IET Information Security

Research Article

IET Journals
The Institution of Engineering and Technology

Encrypted secure polar coding scheme for general two-way wiretap channel

ISSN 1751-8709
Received on 7th September 2018
Revised 12th January 2019
Accepted on 7th February 2019
E-First on 25th March 2019
doi: 10.1049/iet-ifs.2018.5472
www.ietdl.org

Yizhi Zhao[1], Shiwei Xu[1], Hongmei Chi[2] ✉

[1]*College of Informatics, Huazhong Agricultural University, Wuhan, Hubei, People's Republic of China*
[2]*College of Science, Huazhong Agricultural University, Wuhan, Hubei, People's Republic of China*
✉ *E-mail: chihongmei@mail.hzau.edu.cn*

Abstract: The authors consider the problems of key exchange for one-time pad along with the problem of rate sacrifice for secure polar coding over the two-way wiretap channel under the strong security criterion. Based on existing techniques, they present a new hash chaining structure to solve the good bits sacrificing problem for achieving the strong security and constructed encryption embedded secure polar coding scheme for two-way wiretap channel. To implement a one-time pad without any key pre-sharing, they design a secure and reliable transmission for both key and ciphertext coupling with the cooperative jamming strategy, which can also increase the secrecy rate for communication. As proved, extended upper bounds for both achievable secrecy rate pair and effective secrecy rate pair can be achieved under the strong security and reliability criterions.

1 Introduction

Upper layers cryptographic techniques and physical layer secure schemes are the two main methods for securing the communication. For cryptographic-based encryption method, level of security strictly depends on the computational abilities of the eavesdropper. The only encryption method proved to have perfect secrecy [1] is the one-time pad, which is however hard to implement due to the complexities on key exchanging and key arrangement. Therefore, considerable attentions have been turned into the physical layer secure scheme since it can achieve strong security for communication without considering the computational abilities of the eavesdropper [2].

For the study of physical layer security, secrecy capacity achieving has always been an open topic for the wiretap channel model [3, 4]. As a traditional method, low-density parity-check (LDPC) codes have been applied in the research of explicit secure coding and successfully approached the secrecy capacities of some particular wiretap channel models or under certain constrains, such as the key capacity of the binary phase shift keying-constrained Gaussian wiretap channel [5], the secrecy capacity of binary erase wiretap channel model and the binary symmetric wiretap channel model with a noiseless main channel [6, 7]. However, for more general wiretap channel models that both the main channel and wiretap channel are noisy symmetric channels or even asymmetric channels, secure capacity achieving LDPC codes are hard to construct.

Polar codes, invented by Arıkan [8] in 2007, have also been applied in the researches of physical layer secure coding. Comparing with the LDPC codes, polar codes have a better theoretically capacity achieving performance, lower complexity and significantly better adaptability to the general wiretap channel cases. Existing studies of secure polar coding schemes have already successfully achieved the secrecy capacities of several wiretap channel models [9–14], which is however based on rate sacrifice.

The two-way wiretap channel model is one of the multi-user extended wiretap channel models, in which two legitimate users communicate over a noisy bidirectional channel under the observation of a passive eavesdropper. One useful strategy for multi-user model to interfere the eavesdropper is called *cooperative jamming* which was investigated in [15, 16]. Then the achievable strong security rate region of the two-way wiretap channel with cooperative jamming was given by Pierrot and Bloch [17]. Later in [14], an explicit secure polar coding scheme was proposed for asymmetric two-way wiretap channel with polar coded cooperative jamming, and successfully achieved the strong security rate region for, but rate sacrifice is still inevitable.

To increase the secure communication rate for the two-way wiretap channel, an idea of coupling the key exchange and cooperative jamming was proved to be possible by Pierrot and Bloch [17]. Thus in this paper, we consider the extending of this proved idea to construct encryption embedded secure polar coding scheme for symmetric two-way wiretap channel, in the aim of solving the key exchange problem for one-time pad together with rate sacrificing problem.

Based on the framework of [14] for secure polar coding, including asymmetric channel coding [18, 19], Slepian-Wolf coding [20, 21], and polar coded cooperative jamming [14], we further constructed:

- A new *hash chaining structure* to solve the good bits sacrificing problem for achieving both reliability and strong security, also with an increased secrecy rate over the original multi-block chaining structure in [10, 14].
- A key transmission with reliability and strong security guaranteed by polar coding.
- A ciphertext transmission with reliability guaranteed by polar coding and security guaranteed by encryption.

Our construction for two-way wiretap channel with cooperative jamming is under the reliability and strong security criterions. As proved, our proposed scheme has successfully implemented a one-time pad without any key pre-sharing and achieved an extended secrecy rate region with larger upper bounds for both secrecy rate and effective secrecy rate.

The outline of this paper is organised as follow. Section 2 presents the notations and channel model definitions. Section 3 provides the existing techniques for secure polar coding construction. Section 4 presents the hash chaining structure. Section 5 presents the construction of our proposed encryption embedded secure polar coding scheme. Section 6 is an analysis of the proposed scheme. Finally, Section 7 concludes the paper.

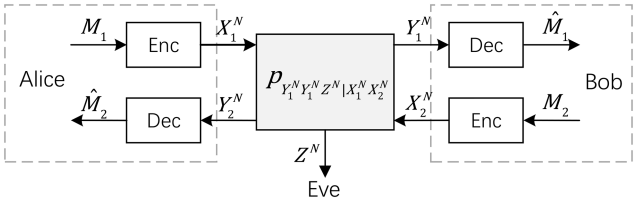

Fig. 1 *Two-way wiretap channel model*

2 Problem statement

Notation: We define the integer interval $[\![a,b]\!]$ as the integer set between $\lfloor a \rfloor$ and $\lceil b \rceil$. For $n \in \mathbb{N}$, define $N \triangleq 2^n$. Denote X, Y, Z,... random variables (RVs) taking values in alphabets $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \ldots$ and the sample values of these RVs are denoted by x, y, z,..., respectively. Then p_{XY} denotes the joint probability of X and Y, and p_X, p_Y denotes the marginal probabilities. Also, we denote a N size vector $X^{1:N} \triangleq (X^1, X^2, \ldots, X^N)$. When the context makes clear that we are dealing with vectors, we write X^N in place of $X^{1:N}$. And for any index set $\mathcal{A} \subseteq [\![1,N]\!]$, we define $X^{1:N}[\mathcal{A}] \triangleq \{X^i\}_{i \in \mathcal{A}}$. For the polar codes, we denote $\boldsymbol{G}_N$ the generator matrix, $\boldsymbol{R}$ the bit reverse matrix, $\boldsymbol{F} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $\otimes$ the Kronecker product, and we have $\boldsymbol{G}_N = \boldsymbol{R}\boldsymbol{F}^{\otimes n}$.

We consider the secure communication problem over a *full-duplex* discrete memoryless two-way wiretap channel which is illustrated in Fig. 1.

In this model, two legitimate users Alice and Bob are communicating with each other simultaneously under the existence of a passive eavesdropper Eve. The communication process is as follows:

- *Alice:* M_1 is encoded into X_1^N and transmitted over the channel to Bob while Y_2^N is received from Bob and decoded into the estimate $\hat{M}_2$.
- *Bob:* M_2 is encoded into X_2^N and transmitted over the channel to Alice while Y_1^N is received from Alice and decoded into the estimate $\hat{M}_1$.
- *Eve:* Z^N is observed by Alice and Bob.

Definition 1: A discrete memoryless two-way wiretap channel is defined as $(\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Z}, p_{Y_1Y_2Z|X_1X_2})$, which have

$$\begin{aligned} \forall (x_1^N, x_2^N, y_1^N, y_2^N, z^N) \in \mathcal{X}_1^N \times \mathcal{X}_2^N \times \mathcal{Y}_1^N \times \mathcal{Y}_2^N \times \mathcal{Z}^N, \\ p_{Y_1^N Y_2^N Z^N | X_1^N X_2^N}(y_1^N, y_2^N, z^N | x_1^N, x_2^N) \\ = \prod_{i=1}^{N} p_{Y_1Y_2Z|X_1X_2}(y_1^{(i)}, y_2^{(i)}, z^{(i)} | x_1^{(i)}, x_2^{(i)}). \end{aligned} \tag{1}$$

Then we define a N length code for the two-way wiretap channel.

Definition 2: Denote a $(2^{NR_1}, 2^{NR_2}, N)$ code $\mathscr{C}_N$ for the two-way wiretap channel, with messages $M_1 \in \mathcal{M}_1 = [\![1, 2^{NR_1}]\!]$, $M_2 \in \mathcal{M}_2 = [\![1, 2^{NR_2}]\!]$. Then the performance of a code $\mathscr{C}_N$ is defined as

- error probability

$$P_e(\mathscr{C}_N) = \Pr\left((M_1, M_2) \neq (\hat{M}_1, \hat{M}_2 | \mathscr{C}_N)\right), \tag{2}$$

- information leakage to Eve

$$L(\mathscr{C}_N) = I(Z^N; M_1 M_2 | \mathscr{C}_N). \tag{3}$$

Definition 3: For two-way wiretap channel, a rate pair (R_1, R_2) is achievable if sequences of codes $\mathscr{C}_N$ exist under any of the criterions listed below:

- reliability criterion

$$\lim_{N \to \infty} P_e(\mathscr{C}_N) = 0, \tag{4}$$

- weak security criterion

$$\lim_{N \to \infty} \frac{1}{N} L(\mathscr{C}_N) = 0, \tag{5}$$

- strong security criterion

$$\lim_{N \to \infty} L(\mathscr{C}_N) = 0. \tag{6}$$

Remark 1: Reliability and security criterions are measures for evaluating the performance of a code $\mathscr{C}_N$. Reliability can be achieved with a vanishing error probability of decoding the messages. Weak security can be achieved with a vanishing information leakage rate. And strong security can be achieved with vanishing information leakage.

