A Feedback-based Secrecy Coding Scheme Using Polar Code over Wiretap Channels

Liuyihan Song[1] Lei Xie[*,1,2] Huifang Chen[1,2] Kuang Wang[1,2]
[1]Dept. of Information Science and Electronic Engineering, Zhejiang University
[2]Zhejiang Provincial Key Laboratory of Information Network Technology
No. 38, Zheda Road, Hangzhou 310027, China
{slyh; xiel; chenhf; wangk}@zju.edu.cn

Abstract — Polar codes can be used to achieve secrecy capacity of degraded wiretap channels. In this paper, we propose a feedback-based secrecy coding scheme using polar code over non-degraded wiretap channels. With the feedback architecture, the proposed secrecy coding scheme can significantly obtain a positive secrecy rate. Moreover, polar codes have low complexity of encoding and decoding, which is good for implementing. Simulation results show that the proposed feedback-based secrecy coding scheme using polar code can transmit confidential messages reliably and securely. Moreover, the impact of the conditions of the forward channels and feedback channels on the performance of the proposed secrecy coding scheme are analyzed.

Keywords—Polar code; feedback; non-degraded wiretap channels; secrecy code

I. Introduction

With the development of wireless networks, security issue becomes more and more important. Achieving both reliable and secure communication over wiretap channels has been a hot research topic during the past few years. Many secrecy coding schemes are proposed to transmit confidential messages reliably between legitimate users, and keep messages be intercepted from the eavesdropper.

In 1975, Wyner introduced the generic degraded wiretap channel model [1]. It is proved that there exists a secrecy capacity $C_S>0$ over degraded wiretap channels, which means that if the secrecy rate is less than C_S, there exist coding schemes achieving both reliable and secure communication asymptotically. In 2007, Arikan invented Polar codes [2], which are the first class of codes be proved to asymptotically achieve the symmetric capacity of discrete memoryless channels and with low encoding and decoding complexity. Because of these advantages, polar codes are used to achieve secrecy capacity over wiretap channels. The secrecy coding schemes based on polar code over degraded wiretap channels were proposed in [3-5]. And it was proved that both the secrecy capacity and the rate-equivocation region are achievable.

However, over non-degrade wiretap channels, Wyner's coding scheme cannot provide any positive secrecy rate to ensure secure communication. In this situation, some mechanisms proposed recently might be used to equivalently transform non-degraded wiretap channels to degraded ones. In [6], a feedback coding structure is proposed to reach this purpose and achieve a strictly positive secrecy rate even though the wiretap channel is less noisy than the channel between legitimate users. However, it was shown in [6] only that the secrecy code exists, and did not present a secrecy coding scheme to achieve the positive rate as large as possible.

In this paper, by introducing the feedback structure and constructing two level polar coding, a feedback-based secrecy coding scheme using polar code to achieve the positive secrecy rate over non-graded wiretap channels is proposed. We prove the reliability and security of the proposed secrecy coding scheme. Simulation results are given to show the proposed secrecy coding scheme can achieve reliable and secure communication. And the impact of the conditions of forward and feedback channels on the performance of the proposed secrecy coding scheme are discussed.

The remainder of the paper is organized as follows. In Section II, the feedback coding structure over non-degrade wiretap channels and the positive achievable secrecy rate is introduced. We present a feedback-based secrecy coding scheme using polar code over non-degrade wiretap channels in Section III. In Section IV, the proposed secrecy coding scheme is evaluated by simulations. Finally, we give the conclusions in Section V.

II. Problem Formulation

In this section, we give a review about the feedback-based coding structure in [6].

As shown in Fig.1, a feedback channel is set up between two legitimate users, Bob and Alice. As an eavesdropper, Eve can also get access to the feedback channel from Bob to Alice. For simplicity, we treat all the channels between users as binary symmetric channels (BSCs). We denote the crossover probability of the forward channel from Alice to Bob be ϵ_f and the crossover probability from Alice to Eve be δ_f. Let the crossover probability of the feedback channel from Bob to Alice be ϵ_b, from Bob to Eve be δ_b. Because the forward wiretap channel are non-degraded, we assume $\epsilon_f \geq \delta_f$.

