SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

November 2021, Vol. 64 212301:1–212301:20
https://doi.org/10.1007/s11432-020-3119-3

Secure polar coding for a joint source-channel model

Haowei WANG, Xiaofeng TAO*, Huici WU, Na LI & Jin XU

National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876*, China*

Received 6 August 2020/Revised 15 October 2020/Accepted 17 November 2020/Published online 14 October 2021

Abstract This paper investigates a joint source-channel model where Alice, Bob, and Eve, observe components of a discrete memoryless source and communicate over a discrete memoryless wiretap channel which is independent of the source. Alice and Bob wish to agree upon a secret key and simultaneously communicate a secret message, both of which are required to be kept concealed from Eve. An achievable tradeoff region between the secret-key and secret-message rates has been established in the literature. In this paper, we propose an explicit polar coding scheme that achieves the tradeoff region for general sources and channels under the strong secrecy criterion. The encoding scheme is constructed based on a nontrivial combination of (1) encoding scheme for secret-key generation using correlated sources, (2) utilizing the generated key as a one-time pad to encrypt the secret message partially, and (3) a modified form of wiretap channel encoding scheme that incorporates the structure of superposition coding.

Keywords polar codes, joint source-channel model, correlated sources, secret-key generation, wiretap channel

Citation Wang H W, Tao X F, Wu H C, et al. Secure polar coding for a joint source-channel model. Sci China Inf Sci, 2021, 64(11): 212301, https://doi.org/10.1007/s11432-020-3119-3

1 Introduction

As a new paradigm addressing security issues of wireless networks, information-theoretic security has received significant attention in the past decades. In the pioneering work [1], Wyner first introduced the wiretap channel and recognized that legitimate users can take advantage of noisy channels to enable secure transmission in the presence of an eavesdropper. Csiszár and Körner [2] later extended this result to general broadcast channels. Along another line, Maurer [3] and Ahlswede and Csiszár [4] first studied the problem of secret-key generation from information-theoretic perspective. It was noted that correlated sources and public communication can be used for generating a secret key. Csiszár and Narayan [5] further considered the case when public communication has a rate constraint. There has arisen a body of studies (see [6–10] and references therein) investigating either the problem of secure transmission over wiretap channels or that of secret-key generation using correlated sources.

There are practical scenarios such as wireless sensor networks where distributed sensor nodes possess correlated information and communicate over noisy wireless channels in the presence of potential eavesdropping. Prabhakaran et al. [11] thus introduced a new joint source-channel model, where Alice, Bob, and Eve observe correlated sources and are also connected by a wiretap channel which is independent of the sources. The two aforementioned problems are then jointly studied in such a model, and an achievable tradeoff region between the secret-key and secret-message rates was established, which is further shown to be optimal when the source and the channel satisfy certain Markov conditions. Concurrently, Khisti et al. [12] considered a similar joint setting but focused solely on the secret-key generation problem. Upper and lower bounds on the secret-key capacity were derived in [12], and these bounds coincide when both the source and channel are degraded in favor of Bob. Roughly, Ref. [12] can be seen as a special case of [11] when Alice and Bob wish to maximize the secret-key rate. In contrast, the other special case of [11] is when Alice and Bob wish to maximize the secret-message rate, which has been considered in [13–16].

* Corresponding author (email: taoxf@bupt.edu.cn)

In the literature, there also exist two types of models closely related to the joint source-channel model. The first type is the wiretap channel with feedback [17–25], in which Alice and Bob exploit feedback signals (instead of correlated sources in the joint model) to agree upon a secret key and then use the key as a one-time pad to augment the secret-message rate. Specifically, feedback signals here include output feedback [17–20], state information feedback [21–24], or generalized feedback [25]. The second type is the wiretap channel with shared key [26–28], in which Alice and Bob share beforehand a secret key of which Eve does not know. To some extent, the second type can be seen as a simplified version of the first one in the sense that legitimate users share a secret key directly. It should also be noted that both types keep maximizing the secret-message rate as the central task (similar to [13–16]), whereas the joint source-channel model features the tradeoff between the secret-key and secret-message rates.