Theorem 1: (Strong security achievable rate region [17]) For a two-way wiretap channel, by using the coded cooperative jamming, the achievable rate region under the reliability and strong security criterions is

$$\mathscr{R} = \bigcup_{p \in \mathscr{P}} \left\{ \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \middle| \begin{array}{ll} R_1 \leq I(Y_1; C_1 | X_2) & -I(C_1; Z) \\ R_2 \leq I(Y_2; C_2 | X_1) & -I(C_2; Z) \\ R_1 + R_2 \leq I(Y_1; C_1 | X_2) & +I(Y_2; C_2 | X_1) \end{array} \right\}, \tag{7}$$

where C_1, C_2 are the RVs representing the generated code for coded cooperative jamming for Alice and Bob, respectively. And for $\mathscr{P}$, have

$$\begin{aligned} \mathscr{P} = \{ & p_{X_1X_2C_1C_2Y_1Y_2Z} \text{ factorising as:} \\ & p_{Y_1Y_2Z|X_1X_2} p_{X_1|C_1} p_{C_1} p_{X_2|C_2} p_{C_2} \}. \end{aligned} \tag{8}$$

In this work, we consider the general two-way wiretap channel case with asymmetric channels and no degradation relationship. Under the reliability and strong security criterions defined above, we focus on the following problems together and construct the polar codes based solution:

- *Key exchange problem for a one-time pad*. Our solution is to construct a secure and reliable key transmission along with protected information.
- *Rate sacrifice problem for secure polar coding.* Our solution is to obtain additional security for the sacrificed rate and reuse it for information transmission.

3 Preliminaries on polar coding

3.1 Source polarisation and asymmetric channel coding

Definition 4: (Bhattacharyya parameter) Consider a pair of RVs (X, Y) with joint distribution p_{XY}, where X is a binary RV and Y is a finite-alphabet RV. To measure the amount of randomness in X given Y, the Bhattacharyya parameter is defined as

$$Z(X|Y) = 2 \sum_{y \in \mathcal{Y}} p_Y(y) \sqrt{p_{X|Y}(0|y) p_{X|Y}(1|y)}. \tag{9}$$

Let $U^N = X^N \boldsymbol{G}_N$, where X^N is N independent copies of the random source X with a non-uniform distribution p_X, and $\boldsymbol{G}_N$ is the generator matrix for polarisation. According to the source polarisation theory [18], as $N \to \infty$, U^N is almost polarised into two types with index sets $\mathcal{H}_X$ and $\mathcal{L}_X$. For $\beta \in (0, 1/2)$, $\delta_N = 2^{-N^\beta}$, have

$$\mathscr{H}_X = \left\{ i \in [\![1, N]\!] : Z\left(U^i \middle| U^{1:i-1}\right) \geq 1 - \delta_N \right\}$$
$$\mathscr{L}_X = \left\{ i \in [\![1, N]\!] : Z\left(U^i \middle| U^{1:i-1}\right) \leq \delta_N \right\} \quad (10)$$

where for $i \in \mathscr{H}_X$, U_i is almost independent from $U^{1:i-1}$ and uniformly distributed. For $i \in \mathscr{L}_X$, U_i is almost determined by $U^{1:i-1}$.

So for asymmetric channel coding, the distribution of the channel input X^N need to be optimal to achieve the channel capacity. By applying the source polarisation technique to the channel polar coding, one can generate a X^N with arbitrary distribution from a uniformly distributed source.

Theorem 2: (Asymmetric channel coding [18, 19]) Consider W^N is N independent copies of a symmetric DMC W with polar channel coding $U^N G_N = X^N$ [8]. Assuming we know the optimal distribution of W^N and the polarised index sets $\mathscr{H}_X$, $\mathscr{L}_X$ for source polarisation, then one can generate the optimally distributed X^N through the polar channel coding by assigning U^N as

- for $i \in \mathscr{H}_X$, U^i is assigned with uniformly distributed information bit;
- for $i \in \mathscr{L}_X$, bit assigned to U^i is determined as

$$u^i = \arg \max_{u \in \{0,1\}} p_{U^i|U^{i-1}}\left(u \middle| u^{1:i-1}\right). \quad (11)$$

Remark 2: For the polarisation matrix $\boldsymbol{G}_N$, it is easy to prove $G_N^{-1} = \boldsymbol{G}_N$. So the source polarisation $U^N = X^N \boldsymbol{G}_N$ equals to $U^N G_N^{-1} = X^N$ and $U^N \boldsymbol{G}_N = X^N$, which is the same formation as the polar channel coding.

3.2 Slepian–Wolf coding

In the two-way wiretap channel, eavesdropper Eve is observing messages from Alice and Bob simultaneously, therefore the best wiretapping strategy for Eve turns into the Slepian–Wolf problem of a 2-users multiple access channel (MAC-2). Arıkan [20] studied this problem and proposed a polar source coding method based on monotone chain rule expansion. Then his method was extended to the polar channel coding with arbitrary distributed channel input in [21].

Definition 5: (MAC-2) Let $(\mathscr{X}_1, \mathscr{X}_2, \mathscr{Y}, p_{Y|X_1X_2})$ be a discrete memoryless MAC-2 with binary inputs, and $p_{X_1X_2}$ is the fixed arbitrary probability distribution on $\mathscr{X}_1 \times \mathscr{X}_2$. The achievable rate region for MAC-2 is

$$\mathscr{R}(p_{Y|X_1X_2}) = \left\{ \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \middle| \begin{matrix} 0 \leq R_1 \leq I(X_1; Y|X_2) \\ 0 \leq R_2 \leq I(X_2; Y|X_1) \\ R_1 + R_2 \leq I(X_1, X_2; Y) \end{matrix} \right\}. \quad (12)$$

Consider blocks (X_1^N, X_2^N) of MAC-2, for $N = 2^n$, $n \geq 1$, define

$$U_1^N = X_1^N G_N \text{ and } U_2^N = X_2^N G_N. \quad (13)$$

Since $G_N^{-1} = G_N$, also holds

$$U_1^N G_N = X_1^N \text{ and } U_2^N G_N = X_2^N. \quad (14)$$

Definition 6: (Monotone chain rule expansion [20]) For the monotone chain rule expansion of $U^N V^N$, define $S^{1:2N} = (S^1, S^2, \ldots, S^{2N})$ as a permutation of $U^N V^N$ which preserved the relative order of U^N and V^N, define a string $b^{1:2N} = b^1 b^2 \cdots b^{2N}$ as the expansion path from $\varnothing$ to $U^N V^N$, where $S^i \in U_1^N$ for $b_i = 0$ and $S^i \in U_2^N$ for $b^i = 1$, and define $\psi_{2N} \triangleq \{0^{1:i} 1^{1:N} 0^{i+1:N}\}$ as a class of path $b^{1:2N}$.

Theorem 3: [20, 21] Let (R_1, R_2) be a given rate pair on the dominant face of $\mathscr{R}(p_{Y|X_1X_2})$. For $N = 2^n$ and chain rule $b^{1:2N}$ on U_1U_2 such that $b^{1:2N} \in \psi_{2N}$, define $\mathscr{S}_{U_1} = \left\{ i \in [\![1, 2N]\!] : b^i = 0 \right\}$ and $\mathscr{S}_{U_2} = \left\{ i \in [\![1, 2N]\!] : b^i = 1 \right\}$. Then there exist a rate pair (R_{U_1}, R_{U_2}) that

$$R_{U_1} = H(X_1) - \frac{1}{N} \sum_{i \in \mathscr{S}_{U_1}} H\left(S^i \middle| Y^{1:N}, S^{1:i-1}\right)$$
$$R_{U_2} = H(X_2) - \frac{1}{N} \sum_{i \in \mathscr{S}_{U_2}} H\left(S^i \middle| Y^{1:N}, S^{1:i-1}\right). \quad (15)$$

For any given $\epsilon > 0$, (R_{U_1}, R_{U_2}) satisfying

$$\left|R_{U_1} - R_1\right| \leq \epsilon \quad \text{and} \quad \left|R_{U_2} - R_2\right| \leq \epsilon. \quad (16)$$

Now we introduce the geometric scaling operation given by Arıkan in [20] which can achieve the polarisation. Considering an original path $b^{1:2N}$ for $U_1^N U_2^N$, and an integer k. Then for the monotone chain rule of $U_1^{1:2^kN} U_2^{1:2^kN}$, denote an extended path $2^k b^{1:2N}$ which preserves the 'shape' of the original path as

$$\underbrace{b^1 \cdots b^1}_{2^k} \underbrace{b^2 \cdots b^2}_{2^k} \cdots \underbrace{b^{2N} \cdots b^{2N}}_{2^k}.$$

Lemma 1: [20] Let $b^{1:2N}$ be a fixed path with rate pair (R_{U_1}, R_{U_2}), and $2^k b^{1:2N}$ is the extended path by geometric scaling operation. If $b^{1:2N} \in \psi_{2N}$ then $2^k b^{1:2N} \in \psi_{2^k 2N}$. And (R_{U_1}, R_{U_2}) is also the rate pair for the path $2^k b^{1:2N}$.

Theorem 4: (Polarisation and code construction [20, 21]) Consider the MAC-2 in Definition 5 and settings in (13). Fix $N_0 = 2^{n_0}$ for $n_0 \geq 1$. Fix a path $b^{1:2n_0}$ for $U_1^{N_0} U_2^{N_0}$. Let (R_{U_1}, R_{U_2}) be the rate pair for $b^{1:2N_0}$. Let $N = 2^k N_0$ and $S^{1:2N}$ be the edge variables for $2^k b^{1:2N_0}$. Let $\boldsymbol{f}_j(i): [\![1, 2N]\!] \to \mathscr{S}_{U_j}$ $(j = 1, 2)$ be the mapping from indices of U_j^N to the corresponding $S^{1:2N}[\mathscr{S}_{U_j}]$ over the path $b^{1:2N}$. For $\beta \in (0, 1/2)$, $\delta_N = 2^{-N^\beta}$, as k goes to infinity, have

$$\frac{1}{2N} \left| \left\{ i \in [\![1, 2N]\!] : \delta_N < Z\left(S^i \middle| Y^{1:N} S^{1:i-1}\right) < 1 - \delta_N \right\} \right| \to 0. \quad (17)$$

The information sets $\mathscr{I}_j$ constructed as

$$\mathscr{I}_j = \mathscr{H}_{S_{U_j}} \cap \mathscr{L}_{S_{U_j}|Y} \quad (18)$$

where

$$\mathscr{H}_{S_{U_j}} = \left\{ i \in [\![1, N]\!] : Z(S^{\boldsymbol{f}_j(i)} | S^{1:\boldsymbol{f}_j(i)_{-1}}) \geq 1 - \delta_N \right\}$$
$$\mathscr{L}_{S_{U_j}|Y} = \left\{ i \in [\![1, N]\!] : Z(S^{\boldsymbol{f}_j(i)} | Y^{1:N} S^{1:\boldsymbol{f}_j(i)_{-1}}) \leq \delta_N \right\}, \quad (19)$$

and satisfy

$$\frac{|\mathscr{I}_1|}{N} \to R_{U_1} \text{ and } \frac{|\mathscr{I}_2|}{N} \to R_{U_2}. \quad (20)$$

