Secure Transmission Scheme for Parallel Relay Channels
Based on Polar Coding

Ce Sun, Zesong Fei*, Dai Jia, Congzhe Cao, and Xinyi Wang

Abstract: This paper considers the use of polar codes to enable secure transmission over parallel relay channels. By exploiting the properties of polar codes over parallel channels, a polar encoding algorithm is designed based on Channel State Information (CSI) between the legitimate transmitter (Alice) and the legitimate receiver (Bob). Different from existing secure transmission schemes, the proposed scheme does not require CSI between Alice and the eavesdropper (Eve). The proposed scheme is proven to be reliable and shown to be capable of transmitting information securely under Amplify-and-Forward (AF) relay protocol, thereby providing security against passive and active attackers.

Key words: polar codes; parallel channel; relay channel; secure transmission

1 Introduction

The wiretap channel model was introduced by Wyner in 1975[1], as shown in Fig. 1, and consists of a legitimate transmitter (Alice) sending a secret message to a legitimate receiver (Bob) through the main channel \( W \) with an eavesdropper (Eve) also seeing the transmission through a wiretap channel \( W^* \). The aim of secure transmission in this respect is to reliably send the message to Bob while hiding the information in contains from Eve[2].

The relay channel is a basic model for user cooperation and is the immediate research focus area. The common relay channel has three nodes: a source, destination, and relay. Amplify-and-Forward (AF) and Decode-and-Forward (DF) are two widely used relaying protocols[3] and as a natural extension, research is being focused on enable secure transmission for relay channels. The secrecy capacity of the relay-eavesdropper channel with orthogonal components has been studied in Ref. [4], and the maximum perfect secrecy rate under the DF protocol has been proposed in Ref. [5]. Furthermore, the lower and upper bounds on the perfect secrecy rate of the parallel relay channel have been established for the Gaussian memoryless channel[6]. However, if the source-relay channel condition is poor, the relay can generate decode errors during decoding for the DF protocol, and if the destination receives the erroneous bits, the performance of system subsequently deteriorates.

To achieve high reliability and security, the channel coding scheme has been utilized in a physical layer relay channel[7]. Polar codes[8] have been proven to achieve the capacity of arbitrary Binary-input Discrete Memoryless Channels (B-DMCs), and they have the advantage of a low decoding complexity with certain optimized decoding...
algorithms\textsuperscript{[9–11]}. They can also be used to achieve strong security\textsuperscript{[12–14]}. In one study, information bits were allocated to bit channels\textsuperscript{[15]}, which is positive for Bob and negative for Eve. In addition, the security key has been discussed\textsuperscript{[16–18]}, where the index and value of frozen bits of polar codes were hidden from Eve. A further study\textsuperscript{[19]} presented secure transmission based on polar codes for fading wiretap channels, and another\textsuperscript{[20]} designed an encoding and decoding scheme for polar codes over the general wiretap channel. In addition to the serial channel model, the parallel channel model is also useful in many practical scenarios, such as transmission over block fading channels, and in multi-subcarrier communication and network coding; in this respect, the construction of polar codes over parallel channels has been presented\textsuperscript{[21]}. However, with all of the above schemes it is necessary to know the instantaneous or statistic Channel State Information (CSI) between Alice and Eve, and most of these existing schemes assume that wiretap channels are the degraded channels of main channels, which limits the application of secure transmission.

This paper proposes a polar codes secure transmission scheme with an AF relay protocol. In the proposed scheme, Bob first transmits the training sequence to Alice, and Alice estimates the CSI between Alice and Bob. As a result, Eve cannot obtain this CSI. Alice then maps the polar encoded message based on the CSI of the main channel and transmits the message via the parallel channels with AF relay protocol. The mapping function determines the polarization results of the polar codes. A previously proposed mapping function\textsuperscript{[22]} is also employed; this has been proven to achieve higher reliability than original random mapping functions. Eve does not have the CSI of the main channel, and she cannot obtain the mapping function. Therefore, Eve cannot recover Alice’s message. Thus, the proposed scheme can transmit the message securely without any knowledge of CSI between Alice and Eve; this relaxes the need for the wiretap channel to be the degraded channel of the main channel. In this study, the reliability and the security of the proposed scheme is analyzed using both a passive attacker and an active attacker, and simulation results show that Alice can transmit information to Bob, both reliably and securely.

