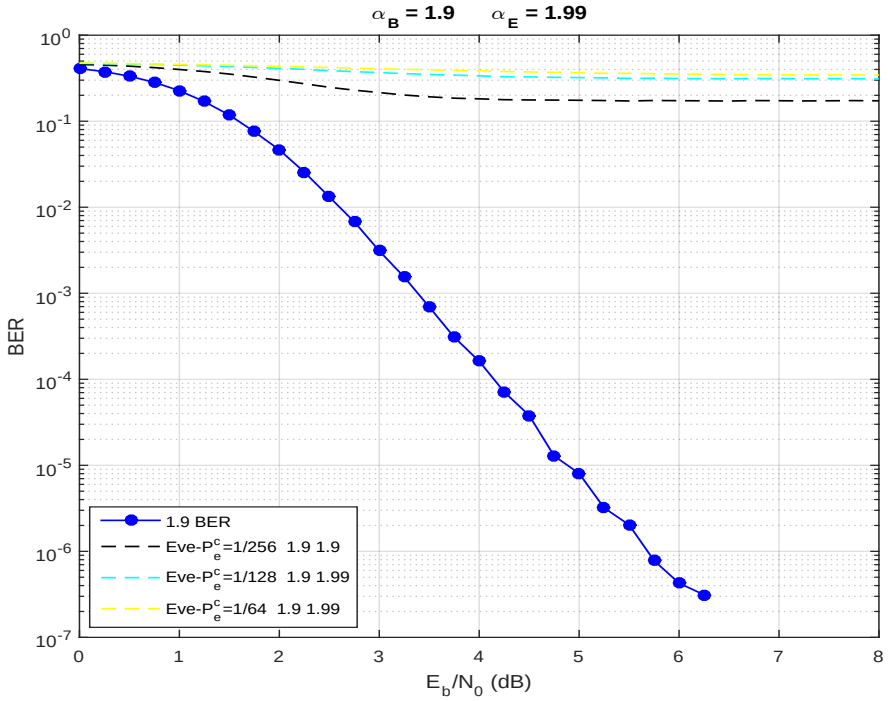

Figure 5.8: BER performance of proposed coding scheme, where the main channel ($\alpha_B = 1.9$) is worse than the wiretap channel ($\alpha_E = 1.99$).

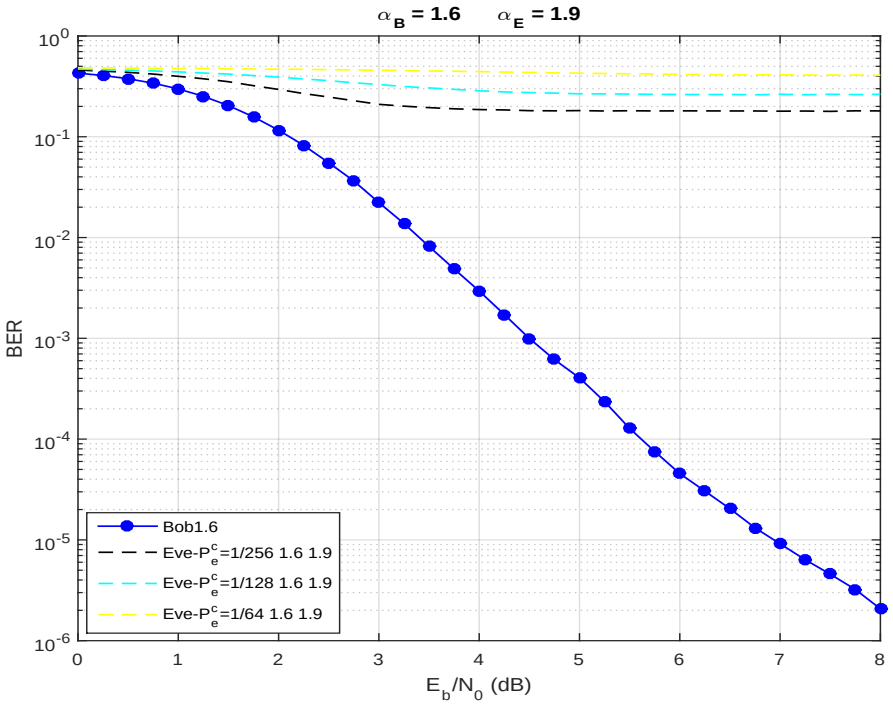

Figure 5.9: BER performance of proposed coding scheme, where the main channel ($\alpha_B = 1.6$) is worse than the wiretap channel ($\alpha_E = 1.9$).

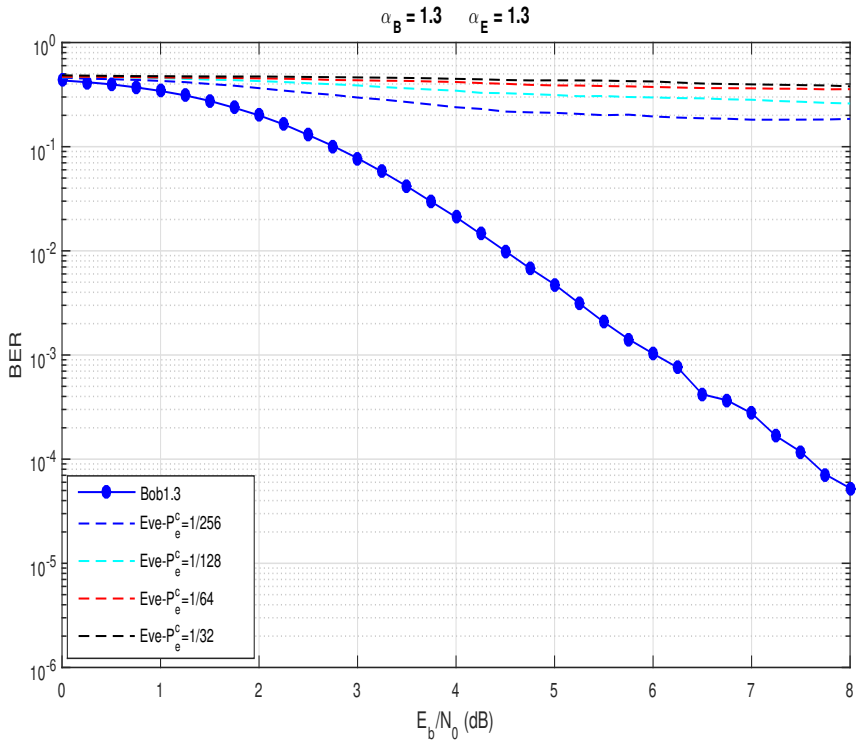

Figure 5.10: BER performance of proposed coding scheme, where the main channel and wiretap channel have the same value of $\alpha_B = \alpha_E = 1.3$.

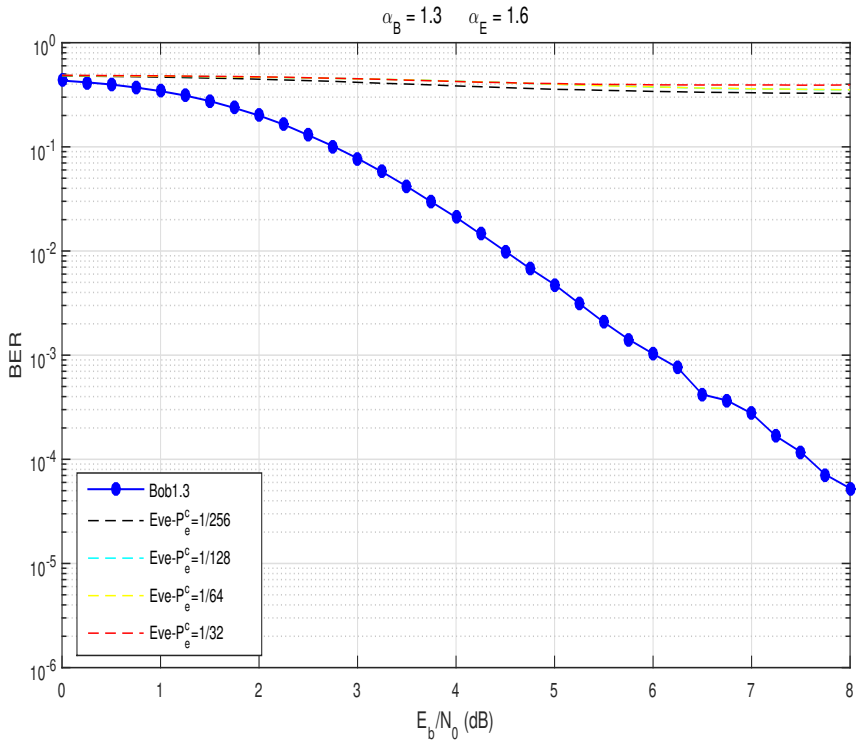

Figure 5.11: BER performance of proposed coding scheme, where the main channel ($\alpha_B = 1.3$) is worse than the wiretap channel ($\alpha_E = 1.6$).

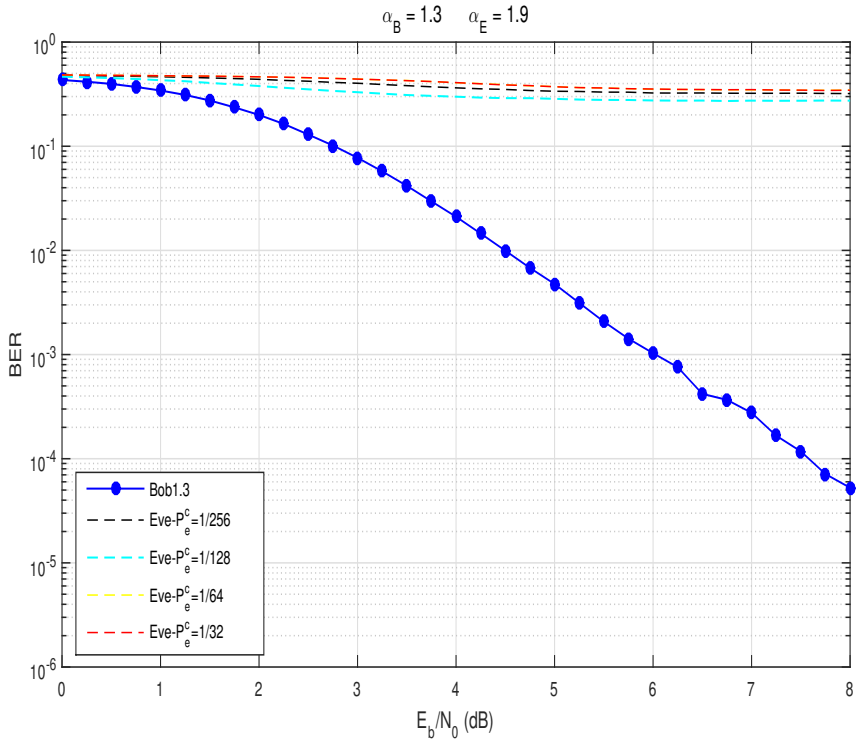

Figure 5.12: BER performance of proposed coding scheme, where the main channel ($\alpha_B = 1.3$) is impulsive than the wiretap channel ($\alpha_E = 1.9$).

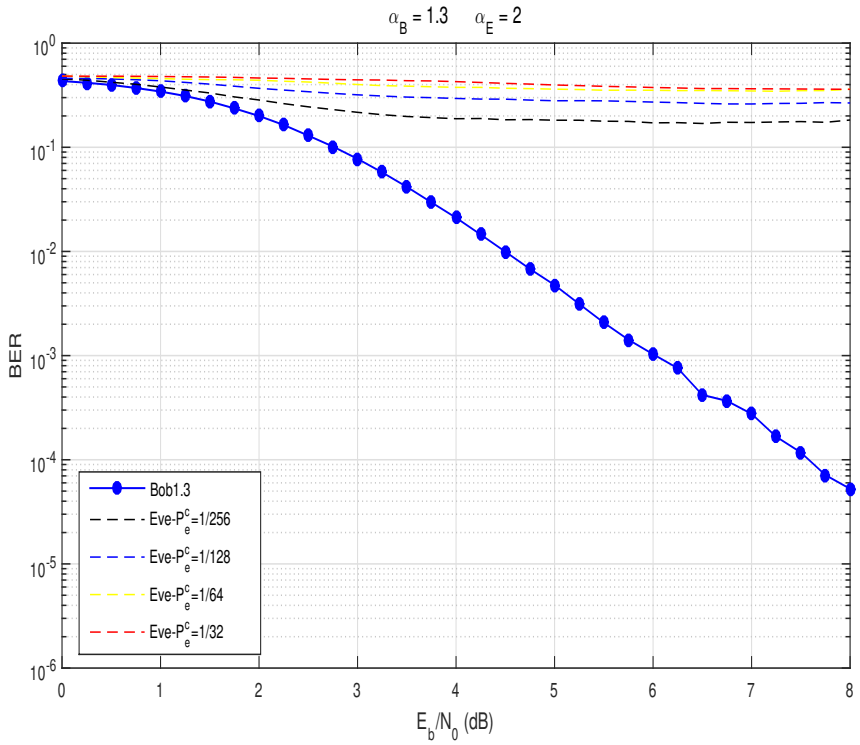

Figure 5.13: BER performance of proposed coding scheme, where the main channel is impulsive channel ($\alpha_B = 1.3$) and the wiretap channel is AWGN channel.