3.3 Coded cooperative jamming

Coded cooperative jamming was first introduced by Tekin and Yener in [15, 16], which is the strategy for increasing the communication rate of two-way wiretap channel by jamming Eve

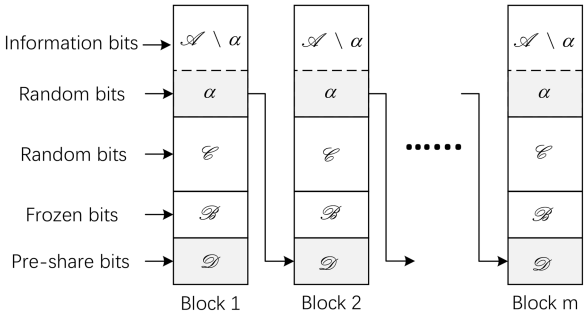

Fig. 2 *Original multi-block chaining structure of [10]*

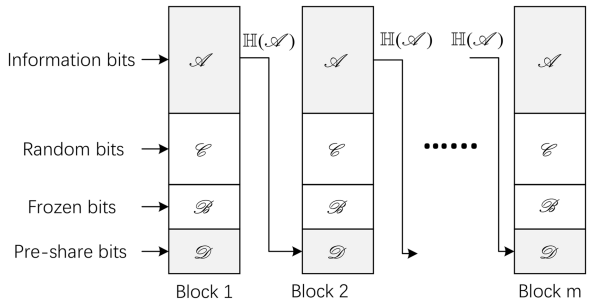

Fig. 3 *Hash chaining structure*

with cooperative noise under an acceptable level of information rate sacrifice.

Definition 7: Define two uniformly distributed auxiliary messages $M'_1 \in \mathscr{M}'_1 = [\![1, 2^{NR'_1}]\!]$ and $M'_2 \in \mathscr{M}'_2 = [\![1, 2^{NR'_2}]\!]$ for performing the cooperative jamming and introducing noise to the eavesdropper. And reliability is required for legitimate users decoding the auxiliary messages. Define C_1 and C_2 as the generated codes for cooperative jamming with fixed distributions p_{C_1} and p_{C_2}.

The normalised construction method for coded cooperative jamming was given by Pierrot and Bloch [17]. For $j = 1, 2$, generate $\lceil 2^{NR_j} \rceil \lceil 2^{NR_{j'}} \rceil$ i.i.d. sequence $c_j^{1:N}(\mu_j, \mu_{j'})$ with $(\mu_j, \mu_{j'}) \in \mathscr{M}_j \times \mathscr{M}_{j'}$ according to p_{C_j}, where μ_j is the indices of the main message M_j and $\mu_{j'}$ is the indices of the auxiliary message $M_{j'}$. To obtain the final channel input $x_j^{1:N}$, one needs to transmit the generated $c_j^{1:N}(\mu_j, \mu_{j'})$ through a prefixed virtual discrete memoryless channel with transition probability $p_{X_j|C_j}$, which is called *the prefixing technique* [22]. Then as a combination with secure polar coding, a *polar coded cooperative jamming* construction method was proposed by Zheng *et al.* [14].

Theorem 5: (Polar coded cooperative jamming [14]) Consider the index sets partition for the secure polar coding scheme in [9, 10], for $j = 1,2$, let index set $\mathscr{I}_j$ be the information set, let index set $\mathscr{R}_j$ be the random set, let index set $\mathscr{F}_j$ be the frozen set. Let $U_j^N = C_j^N \boldsymbol{G}_N$ and $V_j^N = X_j^N \boldsymbol{G}_N$.

- *Code generation:* main messages are assigned to $u_j^{1:N}[\mathscr{I}_j]$ to obtain reliability and security. Randomly auxiliary messages are assigned to $u_j^{1:N}[\mathscr{R}_j]$ to obtain reliability. Frozen bits are assigned to $u_j^{1:N}[\mathscr{F}_j]$. Then $c_j^{1:N}$ can be generated by $c_j^{1:N} = u_j^{1:N} \boldsymbol{G}_N$.
- *Channel prefixing:* consider X_j and C_j as two correlated sources, for $\beta \in (0, 1/2)$, $\delta_N = 2^{-N^\beta}$, define

$$\mathscr{L}_{X_j|C_j} = \left\{ i \in [\![1, N]\!] : Z(V_j^i \middle| V_j^{1:i-1}, C_j^{1:N}) \right\}. \tag{21}$$

For $i \in (\mathscr{L}_{X_j|C_j})^c$, v_j^i is assigned with uniformly distributed random bits; for $i \in \mathscr{L}_{X_j|C_j}$,

$$v_j^i = \arg \max_{v \in \{0,1\}} p_{V_j^i | V_j^{1:i-1} C_j^{1:N}} \left(v \middle| v_j^{1:i-1}, c_j^{1:N} \right). \tag{22}$$

Then $x_j^{1:N}$ can be calculated from $v_j^{1:N}$ by $x_j^{1:N} = v_j^{1:N} \boldsymbol{G}_N$.

4 Hash chaining structure

In this section, we propose a new method for achieving both reliability and strong security, together with an increased secrecy rate over the original multi-block chaining structure in [10, 14]. The new strong security achieving method will also be applied in the construction of secure polar coding scheme in the next section.

4.1 Problem of achieving strong security

Consider a binary input DMC one-way wiretap channel $\mathscr{U} \to \mathscr{X} \to \mathscr{Y}, \mathscr{Z}$ from Alice to Bob and the eavesdropper Eve with $p_{YZ|X}$. For channel polarisation, $\beta \in (0, 1/2)$, $\delta_N = 2^{-N^\beta}$, have

$$\begin{aligned}
\mathscr{H}_{X|Y} &= \left\{ i \in [\![1, N]\!] : Z\left(U^i \middle| U^{1:i-1}, Y^{1:N}\right) \geq 1 - \delta_N \right\} \\
\mathscr{L}_{X|Y} &= \left\{ i \in [\![1, N]\!] : Z\left(U^i \middle| U^{1:i-1}, Y^{1:N}\right) \leq \delta_N \right\} \\
\mathscr{H}_{X|Z} &= \left\{ i \in [\![1, N]\!] : Z\left(U^i \middle| U^{1:i-1}, Z^{1:N}\right) \geq 1 - \delta_N \right\} \\
\mathscr{L}_{X|Z} &= \left\{ i \in [\![1, N]\!] : Z\left(U^i \middle| U^{1:i-1}, Z^{1:N}\right) \leq \delta_N \right\},
\end{aligned} \tag{23}$$

where $\mathscr{H}_{X|Y}$ and $\mathscr{L}_{X|Y}$ are the index sets for almost full-noise bits and almost non-noise bits to Bob, respectively; $\mathscr{H}_{X|Z}$ and $\mathscr{L}_{X|Z}$ are the index sets for almost full-noise bits and almost non-noise bits to Eve, respectively. Then divides the index $[\![1, N]\!]$ into

$$\begin{aligned}
\mathscr{A} &= \mathscr{L}_{X|Y} \cap \mathscr{H}_{X|Z} \\
\mathscr{B} &= (\mathscr{L}_{X|Y})^c \cap \mathscr{H}_{X|Z} \\
\mathscr{C} &= \mathscr{L}_{X|Y} \cap (\mathscr{H}_{X|Z})^c \\
\mathscr{D} &= (\mathscr{L}_{X|Y})^c \cap (\mathscr{H}_{X|Z})^c,
\end{aligned} \tag{24}$$

and $\mathscr{A} \cup \mathscr{B} \cup \mathscr{C} \cup \mathscr{D} = [\![1, N]\!]$ holds. According to the channel polarisation result, a subset $\mathscr{A}$ is reliable and secure, so it is for information bits; subset $\mathscr{B}$ is not reliable but secure, so it is for frozen bits; the subset $\mathscr{C}$ is reliable but not secure, so it is for random bits. Then the remaining problem is the subset $\mathscr{D}$ since it is neither reliable nor secure [9]. If the subset $\mathscr{D}$ is set for random bits, a reliable criterion cannot be achieved when decoding these random bits. If the subset $\mathscr{D}$ is set for frozen bits, the strong security criterion cannot be achieved.

One notable solution for this problem is the multi-block chaining structure proposed by Şaşoğlu and Vardy [10] as illustrated in Fig. 2. In the structure, communication contains m independent N-length blocks. For each block, a $|\mathscr{D}|$ length index set α is separated from $\mathscr{A}$. For the block i, $\mathscr{D}$ is for the random bits in α of block $i - 1$. When decoding the bits in $\mathscr{D}$, use the random bits decoded from α in the last block as the replacement. Since α is reliable and secure, the reliability of $\mathscr{D}$ can be achieved under the strong security criterion.

However, since the reliability of $\mathscr{D}$ is obtained by sacrificing parts of the $\mathscr{A}$, when $|\mathscr{D}|$ is close to $|\mathscr{A}|$, $\mathscr{A} \setminus \alpha$ becomes too small for information bits transmission.

4.2 Hash chaining structure

For the dilemma of the subset $\mathscr{D}$, we present a new solution called *hash chaining structure* which can achieve the reliability under the constrain of strong security without good bits sacrifice. As illustrated in Fig. 3, the hash chaining structure also divides the transmission process into m independent N-length blocks.

Definition 8: Define a hash bits generating process $\mathbb{H}(\cdot)$, denote $\mathbb{H}(\mathscr{A})$ the hash bits generated from $U^N[\mathscr{A}]$ with length $|\mathscr{D}|$. Basically in $\mathbb{H}(\cdot)$, the hash value of $U^N[\mathscr{A}]$ is calculated by

$h(U^N[\mathscr{A}])$ and then is extended to $|\mathscr{D}|$-length bits with a certain approach. Note that $\mathbb{H}(\cdot)$ is based on a hash algorithm, so $U^N[\mathscr{A}]$ cannot be decrypted from $\mathbb{H}(\mathscr{A})$, which guarantees the security.

Then the structure is as follows. For polar coding of each block, $\mathscr{A}$ is for information bits, $\mathscr{B}$ is for frozen bits, $\mathscr{C}$ is for uniformly distributed random bits. For block 1, $\mathscr{D}$ is for the pre-shared bits. For the block $i > 1$, $\mathscr{D}$ is for the hash bits calculated from $U^N[\mathscr{A}]$ of block $i-1$ by $\mathbb{H}(\mathscr{A})$. When successive cancellation (SC) decoding, for block 1, bits in $\mathscr{D}$ are replaced by the pre-shared bits, for the block $i > 1$, bits in $\mathscr{D}$ are replaced by $\mathbb{H}(\mathscr{A})$ from $\hat{U}^N[\mathscr{A}]$ of block $i-1$.