The remainder of this paper is organized as follows. The system model of parallel wiretap channels is presented in Section 2. The secure transmission scheme is proposed in Section 3. Section 4 and Section 5 analyze the reliability and security of the proposed scheme respectively. Finally, Section 6 presents the conclusions of this paper.

\section{Polar Codes}

Polar codes exploit the channel polarization phenomenon and have been proven to achieve the capacity of arbitrary B-DMCs. Let $W : \mathcal{X} \rightarrow \mathcal{Y}$ be a Binary Erasure Channel (BEC), the transition probability of $W$ is $\{W(y|x)\}$, where $x \in \mathcal{X} = \{0, 1\}$ is input and $y \in \mathcal{Y} = \{0, 1\}$ is output. The capacity of the $W$ is defined as

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

The polar coding is based on the single-step transform of a BEC $W$ which can be denoted as $(W^{-}, W^{+})$. $W^{-}$ and $W^{+}$ are the polarized channels which are defined by transition probability:

$$W^{-}(y_{1}, y_{2}|x_{1}) = \frac{1}{2} \sum_{x_{2} \in \{0, 1\}} W(y_{1}|x_{1} \oplus x_{2})W(y_{2}|x_{2}),$$

$$W^{+}(y_{1}, y_{2}, x_{1}|x_{2}) = \frac{1}{2} W(y_{1}|x_{1} \oplus x_{2})W(y_{2}|x_{2}).$$

$W^{-}$ is the degraded channel and $W^{+}$ is the upgraded channel, both of them satisfy the following conditions:

$$I(W^{-}) + I(W^{+}) = 2I(W),$$

$$I(W^{-}) \leq I(W^{+}).$$

The same polarization process is then repeated until that the $N$-size polarized channels are constructed recursively as shown in Fig. 2.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{fig2.png}
\caption{Recursive construction of channel polarization.}
\end{figure}
Channel polarization is described as follows:

**Theorem 1** For any B-DMCs $W_i$, 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 $i \in \{1, \ldots, N\}$ 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 $1-I(w)$.

### 2.1 Encoding

According to Theorem 1, the information bits are set within the sub-channel set which $I(W_N^{(j)}) \in (1-\delta, 1]$ and the frozen bits are set in the other sub-channels to construct the information block $u$. Prior to setting the information bits and frozen bits, it is necessary to calculate the reliability of the $N$ sub-channels and to decide which sub-channels should have information bits set within them. The common algorithms for calculating reliability include the algorithm of Bhattacharyya parameters, Density Evolution (DE), and Gaussian Approximation (GA). Subsequently, $u$ is sent into the polar encoder for encoding. The polar encoding is denoted as $x_N = u_N G_N$, where $x_1 = x_1, x_2, \ldots, x_N$ is the codeword, $u_N = u_1, u_2, \ldots, u_N$ is the information block, and $G_N$ is the generator matrix of order $N$. Furthermore, the recursive definition of $G_N$ is given by

$$G_N = B_N F_2^\otimes n, \quad F_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

### 2.2 Decoding

All of the existing polar code decoders are based on the Successive Cancellation (SC) decoder which generates its decision $\hat{u}_N^n$ by computing

$$\hat{u}_i = \begin{cases} u_i, & \text{if } i \in A^c; \\ h_i(y_i, \hat{u}_{i-1}^{i-1}), & \text{if } i \in A \end{cases}$$

where

$$h_i(y_i, \hat{u}_{i-1}^{i-1}) = \begin{cases} 0, & \text{if } w(0|y_i, \hat{u}_{i-1}^{i-1}) \geq 1; \\ 1, & \text{otherwise} \end{cases}$$

and $y_i = y_1, y_2, \ldots, y_N$ denotes the received message.