In Fig. 5.8, the polar code is transmitted over a slightly impulsive channel $\alpha_B = 1.9$, and the eavesdropper channel is better with $\alpha_E = 1.99$. In Fig. 5.9 we consider a more impulsive noise channel system ($\alpha_B = 1.6, \alpha_E = 1.9$). In Fig. 5.10, the polar code is transmitted over an extremely impulsive channel ($\alpha_B = \alpha_E = 1.3$) on Bob and Eve's channel. In Fig. 5.11 and Fig. 5.12 we consider the main channel to be more impulsive than the wiretap channel and in Fig. 5.13 we consider a special case, in which only the eavesdropper channel is AWGN. This means that in both figures the main channel is more impulsive than the eavesdropper's channel.

We observe that the BER of Bob approaches zero with increasing SNR and for all values of α, but most importantly the BER of Eve is very close to 0.5 with increasing value of P_e^c. We can observe from Fig.s 5.10 to 5.13 that even when $P_e^c = \frac{1}{256}$, the BER performance of Eve is still close to 0.5. This shows that the proposed joint polar coded physical layer security scheme using ARQ with selected frozen bits can achieve excellent security, even when the main channel is more impulsive than the wiretap channel. Most significantly, this work shows that we have increased the effectiveness of the ARQ protocol proposed by [33].

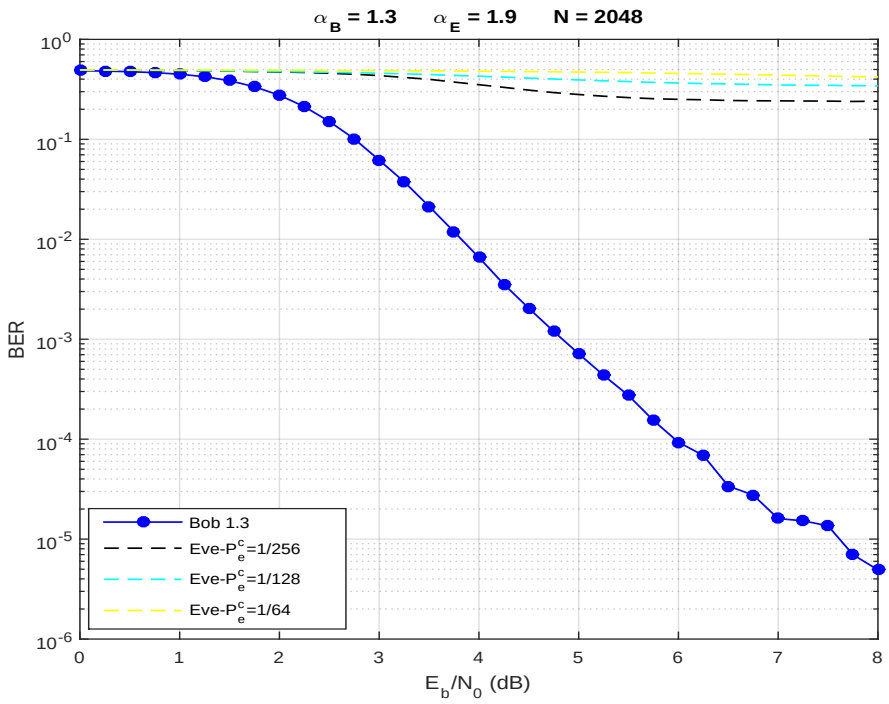

Figure 5.14: BER performance of proposed coding scheme, where the main channel ($\alpha_B = 1.3$) is impulsive than the wiretap channel ($\alpha_E = 1.9$), the length of polar codes is $N = 2048$.

Moreover, to prove that our proposed scheme is able to achieve secure and reliable

communication in polar codes with larger code length and to verify it increase the secrecy rate to 0.5 which is larger than chapter 4 we give the simulation results in Fig. 5.14 for a polar code with code length $N = 2048$ and code rate 0.5 constructed using DE and transmitted over an impulsive channel ($\alpha_B = 1.3$) from Alice to Bob, while the wiretap channel is less impulsive with $\alpha_E = 1.9$.

5.6 Conclusion

In this chapter, we have proposed a frozen bit selection scheme for polar codes combined with physical layer security in the presence of AWGN noise and impulsive noise. By flipping certain frozen bits we can maximise the BER performance of the eavesdropper's channel, ensuring that no information can be obtained from the communication between the legitimate users. An ARQ scheme is utilized to feedback random frozen bits from Bob to Alice without errors, which feeds back only a small proportion of the random frozen bits to Alice, unlike [33] where all random frozen bits are fed back. This increases the secrecy rate significantly. Simulation results show that the BER of Eve is always close to 0.5 even if there is only a single bit error in Eve's received frozen bits obtained from Bob. However, the BER of Bob is unaffected even when Bob's channel is more impulsive than Eve's channel. This chapter has shown that our proposed work can ensure excellent security on different impulsive noise channels, while significantly increasing the secrecy rate so that it matches the code rates of conventional polar codes.

Here we explain the complexity and practical limitations caused by ARQ. As we noted, ARQ can obtain a 3dB gain in performance, while complexity doubles with each retransmission. In real communication, if channel conditions are too poor, retransmissions cannot guarantee accuracy, which will cause decoding errors. In order to ensure correctness, random bits need to retransmit several times, so the delay is too large. In our work, we use ARQ to ensure random information which Bob sends to Alice is error free, so we do not need to consider the ARQ protocol in detail.

Chapter 6

Performance of Rate-compatible Polar Codes on Wiretap Channels with Impulsive Noise

6.1 Introduction

In chapter four, we have shown the BER performance of DE-constructed and heuristic constructed polar codes on SαS channels for various values of α. We also examined the construction of polar codes using DE and a heuristic method on the wiretap channel in the presence of impulsive noise with SαS distributions. These appear to be the first results evaluating the performance of polar codes combined with physical layer security when the noise is impulsive. Most importantly, it was shown that polar codes can still ensure a secure channel between Alice and Bob at all SNRs, even when the main channel is more impulsive than the eavesdropper's channel. However, the secrecy code rate was quite low. Hence, in chapter 5 we proposed an ARQ-aided polar coding scheme based on changing frozen bits in the decoding process to increase the secrecy code rate to 0.5 and ensure secure communication at the same time. An ARQ channel is a kind of degraded channel, but in this work the main channel from Alice to Bob is worse than the eavesdropper channel between Alice and Eve. A conventional polar code can have any code rate by adding or deleting the polarized bit channels which used for transmit information bits, however the code length is limited to a power of two and as a result polar codes cannot be employed on arbitrary modulation schemes.

As sated in the literature, punctured polar codes can have any code rate without the limitation of block length. Thus the main contribution of this chapter is to apply punctured polar codes to physical layer security in the presence of SαS noise. All of our previous work was based on BPSK modulation, so in this chapter we will also examine the performance of polar codes with higher modulations.

The contributions of this chapter are as follows: First, we find the optimal puncturing patterns by selecting them from the frozen bits channels based on the observation that the block error probability is mainly determined by the worst bit channels. In addition, the performance of our proposed puncturing polar codes on impulsive noise channels with different values of α are investigated and compared with the method proposed by [1]. Second, we examine the performance of the proposed polar codes for M-QAM schemes on SαS noise channels. Finally, the performance and security of these punctured polar codes are evaluated for BPSK and M-QAM schemes on the wiretap channel with different levels of impulsiveness.

6.2 The Optimal Puncturing Scheme for SαS Noise Channels

In this section, we propose a puncturing method and show how to select the puncturing patterns only from the frozen bits. First, in Fig. 6.1 we show the error probability value of each bit channel when the polar code length is $N = 32$ and the signal to noise ratio is 3dB. Our design scheme is based on the error probability of sub-channels. In this chapter, we use K to denote the number of the information bits, N to denote the code length of the conventional polar codes, and L to denote the code length of the punctured polar codes, where $K \leq L \leq N$. The index set of the punctured bits is denote by A_p, and $|A_p| = N - L$ denotes the length of the punctured bits. The code rate R of the punctured codes is $R = K/L$.

6.2.1 Proposed Puncture Method

In [1], the puncturing scheme for polar codes proposes that the punctured bits are selected only from the frozen bits and are known to the decoder. Due to the worst sub-channels having a significant effect on the block error probability, improving the performance of the worst sub-channels reduces the block error probability, and

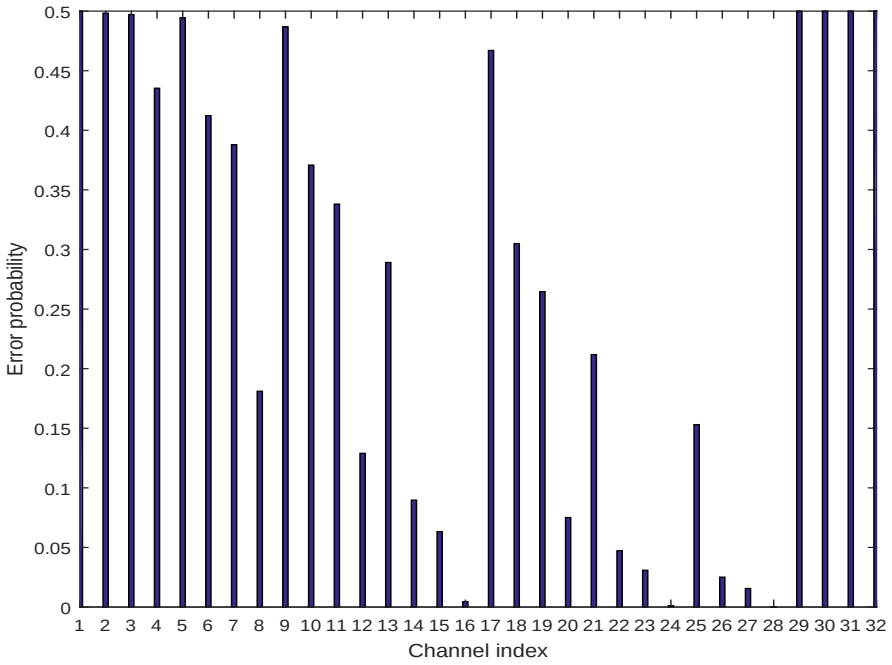

Figure 6.1: Error probability performance of bit channels of polar codes with code length $N = 32$ and code rate $R = 0.5$.

