Encrypted Polar Codes for Wiretap Channel

Fantao Wu
Institute of Signal Processing & Transmission
Nanjing University of Posts & Telecommunications
Nanjing, China
1010010426@njupt.edu.cn

Chao Xing
Institute of Signal Processing & Transmission
Nanjing University of Posts & Telecommunications
Nanjing, China
dongni_xc@163.com

Shengmei Zhao
Institute of Signal Processing & Transmission
Nanjing University of Posts & Telecommunications
Nanjing, China
zhaosm@njupt.edu.cn

Feng Gao
Institute of Signal Processing & Transmission
Nanjing University of Posts & Telecommunications
Nanjing, China
peak.up@163.com

***Abstract*—The wiretap channel proposed by Wyner is an important model of physical layer for security, where the channel between legal users (Alice and Bob) is called the main channel and the channel between eavesdropper and legal users is called eavesdropping channel. The channel coding technique has proven to good means to ensure the security of the Wyner wiretap channel. Recently, polar codes attract a lot of attentions due to their capacity-achieving property. In this paper, we propose a novel construction method for achieving more large secrecy capacity of wiretap channel with polar codes. In the scheme, we integrate encryption algorithm to the construction of polar code and prove the validity, reliability, and security of the proposed scheme in theory. Later, we present the transmission rate of the scheme by numerical simulations. The numerical simulation results show that the secrecy transmission rate can be improved significantly and a larger secrecy transmission rate could be achieved by the proposed scheme.**

Keywords-Wiretap channel; polar codes; channel polarization; encryption

I. INTRODUCTION

The security of wireless communications brings a big challenge to us with the more and more applications within wireless communications [1]. The encryption technology that have used in the high-level information security technologies, are now difficult to achieve, because of the emergence of a variety of wireless networks and the too complicated algorithms [1]. Currently, the physical layer security becomes an important branch of information security, where the wiretap channel is an important eavesdropping model, and the secrecy capacity is an important parameter for Wiretap channel. Here, the secrecy capacity C_s is defined as the biggest transmission rate of the system when the eavesdropper has the largest uncertainty about the message [2].

It is shown that the channel coding technique is a good means to ensure the security of the Wyner wiretap channel [1]. For example, in 2005, A. Thangara et.al discussed the way to get the secrecy capacity of the system using low-density parity-check (LDPC) codes in the wiretap channel, in which the main channel is noiseless channel and the wiretap channel is binary erasure channel(BEC) [3,4]; In 2009, D. Klinc studied Gaussian wiretap channel using puncturing LDPC codes to make the eavesdropper hardly get any information when the Signal to Noise Ratio(SNR) of the wiretap channel is smaller than the SNR of the main channel[5]; In 2011, V. Rathi et.al researched BEC wiretap channel using convolutional LDPC codes to make the transmission rate get the whole rate-achieving area [6].

Compared with LDPC codes, Polar codes have low complexity encoding and decoding algorithm, and have been proven to be capacity-achieving codes for Binary Symmetric Channel (BSC), and then or arbitrary binary-input discrete memoryless channels (DMCs) [7,8]. Since Polar codes have capacity-achieving property, they attract attentions and the application in Wyner wiretap channel [9-15]. In 2010, E.Hof and S.Shamai considered the use of Polar Codes in Wyner wiretap channel, and studied the construction of Polar codes to reach the secrecy capacity [14]. Meanwhile, H.Mahdavifar and A.Vardy presented the construction from the strong security condition and weak security condition [15]. However, in both cases, the information bits could be only transmitted through the bit-channels good for Bob but bad for Eve. That will limit the secrecy capacity of the Wyner wiretap channel.

In this paper, we propose a construction method for achieving larger secrecy capacity by integrating the encryption technique into the construction of Polar codes. We analyze the performance of the proposed construction method both from the theoretical proof and the numerical simulations. All the results show that the novel construction method could improve the secrecy capacity significantly.

This paper is organized as following. In section II, we shortly review construction method with Polar codes in the Wyner wiretap channel. In section III, we present our novel construction method with Polar codes and encryption, and discuss about our new scheme in theory. In section IV, we analyze the performance of encrypted Polar codes in the wiretap channels through the numerical simulation. In section V, we draw the conclusion.