The SC decoder of polar codes can be regarded as a greedy search algorithm based on the compact-stage code tree. Two paths associated with an information bit at a certain layer are considered to be candidates, but the path that has the larger probability can be selected for further processing. Based on the SC decoder, the Successive Cancellation List (SCL) decoder searches the code tree layer by layer with the same manner as the SC. Be different from SC, the SCL decoder allows a maximum of $L$ candidate paths to be used in the further processing.

### 3 System Model

This paper considers the construction of secure transmission based on polar codes over parallel channel with AF relay protocol. There are three legitimate nodes in this model, source (Alice), relay (R), and destination (Bob). $W_{AB}$, $W_{AR}$, and $W_{RB}$ denote the Alice-to-Bob, Alice-to-R, and R-to-Bob link, respectively. These channels make up the main channel $W$. An eavesdropper (Eve) can see the transmission, and the channels between Alice and Eve and between relay and Eve are regarded as $W_{AE}$ and $W_{RE}$, respectively. $W_{AE}$ and $W_{RE}$ constitute the wiretap channel $W'''$. Both main channel and wiretap channel are parallel channels. Different from serial channels, parallel channels have a group of independent sub-channels with different channel parameters (i.e., the variance of AWGN or erasure probability of BEC). The main difference between the proposed scheme and existing schemes is that the single-step transform of polar codes over parallel channel is based on two different channels, e.g., $(W_1, W_2) \Rightarrow (W', W'')$. Ni et al. proved that:

1. $I(W') + I(W'') = I(W_1) + I(W_2)$
2. $I(W') \leq \min(I(W_1), I(W_2))$
3. $I(W'') \geq \max(I(W_1), I(W_2))$

As illustrated in Fig. 3, both the main and wiretap channels contain $J$ parallel sub-channels $\{W_1, W_2, \ldots, W_J\}$. It is assumed that all sub-channels have the same input symbol alphabet $\mathcal{X}$ and the same output symbol alphabet $\mathcal{Y}$. All the sub-channels are independent from each other and the transition function of the $j$-th sub-channel is $W_j(y|x)$, where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. Let $y_{AB}$, $y_{AE}$, $y_{RB}$, and $y_{RE}$ denote the received message at Bob and Eve from Alice and relay, respectively.

Note that there are $J$ parallel sub-channels in every channel between four nodes. For transmission of $N$ bits message, each sub-channel is used $M = N/J$ times. We take $W_{AR}$ as example. Let $W_{AR_j}^m$ denote the $m$-th use of $W_{AR}$’s sub-channel $W_{AR_j}$, where $j = 1, 2, \ldots, J$, $m = 1, 2, \ldots, M$. Further $W_{AR_j}^N$ represents a set of channels from $W_{AR_1}$ to $W_{AR_N}$, and the $n$-th channel $W_{AR_n}$ is related to the channel uses $W_{AR_j}^m$ with a mapping $\pi$. We denote the mapping function by $\pi(n) = (j, m)$, which means the $n$-th channel is mapped to the $j$-th sub-channel.
of the $m$-th use. The polarization of channel $W_{AB}$ and $W_{AE}$ is the same as $W_{AR}$. In addition, the relay amplifies the received message and forwards it to destination through $W_{RB}$.

4 Secure Transmission Scheme

This section proposes a secure transmission scheme based on polar coding. The equivalent SNR used to evaluate the reliability of polarized channels is firstly calculated, and the proposed polar encoder and decoder are then described.