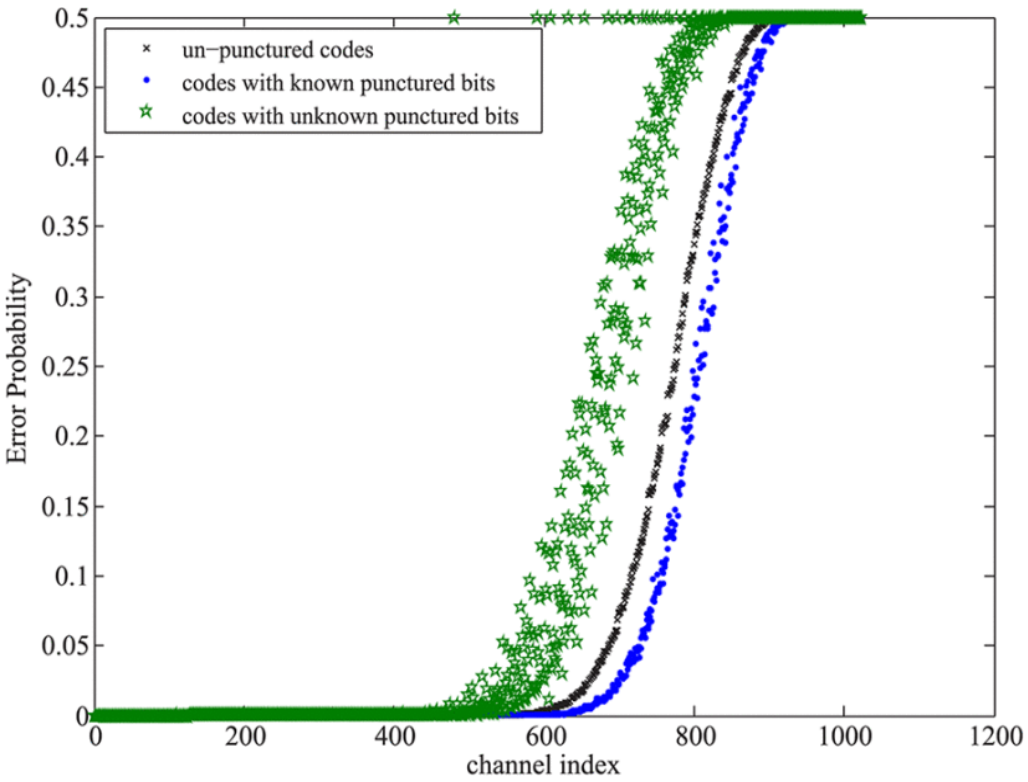

Figure 6.2: The comparison of the error probability of the sub-channels of the conventional polar codes, the polar codes without the knowledge of the punctured bits and polar codes with known punctured bits with code lengths $L = 896$ in BI-AWGNC with SNR = 3 dB [1].

shown in Fig. 6.2 [1]. It is clear that the error probability of the punctured codes with known bits (where the initial value of LLRs are set as infinity) are lower than those punctured by the the conventional method, especially for bad bit channels.

The simulation shows that the punctured polar codes proposed by [1] outperform the conventional punctured codes. However, for this method, when designing the codes, it focuses on selecting the puncturing pattern first and then re-selecting the information bits. Therefore, we will consider if the information is selected at first and fixed, then puncturing the codes from the frozen bit channels, will result in the punctured polar codes still showing good performance. Indeed, it has been proven that having a fixed information set and then puncturing the coded bits corresponding to the worst quality bit channels can reduce the bit channel quality loss at the punctured positions can achieve excellent performance in [92].

Inspired by the works of [1] and [92] we propose a new method to puncture polar codes. In our method, the information bits channels are fixed and selected at first, and the punctured bits are selected from the frozen bits channels which have the worst channel conditions. For the punctured bits we let the decoder have the knowledge of them.

Our proposed method is explain as follows:

- Use DE to calculate the error probability of each bit channel corresponding to the reliability of each bit channels, and sort them.
- Select K bit channels with high reliability as information bits and others set as frozen bits.
- Choose the lowest reliability bit channels as punctured bit channels, which is obviously among the frozen bits.
- Generate the polar codeword, then puncture the codeword by A_p.
- At the receiver, fill the information of the punctured position by setting the LLRs of the puncture bits to infinity, which means the punctured bits are known to both encoder and decoder.

6.2.2 Comparison with Method Proposed in [1]

In order to compare our proposed puncture method with method proposed in [1] (in this chapter we named it as WRX's method), we shall first review the implementa-

tion of the WRX's scheme:

- For a given code length L, select the initial puncturing pattern be $A_{p1} = \{L+1, L+2, \cdots, N\}$.
- Set $\{L+1, L+2, \cdots, N\}$ to be frozen bits.
- Choose other frozen bits by the density evolution method.
- Generate the codeword bits, then puncture the codeword by A_p.
- At the receiver, fill the information of the punctured position by setting the LLRs of the puncture bits to infinity.

We will see the difference of the puncture sets of our proposed puncture method and WRX's puncture method. As an example, assume a conventional polar code length $N = 32$ and final code length $L = 28$. The puncture set of our proposed method is $\{29, 30, 31, 32\}$, WRX's puncture set is $\{8, 16, 24, 32\}$. Both methods use density evolution to calculate the bit channels reliability. From Fig. 6.1 we can see all of our puncture bits are bit channels with largest error probability, while WRX's puncture bits include bits channels with good conditions, which will cause bit channel quality loss. In addition, by puncturing the worst bit channels, the block error probability will be reduced according to [1]. We will show the performance of our proposed puncture polar codes on impulsive noise channels with different modulation schemes in the results section.

6.3 Punctured Polar Codes for Secure Communication Systems in the Presence of Impulsive Noise

6.3.1 System Model

Fig. 6.3 is the system model with our proposed punctured polar codes.

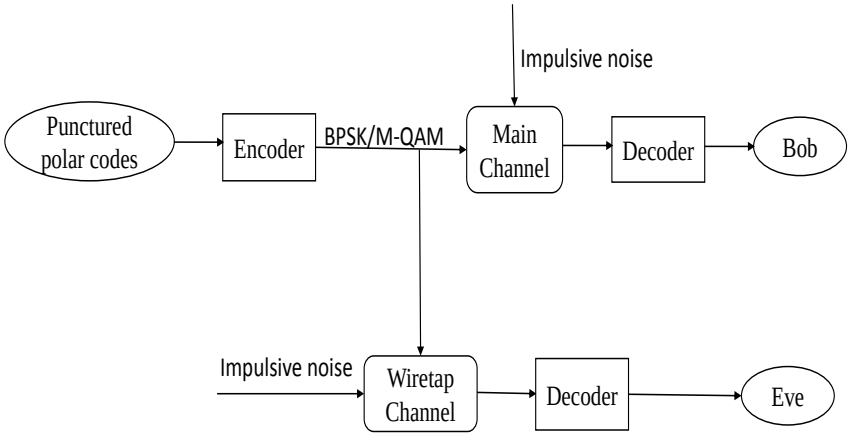

Figure 6.3: Punctured polar coding scheme security system mode.

6.3.2 Secure Coding Scheme

In this subsection we will explain how to achieve secure communication by applying punctured polar codes. In this system, the information Alice wants to send to Bob is assigned to the information bit channels of the punctured polar code. Then we generate the polar codeword with some bits deleted due to the puncturing method. After BPSK or M-QAM (M = 4, 16, 64) modulation, the codeword is transmitted to Bob via the main channel with impulsive noise modelled by SαS distributions in the presence of Eve. In our proposed security coding scheme we use punctured bits to achieve security.

- Start with a mother polar code with code length N.
- Use density evolution to calculate the error probability of N bit channels which correspond to the reliability of each bit channels, and sort them.
- Select the K bit channels with high reliability as information bits, others set as frozen bits.
- Choose the lowest reliability bit channels as puncture bits channels and set the puncture sets as A_p.
- Generate the polar codeword bits, then puncture the codeword by A_p.
- The polar codeword after puncturing will be modulated by BPSK/MQAM modulation, then sent to Bob on an impulsive noise channel, while Eve can intercept the information through the wiretap channel.

- At Bob's receiver, fill the information of the punctured position by setting the LLRs of the puncture bits to infinity.
- At Eve's receiver, we assume she knows there are some bits that been deleted but she has no information of the position of the puncture bits, even if she know the puncture bits are selected from the frozen bits.

6.4 Results and Discussion

In this section, simulation results are presented for the proposed punctured polar codes on impulsive noise channels with BPSK and MQAM modulations. In addition, these punctured polar codes are combined with physical layer security in the presence of SαS noise. The SC decoding algorithm is employed and all the polar codes employed are constructed using density evolution.

6.4.1 Performance of Punctured Polar Codes for BPSK and M-QAM Schemes on Impulsive Noise Channels

In Figs. 6.4 to Fig. 6.6, the BER performance of our proposed method along with method proposed in [1] and BPSK modulation on impulsive noise channels with different values of α are shown. The corresponding FER is shown in Fig. 6.7 to Fig. 6.9. In Fig. 6.4 the block length of the polar code is $N = 512$. After puncturing the final code length is $L = 320$ and the code rate is $R = 0.7$. For $\alpha = 1.99$, that means the channel is slightly impulsive and we observe that the polar codes punctured by our proposed method outperforms punctured polar codes proposed by [1] and achieves a gain of about 0.8 dB at a BER = 10^{-3}. In addition, there is an interesting result that shows when the channel becomes more impulsive, the gain is higher, which can be seen from the simulation results of impulsive noise channels with $\alpha = 1.8$ and $\alpha = 1.5$. In Fig. 6.10 and Fig. 6.11 we give the BER performance for a code rate $R = 0.8$.

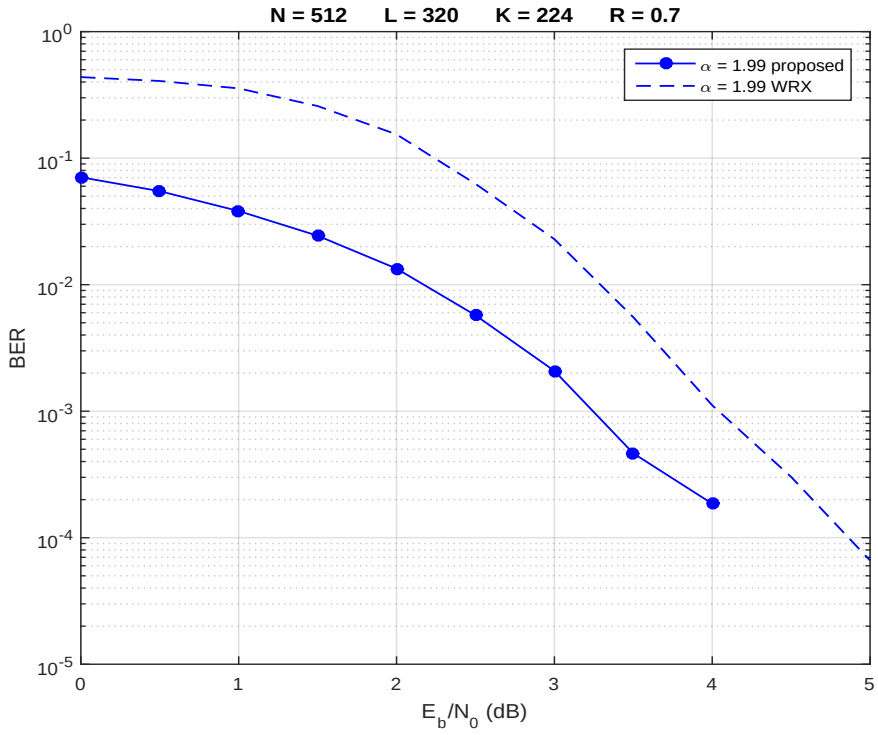

Figure 6.4: The BER performance on SαS impulsive channel($\alpha = 1.99$) of punctured polar codes with code length $L = 320$ and code rate $R = 0.7$.

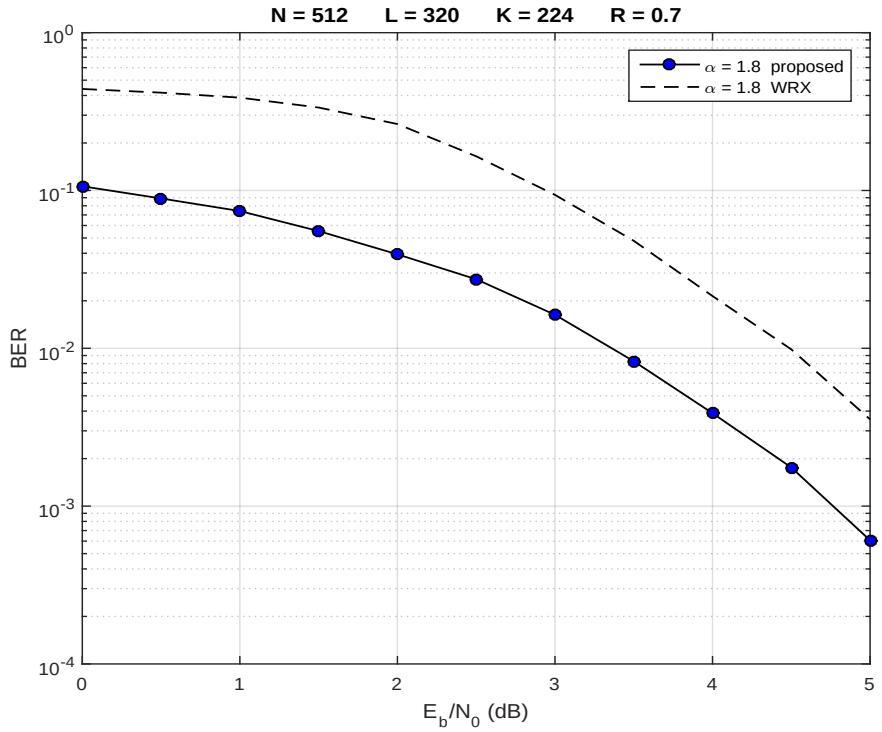

Figure 6.5: The BER performance on SαS impulsive channel($\alpha = 1.8$) of punctured polar codes with code length $L = 320$ and code rate $R = 0.7$.