4.3 Performance analyses

Now we analyse the performance of the hash chaining structure.

Lemma 2: [8] Considering an arbitrary subset $\mathscr{G}$ of the index N for DMC W, in case of $\mathscr{G}$ used as the information set and $\mathscr{G}^c$ used as a frozen set for polar coding, by applying the SC decoding, for $\beta \in (0, 1/2)$, $\delta_N = 2^{-N^\beta}$, when

$$\mathscr{G} \subseteq \left\{ i \in [\![1, N]\!] : Z\left(U^i \middle| U^{1:i-1}\right) \le \delta_N \right\}, \tag{25}$$

have

$$P_e(\mathscr{G}) \le \sum_{i \in \mathscr{G}} Z(U^i \middle| U^{1:i-1}, Y^N) = O(2^{-N^\beta}). \tag{26}$$

Lemma 3: [10] Considering the polar subset division of the multi-block chaining structure, for $t \in [\![1, m]\!]$, let $\boldsymbol{M}^t$ be the message, $\boldsymbol{A}^t = U^N[\alpha^t]$, $\boldsymbol{Z}^t = (Z^N)^t$, $I^{1:t} = I(\boldsymbol{M}^{1:t}\boldsymbol{A}^t; \boldsymbol{Z}^{1:t})$. Then have

$$I^{1:t} \le I^{1:t-1} + I(\boldsymbol{M}^t\boldsymbol{A}^t; \boldsymbol{Z}^t). \tag{27}$$

Definition 9: For an arbitrary subset $\mathscr{G}$ of the index N, define $g^1 < g^2 < \cdots < g^{|\mathscr{G}|}$ be the correspondent indices of the elements $U^{1:N}[\mathscr{G}]$, and

$$U^{1:N}[\mathscr{G}] \triangleq U^{g^1:g^{|\mathscr{G}|}} = U^{g^1}, U^{g^1}, \ldots, U^{g^{|\mathscr{G}|}}. \tag{28}$$

Lemma 4: [13] Considering the polar subset division of index N, for arbitrary $\mathscr{G} \subseteq \mathscr{H}_{X|Z}$, $i \in [\![1, |\mathscr{G}|]\!]$, $g^i \in \mathscr{G}$, $\beta \in (0, 1/2)$, $\delta_N = 2^{-N^\beta}$, have

$$\begin{aligned} H(U^{g^i} \middle| U^{q^1:q^{i-1}}, Z^N) &\ge H(U^{q^i} \middle| U^{1:q^{i-1}}, Z^N) \\ &\ge 1 - O(N^2 2^{-N^\beta}). \end{aligned} \tag{29}$$

Proposition 1: (Performance of hash chaining structure) For the B-DMC one-way wiretap channel defined in this section, with a fixed block number m, the proposed hash chaining structure can achieve a greater secrecy rate than the original multi-block chaining structure under the reliability and strong security criterions.

Proof: Denote $\mathscr{C}_H$ the code of hash chaining structure with secrecy rate R_H. Denote $\mathscr{C}_{MB}$ the code of multi-block chaining structure with secrecy rate R_{MB}.

Reliability: since the hash bits for $\mathscr{D}$ is calculated from $U^N[\mathscr{A}]$ of the last block, have

$$\begin{aligned} P_e(\mathscr{C}_H) &\le (m-1) \sum_{i \in \mathscr{A}} Z(U^i \middle| U^{1:i-1}, Y^{1:N}) \\ &\quad + m \sum_{i \in \mathscr{A} \cup \mathscr{C}} Z(U^i \middle| U^{1:i-1}, Y^{1:N}) \\ &\overset{(a)}{\le} (m-1) mo(2^{-N^\beta}) + mo(2^{-N^\beta}) \\ &= (2m-1) o(2^{-N^\beta}), \end{aligned} \tag{30}$$

where (a) is based on Lemma 2. So the reliability criterion is achieved.

Strong security: for hash chaining structure, $t \in [\![1, m]\!]$, denote $\boldsymbol{H}^t = \mathbb{H}(\mathscr{A}^t)$. Same as the multi-block chaining structure [10], for hash chaining structure, the following Markov chains also hold for applying Lemma 3:

$$\begin{aligned} &\boldsymbol{M}^{1:t-1} \to \boldsymbol{M}^t\boldsymbol{H}^t \to \boldsymbol{Z}^t, \\ &\boldsymbol{M}^t\boldsymbol{H}^t\boldsymbol{Z}^t \to \boldsymbol{M}^{1:t-1}\boldsymbol{H}^{t-1} \to \boldsymbol{Z}^{0:t}. \end{aligned} \tag{31}$$

Thus for all m blocks

$$\begin{aligned} L(\mathscr{C}_H) &= I(\boldsymbol{M}^{1:m}; \boldsymbol{Z}^{1:m}) \\ &\le I(\boldsymbol{M}^{1:m}\boldsymbol{H}^m; \boldsymbol{Z}^{1:m}) \\ &\overset{(a)}{\le} \sum_{t=1}^{m} I(\boldsymbol{M}^t\boldsymbol{H}^t; \boldsymbol{Z}^t) + I(\boldsymbol{H}^0; \boldsymbol{Z}^0) \\ &\overset{(b)}{=} \sum_{t=1}^{m} I(\boldsymbol{M}^t\boldsymbol{M}^t; \boldsymbol{Z}^t) + I(\boldsymbol{H}^0; \boldsymbol{Z}^0) \\ &= \sum_{t=1}^{m} I(\boldsymbol{M}^t; \boldsymbol{Z}^t) + I(\boldsymbol{H}^0; \boldsymbol{Z}^0), \end{aligned} \tag{32}$$

where (a) is due to Lemma 3, (b) is due to the hash bits generation, and $I(\boldsymbol{H}^0; \boldsymbol{Z}^0)$ is the information leakage of pre-shared bits which should be 0.

$$\begin{aligned} I(\boldsymbol{M}^t; \boldsymbol{Z}^t) &= I(U^N[\mathscr{A}^t]; Z^N) \\ &= \sum_{i=1}^{|\mathscr{A}^t|} I(U^{q^i}; Z^N \middle| U^{q^{1:q^{i-1}}}) \\ &\overset{(a)}{=} \sum_{i=1}^{|\mathscr{A}^t|} I(U^{q^i}; U^{q^{1:q^{i-1}}} Z^N) \\ &\overset{(b)}{\le} O(N^3 2^{-N^\beta}), \end{aligned} \tag{33}$$

where (a) is because U^{q^i} is independent of each other, (b) is due to Lemma 4 with $\mathscr{A} \subseteq \mathscr{H}_{X|Z}$. Therefore, have

$$L(\mathscr{C}_H) \le mO(N^3 2^{-N^\beta}). \tag{34}$$

So the strong security criterion is achieved.

Secrecy rate: under the reliability and strong security criterions, for multi-block chaining structure, from [10] have

$$R_{MB} = \frac{m(|\mathscr{A}| - |\alpha|)}{mN} = \frac{|\mathscr{A} \cup \mathscr{C}| - |\mathscr{D} \cup \mathscr{C}|}{N} = C_s. \tag{35}$$

For hash chaining structure, have

$$R_H = \frac{m|\mathscr{A}|}{mN} = R_{MB} + \frac{|\mathscr{D}|}{N} = C_s + \frac{|\mathscr{D}|}{N}. \tag{36}$$

Thus, additional secrecy rate has been achieved. □

5 Encrypted polar coding scheme

In this section, we construct encryption embedded secure polar coding scheme for two-way wiretap channel. In the aim of implementing a one-time pad for both legitimate users, we construct a secure and reliable transmission for both secret keys and ciphertexts simultaneously based on the secure polar coding scheme of [14]. Our proposed scheme also achieves an additional secrecy rate under the reliability and strong security criterions.

5.1 Encryption strategy

Definition 10: (One-time pad [1]) Let $\pi^{1:l}$ be binary plaintext sequence. Let $k^{1:l}$ be a binary keystream. Let $e^{1:l}$ be binary ciphertext. Define the process of the one-time pad as

$$\begin{aligned} e^{1:l} &= \mathbb{E}(\pi^{1:l}, k^{1:l}) = \pi^{1:l} \oplus k^{1:l} \\ \pi^{1:l} &= \mathbb{D}(e^{1:l}, k^{1:l}) = e^{1:l} \oplus k^{1:l}, \end{aligned} \tag{37}$$

where $\mathbb{E}(\cdot)$ denotes the encryption, $\mathbb{D}(\cdot)$ denotes the decryption, keystream $k^{1:l}$ is a true random stream and can only be used once. For secure polar coding, $j = 1, 2$, define $\mathscr{K}_j$ as the index set for key transmission and define $\mathscr{E}_j$ as the index set for ciphertext transmission.

Note that to implement the one-time pad, the length of keystream must be no less than the length of plaintext. So when constructing the encrypted polar coding scheme, if setting $|\mathscr{K}_j| \geq |\mathscr{E}_j|$, legitimate users can directly transmit the keystream along with the ciphertext, which however will reduce the *rate for ciphertext (effective secrecy rate)*. In the case of $|\mathscr{K}_j| < |\mathscr{E}_j|$ and $|\mathscr{K}_j| \ll |\mathscr{E}_j|$, although a much higher rate can be achieved for ciphertext, one-time pad cannot be applied since the transmitted keystream is too short for decryption.

To achieve a high rate for ciphertext and implement the one-time pad, we introduce the *binary chaotic keystream generator* (BCKSG) algorithm to modify the one-time pad. BCKSG is the pseudo-random number generator based on a chaotic system with low complexity. Since the chaotic system has unique characteristics of irregularity, aperiodicity and extremely sensitive to the intimal conditions [23–25], the generated chaotic sequence is suitable for keystream. There are many rigorously proofed chaos pseudo-random number generator, such as [26, 27], can be used as BCKSG, so in our scheme, we just focus on the encrypted coding construction and consider the BCKSG in a general formation.

Definition 11: (BCKSG) Let φ be a l' length binary seed that $l' < l$. Define the BCKSG as $\mathbb{C}(\varphi) = \tilde{k}^{1:l}$, which is the mapping from the seed φ to l length binary keystream $\tilde{k}^{1:l}$.

Thus, we have

$$\begin{aligned} e^{1:l} &= \mathbb{E}\big(\pi^{1:l}, \mathbb{C}(\varphi)\big) = \pi^{1:l} \oplus \tilde{k}^{1:l} \\ \pi^{1:l} &= \mathbb{D}\big(e^{1:l}, \mathbb{C}(\varphi)\big) = e^{1:l} \oplus \tilde{k}^{1:l}, \end{aligned} \tag{38}$$

where φ is also considered as the secret key for encryption and decryption.