The process of transmitting confidential messages using the feedback-based secrecy coding structure can be conceptually described as follow.

[*] Corresponding author: Lei Xie, xiel@zju.edu.cn, +86-571-8795-2017

This work was partly supported by the National High Technology Research and Development Program (863) of China (No. 2012AA01A502), the Zhejiang Provincial Natural Science Foundation of China (No. LY14F010014).

978-1-4799-7339-2/14/$31.00 ©2014 IEEE

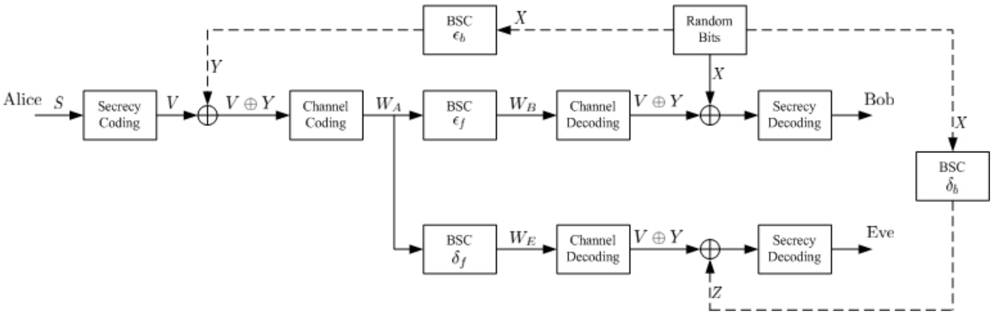

Fig.1 Feedback-based secrecy coding model over wiretap channels

(1) When a transmission starts, Bob feeds back an n-bit sequence $\mathbf{x}$ to Alice. The sequence $\mathbf{x}$ is generated by the independent realizations of a Bernoulli random variable with expectation 0.5 for n times. Since the sequence bits are i.i.d and the error probabilities of each bits are corresponding to the crossover probability of feedback channels, the feedback sequences received by Alice and Eve are $\mathbf{y}$ and $\mathbf{z}$, respectively.

(2) Assuming both forward channels from Alice to Bob and from Alice to Eve are error-free. If Alice wants to send an n-bit sequence $\mathbf{v}$ to Bob, she must send $\mathbf{v} \oplus \mathbf{y}$ instead, here $\oplus$ denotes mod 2 addition. Hence, Alice and Bob receive $\mathbf{v} \oplus \mathbf{y}$ without any errors.

(3) After the sequence $\mathbf{v} \oplus \mathbf{y}$ received, the optimal strategy for Bob to recover $\mathbf{v}$ is to calculate $\mathbf{v} \oplus \mathbf{y} \oplus \mathbf{x}$, and the optimal way for Eve is to calculate $\mathbf{v} \oplus \mathbf{y} \oplus \mathbf{z}$.

As a consequence of the feedback-based secrecy coding structure, the equivalent bit error probability to Bob denoted as e_B is ϵ_b, while to Eve e_E is $\epsilon_b + \delta_b - 2\epsilon_b\delta_b$. As $e_E - e_B = \delta_b(1 - 2\epsilon_b) \geq 0$, we obtain an equivalent system where the wiretap channel after channel decoding is a degraded version of the main channel, as shown in Fig. 2.

To obtain the equivalent degraded wiretap channel, the only limitation is that the forward channels are not really error-free. However, according to the channel coding theory, if the n-bit sequence $\mathbf{v} \oplus \mathbf{y}$ is transmitted at a rate less than the capacity of the channel from Alice to Bob, there exists a coding scheme achieving error-free transmission asymptotically. Here, since $C_{AB} = 1 - h(\epsilon_f)$, $C_{AE} = 1 - h(\delta_f)$, $C_{AE} \geq C_{AB}$. Hence, the reliable transmission is achievable asymptotically as long as the transmission rate is less than C_{AB}.