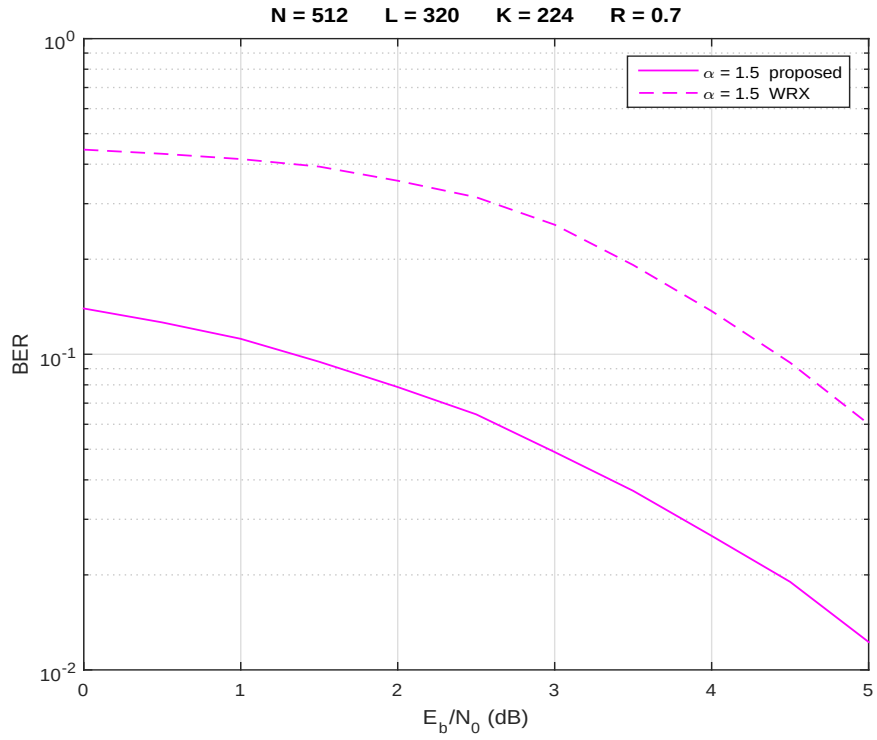

Figure 6.6: The BER performance on SαS impulsive channel($\alpha = 1.5$) of punctured polar codes with code length $L = 320$ and code rate $R = 0.7$.

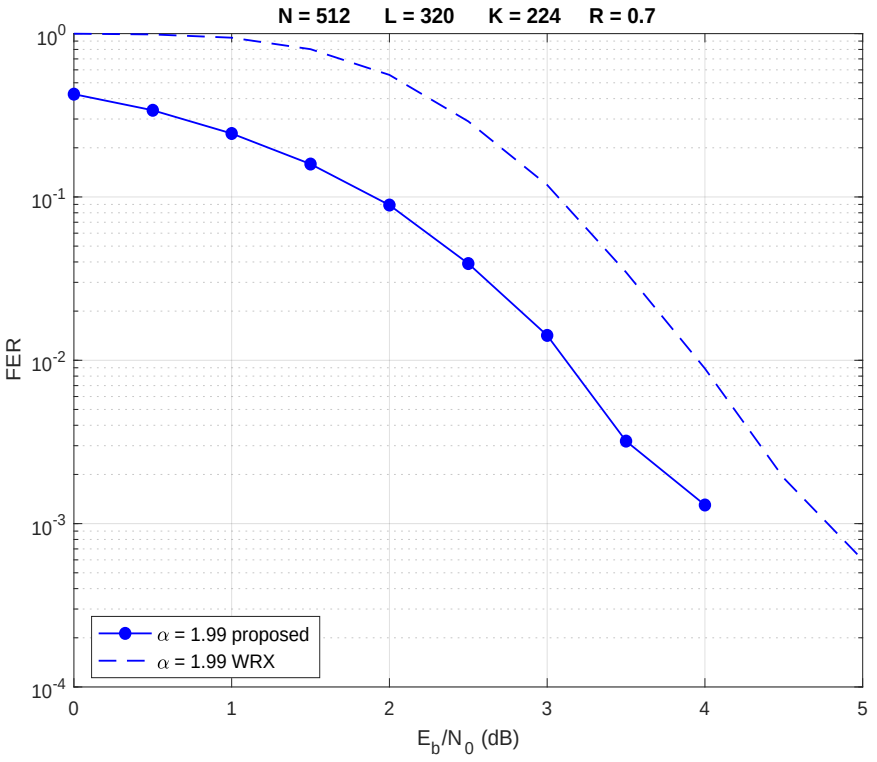

Figure 6.7: The FER performance on SαS impulsive channel($\alpha = 1.99$) of punctured polar codes with code length $L = 320$ and code rate $R = 0.7$.

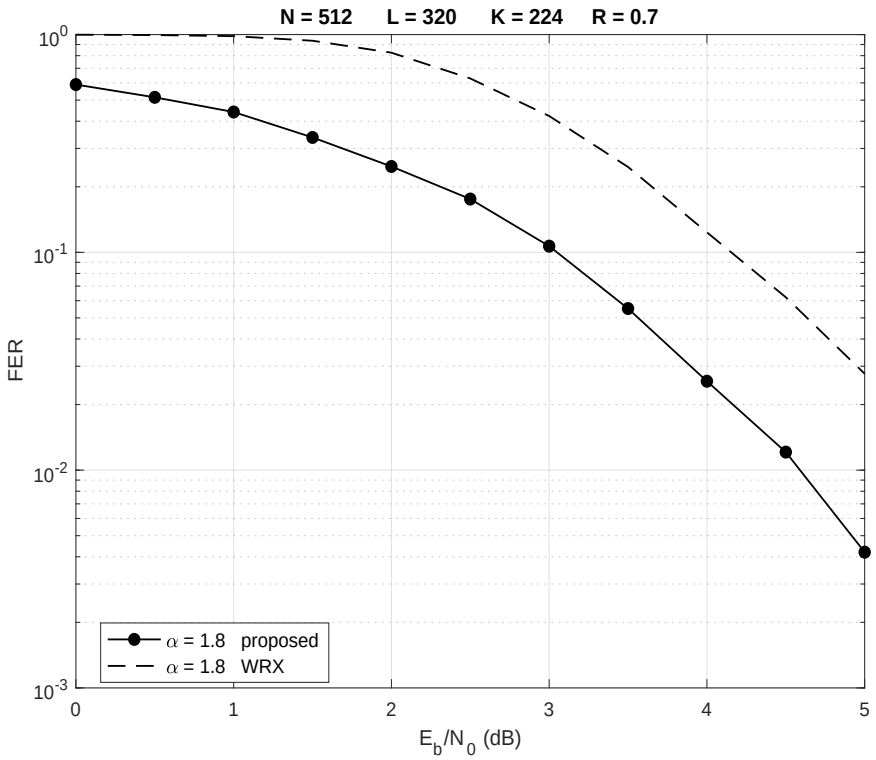

Figure 6.8: The FER performance on SαS impulsive channel($\alpha = 1.8$) of punctured polar codes with code length $L = 320$ and code rate $R = 0.7$.

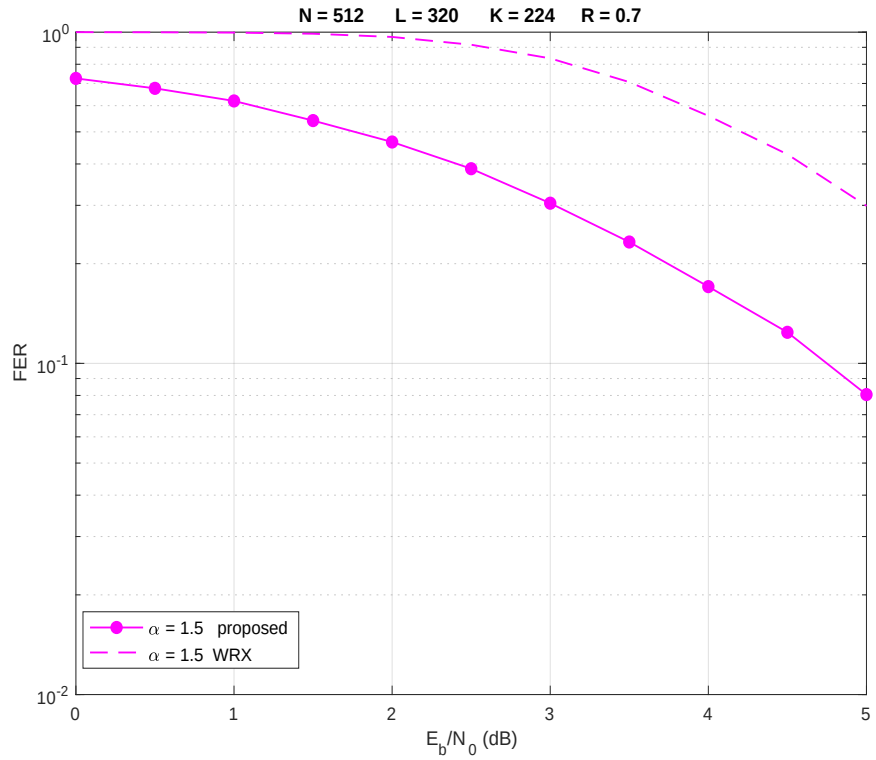

Figure 6.9: The FER performance on SαS impulsive channel($\alpha = 1.5$) of punctured polar codes with code length $L = 320$ and code rate $R = 0.7$.

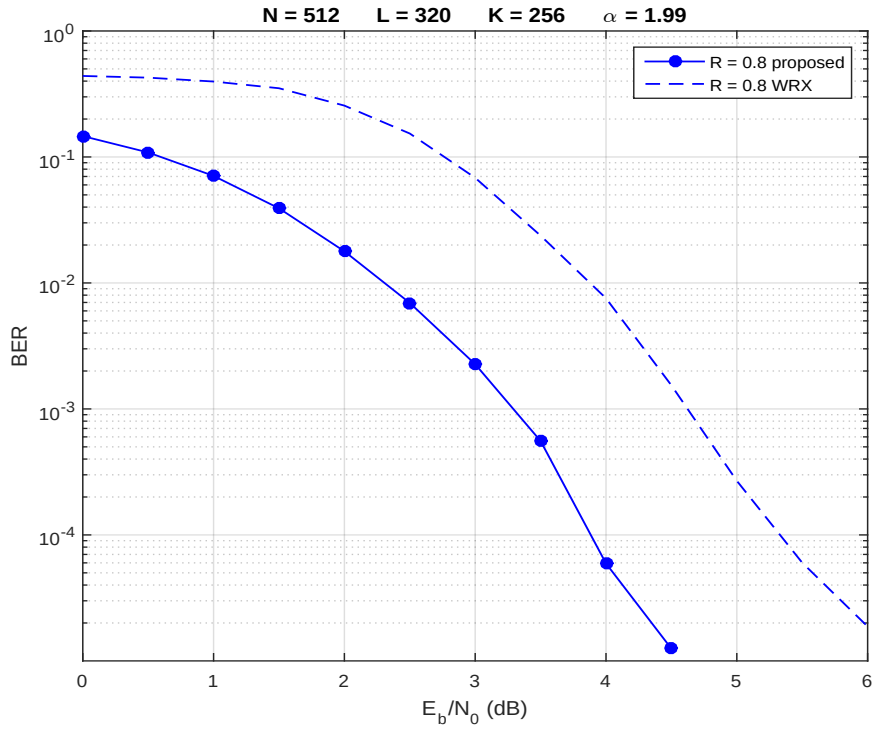

Figure 6.10: The BER performance on SαS impulsive channel($\alpha = 1.99$) of punctured polar codes with code length $L = 320$ and code rate $R = 0.8$.