Therefore, the *overall encryption strategy of our scheme* for the two-way wiretap channel can be summarised as follows:

- The legitimate sender uses a relatively short secret key φ to generate a key stream $\tilde{k}^{1:l}$ and encrypts the plaintext as in (38).
- Then legitimate sender transmits the secret key along with the ciphertext to the legitimate receiver over the channel. Reliability and security for secret key and ciphertext transmission are guaranteed by secure polar coding.
- Since the length of the secret key can be much shorter than the ciphertext, the rate for ciphertext can be increased as much as possible when constructing the polar coding.
- The legitimate receiver decodes both ciphertext and secret key correctly and then recovers the plaintext by the decryption process in (38).
- Based on the constructed key transmission, a secret key φ can be renewed in each round for implementing a one-time pad without any key pre-sharing.

5.2 Encrypted polar coding scheme

Considering the two-way wiretap channel given in Definition 1 with $\mathscr{P} = \{p_{X_1X_2C_1C_2Y_1Y_2Z}\}$ for the polar coded cooperative jamming given in Theorem 1. For $j = 1, 2$, again, let $U_j^N = C_j^N \boldsymbol{G}_N$ and $V_j^N = X_j^N \boldsymbol{G}_N$. Assuming that we know the optimal distribution of C_j and X_j for the asymmetric channel.

For communication from Alice to Bob, X_2 can be treated as the side information on the Bob side, and the transition probability from Alice to Bob with cooperative jamming is

$$\begin{aligned} &p \in \mathscr{P}, p_{Y_1|C_1X_2}(y_1|c_1, x_2) \\ &\quad = p_{Y_1|X_1X_2}(y_1|x_1, x_2) p_{X_1|C_1}(x_1|c_1). \end{aligned} \tag{39}$$

Similarly for communication from Bob to Alice, X_1 can be treated as the side information on the Alice side, and transition probability from Bob to Alice with cooperative jamming is

$$\begin{aligned} &p \in \mathscr{P}, p_{Y_2|C_2X_1}(y_2|c_2, x_1) \\ &\quad = p_{Y_2|X_1X_2}(y_2|x_1, x_2) p_{X_2|C_2}(x_2|c_2). \end{aligned} \tag{40}$$

For the eavesdropper Eve, the transition probability is

$$\begin{aligned} &p \in \mathscr{P}, p_{Z|C_1C_2}(z|c_1, c_2) \\ &\quad = p_{Z|X_1X_2}(z|x_1, x_2) p_{X_1|C_1}(x_1|c_1) p_{X_2|C_2}(x_2|c_2). \end{aligned} \tag{41}$$

Thus for asymmetric two-way wiretap channel, consider the polarisations between two legitimate users with cooperative jamming.

Source polarisation

$$\begin{aligned} \mathscr{H}_{C_1|X_2} &= \left\{ i \in [\![1, N]\!] : Z(U_1^i \big| U_1^{1:i-1}, X_2^{1:N} \geq 1 - \delta_N) \right\} \\ \mathscr{H}_{C_2|X_1} &= \left\{ i \in [\![1, N]\!] : Z(U_2^i \big| U_2^{1:i-1}, X_1^{1:N} \geq 1 - \delta_N) \right\}. \end{aligned} \tag{42}$$

Channel polarisation

$$\begin{aligned} \mathscr{L}_{C_1|Y_1X_2} &= \left\{ i \in [\![1, N]\!] : Z(U_1^i \big| U_1^{1:i-1}, Y_1^{1:N}, X_2^{1:N} \leq \delta_N) \right\} \\ \mathscr{L}_{C_2|Y_2X_1} &= \left\{ i \in [\![1, N]\!] : Z(U_2^i \big| U_2^{1:i-1}, Y_2^{1:N}, X_1^{1:N} \leq \delta_N) \right\}. \end{aligned} \tag{43}$$

Prefix polarisation

$$\begin{aligned} \mathscr{L}_{X_1|C_1} &= \left\{ i \in [\![1, N]\!] : Z(V_1^i \big| V_1^{1:i-1}, C_1^{1:N} \leq \delta_N) \right\} \\ \mathscr{L}_{X_2|C_2} &= \left\{ i \in [\![1, N]\!] : Z(V_2^i \big| V_2^{1:i-1}, C_2^{1:N} \leq \delta_N) \right\}. \end{aligned} \tag{44}$$

For the polarisation of an eavesdropper, Slepian–Wolf coding is concerned as Theorem 4.

Source polarisation

$$\mathscr{H}_{S_{U_j}} = \left\{ i \in [\![1, N]\!] : Z(S^{\boldsymbol{f}_j(i)} \big| S^{1:\boldsymbol{f}_j(i)_{-1}}) \geq 1 - \delta_N \right\}. \tag{45}$$

Channel polarisation

$$\begin{aligned} \mathscr{H}_{S_{U_j}|Z} &= \left\{ i \in [\![1, N]\!] : Z(S^{\boldsymbol{f}_j(i)} \big| Z^{1:N} S^{1:\boldsymbol{f}_j(i)_{-1}}) \geq 1 - \delta_N \right\} \\ \mathscr{L}_{S_{U_j}|Z} &= \left\{ i \in [\![1, N]\!] : Z(S^{\boldsymbol{f}_j(i)} \big| Z^{1:N} S^{1:\boldsymbol{f}_j(i)_{-1}}) \leq \delta_N \right\}. \end{aligned} \tag{46}$$

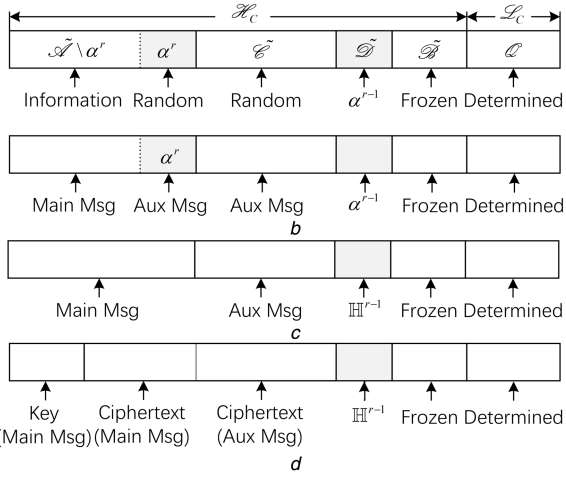

Fig. 4 *Comparison between the original secure polar coding structure of [14] and our proposed encrypted polar coding structure of index* $[\![1,N]\!]$ *for the block r,* $r \in [\![1,m]\!]$*, footnotes are omitted*

(a) Secure polar coding for the asymmetric channel of [14], ***(b)*** Secure polar coding with cooperative jamming of [14], ***(c)*** Coded cooperative jamming with our hash chaining structure, ***(d)*** Our proposed encrypted polar coding with cooperative jamming

Remark 3: Messages X_1 and X_2 are independent, so that

$$\begin{aligned}\mathscr{H}_{C_1|X_2} &= \mathscr{H}_{C_1} = \left\{i \in [\![1,N]\!] : Z(U_1^i \middle| U_1^{1:i-1} \geq 1-\delta_N)\right\}\\ \mathscr{H}_{C_2|X_1} &= \mathscr{H}_{C_2} = \left\{i \in [\![1,N]\!] : Z(U_2^i \middle| U_2^{1:i-1} \geq 1-\delta_N)\right\}\\ \mathscr{H}_{S_{U_1}} &= \mathscr{H}_{C_1},\ \mathscr{H}_{S_{U_2}} = \mathscr{H}_{C_2}.\end{aligned} \tag{47}$$

Define two parameter variable m_j and l'_j that m_j is the number of blocks for the multi-block chaining structure and l'_j is the length of the secret key φ_j.

Consider the secure polar coding from Alice to Bob with multi-block chaining structure and asymmetric channel coding, for the block $r \in [\![1,m]\!]$, the index $[\![1,N]\!]$ can be divided by

$$\begin{aligned}\widetilde{\mathscr{A}}_1 &= \mathscr{H}_{C_1} \cap \mathscr{L}_{C_1|Y_1X_2} \cap \mathscr{H}_{S_{U_1}|Z}\\ \widetilde{\mathscr{B}}_1 &= \mathscr{H}_{C_1} \cap (\mathscr{L}_{C_1|Y_1X_2})^c \cap \mathscr{H}_{S_{U_1}|Z}\\ \widetilde{\mathscr{C}}_1 &= \mathscr{H}_{C_1} \cap \mathscr{L}_{C_1|Y_1X_2} \cap (\mathscr{H}_{S_{U_1}|Z})^c\\ \widetilde{\mathscr{D}}_1 &= \mathscr{H}_{C_1} \cap (\mathscr{L}_{C_1|Y_1X_2})^c \cap (\mathscr{H}_{S_{U_1}|Z})^c\\ \mathscr{Q}_1 &= (\mathscr{H}_{C_1})^c\end{aligned} \tag{48}$$

satisfying

$$\widetilde{\mathscr{A}}_1 \cup \widetilde{\mathscr{B}}_1 \cup \widetilde{\mathscr{C}}_1 \cup \widetilde{\mathscr{D}}_1 \cup \mathscr{Q}_1 = [\![1,N]\!]. \tag{49}$$

In the original secure polar coding scheme of [14], to achieve the strong security, the multi-block chaining structure is applied with a subset α_1 construction that $\alpha_1 \subset \widetilde{\mathscr{A}}_1$, $|\alpha_1| = |\widetilde{\mathscr{D}}_1|$. However, for our encrypted construction, in case of multi-block chaining structure, good bits of $\widetilde{\mathscr{A}}_1$ are partly sacrificed for obtaining the reliability of subset $\widetilde{\mathscr{D}}_1$, which may lead the problem that good bits left in $\widetilde{\mathscr{A}}_1$ is not enough for constructing a secure key transmission when $\widetilde{\mathscr{D}}_1$ is too large.

Therefore, to avoid this problem, we use the hash chaining structure instead of the encrypted polar coding construction. The comparison of the structures between the original secure polar coding scheme of [14] and our encrypted secure polar coding scheme is illustrated in Fig. 4.