4.1 Equivalent SNR

For AF relay protocol, the relay node amplifies and forwards the message received from Alice. Therefore, the channels $W_{AB}$, $W_{AR}$, and $W_{RB}$ are considered equivalent to one main channel with an equivalent SNR. Before polar encoding, the reliability of polarized channels should be obtained based on SNR. So the equivalent SNR should be calculated first. For a brief discussion, the channel gains of $W_{AB}$, $W_{AR}$, and $W_{RB}$ are denoted as $h_{AB}$, $h_{AR}$, and $h_{RB}$, respectively, the amplification factor of relay node is regarded as $1/h_{AR}$. Moreover, $n_{AB}$, $n_{AR}$, and $n_{RB}$ denote the respective AWGN at $W_{AB}$, $W_{AR}$, and $W_{RB}$ with zero mean and variance $\sigma^2_{AB}$, $\sigma^2_{AR}$, and $\sigma^2_{RB}$. For the parallel channel, the channel gain $h$ is an $N \times N$ diagonal matrix with the $N/J$ uses of channel gains of $J$ sub-channels in the diagonal. $n$ and $\sigma$ are $N \times 1$ matrices. The transmission includes two time slots. In the first time slot, Alice transmits the message $x_A$ to R and Bob through $W_{AB}$ and $W_{AR}$. The received messages at R and Bob are regarded as $y_{AR}$ and $y_{AB}$, where $y_{AR} = h_{AR}x_A + n_{AR}$ and $y_{AB} = h_{AB}x_A + n_{AB}$. In the second time slot, the relay amplifies $y_{AR}$ and forwards it to Bob, and this message is regarded as $y_{RB}$, where

$$y_{RB} = h_{RB}y_{AR}/h_{AR} + n_{RB} = h_{RB}x_A + h_{RB}n_{AR}/h_{AR} + n_{RB}$$

Bob combines $y_{AB}$ and $y_{RB}$ by Maximal Ratio Combining (MRC):

$$y = h^*_A y_{AB} + h^*_R y_{RB} = (|h_{AB}|^2 + |h_{RB}|^2)x_A + \frac{|h_{RB}|^2 n_{AR}}{h_{AR}} + h^*_A n_{AB} + h^*_R n_{RB}$$

As above $W_{AB}$, $W_{AR}$, and $W_{RB}$ are equivalent to the main channel, and $|h_{AB}|^2 + |h_{RB}|^2$ is equivalent to the channel gain of the main channel, and $\frac{|h_{RB}|^2 n_{AR}}{h_{AR}} + h^*_A n_{AB} + h^*_R n_{RB}$ is equivalent to the noise of the main channel. Therefore the equivalent SNR is

$$\text{SNR}_{\text{equ}} = S/N = \frac{E_S(|h_{AB}|^2 + |h_{RB}|^2)^2}{|h_{AB}|^2 \sigma^2_{AB} + |h_{RB}|^2 \sigma^2_{RB} + \frac{h_{RB}}{|h_{AR}|} \sigma^2_{AR}}$$

where $S$ and $N$ denote the power of signal and noise respectively. Then equivalent SNR of $N/J$ uses of $J$ sub-channels is calculated.

4.2 Encoder

After obtaining the equivalent SNR, the reliability of polarized channels can be calculated. Let $K$ denote the length of information block, and $R_0$ denotes the pre-set code rate. The code length $N$ of polar codes is designed to be the minimum power of 2 which is bigger than $K/R_0$, and the real code rate $R = K/N$. To construct a polar code with the code length $N = 2^n$, the $K$ most reliable polarized channels $\{W_{ij}^{(n)}\}$ with indices $i \in A$ are selected for transmitting secret information bits, where $A$ denotes the index set of good bit channels with the size $K$. And the bits called frozen bits are transmitted over bad bit channels. The value of the frozen bits are known by transmitter and receiver. The process of transformation $G_N$, which is the same as traditional polar codes, is executed. The coded bits are transmitted over a set of parallel channels consisting of

\[1\]
4.3 Decoder

The message received by Bob and Eve are $y_{AB}$, $y_{RB}$, and $y_{AE}$, $y_{RE}$, respectively. Bob and Eve combine the received message by MRC and then attempt to decode the message by using the SCL algorithm.

Section 5 demonstrates that the decoding algorithm cannot recover the message without knowing the indices set $A$ for the good bits.