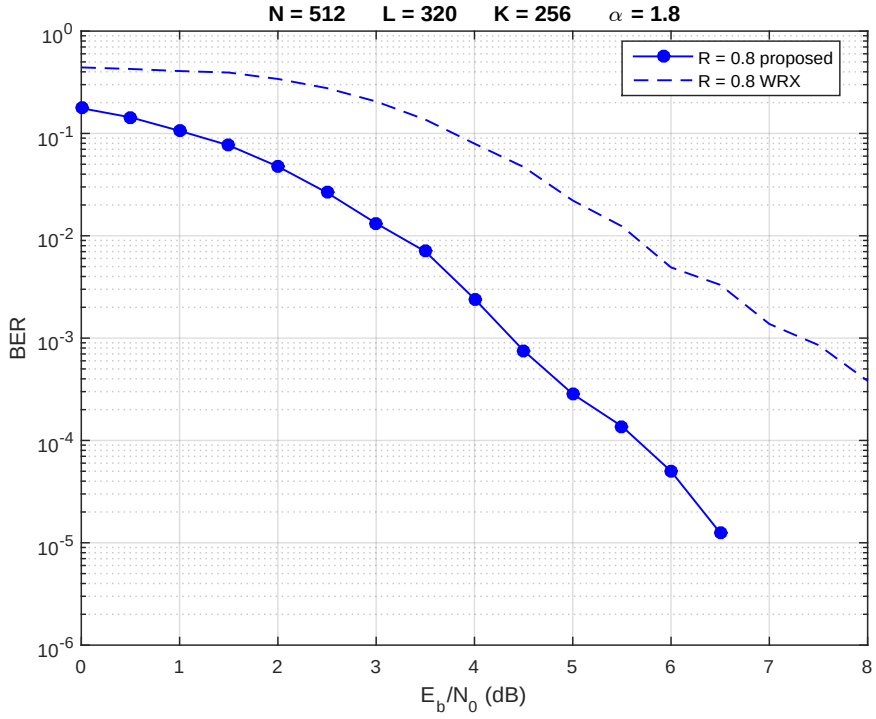

Figure 6.11: The BER performance on SαS impulsive channel($\alpha = 1.8$) of punctured polar codes with code length $L = 320$ and code rate $R = 0.8$.

In Fig. 6.12, we investigate the BER performance of polar codes with a final block length $L = 320$, code rate $R = 0.8$ with 4, 16 and 64QAM modulations on an impulsive noise channel ($\alpha = 1.9$). We can see the punctured polar codes can obtain any block length suitable for any modulation scheme. Simulation results show our proposed puncture scheme is better than [1] for 4, 16, and 64QAM.

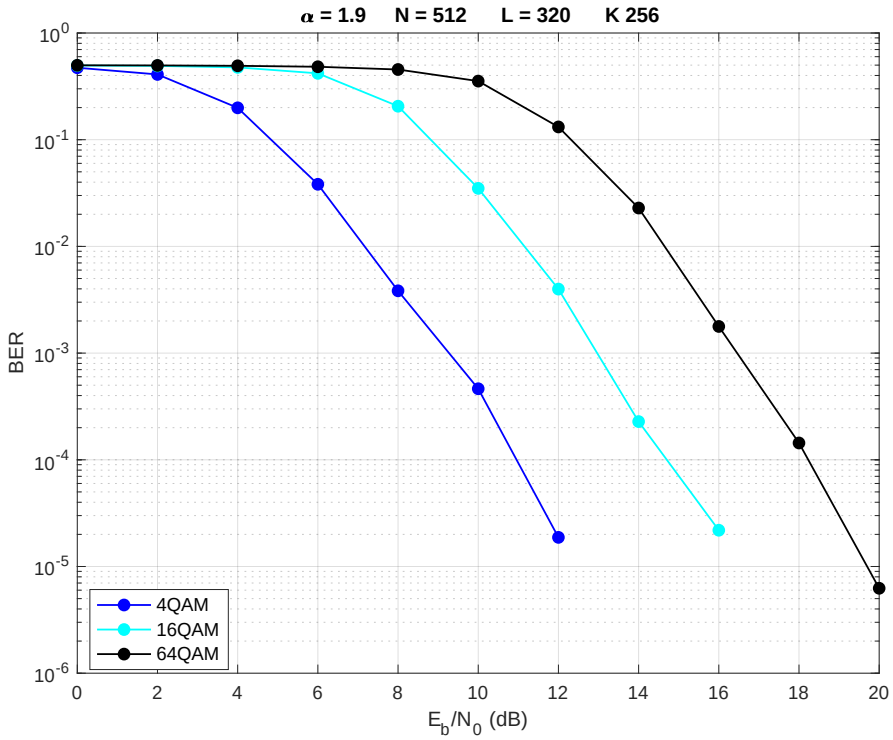

Figure 6.12: The BER performance on SαS impulsive channel of punctured polar codes with code length $L = 320$ with 4, 16, and 64-QAM modulations.

6.4.2 Secure Performance of Punctured Polar Codes for BPSK and M-QAM Schemes on the Wiretap Channel Systems with Impulsive Noise

The results of the security performance of our proposed punctured polar codes on wiretap channels with BPSK modulation scheme are shown in Figs. 6.13 to Fig. 6.18.

In Fig. 6.13 we employ the punctured polar codes with a final block length $L = 320$, code rate $R = 0.8$. After BPSK modulation, the codeword is transmitted over an impulsive noise channel with $\alpha = 1.9$ to Bob and Eve's channel, which has the same channel condition. We can observe that the BER performance of Bob is better than Eve, especially when the SNR is smaller than 8dB. That means security

can be achieved in a range of SNRs. In Fig. 6.14 the eavesdropper channel from Alice to Eve is much better($\alpha = 1.99$) than the main channel ($\alpha = 1.9$) between Alice to bob. From the BER curves we can see that due to the advantage of Eve's channel BER is better than Fig 6.13, and the security SNR range is reduces to 7dB.

In Figs. 6.15 to 6.18 we employ the punctured polar codes with final block length $L = 1280$ and code rate $R = 0.8$. After BPSK modulation, in Fig. 6.15 the codeword is transmitted over an impulsive noise channel with $\alpha_B = 1.1$ from Alice to Bob in the presence of eavesdropper, and the eavesdropper channel has the same channel condition. We can observe that the BER performance of Bob is better than Eve. When the SNR is smaller than 20.7dB, the BER of Eve is larger than 0.1. In Fig. 6.16, both the eavesdropper channel from Alice to Eve and the main channel between Alice to bob are impulsive noise channels with $\alpha_B = \alpha_E = 1.5$, the BER of Eve is larger than 0.1 when SNR is smaller than 12.5 dB. When the channel is slightly impulsive ($\alpha_b = \alpha_E = 1.9$) in Fig. 6.17, secure communication can be achieve when the SNR is smaller than 7.7dB. We can observe that when both the main channel and eavesdropper channel are extremely impulsive, the SNR range for security is larger. In Fig. 6.18, we consider a special situation, where the channel from Alice to Bob is much more impulsive with $\alpha_B = 1.5$ than the channel between Alice to Eve with $\alpha_E = 1.9$. Simulation results show Bob still outperforms Eve.

The secure performance of our proposed polar codes on impulsive noise wiretap channel systems with 4, 16 and 64QAM schemes are shown in Fig. 6.19, Fig. 6.20 and Fig. 6.21. The simulation results indicate that Eve performance is bad over a range of SNR for 4, 16 and 64QAM.

In Fig. 6.19 to 6.21 we employed the punctured polar codes with final code length $L = 420$ and code rate $R = 0.6095$. After 4QAM modulation, the codeword is transmitted over an impulsive noise channel with $\alpha_B = 1.9$ from Alice to Bob and Eve's channel is under the same channel condition. From Fig. 6.19 we observe that the when SNR is between 2dB and 8dB, the BER of Eve is larger than 0.1. For the same codes in Fig. 6.20, when modulated by 16QAM, the punctured polar coding scheme shows good performance from 5dB to 15.5dB. However, in Fig. 6.21 for 64QAM the SNR range changes from 8.5dB to 15.5dB.

Using the proposed puncturing coding scheme, we can increase the secrecy code rate with any code block length and extend the polar codes for any modulation.

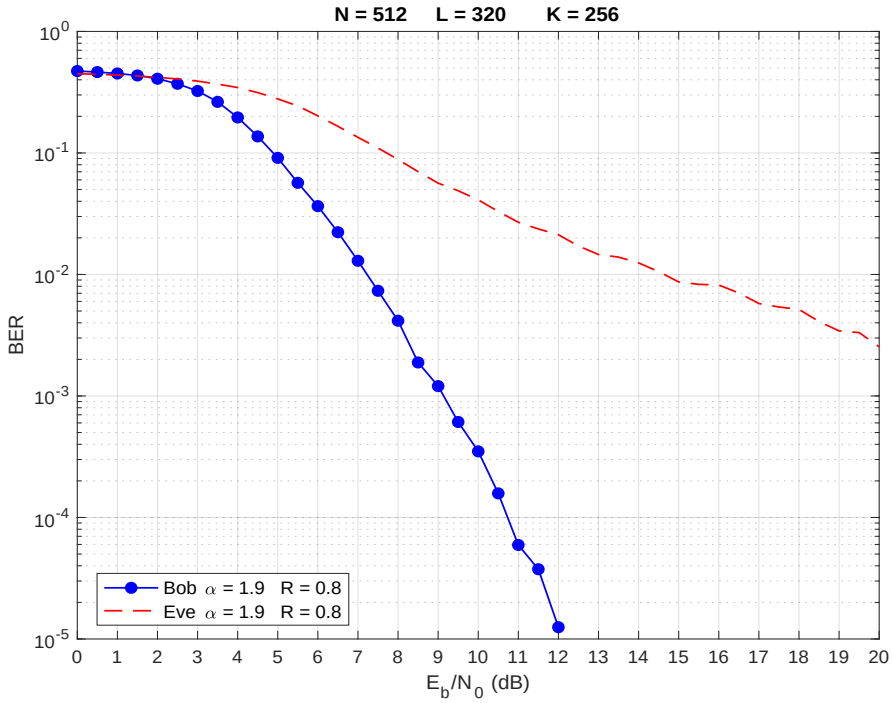

Figure 6.13: BER performance of punctured polar codes with BPSK modulation on wiretap channel, where the main channel is same impulsive with the eavesdropper channel ($\alpha = 1.9$), where the code length $L = 320$ and code rate $R = 0.8$.

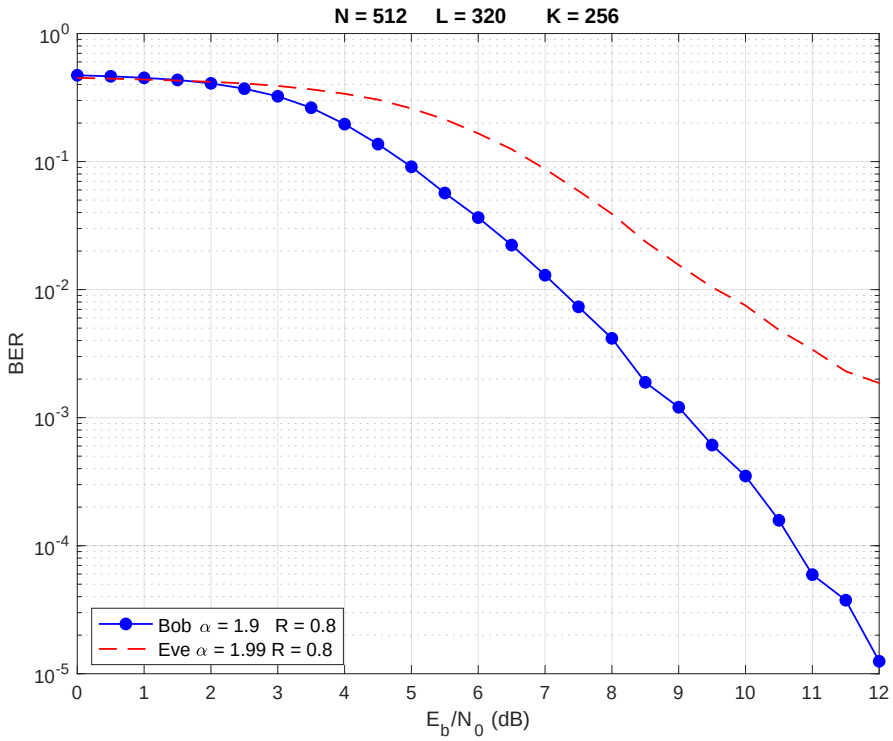

Figure 6.14: BER performance of punctured polar codes with BPSK modulation on wiretap channel, where the main channel is impulsive with $\alpha = 1.9$, and the eavesdropper channel is slightly impulsive with $\alpha = 1.99$, where the code length $L = 320$ and code rate $R = 0.8$.