Fig. 4*a* illustrates the subsets division of (48) with multi-block structure, same as [14]. $\widetilde{\mathscr{A}}_1 \setminus \alpha_1$ is reliable and secure and for information bits, α_1 is reliable and secure and for functional random bits, $\widetilde{\mathscr{B}}_1$ is not reliable but secure and for frozen bits, $\widetilde{\mathscr{C}}_1$ is reliable but not secure and for random bits, $\widetilde{\mathscr{D}}_1$ is neither secure nor reliable and for the bits in α_1 of the last block. Additionally, $\mathscr{Q}_1$ is for determined bits to construct optimally distributed channel inputs.

Fig. 4*b* is the structure of the original polar coded cooperative jamming in [14]. $\widetilde{\mathscr{A}}_1 \setminus \alpha_1$ is set for main messages since security and reliability are required, $\widetilde{\mathscr{C}}_1$ is set for auxiliary messages since reliability is required. α_1 can also for auxiliary messages since it can obtain reliability. In this construction, considering the rate pair of cooperative jamming $(R_1, R_{1'})$ for the main message and auxiliary message, have

$$R_1 = \frac{1}{N}\left|\widetilde{\mathscr{A}}_1 \setminus \alpha_1\right| \text{ and } R'_1 = \frac{1}{N}(|\alpha_1| + |\widetilde{\mathscr{C}}_1|). \tag{50}$$

Different from [14], in our polar coding structure, the hash chaining structure is applied. As illustrated in Fig. 4*c*, without constructing the subset α_1, hash bits are generated from $\widetilde{\mathscr{A}}_1$ as $\mathbb{H}(\widetilde{\mathscr{A}}_1)$ for the subset $\widetilde{\mathscr{D}}_1$ of the next block. Thus the structure of coded cooperative jamming is also changed. $\widetilde{\mathscr{A}}_1$ is set for main messages since security and reliability are required, $\widetilde{\mathscr{C}}_1$ is set for auxiliary messages since reliability is required. Note that in the original cooperative jamming structure in [14], α_1 can only be used as an auxiliary message since information in this subset will be exposed to Eve owing to the multi-block chaining structure. However, in our hash chaining structure, information in α_1 is secure from Eve, so can be used as the main message.

Further, to construct the encrypted secure polar coding scheme, rearrangements of the divided subsets are also made. As illustrated in Fig. 4*d*, part of $\widetilde{\mathscr{A}}_1$ is separated and used for secret key also as the main message. The rest part of $\widetilde{\mathscr{A}}_1$ is for ciphertext also as the main message. $\widetilde{\mathscr{C}}_1$ is for ciphertext also as the auxiliary message for cooperative jamming.

Thus, the specific partition of index $[\![1,N]\!]$ and definition of subsets for our proposed encrypted polar coding is as follows:

- $\mathscr{K}_1$ denotes the index set for a secret key with rate R_1^k, satisfying $|\mathscr{K}_1| = l'$ and $\mathscr{K}_1 \subseteq \widetilde{\mathscr{A}}_1 \setminus \alpha_1$. Reliability and security are provided by polar coding. Used as the main message for cooperative jamming.
- $\mathscr{E}_1^M$ denotes the index set for ciphertext with rate R_1^{em}, satisfying $\mathscr{E}_1^M = \widetilde{\mathscr{A}}_1 \setminus \mathscr{K}_1$. For $\mathscr{E}_1^M$, reliability and security are provided by polar coding. Used as the main message for cooperative jamming.
- $\mathscr{E}_1^A$ denotes the index set for ciphertext with rate R_1^{ea}, satisfying $\mathscr{E}_1^A = \widetilde{\mathscr{C}}_1$. Reliability is provided by polar coding, security is provided by encryption. Used as the auxiliary message for cooperative jamming.

- $\mathscr{F}_1$ denotes the index set for frozen bits with rate R_1^f, satisfying $\mathscr{F}_1 = \widetilde{\mathscr{B}}_1$. Unreliable, but security is provided by polar coding.
- $\mathscr{T}_1$ denotes the index set for the hash bits calculated from $\widetilde{\mathscr{A}}_1$ of the last block, with the rate R_1^t. Insecure, but reliability is provided by the hash chaining structure.
- $\mathscr{Q}_1$ denotes the index set for determined bits with rate R_1^q, bits are calculated from the bits of the previous index. Reliability and security are not concerned.

The relation between our encrypted polar partition and the original polar partition of (48) is illustrated in Fig. 5. Note that the rate pair of the encrypted coding scheme $(\tilde{R}_1, \tilde{R}_1')$ is also different from the original rate pair (R_1, R_1'), that

$$\begin{aligned} \tilde{R}_1 &= R_1^k + R_1^{em} \quad \text{and } \tilde{R}_1' = R_1^{ea}, \\ R_1 &= R_1^k + R_1^{em} - R_1^t \quad \text{and } R'_1 = R_1^{ea} + R_1^t. \end{aligned} \tag{51}$$

Now we introduce the encryption and transmission process from Alice to Bob over the two-way wiretap channel.

To begin with, we fix a l_1' as the length of the secret key φ_1 and $|\mathscr{K}_1|$ with the following constrains:

- l_1' should be long enough for the demand of secure encryption.
- $l' \le |\widetilde{\mathscr{A}}_1|$ for constructing a secure and reliable key transmission.
- $l_1' < |\widetilde{\mathscr{C}}_1| + |\widetilde{\mathscr{D}}_1|$ for bigger effective secrecy rate than the original secure polar coding.

Then the length of the ciphertext l_1 for every block can be calculated by $l_1 = |\widetilde{\mathscr{A}}_1| + |\widetilde{\mathscr{C}}_1| - l_{1'}$. Thus the block number m_1 can be calculated by $m_1 = \lceil L_1/l_1 \rceil$, where L_1 is the length of the plaintext message that Alice wants to send.

Encryption: Divide the plaintext message π_1 into m_1 pieces $(\pi_1^1, \pi_1^2, \ldots, \pi_1^{m_1})$, and encrypt them into ciphertexts as

$$e_1^r = \mathbb{E}(\pi_1^r, \mathbb{C}(\varphi_1^r)), r \in [\![1, m_1]\!] \tag{52}$$

where r is the block number and φ_1^r is the corresponding secret key.

Encoding: For the block r, $r \in [\![1, m_1]\!]$,

- $u_1^{1:N}[\mathscr{K}_1]$ is assigned with φ_1^r.
- $u_1^{1:N}[\mathscr{E}_1^M]$ and $u_1^{1:N}[\mathscr{E}_1^A]$ is assigned with e_1^r.
- $u_1^{1:N}[\mathscr{F}_1]$ is assigned with frozen bits.
- $u_1^{1:N}[\mathscr{T}_1]$ is assigned with hash bits $\mathbb{H}(\widetilde{\mathscr{A}}_1^{r-1})$ for $r > 1$, or assigned with a pre-shared random bits for $r = 1$.
- $u_1^{1:N}[\mathscr{Q}_1]$ is assigned with determined bits calculated from the bits of the previous index as

$$u_1^i = \arg \max_{u \in \{0,1\}} p_{U_1^i | U_1^{i-1}}\left(u \middle| u_1^{1:i-1}\right). \tag{53}$$

Then $c_1^{1:N}$ is calculated by $c_1^{1:N} = u_1^{1:N}\boldsymbol{G}_N$. To obtain the channel input $x_1^{1:N}$, one approach is to transmit $c_1^{1:N}$ through a prefixed DMC with transition probability $p_{X_1|C_1}$, another approach is the construction method in Theorem 5. Consider the prefixing polarisation:

$$\mathscr{L}_{X_1|C_1} = \left\{ i \in [\![1, N]\!] : Z(V_1^i \middle| V_1^{1:i-1}, C_1^{1:N} \le \delta_N) \right\}. \tag{54}$$

For $i \in (\mathscr{L}_{X_1|C_1})^c$, v_1^i is assigned with uniformly distributed random bits; for $i \in \mathscr{L}_{X_1|C_1}$,

$$v_1^i = \arg \max_{v \in \{0,1\}} p_{V_1^i | V_1^{1:i-1} C_1^{1:N}}\left(v \middle| v_1^{1:i-1}, c_1^{1:N}\right). \tag{55}$$

Then $x_1^{1:N}$ is calculated from $v_1^{1:N}$ by $x_1^{1:N} = v_1^{1:N}\boldsymbol{G}_N$, and is sent to Bob over the two-way wiretap channel.

Decoding: For the block r, $r \in [\![1, m_1]\!]$, $y_1^{1:N}$ is received from the channel at the Bob side. Bob uses the SC decoder [8] to obtain the estimated $\hat{u}_1^{1:N}$.

- For $i \in \mathscr{F}_1$, $\hat{u}_1^i = u_1^i$.
- For $i \in \mathscr{T}_1$, if $r = 1$, $\hat{u}_1^i = u_1^i$, if $r > 1$, $\hat{u}_1^{1:N}[\mathscr{T}_1] = \mathbb{H}(\hat{u}_1^{1:N}[\widetilde{\mathscr{A}}_1^{r-1}])$.
- For $i \in \mathscr{Q}_1$,

$$\hat{u}_1^i = \arg \max_{u \in \{0,1\}} p_{U_1^i | U_1^{1:i-1}}\left(u \middle| \hat{u}_1^{1:i-1}\right). \tag{56}$$

- For $i \in \mathscr{K}_1 \cup \mathscr{E}_1^M \cup \mathscr{E}_1^A$,

$$\hat{u}_1^i = \arg \max_{u \in \{0,1\}} p_{U_1^i | U_1^{1:i-1} Y_1^{1:N} X_2^{1:N}}\left(u \middle| \hat{u}_1^{1:i-1} y_1^{1:N} x_2^{1:N}\right). \tag{57}$$

Decryption: For the block r, $r \in [\![1, m_1]\!]$, extract the ciphertext $\hat{e}_1^r$ and secret key $\hat{\varphi}_1^r$ from estimated $\hat{u}_1^{1:N}$. Then decrypt the $\hat{e}_1^r$ to obtain the plaintext $\hat{\pi}_1^r$ by

$$\hat{\pi}_1^r = \mathbb{D}\left(\hat{e}_1^r, \mathbb{C}(\hat{\varphi}_1^r)\right). \tag{58}$$

After m_1 blocks of transmission, Bob obtains the plaintext as $\hat{e}_1 = (\hat{e}_1^1, \hat{e}_1^2, \ldots, \hat{e}_1^{m_1})$.

The construction of the encrypted coding scheme from Bob to Alice is similar to the construction from Alice to Bob.

6 Performance

Let $\mathscr{C}_A$ be our proposed encryption embedded polar codes for the transmission from Alice to Bob. Let $\mathscr{C}_B$ be the proposed encryption embedded polar codes for the transmission from Bob to Alice.