Let $R_{s,u}$ be the maximum secrecy rate after secrecy coding. That is,

$$R_{s,u} = h(\epsilon_b + \delta_b - 2\epsilon_b\delta_b) - h(\epsilon_b) \tag{1}$$

In the feedback-based secrecy coding structure, we use k_1 bits carrying $nR_{s,u}$ secrecy bits, and then encode the k_1 bits to be the n-bit sequence $\mathbf{v}$. Assume Alice transmits confidential messages $\mathbf{v} \oplus \mathbf{y}$ at rate R_{AB} and let $R_{AB} < C_{AB}$. So, after channel coding, the transmitting sequence w_A is $\frac{n}{R_{AB}}$ bit. Then, we obtain an overall secrecy rate, $R_{s,0}$, as

$$R_{s,0} = \frac{nR_{s,u}}{n/R_{AB} + n} = R_{s,u}\frac{R_{AB}}{R_{AB} + 1} \tag{2}$$

In (2), the overall secrecy rate is always less than the equivalent rate $R_{s,u}$ with a coefficient $\frac{R_{AB}}{R_{AB}+1}$ which is the trade-off after introducing feedback.

To achieve the secrecy rate $R_{s,0}$ as large as possible, we should design a secrecy coding scheme to make both $R_{s,u}$ and R_{AB} be maximum simultaneously, where $R_{s,u}$ and R_{AB} denote the secrecy capacity over the equivalent degraded wiretap channels and the forward channel capacity from Alice to Bob, respectively.

III. Proposed Secrecy Coding Scheme Using Polar Code

A. Secrecy Coding Scheme

The proposed secrecy coding scheme is divided into two parts, secrecy coding over the equivalent degraded wiretap channels and channel coding over the forward non-degraded channels.

First, after generating the confidential message $\mathbf{v}$, Alice computes $\mathbf{v} \oplus \mathbf{y}$, and uses a channel coding encoder to achieve the forward channel capacity from Alice to Bob.

The proposed channel coding scheme is by carefully choosing suitable $M = 2^k, k \in N^*, \beta_c < \frac{1}{2}$ so that $|\{i \in [M], Z(W_{AB}^{(i)}) < \frac{2^{-M^{\beta_c}}}{M}\}| = n$. The notation $|\mathcal{S}|$ denotes the size of set $\mathcal{S}$, $Z(W)$ denotes the Bhattacharyya parameter.

Second, we will consider the feedback-based secrecy coding over the equivalent degraded channels. In the equivalent degraded wiretap channel model, it is assumed that the main channel W^* is BSC with crossover probability ϵ_b and the degraded wiretap channel W is also BSC with crossover probability $\epsilon_b + \delta_b - 2\epsilon_b\delta_b$. For any fixed positive constant $\beta < \frac{1}{2}$, we define the good channels set $\mathcal{G}_n(W, \beta)$ and the bad channels set $\mathcal{B}_n(W, \beta)$ as

$$\begin{aligned} \mathcal{G}_n(W, \beta) &= \{i \in [n] : Z(W_n^{(i)}) < \frac{2^{-n^\beta}}{n}\} \\ \mathcal{B}_n(W, \beta) &= \{i \in [n] : Z(W_n^{(i)}) \geq \frac{2^{-n^\beta}}{n}\} \\ [n] &= \{1, 2, \ldots, n\} \end{aligned} \tag{3}$$

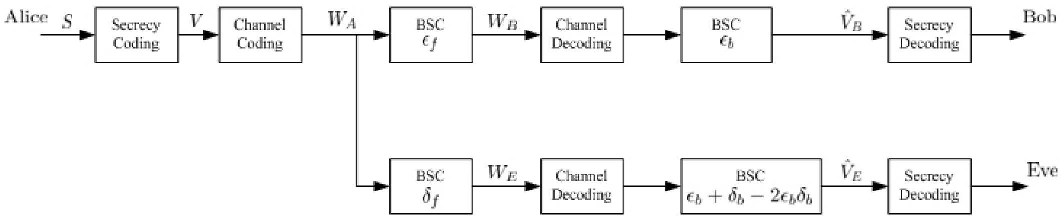

Fig. 2 The equivalent degraded wiretap channel

Because polar code requires the code length to be the exponent of 2, the input length of channel encoder does not always equal to the length of the secrecy encoder output. Since we should find a large enough integer $s \le n$, $s = 2^{n_1}, n = s + n_2, n_2 < s, n_1 \in N, n_2 \in N$.