II. WIRETAP CHANNEL WITH POLAR CODES

A. Wiretap channel model

The notion of wiretap channels was put forward by Aaron Wyner [2]. In the model, the legal users, Alice and Bob, send messages through a communication channel C_m, called the main channel, and the eavesdropper Eve steals the information from another channel C_w, called the wiretap channel. This is illustrated in Figure 1, wherein U denotes a k-bits message that

Alice will send to Bob, and U is considered as a random bits that takes values in $\{0,1\}^k$; U will be encoded to a sequence X of n-bit by coding. This sequence is transmitted across the main channel and the wiretap channel resulting in the corresponding channel outputs Y and Z. Finally, the decoder maps Y into an estimate $\hat{U}$ of the original message. Wyner has proven the existence of the channel coding that can ensure the information transmission between legal users effectively and securely for degradation channel [2].

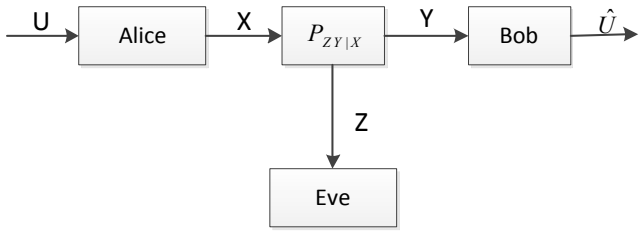

Figure 1. The model of the wiretap channel

B. Polar code

Polar codes were introduced by Arikan in 2007 and were shown to be capacity achieving for a large class of channels [7].Channel polarization is the critical theory of polar codes [7,8]. Channel polarization is an operation by which one manufactures out of N independent copies of a given binary-input discrete memoryless channel (B-DMC) W a second set of N channels $\left\{W_N^{(i)} : 1 \le i \le N\right\}$ that show a polarization effect in the sense that, as N becomes large, the bit-channel is close to either a noiseless channel or a pure-noise channel[7]. This operation consists of a channel combining phase and a channel splitting phase, combining N copies of a given B-DMC W in a recursive manner to produce a vector channel W_N or splitting W_N back into a set of N binary-input coordinate channels $W_N^{(i)}$ where N can be any power of two, $N = 2^n$, $n \ge 0$ [7]. Given a B-DMC W, there are two channel parameters of primary interest: the symmetric capacity I(W) and the Bhattacharyya parameter Z(W). These parameters are used as measures of rate and reliability, respectively. I(W) is the highest rate at which reliable communication is possible across W. Z(W) is an upper bound on the probability of maximum-likelihood (ML) decision error when W is used only once to transmit a 0 or 1[7].

Polar codes can be identified by a parameter vector (N, K, A, u_{A^c}), where K is the dimension of the information and N is the length of the code, a subset A of the bits, set $u(i) = 0$ for $i \in A^c$. We call A^c the frozen set, and the bits $\{u(i)\}_{i \in A^c}$ frozen bits. If we use u_A to represent the information to be transmitted, u_{A^c} are frozen bits or vector which is used to transmit fix information. The encode mapping of polar codes can be written as

$$x_1^N = u_A G_N(A) \tag{1}$$

where $G_N(A)$ is the submatrix of G formed by rows with indices in A. In addition to successive cancellation (SC) decoding algorithm, belief propagation (BP) decoding algorithm has applied to obtain better performance while keeping the decoding complexity at $O(N \log N)$ [16].

C. Construction method in Wiretap channel with Polar code

In order to achieve the secrecy capacity of wiretap channel, a construction method for the construction of polar code was described [15]. Because the wiretap channel is the degradation channel of the main channel, we could divide the bit-channels into three parts after channel polarization, such as, bit-channels good both for Bob and Eve, bit-channels good for Bob but bad for Eve, bit-channels bad for both Bob and Eve. The information bits are only transmitted through the bit-channels good for Bob but bad for Eve for security, we name them the secrecy bits S.

However, when the length of the code N is limited or the degradation degree of the wiretap channel is small, the transmission rate of the construction method may not be good. Furthermore, a lot of information bits, bit-channels good for Bob are unused, and the secrecy capacity is limited. In next section, we will discuss a new construction method that can transmit information securely and use the information bits efficiently. The new scheme could enhance the secrecy transmission rate when the secrecy bits S is limited.