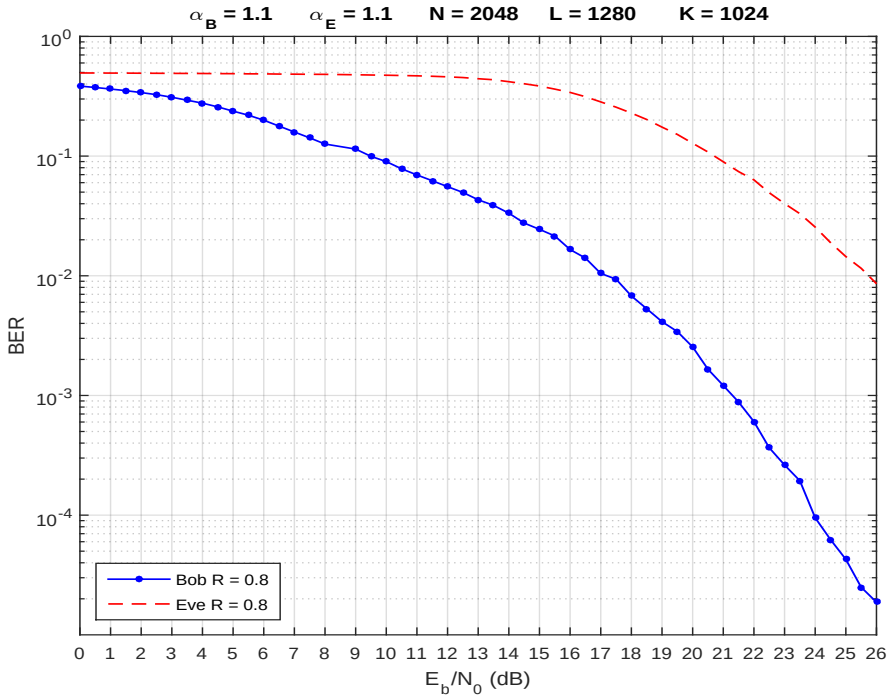

Figure 6.15: BER performance of punctured polar codes with BPSK modulation on wiretap channel, where the main channel is same impulsive with the eavesdropper channel ($\alpha_B = \alpha_E = 1.1$), where the code length $L = 1280$ and code rate $R = 0.8$.

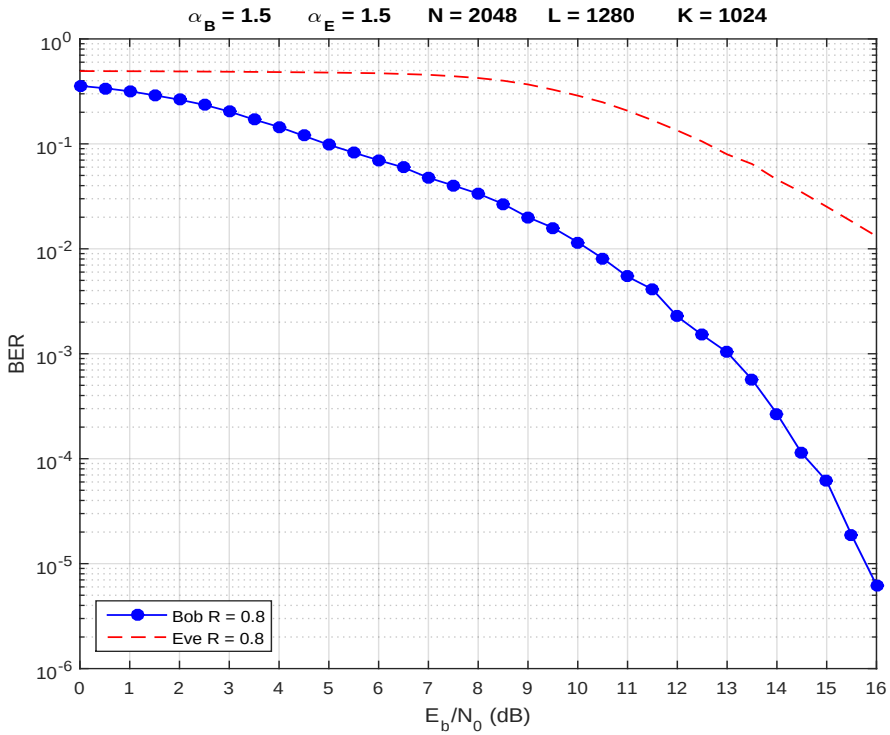

Figure 6.16: BER performance of punctured polar codes with BPSK modulation on wiretap channel, where the main channel is same impulsive with the eavesdropper channel ($\alpha_B = \alpha_E = 1.5$), where the code length $L = 1280$ and code rate $R = 0.8$.

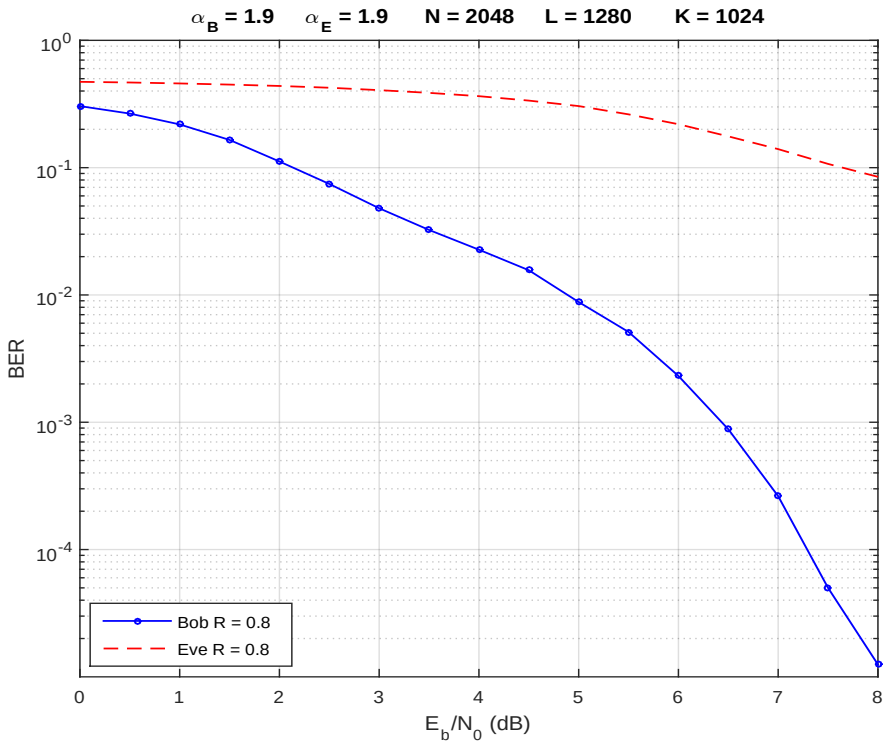

Figure 6.17: BER performance of punctured polar codes with BPSK modulation on wiretap channel, where the main channel is same impulsive with the eavesdropper channel ($\alpha_B = \alpha_E = 1.9$), where the code length $L = 1280$ and code rate $R = 0.8$.

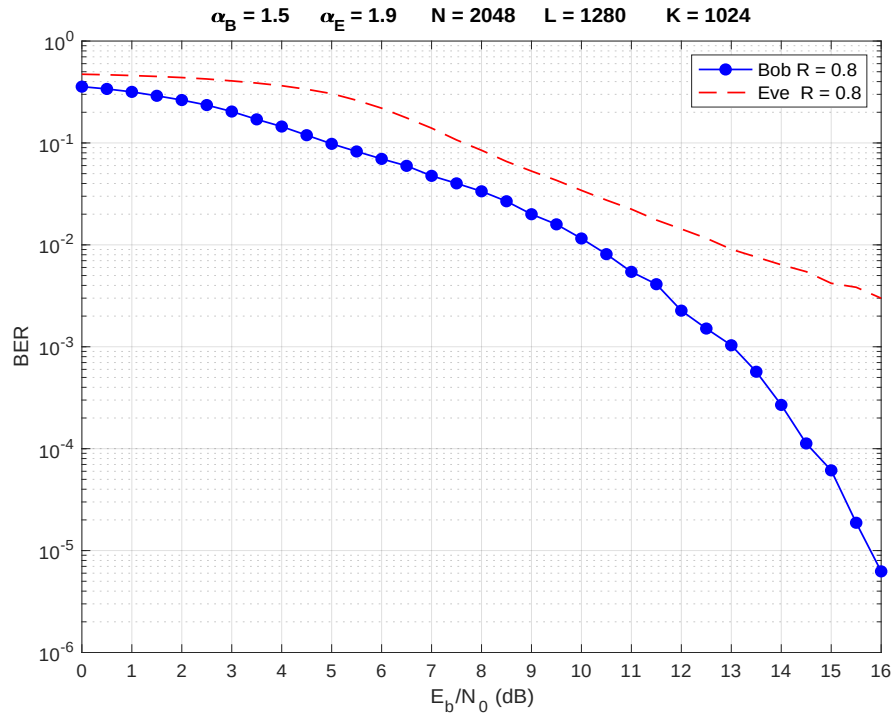

Figure 6.18: BER performance of punctured polar codes with BPSK modulation on wiretap channel, where the main channel is impulsive with $\alpha_B = 1.5$, and the eavesdropper channel is less impulsive with $\alpha_E = 1.9$, where the code length $L = 1280$ and code rate $R = 0.8$.

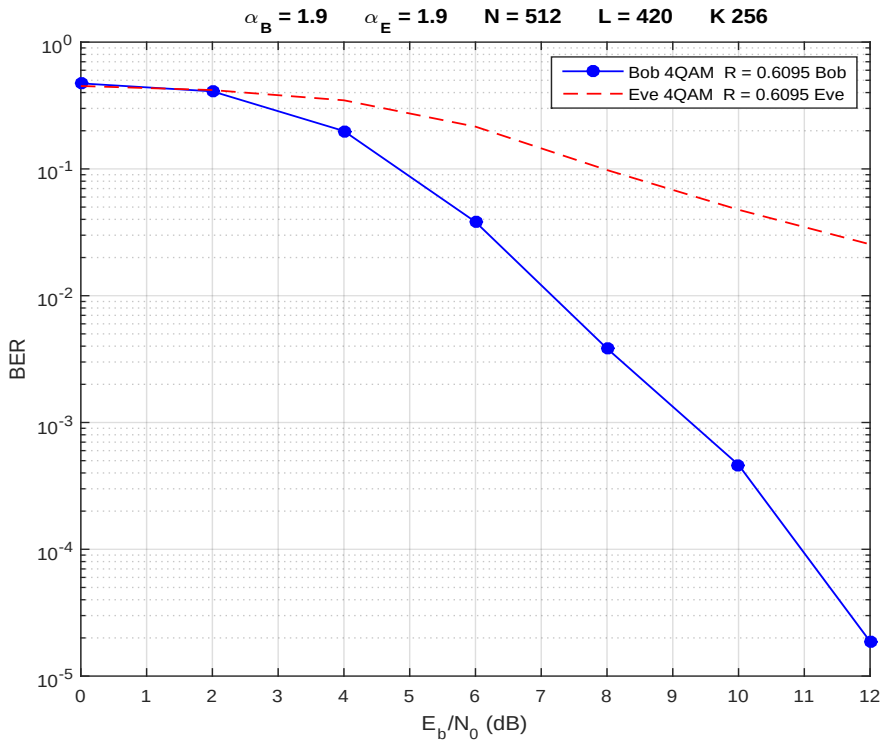

Figure 6.19: BER performance of punctured polar codes with 4-QAM modulation on wiretap channel, where the main channel is same impulsive with the eavesdropper channel ($\alpha_B = \alpha_E = 1.9$), where the code length $L = 420$ and code rate $R = 0.6095$.