For a given s and a fixed $\beta_s < \frac{1}{2}$, the secrecy coding sequence is divided into three subsets,

$$\begin{aligned} \mathcal{R} &\triangleq \mathcal{G}_s(W, \beta_s) \\ \mathcal{A} &\triangleq \mathcal{G}_s(W^*, \beta_s) \setminus \mathcal{G}_s(W, \beta_s) \\ \mathcal{B} &\triangleq \mathcal{B}_s(W^*, \beta_s) \end{aligned} \tag{4}$$

Notice that $\mathcal{R} \cup \mathcal{A} \cup \mathcal{B} = [s]$. The subset $\mathcal{A}$ represents the bit-channels which are good for Bob but bad for Eve, $\mathcal{R}$ is the good bit-channels set for Bob and Eve, and $\mathcal{B}$ corresponds to the set of the bit-channels that are bad for Bob and Eve.

Let $|\mathcal{A}| = k_1, |\mathcal{R}| = r$, the secrecy sequence $\mathbf{s} = m_{\mathcal{A}}$. We define $m_{\mathcal{S}} = [m_i : m_i \in \mathbf{m}, i \in \mathcal{S}]$, which denotes the projection of $\mathbf{m}$ on the coordinates in $\mathcal{S}$.

The encoding and decoding algorithms described as follows.

Encoding: The input sequence $\mathbf{m}$ is divided into three parts, $m_{\mathcal{A}}$, $m_{\mathcal{R}}$ and $m_{\mathcal{B}}$. $m_{\mathcal{A}}$ carries the secrecy bits generated from the secrecy source, $m_{\mathcal{R}}$ is selected by Alice uniformly from independent (0,1) Bernoulli experiments. $m_{\mathcal{B}}$ is considered as frozen bits set which are already known to Bob and Alice. According to the standard polar coding method, the output sequence $\mathbf{v} = \mathbf{m}G_s = \mathbf{m}R_s F^{\otimes k_1}$.

Decoding: Formally, the successive cancellation (SC) decoding algorithm is used to recover the confidential message $\hat{m}_{\mathcal{A}}$ at the decoder.

Since the length of secrecy sequence and channel sequence is a power of 2, sometimes we cannot make full use of *n* good bit channels in the forward channel. This is the limitation of the feedback-based secrecy coding scheme using polar code.

The complexity of encoding and decoding implementation is $O(nlogn)$, for secrecy coding is $O(slogs)$ while channel coding is $O(nlogn)$.

Therefore, the overall feedback-based secrecy coding scheme uses two level polar coding. The first level implements secrecy coding, and the second level implements channel coding.

B. Performance Analysis

It has been proved in [3] that the secrecy coding scheme can achieve the secrecy capacity C_s over the degraded wiretap channels. Let the secrecy rate $R_1 = \frac{k_1}{s}$, $\lim_{n\to\infty} R_1 = C_s = C(W^*) - C(W)$.

Theorem 1 [7]: For the channel coding, if we choose suitable $M, \beta_c < \frac{1}{2}$ so that $|\{\mathcal{G}_M(W_{AB}, \beta_c)\}| = n$. Denote W_{AB} as the forward channel from Alice to Bob, the rate R_{AB} has the limitation

$$\lim_{n\to\infty} R_{AB} = \lim_{n\to\infty} \frac{n}{M} = C_{AB} \tag{5}$$

Proposition 2: When the length of the secrecy sequence equals to the total number n of good channel bits over the forward channel, the proposed feedback-based secrecy coding scheme using polar code achieves the overall secrecy rate

$$R_{s,0} = R_{s,u} \frac{C_{AB}}{1 + C_{AB}} \tag{6}$$

Proof: With the feedback secrecy coding structure, we obtain [6]

$$R_{s,0} = R_{s,u} \frac{R_{AB}}{1 + R_{AB}} \tag{7}$$

As the code length asymptotically goes to infinity, the secrecy rate $R_{s,u}$ achieves the secrecy capacity C_s while the channel transmission rate R_{AB} can be written as

$$R_{AB} = C_{AB} \frac{s}{n} \tag{8}$$

The overall secrecy rate is

$$\begin{aligned} R_{s,0} &= R_{s,u} \frac{sC_{AB}/n}{1 + sC_{AB}/n} \\ &= R_{s,u} \frac{C_{AB}}{C_{AB} + n/s} \end{aligned} \tag{9}$$