5 Analysis

5.1 Reliability

Arikan[8] proved that polar codes can achieve the capacity of BEC. Refer to that method, we prove that the error probability of each encoded bit approaches 0 over parallel channel. Reliability of secure transmission is measured in terms of the probability of error in recovering the message and the reliability condition is described as follows. That is, in this section we prove that the proposed scheme can meet the requirements of reliability:

$$\lim_{K \to \infty} \Pr\{\hat{u}_k^N \neq u_k^N\} = 0$$

(7)

The Bhattacharyya parameter $Z(W)$ is an upper bound of the error probability of Maximum-Likelihood (ML). It is therefore necessary to prove that $\lim_{k \to \infty} Z(W) = 0$ in order to prove the reliability. Polar codes with the code length $N$ need $\log_2 N$-levels channel polarization. The Bhattacharyya parameter $Z(i)$ of the $i$-th level channel polarization is regraded as $Z_{i,j}$, where $1 \leq i \leq \log_2 N$, and $j$ denotes the $j$-th output after the $i$-th level channel polarization, $1 \leq j \leq N$. By Proposition 7 in Ref. [4], we have

$$\begin{align*}
Z_{i+1,j} &\leq Z_{i,j} + Z_{i,j+1} - Z_{i,j}Z_{i,j+1} \\
Z_{i+1,j+1} &\leq Z_{i,j}Z_{i,j+1}
\end{align*}$$

(8)

and for $\beta \geq 0$ and $m \geq 0$, we define

$$T_m(\beta) \triangleq \{j : Z_{i,j} \leq \beta \text{ for all } i \geq m\}.$$ 

As the operation of polarization works in pairs, we get the maximal pair $\{Z_{i,j}, Z_{i,j+1}\}$ of $Z$, where $i \in m$ and $j \in T_m(\beta)$. We have

$$\begin{align*}
\frac{Z_{i+1,j+1}}{Z_{i,j}} &\leq 1 + \frac{Z_{i+1,j+1}}{Z_{i,j}} - Z_{i,j+1} \\
\frac{Z_{i+1,j+1}}{Z_{i,j}} &\leq 1 + \frac{Z_{i+1,j+1}}{Z_{i,j}} - Z_{i,j}
\end{align*}$$

(9)

and

$$\begin{align*}
\frac{Z_{i+1,j+1}}{Z_{i,j}} &\geq Z_{i,j+1} \\
\frac{Z_{i+1,j+1}}{Z_{i,j}} &\geq Z_{i,j}
\end{align*}$$

(10)

We set $\alpha = 1 + \frac{Z_{i+1,j+1}}{Z_{i,j}}$, so

$$Z_{i+1} = \frac{Z_i}{\alpha}, \quad \text{if } B_{i+1,j} = 0;$$

$$Z_{i+1} = \frac{Z_i}{\beta}, \quad \text{if } B_{i+1,j} = 1$$

(11)

where $Z_{i+1}$ and $Z_i$ denote any one of the Bhattacharyya parameter pair of the $(i + 1)$-th and $i$-th level channel polarization respectively. A parameter $B_{i+1,j}$ is introduced. $Z_{i+1,j}$ and $Z_{i+1,j+1}$ are the Bhattacharyya parameter pair of channels polarized by the channels of $Z_{i,j}$ and $Z_{i,j+1}$. If the Bhattacharyya parameter is $Z_{i+1,j}$, we set $B_{i+1,j} = 0$; if the Bhattacharyya parameter is $Z_{i+1,j+1}$, we set $B_{i+1,j} = 1$. This implies

![Fig. 4 The block diagram of the parallel polar encoder.](image-url)
For $n > m \geq 0$ and $0 < \eta < 1/2$, we define

$$U_{m,n}(\eta) \triangleq \{j : \sum_{i=m+1}^{n} B_{i,j} > (1/2 - \eta)(n-m)\},$$

then we have

$$Z_{n,j} \leq c \cdot 2^{\lfloor (1/2+\eta)ht+(1/2-\eta)nt \rfloor}, \quad j \in T_{m}(\beta) \cap U_{m,n}(\eta)$$

(13)

where

$$c = 2^{-(1/2+\eta)+(1/2-\eta)n} = 2^{-(1/2+\eta)+(1/2-\eta)n}, \quad j \in T_{m}(\beta) \cap U_{m,n}(\eta).$$