Given a particular model, the secrecy or secret-key capacity is typically approached by random coding arguments, for instance, in all the aforementioned works. To develop practical schemes achieving those theoretic results is a crucial follow-up work and of great interest. In this paper, we consider polar codes [29], which are the first class of provable capacity-achieving codes for a number of channels and enjoy low encoding and decoding complexity. The recent decade has seen various secrecy-capacity-achieving polar codes designed for wiretap channels such as [30–35]. While secret-key agreements usually rely on reconciliation and privacy amplification techniques [36], Chou et al. [37, 38] proposed alternative polar coding schemes for achieving the secret-key capacity. To our best knowledge, there has been no practical coding scheme ever developed for the joint source-channel model. In this paper, our main contribution is to fill the gap using polar codes. Specifically, we follow the setup of [11], and prove that our polar coding scheme achieves the tradeoff region derived in [11] for general sources and channels under strong secrecy criterion.

The encoding scheme mainly consists of two steps that handle the correlated sources and the wiretap channel successively. Firstly, Alice quantizes its source sequence and extracts a public message M that carries the side information necessary for Bob to reconstruct the quantized sequence, and a secret key K that will be later used as a one-time pad. Secondly, Alice transmits over the wiretap channel the public message M and a secret message S partially encrypted by the secret key K. For the first step, we refer to the encoding scheme proposed in [38, Model 2] for a secret-key generation with rate-limited public communication. Note that in [38, Model 2] the public message M is sent directly over the noiseless public channel, while in the present work M needs to be encoded into wiretap channel codes. For the second step, we develop a modified form of wiretap channel encoding scheme that incorporates the structure of superposition coding. In a previous work of ours [33], we proposed a polar coding scheme for wiretap channels with a shared key, which involves a similar coding structure. However, in [33], we only have to worry about how to use the pre-shared key properly to increase the secret-message rate. In this paper, we investigate the simultaneous secret-message transmission along with secret-key generation using correlated sources, thus the present scheme is more general and involved than that in [33].

A detailed analysis is finally provided to validate the performance of the proposed scheme. It is worth noting that the public message M is shown to be nearly uniform and independent of Eve's source observations. Subsequently, we can prove that the induced joint distribution by our scheme is close to the target one by which the polarization sets are defined, which is necessary for the evaluation of reliability and strong secrecy.

Organization. The rest of this paper is organized as follows. Section 2 formally introduces the joint source-channel model [11] and recaps previous theoretic results of this model. Section 3 presents our polar coding scheme for achieving the tradeoff region for general sources and channels under the strong secrecy criterion. Section 4 presents a detailed analysis of the proposed scheme. Finally, Section 5 concludes this paper.

Notations. We use $[n]$ to indicate the index set $\{1, 2, \ldots, n\}$. For any random variable X, $X^{1:n}$ represents a sequence of size n, i.e., $X^{1:n} \triangleq (X^1, X^2, \ldots, X^n)$. For any subset $\mathcal{T} \subseteq [n]$, $X^{1:n}[\mathcal{T}]$ indicates $\{X^i\}_{i\in\mathcal{T}}$. For two probability distributions p_X and q_X on $\mathcal{X}$, $D(p_X||q_X)$ and $V(p_X, q_X)$ are the Kullback-Leibler divergence and the total variation distance between p_X and q_X, respectively. G_n denotes the generator matrix of polar codes [29].

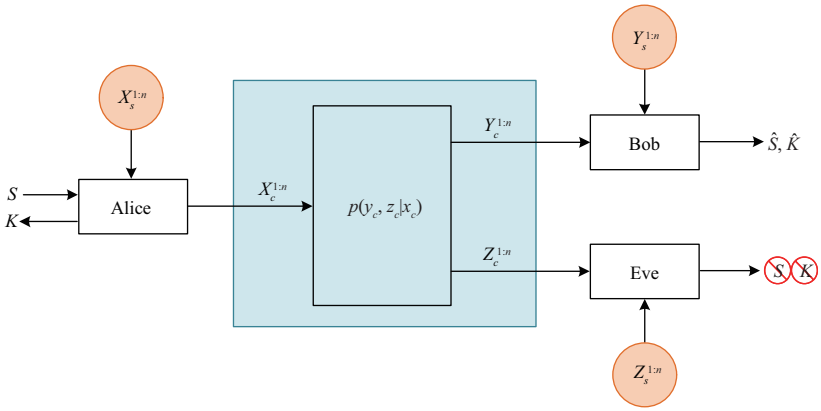

Figure 1 (Color online) The joint source-channel model. Three terminals observe components of a discrete memoryless source and communicate over a discrete memoryless wiretap channel. Alice and Bob intend to share a secret message S and a secret key K, both of which are required to be kept concealed from Eve.