Since both the length of the secrecy code and the length of the channel code are required as the exponent of 2, the coefficient $c = \frac{n}{s}$ is added in the denominator. As $\frac{n}{s} \ge 1$, the maximum of the overall secrecy rate $R_{s,0}$ is $R_{s,u} \frac{C_{AB}}{C_{AB}+1}$ when $s = n$. Hence, only special cases, such as $C_{AB} = 2^{-n}, n \in N$, would achieve the maximum secrecy rate. □

From Proposition 2, we also find that the positive secrecy rate is always achievable by the proposed secrecy coding scheme.

As a secrecy coding scheme, its reliability and security need to be proved theoretically. Here, two metrics are used to explain the proposed secrecy coding scheme can achieve both reliability and security.

$$\begin{aligned} \text{reliability: } \lim_{n\to\infty} P_e &= \lim_{n\to\infty} Pr\{\hat{s} \neq s\} = 0 \\ \text{security: } \lim_{k\to\infty} \Delta &= \lim_{k\to\infty} \frac{1}{k} I(S; W_E) = 0 \end{aligned} \tag{10}$$

where, P_e measures the reliability. If P_e =0, confidential messages are transmitted without errors. Δ denotes the equivocation, which means the average uncertainty for confidential messages after the eavesdropper has received the estimations of confidential messages from the wiretap channel. If the equivocation equals to zero, it means that the eavesdropper cannot get effective information of confidential messages. In the other words, the transmission is secure.

Theorem 3: The proposed feedback-based secrecy coding scheme using polar code achieves both reliability and security asymptotically.

Proof: Assume that the receiver uses successive cancellation decoder. Let the channel W_{XY} be the one from user X to user Y, and $\mathcal{A}_M = \mathcal{G}_M(W_{AB}, \beta)$. Hence, the block error rate in the channel W_{AB} is

$$Pr\{\hat{v} \neq v\} \leq \sum_{i\in\mathcal{A}_M} Z(W_{AB}^{(i)}) \leq 2^{-M^{\beta}} \tag{11}$$

Let $Pr\{\hat{v} \neq v\} \triangleq e_M$, $\lim_{n\to\infty} e_M = 0$. Let $\phi(.)$ be the output of the secrecy decoder. Hence, we have

$$\begin{aligned} Pr\{\hat{s} \neq s\} &\overset{(a)}{\leq} (1 - e_M) Pr\{\phi(\hat{v}) \neq s\} + e_M \\ &\leq (1 - e_M) \sum_{i\in\mathcal{A}} Z(W_{BA}^{(i)}) + e_M \\ &\leq (1 - e_M) 2^{-n^{\beta_s}} + e_M \end{aligned} \tag{12}$$

Then,

$$\lim_{n\to\infty} Pr\{\hat{s} \neq s\} = 0 \tag{13}$$

where, the inequality (a) is satisfied for the reason that the block error rate of confidential messages is no more than the block error rate of transmitting over forward channel plus the block error rate for transmitting correctly over forward channel but secrecy decoding wrongly.

The equivocation of the eavesdropper Eve increases after introducing channel coding as

$$\begin{aligned} H(s|w_E, x \oplus e_{bE}) &\overset{(b)}{\geq} H(s|v \oplus y, x \oplus e_{bE}) \\ &= H(s|v \oplus e_{bE} \oplus e_{bA}, x \oplus e_{bE}) \\ &= H(s|v \oplus e_{bE} \oplus e_{bA}) \end{aligned} \tag{14}$$

where, the inequality (b) is satisfied because $s \to v \oplus y \to w_E$ forms Markov chain. Hence,

$$\begin{aligned} & I(s; w_E|x \oplus e_{bE}) \leq I(s; v \oplus y|x \oplus e_{bE}) \\ & H(s|x \oplus e_{bE}) - H(s|w_E, x \oplus e_{bE}) \leq \\ & H(s|x \oplus e_{bE}) - H(s|v \oplus y, x \oplus e_{bE}) \\ & H(s|w_E, x \oplus e_{bE}) \geq H(s|v \oplus y, x \oplus e_{bE}) \end{aligned} \tag{15}$$

Let W_E be the output of the wiretap channel, V_E is also the output of the wiretap channel but considered as a noiseless channel. As shown in (14), $I(S; W_E) \leq I(S; V_E)$.