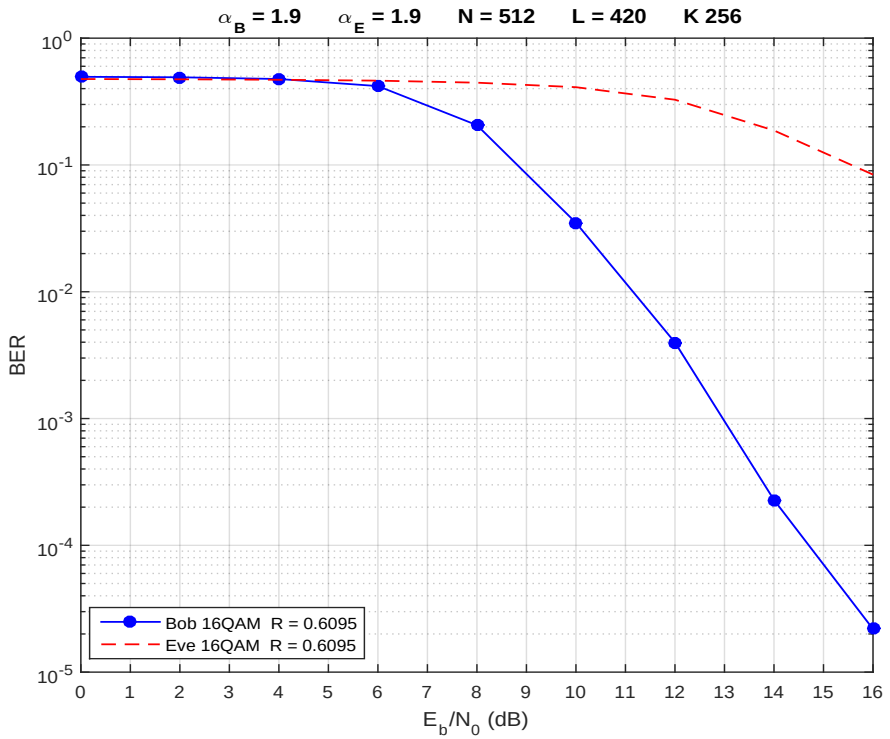

Figure 6.20: BER performance of punctured polar codes with 16-QAM modulation on wiretap channel, where the main channel is same impulsive with the eavesdropper channel ($\alpha_B = \alpha_E = 1.9$), where the code length $L = 420$ and code rate $R = 0.6095$.

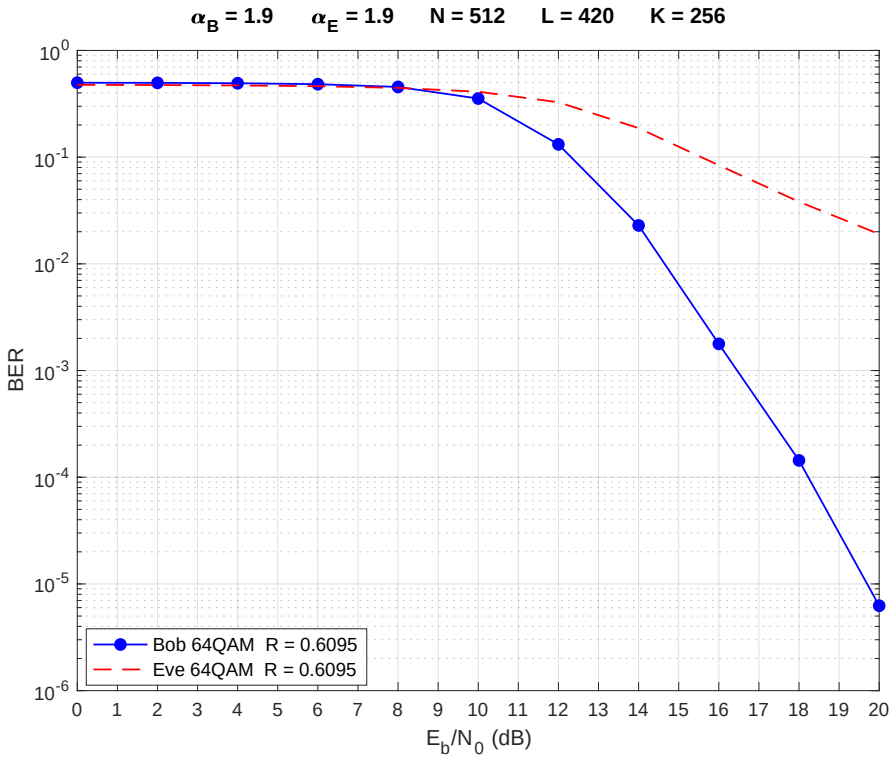

Figure 6.21: BER performance of punctured polar codes with 64-QAM modulation on wiretap channel, where the main channel is same impulsive with the eavesdropper channel ($\alpha_B = \alpha_E = 1.9$), where the code length $L = 420$ and code rate $R = 0.6095$.

6.5 Conclusion

In this chapter, we first proposed a puncturing method to solve the block length of polar code being restricted to 2^n, $n = 0, 1, 2, \ldots$. This can be obtained by removing certain bits and shortening the block length so that arbitrary block lengths can be used. The design method was proposed to puncture a polar code on impulsive noise channels modelled as a symmetric alpha-stable distribution and compared with method proposed in [1]. Then we applied the proposed punctured polar codes to 4, 16, and 64-QAM modulation schemes. Simulation results are presented showing that these rate-compatible polar codes achieve better performance than in [1]. In addition, we use theses codes to achieve security on the wiretap channel with impulsive noise and different orders of QAM modulation. Simulation results show the proposed coding scheme can achieve very good security performance over a certain range of SNRs but not all the SNRs. The reason is that in our secure coding scheme, we assume Eve has knowledge of that punctured bits selected from the frozen bits and the length of the punctured bits but has no idea of the exact positions of the punctured bits. However, if Eve knew nothing of the punctured bits, the BER of

Eve would be even worse, but this cannot be guaranteed in a real communication system. Therefore, how to achieve very good security performance over all SNRs is recommended for future work.

Chapter 7

Conclusions and Future Research

7.1 Conclusion

This thesis has investigated the performance and security of polar codes combined with physical layer security on the wiretap channel system where all users experience impulsive noise that modeled by SαS distribution. Until now, the effect of impulsive noise on this type of system had not been considered and it opened up new problems to solve, such as the design of polar codes combined with physical layer security on impulsive noise channels and assessing the effect on the security of this system. In particular, the scenario where the main channel between Alice and Bob was more impulsive than the unauthorised channel between Alice and Eve was investigated, which would appear to give Eve an advantage to intercept the communication between Alice and Bob, due to Eve's channel being less harsh. However, it was shown that good polar codes could still be designed to ensure Bob's BER performance was very good, but Eve's BER performance was still poor at all signal-to-noise ratios. The contributions from chapter four to six are now summarised.

In chapter four, the construction of secure polar codes combined with physical layer security on impulsive noise channels was presented. A density evolution method was proposed that used knowledge of the probability density function of the symmetric alpha-stable noise to construct polar codes that outperformed those constructed from a heuristic method. The security of the system was also maintained, with Bob achieving a very good BER performance while Eve's performance was flat at a very high BER over all signal-to-noise ratios and for varying levels of impulsiveness. However, for a fixed code rate of polar code constructed from this

method, the secrecy rate is always low due to the small number of available bit channels for the secure message.

Although the proposed construction of polar codes combined with physical layer security can make sure a secure system in the present of impulsive noise, even when the main channel is more impulsive than the wiretap channel, but it has been observed that there is a trad off of the secrecy code rate. For a fixed code rate of the conventional polar codes, due to the large number of information bit channels which are use to transmit to random bits, the left amount of information bit channels for secure message is quit lower. Hence, we have proposed a coding scheme to increase the secrecy code rate in Chapter 5.

Chapter five followed on from the work in the previous chapter and addressed the issue of the inherent low secrecy code rates in the designed polar codes. The secrecy code rate was increased by removing random bits from the bit channels of the polar code and transmitting all information bits, so that the secrecy code rate was equal to the code rate. However, to ensure the security of the scheme, random bits are introduced into the frozen bits so that Eve does not receive information about the message and good performance at Bob is achieved by adding an ARQ feedback channel from Bob to Alice. Due to feeds back only a small proportion of the random frozen bits to Alice, unlike [33] where all random frozen bits are fed back, which increases efficiency. Hence, good, secure polar codes with high secrecy code rates can now be designed, improving the efficiency of the polar-coded physical layer security system.

Chapter six addresses a major issue affecting the polar codes in both chapters four and five, where the block length of the polar code is restricted to 2^n, where n is a positive integer. This can be achieved by employing a puncturing scheme to the polar code to remove certain bits and shorten the code so that numerous block lengths can be used. A design method was proposed to puncture a polar code on impulsive noise channels modelled as a symmetric alpha-stable distribution. Lifting the restriction on the block length means that it now simpler to map the coded bits to other modulation schemes, such as 4, 16, and 64-QAM. Simulation results are presented showing that these rate-compatible polar codes achieve very good performance and security on the wiretap channel with impulsive noise and different order of QAM modulation.

In conclusion, new polar codes have been designed and constructed that offer

very good security when combined with physical layer security. The design methods described in the thesis allow significant flexibility in several coding parameters, such as secrecy rate, code rate and block length, so that a secure polar code can be designed to satisfy the requirements of any communication system in impulsive environments.

7.2 Future Research

The thesis has focused on the design of polar codes combined with physical layer security on impulsive noise channels. However, this could be extended to different channels, such as fading channels. Due to the severe fading effects, error correction is not sufficient to correct errors and additional signal processing techniques to mitigate the fading effects are needed, such as channel equalisation or Orthogonal Frequency Division Multiplexing (OFDM). Therefore, there is scope for new receiver designs that incorporate error-correcting codes, physical layer security and equalisation/OFDM to produce a high performance and high security communication scheme on wireless fading channels.

With the development of 5G communications, it is clear that massive multiple-input-multiple-output (MIMO) technology will play a significant role in achieving very high data rates. The security of 5G communications is also as important and there is scope to extend the work presented in this thesis to massive MIMO systems.

There are some simplifications to the methods proposed in this thesis that could also be investigated. The density evolution method to construct polar codes for impulsive noise channels has a high complexity due to the symmetric alpha-stable distributions used to model the noise. The probability density functions of these distribution are complicated, but they are well known to accurately model impulsive noise in a wireless communication channel. It would be interesting to approximate the symmetric alpha-stable distributions with a simpler probability density function equation, such as the Gaussian-Cauchy mixture model, and evaluate the trade-off between the performance, security and complexity.

Finally, to improve the performance of the polar-coded physical layer security system, the design of non-binary polar codes could be investigated. This is an extremely niche area with few papers in the literature. However, it is well-known that non-binary codes can outperform binary codes, particularly on channel where

burst errors occur, and they could enhance the performance and may be even the security of the polar-coded physical layer security system on harsh channels.

References

[1] R. Wang and R. Liu, "A novel puncturing scheme for polar codes," *IEEE Communications Letters*, vol. 18, no. 12, pp. 2081–2084, 2014.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[5] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

[6] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.* IEEE, 2005, pp. 2152–2155.

[7] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory.* IEEE, 2006, pp. 356–360.

[8] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[9] R. G. Gallager, "Low-density parity-check codes," *IRE Trans.Inf. Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[10] D. J. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, 1999.

[11] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of ldpc codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[12] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[13] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "Ldpc codes for the gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, 2011.

[14] M. H. Taieb and J.-Y. Chouinard, "Enhancing secrecy of the gaussian wiretap channel using rate compatible ldpc codes with error amplification," in *2015 IEEE 14th Canadian Workshop on Information Theory (CWIT)*. IEEE, 2015, pp. 41–45.

[15] A. Payandeh, M. Ahmadian, and M. R. Aref, "Adaptive secure channel coding based on punctured turbo codes," *IEE Proceedings-Communications*, vol. 153, no. 2, pp. 313–316, 2006.

[16] J. Almeida and J. Barros, "Random puncturing for secrecy," in *2013 Asilomar Conference on Signals, Systems and Computers*. IEEE, 2013, pp. 303–307.

[17] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes," in *2008 IEEE International Symposium on Information Theory*. IEEE, 2008, pp. 1173–1177.

[18] ——, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[19] ——, "A performance comparison of polar codes and reed-muller codes," *IEEE Communications Letters*, vol. 12, no. 6, pp. 447–449, 2008.

[20] R. Mori and T. Tanaka, "Performance of polar codes with the construction using density evolution," *IEEE Communications Letters*, vol. 13, no. 7, 2009.

[21] D. Wu, Y. Li, and Y. Sun, "Construction and block error rate analysis of polar codes over awgn channel based on gaussian approximation," *IEEE Communications Letters*, vol. 18, no. 7, pp. 1099–1102, 2014.

[22] I. Tal and A. Vardy, "List decoding of polar codes," in *2011 IEEE International Symposium on Information Theory Proceedings*. IEEE, 2011, pp. 1–5.

[23] K. Chen, K. Niu, and J. Lin, "List successive cancellation decoding of polar codes," *Electronics letters*, vol. 48, no. 9, pp. 500–501, 2012.