III. WIRETAP CHANNEL WITH ENCRYPTED POLAR CODES

In this section, we propose a novel construction of polar codes in Wyner wiretap channel. Here, we combine polar codes with the encryption method to improve the secrecy transmission rate. This is illustrated in Figure 2. In Wyner wiretap channel, the wiretap channel is the degradation channel of the main channel, so the bit-channels could be divided into three parts by channel polarization in polar codes. The first part is the bit-channels which are good both for Bob and Eve, which is used to transmit the random bit in [14], now we use it to transmit the encrypted information bit. The second part is the bit-channels which are good for Bob but bad for Eve, we use it to transmit the keys instead of information bits in [14]. And the third part is the bit-channels bad for both Bob and Eve, we keep them as the frozen bits. In order to keep the security, we may use one-time padding encryption strategy. Since the keys are transmitted through those bit-channel good for Bob but bad for Eve, Bob could retrieve the keys and Eve has no possibility to access the keys. Of course, after the key distribution, the bit-channel good for Bob could be used to transmit the encrypted information bits. The novel construction could be described by Fig.2.

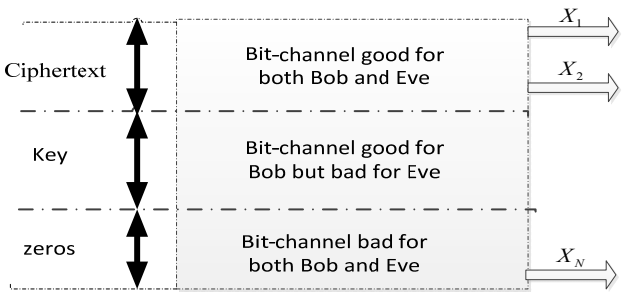

Figure 2. The schematic of the novel construction method

Here we describe the construction method in detail

(1) Distributing the key bits. Alice produces a random sequence as a short key, and then expands it into the sequence as long as the message U. Here, we choose part of the bit-channels good for Bob but bad for Eve to transmit the short key to promise that the rest of bit-channels good for Bob are multiples of the short key. There are many ways to expand the short key, here, we choose the most simple reproduction mode to expand and each short key is used only once. The key is described as

$$k = random(j_1, j_2, \cdots, j_t), t < |u|, j = 0,1 \quad (2)$$

$$u_k = (k, k, \cdots, k), |u_k| = |U| \quad (3)$$

(2) Encrypting the information. Alice encrypts the information bits U to get the ciphertext. There are various encryption methods, here we use the simple way, where the cipertext is

$$m = E_k(u) = u \oplus u_k \quad (4)$$

(3) Constructing Polar Code with the ciphertext and key. We let the bit-channels good for Bob be divided into two parts to transmit the ciphertext and the key, respectively. Here, we also use S to denote bit-channels those are used to transmit the key. From Eq (1), we can know that the encoding can be described as

$$x = mG_n(A_m \setminus S) + kG_n(S) \quad (5)$$

After channel encoding, the code words X is sent to Bob and Eve through the main channel and the wiretap channel.

(4) Decoding at the legal user and eavesdropper user. After decoding, Bob first get the key, and then the information bits, so he can get the right information. Eve can not get the key, so she can not get the information through decryption.

We could prove the validity, reliability and security of the proposed construction method. We denote the channel capacity of the main channel C_M and the wiretap channel C_W. The secrecy capacity $C_s = C_M - C_W$, and $C_s < C_M$ according to the definition of the secrecy capacity. When the degree of degradation of Wyner wiretap channel is small, $C_s \ll C_M$.

The validity. The validity means the efficiency of the information transmission. The bigger the transmission rate, the higher the validity is. The difference between our construction method and the former is that the secrecy bits S are used to send the key instead of the information. When $C_s \ll C_M$, the length of S is far smaller than the number of the information bits, $|S| \ll |A_m|$, then the transmission rate is:

$$R_k = \frac{|k|}{N}, |k| \le |S| \quad (6)$$

$$R_m = \frac{|A_m| - |k|}{N} \quad (7)$$

$$R = R_m + R_k \quad (8)$$

Where N is the length of the code, R_k is the transmission rate of the key, $|A_m|$ is the good bit-channels number of the main channel, R_m is the transmission rate of the ciphertext. The transmission rate R is the sum of R_k and R_m. The transmission rate of the information U is same with R_m, $R_m = R_u$. For $|k| \le |S| \ll |A_m|$, we can draw

$$R_u = \frac{|A_m| - |k|}{N} \approx R \quad (9)$$

$$\lim_{R_k \to 0} R_u = R \quad (10)$$

The Eq （10） is an ideal, because $R_k \to 0$ means that the infinite of the code length N or the infinitely small of the key's length, the two situations are not realistic.