Define $\lambda \triangleq Pr\{\hat{m}_{\mathcal{R}} \neq m_{\mathcal{R}}\} \leq \sum_{i\in\mathcal{R}} Z(W_{BE}^{(i)}) \leq 2^{-n^{\beta}}$. With Fano inequality, we have

$$H(M_{\mathcal{R}}|W_E, M_{\mathcal{A}}) \leq h(\lambda) + |\mathcal{R}|\lambda \tag{16}$$

where, $h(p) = -p \log p - (1 - p) \log(1 - p)$. Then,

$$\begin{aligned} I(S; V_E) &= I(M_{\mathcal{A}}; V_E) = I(M_{\mathcal{A}\cup\mathcal{B}}; V_E) \\ &= I(M; V_E) - I(M_{\mathcal{R}}; V_E|M_{\mathcal{A}\cup\mathcal{B}}) \\ &= I(M; V_E) - H(M_{\mathcal{R}}|M_{\mathcal{A}}) + H(M_{\mathcal{R}}|V_E, M_{\mathcal{A}}) \\ &= I(M; V_E) - H(M_{\mathcal{R}}) + H(M_{\mathcal{R}}|V_E, M_{\mathcal{A}}) \\ &\leq nC(W_{BE}) - r + h(\lambda) + r\lambda \\ &= n(C(W_{BE}) - r/n) + h(\lambda) + r\lambda \end{aligned} \tag{17}$$

and

$$\begin{aligned} \lim_{n\to\infty} \frac{I(S; V_E)}{n} &\leq \lim_{n\to\infty} (C(W_{BE}) - r/n) + \lim_{n\to\infty} \frac{1}{n}(h(\lambda) + r\lambda) \\ &\leq \lim_{n\to\infty} (C(W_{BE}) - \frac{|\mathcal{G}_n(W_{BE}, \beta_s)|}{n}) + \\ &\qquad \lim_{n\to\infty} \frac{1}{n}(h(2^{-n^{\beta}}) + r2^{-n^{\beta}}) \\ &= 0 \end{aligned} \tag{18}$$

As $k = \Theta(n)$ and $\lim_{k\to\infty} \frac{I(S;V_E)}{k} = 0$, For $I(S; W_E) \leq I(S; V_E)$,

$$\lim_{k\to\infty} \Delta = \lim_{k\to\infty} \frac{I(S; W_E)}{k} \leq \lim_{k\to\infty} \frac{I(S; V_E)}{k} = 0 \tag{19} \square$$

IV. SIMULATION RESULTS

In this Section, we evaluate the performance of the proposed feedback-based secrecy coding scheme using polar code. The bit error rate (BER) of Bob and Eve is used to show the reliability and security of the proposed scheme. Let P_B and P_E be the BER of Bob and the BER of Eve, respectively. The best condition for the proposed feedback-based secrecy coding scheme using polar code is $P_B \approx 0, P_E \approx 0.5$, where P_B means the reliability and P_E means the security.

For BSCs, a heuristic method presented in [8] is used to construct polar codes. The decoder of polar codes uses the successive cancellation algorithm to recover the messages.

Fig. 3 shows the impact of the code length, *M*, on the reliability and security of the proposed feedback-based secrecy coding scheme using polar code, where the parameters of non-degraded wiretap channels are $\epsilon_f = 0.05, \delta_f = 0.03$, the parameters of the feedback channel are $\epsilon_b = 0.01, \delta_b = 0.2$. As *M* increases, we can always choose suitable β_c and β_s to obtain a secrecy rate $R_s \approx 0.115625$. From Fig. 3, we observe that when the code length increases, the reliability of the proposed secrecy coding scheme, P_B, approaches to 0, and the security of the proposed secrecy coding scheme, P_E, approaches to 0.5. Hence, the proposed feedback-based secrecy coding scheme with polar can achieve reliable and secure communication.