2 The joint source-channel model

Consider a discrete memoryless source $p(x_s, y_s, z_s)$ with three components (X_s, Y_s, Z_s) and their corresponding alphabets $(\mathcal{X}_s, \mathcal{Y}_s, \mathcal{Z}_s)$. In this paper, we assume that $\mathcal{X}_s = \{0, 1\}$. Three terminals, Alice, Bob, and Eve, observe n i.i.d. repetitions of X_s, Y_s, and Z_s, which are denoted by $X_s^{1:n} \triangleq (X_s^1, \ldots, X_s^n)$, $Y_s^{1:n} \triangleq (Y_s^1, \ldots, Y_s^n)$, $Z_s^{1:n} \triangleq (Z_s^1, \ldots, Z_s^n)$, respectively. Furthermore, there is a discrete memoryless wiretap channel $p(y_c, z_c|x_c)$ from Alice to Bob and Eve, where we denote $X_c^{1:n} \triangleq (X_c^1, \ldots, X_c^n)$ the binary input and $Y_c^{1:n} \triangleq (Y_c^1, \ldots, Y_c^n)$, $Z_c^{1:n} \triangleq (Z_c^1, \ldots, Z_c^n)$ the outputs with countable alphabets. The considered model is graphically shown in Figure 1. Note that, a noiseless public channel is not available in the model. The correlated sources and the wiretap channel are assumed to be independent, i.e., $(X_s, Y_s, Z_s) \to X_c \to (Y_c, Z_c)$ holds. Moreover, the source sequences are known to the corresponding terminals before the transmission over the wiretap channel begins, i.e., noncausally.

In this paper, we consider the scenario in which Alice intends to transmit a secret message S (uniformly distributed over the alphabet $\mathcal{S}$) to Bob and to agree upon a secret key K with Bob simultaneously. The secret message and the generated key are both required to be kept concealed from Eve.

Definition 1. A $(2^{nR_{\rm SM}}, 2^{nR_{\rm SK}}, n)$ code consists of a secret-message set $\mathcal{S} \triangleq [1, 2^{nR_{\rm SM}}]$, a secret-key set $\mathcal{K} \triangleq [1, 2^{nR_{\rm SK}}]$, an encoding and key generation function $f : \mathcal{S} \times \mathcal{X}_s^n \to \mathcal{K} \times \mathcal{X}_c^n$, and a decoding and key generation function $g : \mathcal{Y}_c^n \times \mathcal{Y}_s^n \to \mathcal{S} \times \mathcal{K}$.

The performance of a $(2^{nR_{\rm SM}}, 2^{nR_{\rm SK}}, n)$ code is evaluated in terms of: (1) the error probability at Bob, i.e, $\boldsymbol{P}_e(S, K) \triangleq \Pr[(S, K) \neq (\hat{S}, \hat{K})]$; (2) the information leakage to Eve, i.e., $\boldsymbol{L}(S, K) \triangleq I(SK; Z_s^{1:n} Z_c^{1:n})$; and (3) the uniformity of the generated key, i.e., $\boldsymbol{U}(K) \triangleq nR_{\rm SK} - H(K)$.

Definition 2. A rate pair $(R_{\rm SM}, R_{\rm SK})$ is said to be achievable if there exists a sequence of $(2^{nR_{\rm SM}}, 2^{nR_{\rm SK}}, n)$ codes such that

$$\lim_{n\to\infty} \boldsymbol{P}_e(S, K) = 0 \text{ (reliability)}, \tag{1}$$

$$\lim_{n\to\infty} \boldsymbol{L}(S, K) = 0 \text{ (strong secrecy)}, \tag{2}$$

$$\lim_{n\to\infty} \boldsymbol{U}(K) = 0 \text{ (key uniformity)}. \tag{3}$$

As opposed to strong secrecy in Definition 2, weak secrecy in the literature only requires $\lim_{n\to\infty} \frac{1}{n} \boldsymbol{L}(S, K) = 0$. An achievable tradeoff region was established in [11] for general sources and channels satisfying weak secrecy. For convenience, we define

$$\begin{aligned} R_m &\triangleq I(U; X_s) - I(U; Y_s), \\ R_k &\triangleq I(U; Y_s) - I(U; Z_s), \\ R_c &\triangleq I(V_1; Y_c|V_2) - I(V_1; Z_c|V_2). \end{aligned} \tag{4}$$