We then set $t = b(1/2 + \eta + (1/2 - \eta)a)$, with $\eta \triangleq 1/20$ and $\beta \triangleq 2^{-4}$, we obtain $t = 1/2 + \eta + (1/2 - \eta)a < -1$, then we have

$$Z_{n,j} \leq c \cdot 2^{t} = c \cdot N^t, \quad j \in T_{m}(\beta) \cap U_{m,n}(\eta)$$

(15)

where $N$ is the code length of polar codes. The desired bound$^{[3]}$ is used to write

$$P[T_{m}(\beta) \cap U_{m,n}(\eta)] \geq I_0 - \delta.$$

The the size of the set $T_{m}(\beta) \cap U_{m,n}(\eta)$ is denoted as $S_n$, and

$$P[T_{m}(\beta) \cap U_{m,n}(\eta)] = S_n/N \geq I_0 - \delta.$$

Therefore, $S_n \geq N(I_0 - \delta)$, which means Eq. (15) occurs with a sufficiently high probability.

Based on the above analysis, we conclude that there exists a sequence of sets $A_N \subset \{1, \ldots, N\}$ which makes $Z(W_{0}^{N}) \leq O(c \cdot N^t)$ for all $i \in A_N$ so long as that the code length $N$ is long enough. So this conclusion shows that

$$\lim_{K \to \infty} \Pr\{u_{i}^{N} \neq u_{i}^{N}\} = 0$$

(16)

which completes the proof of reliability.

5.2 Security

5.2.1 Passive attacker

Prior to analysis, it is necessary to emphasize that Alice transmits message without any CSI between Alice and Eve in the process of secure transmission. Figures 5–7 present the Block Error Rate (BLER) performance of polar codes with message length $K = 64$, $K = 80$, and $K = 120$, respectively. Bob and Eve attempt to decode the received message with the SC algorithm. The difference between Bob and Eve is that Eve does not know the mapping function. Three pairs of code rate (1/2, 1/3, and 1/6) are simulated over AWGN channels, each pair contains main channel and wiretap channel with the 32 parallel sub-channels. As shown in Figs. 5–7, the decoding results will be very unreliable without the knowledge of the mapping function, when Eve selects a mapping method randomly to attempt to decode the message. In fact, the process of encryption in the proposed scheme...
introduces artificial noise. The estimation of encrypted information with artificial noise needs the knowledge of mapping method. Therefore, despite the fact that observation $y_{AE}$ and $y_{RE}$ can be obtained by Eve, they can not be decoded reliably.

5.2.2 Active attacker

An active attacker can apply several attacks to compromise the proposed scheme. In this subsection, we prove the proposed scheme is secure against certain active attacks.

(1) Brute-force attack

In an active attack, the attacker checks all mapping function methods systematically until the correct functions are simultaneously found. However, the complexity of the attack is so high that the attack is impossible to realize as large as sub-channel set is. In the proposed scheme, the complexity of the brute-force is computed as follows.

Alice permutates the sub-channels by the mapping function $\pi$, the number of the permutation of $n$ sub-channels is given by

$$N_n = A_n^n = n!$$  \hspace{1cm} (17)

The indices of information bits differ for the different mapping functions. There are $n!$ permutations, that is, there are $n!$ selections of information bits. A Resource Block (RB) has 12 sub-channels in Long Term Evolution (LTE). The minimum channel bandwidth in LTE is 1.4 MHz which contains 6 RBs. That is, the number of the available sub-channels is greater than $6 \times 12 = 72$. Set $n = 72$, $N_n = 72! \approx 2^{344}$. This number of the sub-channel permutation will be larger with the more sub-channels.

As calculated above, the sub-channel sets have such a large size that Eve would be unable to find these parameters via an exhaustive search in polynomial time. It is thus considered that the proposed scheme is safe against the active attack.

(2) Rao-Nam attack

The Rao-Nam attack is a plaintext attack. The cryptanalyst is required to go through two steps:

Step 1: The generation matrix $G'$ is solved from a large set of $(M, C)$ pairs.

Step 2: The secret message is obtained using $G'$ solved in the previous steps with wiretapped message.