6.1 Reliability

Proposition 2: (Reliability) For $N \to \infty$, $\beta \in (0, 1/2)$, by choosing a proper m_1 and m_2, $P_e(\mathscr{C}_A, \mathscr{C}_B) = 0$.

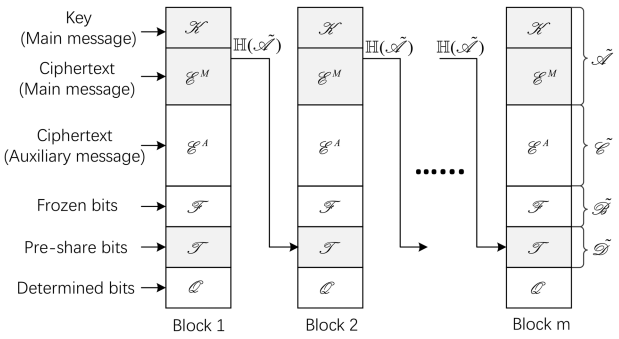

Fig. 5 *Hash chaining structure-based encrypted coding scheme, footnotes are omitted*

Proof: Considering the hash chaining structure and SC decoder, for $\mathscr{C}_A$

$$\begin{aligned} P_e(\mathscr{C}_A) &\le (m_1-1)\sum_{i\in\mathscr{K}_1\cup\mathscr{E}_1^M} Z(U_1^i\big|U_1^{1:i-1},Y_1^{1:N},X_2^{1:N}) \\ &\quad + m_1\sum_{i\in\mathscr{K}_1\cup\mathscr{E}_1^M\cup\mathscr{E}_1^A} Z(U_1^i\big|U_1^{1:i-1},Y_1^{1:N},X_2^{1:N}) \\ &\overset{(a)}{<} (m_1-1)O(2^{-N^\beta}) + m_1O(2^{-N^\beta}) \\ &= (2m_1-1)O(2^{-N^\beta}), \end{aligned} \tag{59}$$

where (a) is based on Lemma 2.

Thus, have $P_e(\mathscr{C}_A) < (2m_1-1)O(2^{-N^\beta})$ and similarly $P_e(\mathscr{C}_B) < (2m_2-1)o(2^{-N^\beta})$. So for fixed m_1, m_2, have

$$\lim_{N\to\infty} P_e(\mathscr{C}_A,\mathscr{C}_B) = 0, \tag{60}$$

which proofs the reliability. □

6.2 Security

Since confidential messages are encrypted before the transmission, we only need to concern the information leakage for the key transmission. Consider the full-duplex case that $m_1 = m_2 = m$ for the multi-block chaining structure. For the block $r \in [\![1,m]\!]$, $j = 1,2$, denote $\boldsymbol{K}_j^r = u_j^{1:N}[\mathscr{K}_j]$, $\boldsymbol{Z}^r = z^{1:N}$, $\boldsymbol{H}^r = \mathbb{H}(\widetilde{\mathscr{A}}_j^r)$.

Proposition 3: (Strong security) For $N\to\infty$, $\beta\in(0,1/2)$, by choosing a proper m, $L(\mathscr{C}_A,\mathscr{C}_B)=0$.

Proof: Considering an arbitrary path for the chain rule expansion for Eve, we apply a similar analysis in [14] for $I(\boldsymbol{K}_1^r\boldsymbol{K}_2^r;\boldsymbol{Z}^r)$. Denote an index set $\{a^1,a^2,\ldots,a^t\}\subset[\![1,2N]\!]$ with $t = |\mathscr{K}_1| + |\mathscr{K}_2|$, such that

$$\{S^{a^1},S^{a^2},\ldots,S^{a^t}\} = \{U_1^{f_1(i_1)},U_2^{f_2(i_2)}: i_1\in\mathscr{K}_1, i_2\in\mathscr{K}_2\}. \tag{61}$$

Thus, we have (see (62)) , where (a) is $H(S^{a_i}\big|S^{1:a_i-1},\boldsymbol{Z}^r)\ge Z(S^{a_i}\big|S^{1:a_i-1},\boldsymbol{Z}^r)^2$ [18]. Thus similarly as Proposition 1, for hash chaining structure, have

$$\begin{aligned} L(\mathscr{C}_A,\mathscr{C}_B) &= I(Z^N;M_1M_2\big|\mathscr{C}_A,\mathscr{C}_B) \\ &\overset{(a)}{=} I(\boldsymbol{K}_1^{1:m}\boldsymbol{K}_2^{1:m};\boldsymbol{Z}^{1:m}) \\ &\le I(\boldsymbol{K}_1^{1:m}\boldsymbol{K}_2^{1:m}\boldsymbol{H}_1^m\boldsymbol{H}_2^m;\boldsymbol{Z}^{1:m}) \\ &\le \sum_{r=1}^m I(\boldsymbol{K}_1^r\boldsymbol{K}_2^r\boldsymbol{H}_1^r\boldsymbol{H}_2^r;\boldsymbol{Z}^r) + I(\boldsymbol{H}_1^0\boldsymbol{H}_2^0;\boldsymbol{Z}^0) \\ &= mO(N2^{-N^\beta}), \end{aligned} \tag{63}$$

where (a) is due to the encrypted polar coding structure. So for a fixed m, have

$$\lim_{N\to\infty} L(\mathscr{C}_A,\mathscr{C}_B) = 0, \tag{64}$$

which proofs the strong security. □

6.3 Achievable rate region

Proposition 4: (Achievable secrecy rate) For our proposed encrypted secure polar coding scheme with a properly constructed $\mathscr{K}_j$ for key transmission and the hush chaining structure, have the achievable secrecy rate pair as $(\tilde{R}_1,\tilde{R}_2)$ and the achievable effective secrecy rate pair for ciphertext transmission as $(\bar{R}_1,\bar{R}_2)$. Then when $N\to\infty$, the upper bounds for both achievable rate pair $(\tilde{R}_1,\tilde{R}_2)$ and $(\bar{R}_1,\bar{R}_2)$ can be greater than the rate upper bound in Theorem 1 for two-way wiretap channel.

Proof: For our proposed secure coding scheme, the secrecy rate pair $(\tilde{R}_1,\tilde{R}_2)$ represents the rate of the main message in the cooperative jamming structure which includes the key bits and part of the ciphertext bits. Thus according to the index subsets partition of our encrypted secure polar coding scheme with hash chaining structure, for the upper bound of achievable secrecy rate $\tilde{R}_1$ have

$$\begin{aligned} \tilde{R}_1 &= \lim_{N\to\infty}\frac{m\big|\mathscr{K}_1\cup\mathscr{E}_1^M\big|}{mN} \\ &= \lim_{N\to\infty}\frac{1}{N}\big|\widetilde{\mathscr{A}}_1\big| \\ &= \lim_{N\to\infty}\frac{1}{N}\big(\big|\widetilde{\mathscr{A}}_1\big| - \big|\widetilde{\mathscr{D}}_1\big| + \big|\mathscr{T}_1\big|\big) \\ &= \lim_{N\to\infty}\frac{1}{N}\big(\big|\widetilde{\mathscr{A}}_1\cup\widetilde{\mathscr{E}}_1\big| - \big|\widetilde{\mathscr{D}}_1\cup\widetilde{\mathscr{E}}_1\big|\big) + \lim_{N\to\infty}\frac{1}{N}\big|\mathscr{T}_1\big| \\ &= \lim_{N\to\infty}\frac{1}{N}\big(\big|\mathscr{H}_{C_1}\cap\mathscr{L}_{C_1|Y_1X_2}\big| - \big|\mathscr{H}_{C_1}\cap\mathscr{L}_{S_{U_1}|Z}\big|\big) + R_1^t \\ &= I(Y_1;C_1|X_2) - I(C_1;Z) + R_1^t, \end{aligned} \tag{65}$$

where R_1^t is the rate for the unreliable and insecure subset $\mathscr{T}_1$. Similarly, for the upper bound of the achievable secrecy rate $\tilde{R}_2$, we have

$$\tilde{R}_2 = I(Y_2;C_2|X_1) - I(C_2;Z) + R_2^t. \tag{66}$$

Hence, these prove that the upper bounds of the achievable rate pair $(\tilde{R}_1,\tilde{R}_2)$ are greater than the strong security achievable rate region in Theorem 1.

Next, we consider the upper bound of the effective secrecy rate pair $(\bar{R}_1,\bar{R}_2)$ that represents the rate for reliable ciphertext transmission. According to the index subsets partition of our encrypted secure polar coding scheme with hash chaining structure, for the upper bound of achievable effective secrecy rate $\bar{R}_1$, has

$$\begin{aligned} I(\boldsymbol{K}_1^r\boldsymbol{K}_2^r;\boldsymbol{Z}^r) &= H(\boldsymbol{K}_1^r\boldsymbol{K}_2^r) - H(\boldsymbol{K}_1^r\boldsymbol{K}_2^r\big|\boldsymbol{Z}^r) \\ &= \sum_{i=1}^t\left[H(S^{a_i}\big|S^{a_1},\ldots,S^{a_{i-1}}) - H(S^{a_i}\big|S^{a_1},\ldots,S^{a_{i-1}},\boldsymbol{Z}^r)\right] \\ &\le \sum_{i=1}^t\left[H(S^{a_i}\big|S^{a_1},\ldots,S^{a_{i-1}}) - H(S^{a_i}\big|S^{1:a_i-1},\boldsymbol{Z}^r)\right] \\ &\overset{(a)}{\le} \sum_{i=1}^t\left[1 - Z(S^{a_i}\big|S^{1:a_i-1},\boldsymbol{Z}^r)^2\right] \\ &\le \sum_{i=1}^t\left[1-(1-\delta_N)^2\right] = O(N2^{-N^\beta}), \end{aligned} \tag{62}$$