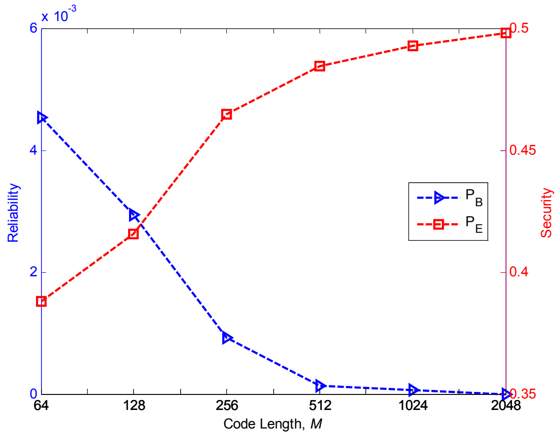

Fig. 3 The impact of the code length on the reliability and security of the proposed secrecy coding scheme, where $\epsilon_f = 0.05, \delta_f = 0.03$, $\epsilon_b = 0.01, \delta_b = 0.2$

Then, the impact of the channel parameters on the performance of the proposed secrecy coding scheme.

Table 1 shows the impact of the parameters of the forward channels, ϵ_f and δ_f, on the reliability and security of the proposed feedback-based secrecy coding scheme using polar code, where the parameters of the feedback channels are $\epsilon_b = 0.01, \delta_b = 0.2$, and $M = 128, R_s = 0.197917$. From Table 1, we observe that when the forward channel between Alice and Bob, W_{AB}, is getting worse, and the forward channel between Alice and Eve, W_{AE}, keeps constant, the reliability of the proposed secrecy coding scheme worsens, while the security of the proposed secrecy coding scheme keeps unchanged. Moreover, when W_{AB} keeps constant, and W_{AE} is getting worse, the reliability of the proposed secrecy coding scheme remains unchanged, while the security of the proposed secrecy coding scheme gets better. In addition, we also observe that a good secure communication achieves when the wiretap channel, W_{AE}, is the degraded version of W_{AB}, for example, for the case of $\epsilon_f = 0.04, \delta_f = 0.05$.

TABLE 1 THE IMPACT OF THE PARAMETERS OF THE FORWARD CHANNELS ON THE RELIABILITY AND SECURITY OF THE PROPOSED SECRECY CODING SCHEME

ϵ_f	δ_f	P_B	P_E
0.02	0.01	0.001012	0.469424
0.04	0.01	0.006891	0.469424
0.04	0.04	0.006891	0.469720
0.04	0.05	0.006891	0.470209

Therefore, when the feedback channels are given, the reliability of the proposed feedback-based secrecy coding scheme using polar code worsens as the condition of the forward channel between Alice and Bob gets worsen, while the security of the proposed feedback-based secrecy coding scheme using polar code gets better as the condition of forward channel between Alice and Eve gets worsen.

Table 2 lists the impact of the parameters of the feedback channels, ϵ_b and δ_b, on the reliability and security of the proposed feedback-based secrecy coding scheme using polar code, where the parameters of the forward channels are $\epsilon_f = 0.01, \delta_f = 0.01, M = 256$ and $R_s = 0.190104$. In Table 2, e_B and e_E denote the parameters of the equivalent degraded wiretap channels with feedback, respectively.

When the feedback channel between Bob and Eve, W_{BE}, gets worse, the reliability and security of the proposed feedback-based secrecy coding scheme using polar code get better. The reason for this phenomenon is that for the equivalent degraded wiretap channels, if the difference between the main channel and the wiretap channel gets wider, we can have more bit-channels good for Alice and bad for Eve to choose. In order to achieve a constant R_s, we could choose the bit-channels better for Bob and worse for Eve, which leads to the improvement of reliability and security.