The reliability. The reliability can be qualified by the bit error rate (BER) of the transmission. We will discuss the reliability of the key and the ciphertext separately. From the above discussion we can know that $S \subset A_m$ and $S \not\subset A_w$, where A_W is the parameter of the wiretap channel, the collection of the noiseless bit-channels. So the BER of Bob and Eve to receive the key are completely different. From the theory of the polar codes, we can know the BER of Bob and Eve to receive the key are

$$P_B^{\,k} \le \sum_{i \in S} Z(W_N^{(i)}) \le 2^{-N^\beta} \quad (11)$$

$$P_E^{\,k}(j) \to 0.5 \quad (12)$$

Where P_B^k and P_E^k are the BER of Bob and Eve to receive the key. Bob can nearly get the right key, but Eve can hardly get the right key.

The reliability to transmit the ciphertext is same with the former scheme of the polar codes. We can easy get the BER of Bob and Eve to receive the ciphertext

$$P_B^m = P_E^m = o(2^{-N^\beta}) \quad (13)$$

The security. Here, the security is defined as the probability for eavesdropper to get the correct information from the ciphertext. From the Eq （11）and（12）, we can know that Bob can get the key, but Eve can not get any information about the key. From the Eq (11) and (13), we can know that:

$$P_B^{\,k}(k \ne \hat{k}) \to 0 \quad (14)$$

$$P_B^{\,m}(m \ne \hat{m}) \to 0 \quad (15)$$

For $\hat{u} = \hat{m} \oplus \hat{u}_k$ and $\hat{m}$, $\hat{u}_k$ are independent of each other, we can know the probability of Bob getting the correct information is

$$P_B(u = \hat{u}) \approx (1 - P_B^{\,k})^{|u|} \cdot (1 - P_B^m)^{|u|} \to 1 \quad (16)$$

Similarly, the probability of Eve getting the correct information is

$$P_E(u = \hat{u}) \approx (1 - P_E^{\,k})^{|u|} \cdot (1 - P_E^m)^{|u|} \approx (\frac{1}{2})^{|u|} \quad (17)$$

The probability for Eve to get the correct information decreases with the length of the information.

From the analysis, we could conclude that the new construction scheme can ensure the security and reliability of the transmitted information bit and improve the validity of the transmission.

IV. SIMULATIONS

In this section, we will verify the proposed construction method by numerical simulation. We assume both the main channel and the wiretap channel are Gaussian channels, and the wiretap channel is the degradation of main channel. Here, we use successive cancellation (SC) decoding algorithm in the simulation.

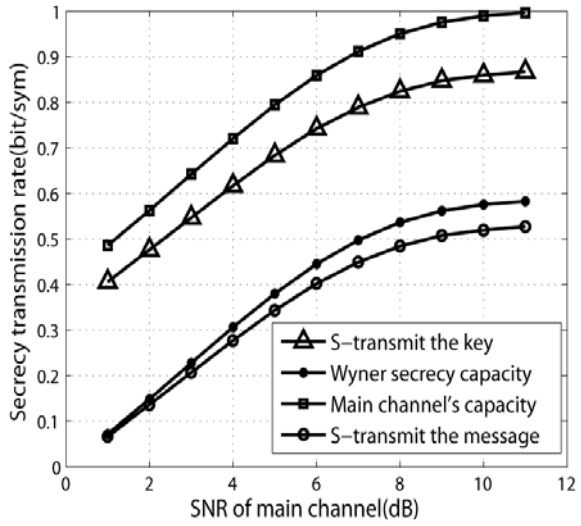

Figure 3. The compare of the secrecy transmission rate

Figure 3 is the compare of the secrecy transmission rate of the two construction method. The code length is set up to 1024, and the SNR of the wiretap channel is set up to 0dB. When the SNR of the main channel is 1dB, the secrecy transmission rate of our new scheme is about 0.4, the secrecy transmission rate of the former scheme is about 0.05, the capacity of the main channel is about 0.5, and the Wyner secrecy capacity is about 0.05; When the SNR of the main channel is 10dB, the secrecy transmission rate of our new scheme is about 0.85, the secrecy transmission rate of the former scheme is about 0.5, the capacity of the main channel is about 1, and the Wyner secrecy capacity is about 0.6. By comparing, we can know that the secrecy transmission rate of our new scheme is much bigger than the former scheme, our new construction method improves the secrecy transmission rate greatly. The limit of the former scheme's secrecy transmission rate is Wyner secrecy capacity. The limit of our new construction method's secrecy transmission rate is the capacity of the main channel. By comparing, we can know that our new construction method improves the secrecy capacity greatly.