[24] K. Niu and K. Chen, "Stack decoding of polar codes," *Electronics letters*, vol. 48, no. 12, pp. 695–697, 2012.

[25] ——, "Crc-aided decoding of polar codes," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1668–1671, 2012.

[26] S. B. Korada, E. Sasoglu, and R. Urbanke, "Polar codes: Characterization of exponent, bounds, and constructions," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6253–6264, 2010.

[27] M. Karzand and E. Telatar, "Polar codes for q-ary source coding," in *2010 IEEE International Symposium on Information Theory*. IEEE, 2010, pp. 909–912.

[28] R. Mori and T. Tanaka, "Non-binary polar codes using reed-solomon codes and algebraic geometry codes," in *2010 IEEE Information Theory Workshop*. IEEE, 2010, pp. 1–5.

[29] N. Hussami, S. B. Korada, and R. Urbanke, "Performance of polar codes for channel and source coding," in *2009 IEEE International Symposium on Information Theory*. IEEE, 2009, pp. 1488–1492.

[30] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *2010 IEEE Information Theory Workshop*. IEEE, 2010, pp. 1–5.

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

[32] H. Bai, L. Jin, and M. Yi, "Artificial noise aided polar codes for physical layer security," *China Communications*, vol. 14, no. 12, pp. 15–24, 2017.

[33] H. Liang, A. Liu, Y. Zhang, and Q. Zhang, "An arq-aided polar coding scheme for security transmission of the wiretap channel," in *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. IEEE, 2017, pp. 1530–1535.

[34] E. Şaşoğlu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *2013 IEEE International Symposium on Information Theory*. IEEE, 2013, pp. 1117–1121.

[35] J. M. Renes, R. Renner, and D. Sutter, "Efficient one-way secret-key agreement and private channel coding via polarization," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2013, pp. 194–213.

[36] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.

[37] Y.-P. Wei and S. Ulukus, "Polar coding for the general wiretap channel," in *2015 IEEE Information Theory Workshop (ITW)*. IEEE, 2015, pp. 1–5.

[38] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2410–2429, 2016.

[39] T. C. Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," *IEEE Transactions on Information Theory*, vol. 63, no. 2, pp. 1311–1324, 2016.

[40] M. Zheng, M. Tao, and W. Chen, "Polar coding for secure transmission in miso fading wiretap channels," *arXiv preprint arXiv:1411.2463*, 2014.

[41] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, 2012.

[42] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communications Letters*, vol. 14, no. 8, pp. 752–754, 2010.

[43] H. Si, O. O. Koyluoglu, and S. Vishwanath, "Achieving secrecy without any instantaneous csi: Polar coding for fading wiretap channels," in *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 2161–2165.

[44] W. Hao, L. Yin, and Q. Huang, "Secrecy transmission scheme based on 2-d polar coding over block fading wiretap channels," *IEEE Communications Letters*, vol. 22, no. 5, pp. 882–885, 2018.

[45] J. Ha, J. Kim, and S. W. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Transactions on information Theory*, vol. 50, no. 11, pp. 2824–2836, 2004.

[46] J. Ha, J. Kim, D. Klinc, and S. W. McLaughlin, "Rate-compatible punctured low-density parity-check codes with short block lengths," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 728–738, 2006.

[47] H. Pishro-Nik and F. Fekri, "Results on punctured low-density parity-check codes and improved iterative decoding techniques," *IEEE Transactions on Information Theory*, vol. 53, no. 2, pp. 599–614, 2007.

[48] A. Eslami and H. Pishro-Nik, "A practical approach to polar codes," in *2011 IEEE International Symposium on Information Theory Proceedings*. IEEE, 2011, pp. 16–20.

[49] K. Niu, K. Chen, and J.-R. Lin, "Beyond turbo codes: Rate-compatible punctured polar codes," in *2013 IEEE International Conference on Communications (ICC)*. IEEE, 2013, pp. 3423–3427.

[50] D.-M. Shin, S.-C. Lim, and K. Yang, "Design of length-compatible polar codes based on the reduction of polarizing matrices," *IEEE Transactions on Communications*, vol. 61, no. 7, pp. 2593–2599, 2013.

[51] L. Zhang, Z. Zhang, X. Wang, Q. Yu, and Y. Chen, "On the puncturing patterns for punctured polar codes," in *2014 IEEE International Symposium on Information Theory*. IEEE, 2014, pp. 121–125.

[52] H. Saber and I. Marsland, "An incremental redundancy hybrid arq scheme via puncturing and extending of polar codes," *IEEE Transactions on Communications*, vol. 63, no. 11, pp. 3964–3973, 2015.

[53] V. Miloslavskaya, "Shortened polar codes," *IEEE Transactions on Information Theory*, vol. 61, no. 9, pp. 4852–4865, 2015.

[54] V. Bioglio, F. Gabry, and I. Land, "Low-complexity puncturing and shortening of polar codes," in *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2017, pp. 1–6.

[55] Q. Kai, Z. Sheng-mei, and S. Peng, "Design of the gaussian wiretap channel with punctured polar codes." *Journal of Signal Processing*, vol. 30, no. 11, 2014.

[56] P. Cardieri, "Modeling interference in wireless ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 4, pp. 551–572, 2010.

[57] P. C. Pinto and M. Z. Win, "Communication in a poisson field of interferers-part ii: Channel capacity and interference spectrum," *IEEE Transactions on Wireless Communications*, vol. 9, no. 7, pp. 2187–2195, 2010.

[58] B. Nikfar, T. Akbudak, and A. H. Vinck, "Mimo capacity of class a impulsive noise channel for different levels of information availability at transmitter," in *18th IEEE International Symposium on Power Line Communications and Its Applications*. IEEE, 2014, pp. 266–271.

[59] D. Zha and T. Qiu, "Underwater sources location in non-gaussian impulsive noise environments," *Digital Signal Processing*, vol. 16, no. 2, pp. 149–163, 2006.

[60] N. Farsad, W. Guo, C.-B. Chae, and A. Eckford, "Stable distributions as noise models for molecular communication," in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.

[61] M. Zimmermann and K. Dostert, "Analysis and modeling of impulsive noise in broad-band powerline communications," *IEEE Trans. Electromagn. Compat.*, vol. 44, no. 1, pp. 249–258, 2002.

[62] B. Hu and N. C. Beaulieu, "On characterizing multiple access interference in TH-UWB systems with impulsive noise models," in *2008 IEEE Radio and Wireless Symposium*, 2008.

[63] D. Middleton, "Non-Gaussian noise models in signal processing for telecommunications: new methods an results for class a and class b noise models," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1129–1149, 1999.

[64] T. Shongwey, A. H. Vinck, and H. C. Ferreira, "On impulse noise and its models," in *2014 18th IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*. IEEE, 2014, pp. 12–17.

[65] M. Shao and C. L. Nikias, "Signal processing with fractional lower order moments: stable processes and their applications," *Proceedings of the IEEE*, vol. 81, no. 7, pp. 986–1010, 1993.

[66] H. Nakagawa, D. Umehara, S. Denno, and Y. Morihiro, "A decoding for low density parity check codes over impulsive noise channels," in *International Symposium on Power Line Communications and Its Applications, 2005.* IEEE, 2005, pp. 85–89.

[67] N. Andreadou and F.-N. Pavlidou, "Mitigation of impulsive noise effect on the plc channel with qc–ldpc codes as the outer coding scheme," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1440–1449, 2010.

[68] Z. Mei, M. Johnston, S. Le Goff, and L. Chen, "Density evolution analysis of LDPC codes with different receivers on impulsive noise channels," in *2015 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2015, pp. 1–6.

[69] ——, "Error probability analysis of m-qam on rayleigh fading channels with impulsive noise," in *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2016, pp. 1–5.

[70] ——, "Finite length analysis of low-density parity-check codes on impulsive noise channels," *IEEE Access*, vol. 4, pp. 9635–9642, 2016.

[71] ——, "Performance analysis of ldpc-coded diversity combining on rayleigh fading channels with impulsive noise," *IEEE Transactions on Communications*, vol. 65, no. 6, pp. 2345–2356, 2017.

[72] D. Umehara, H. Yamaguchi, and Y. Morihiro, "Turbo decoding in impulsive noise environment," in *IEEE Global Telecommunications Conference, 2004. GLOBECOM'04.*, vol. 1. IEEE, 2004, pp. 194–198.

[73] W. Abd-Alaziz, M. Johnston, and S. Le Goff, "Non-binary turbo codes on additive impulsive noise channels," in *2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*. IEEE, 2016, pp. 1–5.

[74] W. Abd-Alaziz, Z. Mei, M. Johnston, and S. Le Goff, "Non-binary turbo-coded ofdm-plc system in the presence of impulsive noise," in *2017 25th European Signal Processing Conference (EUSIPCO)*. IEEE, 2017, pp. 2576–2580.

[75] J. Jin, H.-M. Oh, S. Choi, J. Seo, and J.-J. Lee, "Performance of polar codes with successive cancellation decoding over plc channels," in *2015 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*. IEEE, 2015, pp. 24–28.

[76] A. Hadi, K. M. Rabie, and E. Alsusa, "Polar codes based ofdm-plc systems in the presence of middleton class-a noise," in *2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*. IEEE, 2016, pp. 1–6.

[77] Z. Mei, B. Dai, M. Johnston, and R. Carrasco, "Design of polar codes with single and multi-carrier modulation on impulsive noise channels using density evolution," *arXiv preprint arXiv:1712.00983*, 2017.

[78] M. Chitre, J. Potter, and O. S. Heng, "Underwater acoustic channel characterisation for medium-range shallow water communications," in *OCEANS'04. MTTS/IEEE TECHNO-OCEAN'04*, vol. 1. IEEE, 2004, pp. 40–45.

[79] G. Laguna-Sanchez and M. Lopez-Guerrero, "On the use of alpha-stable distributions in noise modeling for plc," *IEEE Trans. Power Del.*, vol. 30, no. 4, pp. 1863–1870, 2015.

[80] J. G. Gonzalez, J. L. Paredes, and G. R. Arce, "Zero-order statistics: a mathematical framework for the processing and characterization of very impulsive signals," *IEEE Transactions on Signal Processing*, vol. 54, no. 10, pp. 3839–3851, 2006.

[81] G. Samoradnitsky and M. S. Taqqu, *Stable non-Gaussian random processes: stochastic models with infinite variance*. Chapman and Hall/CRC, 1994.

[82] T. Richardson and R. Urbanke, *Modern coding theory*. Cambridge university press, 2008.

[83] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, "Llr-based successive cancellation list decoding of polar codes," *IEEE transactions on signal processing*, vol. 63, no. 19, pp. 5165–5179, 2015.

[84] G. A. Tsihrintzis and C. L. Nikias, "Performance of optimum and suboptimum receivers in the presence of impulsive noise modeled as an alpha-stable process," *IEEE Transactions on communications*, vol. 43, no. 234, pp. 904–914, 1995.

[85] S. Lin, D. J. Costello, and M. J. Miller, "Automatic-repeat-request error-control schemes," *IEEE Communications magazine*, vol. 22, no. 12, pp. 5–17, 1984.

[86] B. Zhao and M. C. Valenti, "Practical relay networks: a generalization of hybrid-arq," *IEEE Journal on selected areas in communications*, vol. 23, no. 1, pp. 7–18, 2005.

[87] Y. Yan, B. Zhang, D. Guo, S. Li, H. Niu, and X. Wang, "Joint beamforming and jamming design for secure cooperative hybrid satellite-terrestrial relay network," in *2016 25th Wireless and Optical Communication Conference (WOCC)*. IEEE, 2016, pp. 1–5.

[88] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *arXiv preprint arXiv:1202.5830*, 2012.

[89] H. Cao, Z. Mei, M. Johnston, and S. Le Goff, "Construction of polar codes combined with physical layer security on impulsive noise channels," in *2018 IEEE 18th International Conference on Communication Technology (ICCT)*. IEEE, 2018, pp. 181–185.

[90] E. Arikan and E. Telatar, "On the rate of channel polarization," in *2009 IEEE International Symposium on Information Theory*. IEEE, 2009, pp. 1493–1495.

[91] Y. Zhang, A. Liu, K. Pan, C. Gong, and S. Yang, "A practical construction method for polar codes," *IEEE Communications Letters*, vol. 18, no. 11, pp. 1871–1874, 2014.

[92] L. Li, W. Song, and K. Niu, "Optimal puncturing of polar codes with a fixed information set," *IEEE Access*, 2019.