TABLE 2 THE IMPACT OF THE PARAMETERS OF THE FEEDBACK CHANNELS ON THE RELIABILITY AND SECURITY OF THE PROPOSED SECRECY CODING SCHEME

ϵ_b	δ_b	e_B	e_E	P_B	P_E
0.01	0.18	0.01	0.1864	0.000393	0.479597
0.01	0.20	0.01	0.2060	0.000342	0.481942
0.01	0.22	0.01	0.2256	0.000300	0.486839
0.01	0.25	0.01	0.2550	0.000199	0.488551

Fig. 4. shows the achievable secrecy rate of the proposed feedback-based secrecy coding scheme using polar code, R_s, with different conditions of the feedback channels, where $\beta_s = \beta_c = 0.3$, M=256, and $\epsilon_f = 0.02, \delta_f = 0.01$.

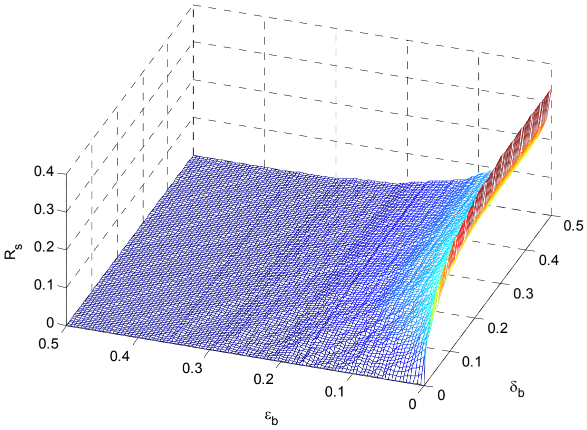

Fig. 4 The achievable secrecy rate of the proposed secrecy coding scheme different conditions of the feedback channels, where $\beta_s = \beta_c = 0.3$, M=256, and $\epsilon_f = 0.02, \delta_f = 0.01$

From Fig. 4, we observe that if the feedback channel W_{BA} gets better and W_{BE} gets worse, the achievable secrecy rate R_s of the proposed feedback-based secrecy coding scheme using polar code becomes larger, which indicates the feedback mechanism works in our proposed scheme. In order to achieve a larger secrecy rate over non-degraded wiretap channels, the forward channel W_{AB} and the feedback channel W_{BA} should be less noisy while the feedback channel W_{BE} should be worse so that the noise gap between W_{BA} and W_{BE} is wide enough to make more confidential messages be transmit.

V. Conclusions

In this paper, we proposed a feedback-based secrecy coding scheme using polar code over non-degraded wiretap channels. In the proposed scheme, by introducing feedback into the non-degraded wiretap channels and constructing a two level polar coding, a strictly positive secrecy rate can be achieved. And achievable maximum $R_{s,0}$ in some special cases are proven. We also prove the reliability and security of the proposed feedback-based secrecy coding scheme using polar code.

Simulation results show that the proposed feedback-based secrecy coding scheme using polar code can transmit confidential message over non-degraded wiretap channel reliably and securely. The reliability of the proposed secrecy coding scheme is improved when the condition of the main channel between Alice and Bob gets better and the condition of the feedback channel between Bob and Eve gets worse. And the security of the proposed secrecy coding scheme is improved when both the condition of the wiretap channel between Alice and Eve and the condition of the feedback channel between Bob and Eve get worse.

References

[1] D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[2] E. Arikan, "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, July. 2009.

[3] H. Mahdavifar, A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *Proc. of IEEE ISIT 2010*, pp. 913-917, June. 2010.

[4] E. Hof, S. Shamai, "Secrecy-achieving polar-coding," *Proc. of IEEE ITW 2010*, pp. 1-5, Aug. 2010.

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

[6] G. T. Amariucai, Shuangqing Wei, "Feedback-based collaborative secrecy encoding over binary symmetric channels," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5248-5266, Aug. 2012.

[7] E. Arikan, E. Telatar, "On the rate of channel polarization," *Proc. of IEEE ISIT 2009*, pp.1493-1495, June. 2009.

[8] E. Arikan, "A performance comparison of polar codes and Reed-Muller codes," *IEEE Communication Letters*, vol. 12, no. 6, pp. 447-449, June. 2008.