Let $M_1$ and $M_2$ be two chosen plaintext vectors differing in the $i$-th position, that is, $M_i = M_j \oplus u_{A^c} \oplus u_{A^c}$ and $C_i = M_iG_iC_j$ and $C_j = M_jG_jC_f$ be two corresponding ciphertexts achieved from $M_1$ and $M_2$, then

$$C_1 \oplus C_2 = (M_1 \oplus M_2)G' \oplus (u_{A^c} \oplus u_{A^c})G_f = g'_i \oplus (u_{A^c} \oplus u_{A^c})G_f$$  \hspace{1cm} (18)

where $g'_i$ is the $i$-th row of the generation matrix. From the same plaintext $M$, two distinct ciphertexts $C_i$ and $C_j$ can be obtained whose difference is $C_i \oplus C_j = (u_{A^c} \oplus u_{A^c})G_f$. Then the $g'_i$ is obtained by

$$g'_i = C_i \oplus C_j \oplus (u_{A^c} \oplus u_{A^c})G_f$$  \hspace{1cm} (19)

To obtain the correct $g'_i$, the steps should be repeated until all possible $u_{A^c}$ pairs are tested. The number of distinct $u_{A^c}$ is given by $N_f = 2^{N_f - K}$, and the number of possible values of $(u_{A^c} \oplus u_{A^c})G_f$ is $(N_f - N_f)$. The solution of $G'$ must be obtained and verified completely, because each $g'_i$ cannot be verified independently. This involves an average work factor $N_{w_f}$ given by

$$N_{w_f} \geq \frac{1}{2} \left( \frac{(N_f - N_f)}{2} \right)^{K}$$  \hspace{1cm} (20)

Clearly, the Rao-Nam attack would be unable to work for a (512,120) polar codes where $N_f = 2^{342}$.

6 Conclusion

This paper proposes a secure information transmission based on polar codes for parallel relay channels. The equivalent SNR which is used to evaluate the reliability of polarized channels is calculated, and the polar encoder and decoder for secure transmission are described. Results show that Alice can transmit message securely without any
CSI knowledge of the channel between Alice and Eve. Analysis of the proposed scheme also proves that Alice can transmit information to Bob, both reliably and securely.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China (No. 61371075) and Beijing Municipal Science and Technology Project (No. D171100006317001).

References


Tsinghua Science and Technology, June 2018, 23(3): 357–365
Ce Sun received the BS degree in electronic engineering from Nanjing Agricultural University (NJAU), Nanjing, China, in 2015. He is currently working toward the PhD degree at the Research Institute of Communication Technology, Beijing Institute of Technology (BIT). His research interests include channel coding and modulation and multiple access.

Congzhe Cao received the BEng degree from the University of Science and Technology Beijing, Beijing, China, in 2012, and the MEng degree from the Beijing Institute of Technology, Beijing, in 2014. He is currently pursuing the PhD degree with the Department of Electrical and Computer Engineering, University of Alberta, Canada. His current research interests are constrained sequence coding and error control coding for communication and emerging data storage systems.

Xinyi Wang received the BS degree in electronic engineering from Beijing Institute of Technology (BIT), Beijing, China, in 2017. He is currently working toward the master degree at the Research Institute of Communication Technology, BIT. His research interests include channel coding and modulation and joint communication and sensing.

Zesong Fei received the PhD degree in electronic engineering from Beijing Institute of Technology (BIT) in 2004. He is currently a professor with the Research Institute of Communication Technology (RICT) of BIT, where he is involved in the design of the next generation high-speed wireless communication systems. His research interests include wireless communications and multimedia signal processing. He is a principal investigator of projects funded by the National Natural Science Foundation of China. He is also a senior member of the Chinese Institute of Electronics and China Institute of Communications.

Dai Jia received the BS degree in electronic engineering from Beijing Institute of Technology (BIT), Beijing, China, in 2012. He is currently working toward the PhD degree at the Research Institute of Communication Technology, BIT. From March 2014 to May 2015, he was with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia, where he was a visiting PhD student under the supervision of Prof. Jinhong Yuan. His research interests include channel coding and modulation, network coding, mobile communication, and cooperative communications.