$$
\begin{aligned}
\bar{R}_1 &= \lim_{N\to\infty}\frac{m\left|\mathscr{C}_1^M\right|}{mN}\\
&= \lim_{N\to\infty}\frac{1}{N}\left(\left|\widetilde{\mathscr{A}}_1\cup\widetilde{\mathscr{C}}_1\right|-\left|\mathscr{K}_1\right|\right)\\
&= \lim_{N\to\infty}\frac{1}{N}\left(\left|\widetilde{\mathscr{A}}_1\cup\widetilde{\mathscr{C}}_1\right|-\left|\widetilde{\mathscr{D}}_1\cup\widetilde{\mathscr{C}}_1\right|\right)\\
&\quad+\lim_{N\to\infty}\frac{1}{N}\left(\left|\widetilde{\mathscr{D}}_1\cup\widetilde{\mathscr{C}}_1\right|-\left|\mathscr{K}_1\right|\right)\\
&= \lim_{N\to\infty}\frac{1}{N}\left(\left|\mathscr{H}_{C_1}\cap\mathscr{L}_{C_1|Y_1X_2}\right|+\lim_{N\to\infty}\frac{1}{N}\left(\left|\widetilde{\mathscr{D}}_1\cup\widetilde{\mathscr{C}}_1\right|-\left|\mathscr{K}_1\right|\right)\right.\\
&= I(Y_1;C_1\left|X_2\right)-I(C_1;Z)+\lim_{N\to\infty}\frac{1}{N}\left(\left|\widetilde{\mathscr{D}}_1\cup\widetilde{\mathscr{C}}_1\right|-\left|\mathscr{K}_1\right|\right)\\
&\overset{(a)}{>} I(Y_1;C_1|X_2)-I(C_1;Z),
\end{aligned}
\tag{67}
$$

where (a) is due to the constrain of subset $\mathscr{K}_1$ that $\left|\mathscr{K}_1\right| < \left|\widetilde{\mathscr{C}}_1\right| + \left|\widetilde{\mathscr{D}}_1\right|$. Similarly, for the upper bound of achievable effective secrecy rate $\bar{R}_2$, has

$$
\bar{R}_2 > I(Y_2;C_2|X_1)-I(C_2;Z)\,. \tag{68}
$$

Therefore, these prove that the upper bounds of the achievable effective secrecy rate pair $(\bar{R}_1,\bar{R}_2)$ are also greater than the strong security achievable rate region in Theorem 1.□

6.4 Discussion

For polar codes, the $\delta_N = 2^{-N^\beta}$, $\beta\in(0,1/2)$ was firstly presented by Arıkan in [28] as follows.

Theorem 6: [28] Let W be any B-DMC with $I(W)>0$, $R<I(W)$ and $\beta<0.5$. Then for $N=2^n$, $n>0$, the best achievable block error probability for polar coding under SC decoding at block length N and rate R satisfies

$$
P_e(N,R) = o(2^{-N^\beta})\,. \tag{69}
$$

Theorem 6 indicates that the decoding error probability of polar codes is bounded by $o(\delta_N)$, which only depends on whether $R<I(W)$ for any block length $N=n^2$. This theorem is also the very theoretical basis of almost all the proof works for reliability, weak security and strong security when analysing the performance of a certain secure polar coding scheme.

Note that, according to the analysis results of our proposed secure polar coding scheme, the decoding error probability is upper bounded by $O(\delta_N)$, the information leakage is upper bounded by $O(N\delta_N)$ and the information leakage rate is upper bounded by $O(\delta_N)$. Thus to obtain theoretically perfect secrecy and reliability, we can assume an infinite block length N to vanish those upper bounds.

For practical cases with finite block length N, although the theoretical perfect secrecy or reliability cannot be achieved, we still can obtain the reliability and security at an acceptable high level by using the secure polar coding with a long enough block length. Also, since those upper bounds are still held for finite blocklength case, both the level of actual information leakage rate and the actual decoding error rate can be measured by the δ_N relatively. Besides, there are some well-studied techniques for improving the polarisation performance of finite length polar codes, such as the finite-length scaling technique [29–31] and the fast polarisation technique [32], which also can be applied for improving the achievable reliability and security of finite length secure polar coding.

However, for the practical case with small block length N, polar codes may not be a good option for secure coding due to the unacceptable low level of polarisation. Under such circumstances, LDPC codes are a more appropriate option since these can maintain much better performance for both reliability and security with small block length. For instance, as presented in [33] for the Gaussian wiretap channel, the secure LDPC codes have approached the ultimate performance limits even with relatively small block lengths.

7 Conclusion

In this paper, we have presented a new hash chaining structure to solve the good bits sacrificing problem for achieving both reliability and strong security. Further on this structure, we have constructed encryption embedded secure polar coding scheme for asymmetric two-way wiretap channel with cooperative jamming, which successfully solves the problems of key exchange for one-time pad and rate sacrifice for secure polar coding. Based on the existing polar coding scheme, we have designed a reliable and secure transmission for both key and ciphertext and implemented a chaotic pseudo-random number generator based one-time pad without any pre-sharing keys. As proved, our proposed scheme can achieve extended upper bounds for both achievable secrecy rate pair and effective secrecy rate pair than the original achievable secrecy rate region under the strong security and reliability criterions.

8 Acknowledgment

This work was supported in part by the Natural Science Foundation of Hubei Province (grant no. 2017CFB398) and the Fundamental Research Funds for the Central Universities (grant nos. 2662017QD042, 2662017QD041).

9 References

[1] Shannon, C.E.: 'Communication theory of secrecy systems', *Bell Labs Tech. J.*, 1998, **15**, p. 57
[2] Shiu, Y.S., Chang, S.Y., Wu, H.C., *et al.*: 'Physical layer security in wireless networks: a tutorial', *IEEE Wirel. Commun.*, 2011, **18**, pp. 66–74
[3] Wyner, A.D.: 'The wire-tap channel', *Bell Syst. Tech. J.*, 1975, **54**, pp. 1355–1387
[4] Csiszár, I., Körner, J.: 'Broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 1978, **24**, pp. 339–348
[5] Wong, C.W., Wong, T.F., Shea, J.M.: 'Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel', *IEEE Trans. Inf. Forensics Secur.*, 2011, **6**, pp. 551–564
[6] Thangaraj, A., Dihidar, S., Calderbank, A.R., *et al.*: 'Applications of LDPC codes to the wiretap channel', *IEEE Trans. Inf. Theory*, 2004, **53**, pp. 2933–2945
[7] Rathi, V., Urbanke, R., Andersson, M., *et al.*: 'Rate-Equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel'. IEEE Int. Symp. Information Theory, 2011, pp. 2393–2397
[8] Arıkan, E.: 'Channel polarization: a method for constructing capacity achieving codes for symmetric binary-input memoryless channels', *IEEE Trans. Inf. Theory*, 2009, **55**, pp. 3051–3073
[9] Mahdavifar, H., Vardy, A.: 'Achieving the secrecy capacity of wiretap channels using polar codes', *IEEE Trans. Inf. Theory*, 2011, **57**, pp. 6428–6443
[10] Şaşoğlu, E., Vardy, A.: 'A new polar coding scheme for strong security on wiretap channels'. IEEE Int. Symp. Information Theory, 2013, pp. 1117–1121
[11] Hassani, S.H., Urbanke, R.: 'Universal polar code'. IEEE Int. Symp. Information Theory, 2014, pp. 1451–1455
[12] Wei, Y.P., Ulukus, S.: 'Polar coding for the general wiretap channel'. Proc. IEEE Information Theory Workshop, 2015, pp. 1–5
[13] Gulcu, T.C., Barg, A.: 'Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component'. Proc. IEEE Information Theory Workshop, 2015, pp. 1–5
[14] Zheng, M., Tao, M., Chen, W., *et al.*: 'Secure polar coding for the two-way wiretap channel'. IEEE Access, 2017, pp. 1–1
[15] Tekin, E., Yener, A.: 'The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming', *IEEE Trans. Inf. Theory*, 2008, **54**, pp. 2735–2751
[16] Tekin, E., Yener, A.: 'Correction to: 'The Gaussian multiple access wire-tap channel' and 'The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming'', *IEEE Trans. Inf. Theory*, 2010, **56**, pp. 4762–4763
[17] Pierrot, A., Bloch, M.: 'Strongly secure communications over the two-way wiretap channel', *IEEE Trans. Inf. Forensics Secur.*, 2011, **6**, pp. 595–605
[18] Arıkan, E.: 'Source polarization'. IEEE Int. Symp. Information Theory, 2010, pp. 899–903
[19] Honda, J., Yamamoto, H.: 'Polar coding without alphabet extension for asymmetric models', *IEEE Trans. Inf. Theory*, 2013, **59**, pp. 7829–7838
[20] Arıkan, E.: 'Polar coding for the Slepian-Wolf problem based on monotone chain rules'. IEEE Int. Symp. Information Theory, 2012, pp. 566–570

[21] Zheng, M., Ling, C., Chen, W., *et al.*: 'A new polar coding scheme for the interference channel'. ArXiv e-prints, 2016. Available at http://arxiv.org/abs/1608.08742
[22] El Gamal, A., Koyluoglu, O.O., Youssef, M., *et al.*: 'New achievable secrecy rate regions for the two-way wiretap channel'. Proc. IEEE Information Theory Workshop, Cairo, Egypt, 2010, pp. 1–5
[23] Mathews, R.: 'On the derivation of a chaotic encryption algorithm', *Cryptrologia*, 1989, **13**, pp. 29–42
[24] May, R.: 'Simple mathematical models with very complicated dynamic', *Nature*, 1976, **261**, pp. 459–467
[25] Baptista, M.S.: 'Cryptography with chaos', *Phys. Lett. A*, 1998, **240**, pp. 50–54
[26] Li, S., Mou, X., Cai, Y.: 'Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography'. Int. Conf. on Cryptology in India, 2001, pp. 316–329
[27] Wang, X.Y., Wang, X.J.: 'Design of chaotic pseudo-random bit generator and its applications in stream-cipher cryptography', *Int. J. Mod. Phys. C*, 2008, **19**, pp. 813–820
[28] Arıkan, E., Telatar, E.: 'On the rate of channel polarization'. IEEE Int. Symp. Information Theory, 2009, pp. 1493–1495
[29] Guruswami, V., Xia, P.: 'Polar codes: speed of polarization and polynomial gap to capacity'. IEEE 54th Annual Symp. on Foundations of Computer Science (FOCS), 2013, pp. 310–319
[30] Mondelli, M., Urbanke, R., Hassani, S.H.: 'Unified scaling of polar codes: error exponent, scaling exponent, moderate deviations, and error floors'. IEEE Int. Symp. Information Theory, 2015, pp. 1422–1426
[31] Goldin, D., Burshtein, D.: 'Improved bounds on the finite length scaling of polar codes', *IEEE Trans. Inf. Theory*, 2014, **60**, pp. 6966–6978
[32] Mahdavifar, H.: 'Fast polarization and finite-length scaling for non-stationary channels'. ArXiv e-prints, 2016. Available at http://arxiv.org/abs/1611.04203
[33] Baldi, M., Ricciutelli, G., Maturo, N., *et al.*: 'Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel'. Proc. IEEE ICC 2015, Int. Conf. on Communications, Workshop on Wireless Physical Layer Security, London, UK, 2015, pp. 446–451