V. CONCLUSION

In this paper, we propose a novel construction method in wiretap channels with polar codes to achieve larger secrecy capacity. We integrate the encryption algorithm to the construction of polar codes for wiretap channel in the construction method. We have proven the validity, reliability and security of the proposed scheme in theory. Meanwhile, we present the performance of the proposed scheme by numerical simulation. The results have shown that we could get the secrecy transmission rate as large as the main channel capacity by the proposed scheme.

ACKNOWLEDGMENT

The work was supported in part by the National Natural Science Foundation of China (Grant No. 61271238), the University Natural Science Research Foundation of JiangSu Province (11KJA510002), the open research fund of National Laboratory of Solid State Microstructures (M25020,M25022), the Foundation (No.NJ210002), the open research fund of Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education (ZD035001 NYKL01), the project funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions, and Image Processing and Image Communication Jiangsu Key Laboratory.

REFERENCES

[1] Mohammad Ghulam Rahman and Hideki Imal, "Security inWireless Communication," Wireless Personal Communication., pp.213-228,2002

[2] A.D.Wyner, "The wire-tap channel," Bell System Tech. vol. 54, no.8, pp.1355–1387, 1975

[3] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin and J.M. Merolla, "On Achieving Capacity on the Wire Tap channel using LDPC Codes." IEEE Int. Symp. Information Theory (ISIT), pp.1498-1502, 2005

[4] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin and J. M. Merolla., "Applications of LDPC Codes to the Wiretap Channel." IEEE Trans. Inf. Theory, vol. 53, no.8, pp.2933-2945, 2007

[5] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros and B. J. Kwak., "LDPC codes for the Gaussian Wiretap Channel." IEEE Trans.Inf. Theory Workshop(ITW), pp.95-99, 2009

[6] V. Rathi, R. Urbanke, M. Andersson and M. Skoglund, "Rate-Equivocation Optimal Spatially Coupled LDPC Codes for the BEC Wiretap Channel." IEEE Int. Symp. Information Theory (ISIT), pp.2393-2397, 2011

[7] E.Arikan, "Channel Polarization: A method for constructing capacity-achieving codes for symmetric bianry-input memoryless channels," IEEE Trans. Inf. Theory, vol.55, no.7, pp.3051-3073, 2009

[8] S.Korada, R.Urbanke, and E.Sasoglu, "Polar codes: Characterization of exponent, bounds, and constructions," IEEE Int. Symp. Informaiton Theory, pp.1483-1487, 2009

[9] S.B. Korada and R.L. Urbanke, "Polar codes are optimal for lossy source coding," IEEE Trans. Inf. Theory, pp.1751 –1768, 2010

[10] M. Karzand and E. Telatar, "Polar codes for Q-ary source coding," In Proc. IEEE Int. Symp. Information Theory (ISIT), pp 909 –912, 2010

[11] R.Mori and T.Tanaka, "Non-binary Polar codes susing Reed-Solomon codes and algebraic geometry codes," IEEE Trans. Inf. Theory Workshop(ITW), pp.1-5, 2010

[12] N. Hussami, S.B. Korada, and R. Urbanke, "Performance of Polar codes for channel and source coding," In Proc. IEEE Int. Symp. Information Theory (ISIT), pp 1488 –1492, 2009

[13] E. Abbe and E. Telatar, "MAC Polar codes and matroids," In Proc. Workshop on Information Theory and Applications (ITA), pp.1–8, 2010

[14] E.Hof and S. Shamai, “Secrecy-achieving polar-coding,” IEEE Trans. Inf. Theory, pp.1-5, 2010

[15] H.Mahdavifar and A.Vardy, “Achieving the secrecy capapcity of Wiretap channels using Polar codes,” IEEE Int. Symp. Information Theory (ISIT), pp.913-917, 2010

[16] E. Arıkan, “A performance comparison of polar codes and Reed-Muller codes,” IEEE Commun. Lett., vol. 12, no.6, pp. 447-449, 2008