Proposition 1 ([11])**.** An achievable tradeoff region for the joint source-channel model is given by

$$\mathcal{R}_{\text{joint}} = \bigcup_{p\in\mathcal{P}_{\text{joint}}} \left\{ (R_{\text{SM}}, R_{\text{SK}}) \middle| \begin{array}{l} R_{\text{SM}} \leqslant I(V_1;Y_c) - R_m \\ R_{\text{SM}} + R_{\text{SK}} \leqslant [R_c]^+ + [R_k]^+ \end{array} \right\}, \tag{5}$$

where $[a]^+ \triangleq \max[0, a]$ and

$$I(V_1;Y_c) \geqslant R_m. \tag{6}$$

The union is taken over $\mathcal{P}_{\text{joint}}$, the set of all probability distributions given by

$$\mathcal{P}_{\text{joint}} = \big\{p(u, x_s, y_s, z_s, v_2, v_1, x_c, y_c, z_c) = p(u)p(x_s|u)p(y_s, z_s|x_s)p(v_2)p(v_1|v_2)p(x_c|v_1)p(y_c, z_c|x_c)\big\}.$$

Remark 1. The tradeoff region (5) was derived under the weak secrecy criterion. While it can be improved to strong secrecy with privacy amplification techniques [36], we develop the polar coding scheme in this paper satisfying strong secrecy directly.

Remark 2. In this paper, we consider the case of matched bandwidth, i.e, the length of source sequences is equal to that of channel codewords, which are both assumed to be n. There is no fundamental difficulty in extending our scheme to the case of mismatched bandwidth [11].

3 Polar coding scheme for the joint source-channel model

In this section, we develop the polar coding scheme that achieves the tradeoff region (5) for general sources and channels under the strong secrecy criterion. First, we assume that $R_k > 0$ and $R_c > 0$ such that the correlated sources and the wiretap channel are simultaneously explored in our scheme. Next, notice that a secret message automatically satisfies the constraints of a secret key, thus it suffices to achieve the rate pair $(R_{\text{SM}}, R_{\text{SK}})$, where

$$\begin{aligned} &R_{\text{SM}} = \min[I(V_1;Y_c) - R_m, R_c + R_k], \\ &R_{\text{SK}} = [R_c + R_k - (I(V_1;Y_c) - R_m)]^+ = [R_m + R_k - (I(V_2;Y_c) + I(V_1;Z_c|V_2))]^+, \end{aligned} \tag{7}$$

where the last equality holds by the Markov chain $V_2 \to V_1 \to Y_c$. Thus, we should consider the following two cases:

- Case 1: $R_m + R_k \geqslant I(V_2;Y_c) + I(V_1;Z_c|V_2)$

$$R_{\text{SM}} = I(V_1;Y_c) - R_m, \quad R_{\text{SK}} = R_m + R_k - (I(V_2;Y_c) + I(V_1;Z_c|V_2)). \tag{8}$$

- Case 2: $R_m + R_k < I(V_2;Y_c) + I(V_1;Z_c|V_2)$

$$R_{\text{SM}} = R_c + R_k, \quad R_{\text{SK}} = 0. \tag{9}$$

We present the polarization results w.r.t. the correlated sources and the wiretap channel, respectively, in Subsection 3.1. Then we mainly describe the polar coding scheme for achieving the rate pair (8) in Subsection 3.2. Finally, we briefly discuss the scheme for achieving the rate pair (9) at the end of this section. The analysis of our scheme is later given in Section 4.

3.1 Preliminary results

3.1.1 *Polarization w.r.t. the correlated sources*

Let $U^{1:n}$ be a vector of n i.i.d. components drawn from the marginal distribution p_U. The polar transform of $U^{1:n}$ is defined as $A^{1:n} = U^{1:n}G_n$. For $\delta_n \triangleq 2^{-n^\beta}$, $\beta \in (0, 0.5)$, we consider the following polarization

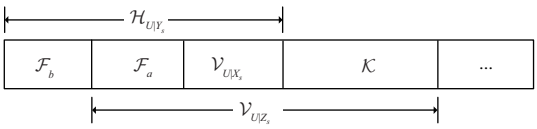

Figure 2 Partition of the index set $[n]$ for $A^{1:n}$.

sets:

$$\begin{aligned}
&\mathcal{H}_U \triangleq \{i \in [n] : H(A^i|A^{1:i-1}) \geqslant \delta_n\},\\
&\mathcal{V}_{U|X_s} \triangleq \{i \in [n] : H(A^i|A^{1:i-1}, X_s^{1:n}) \geqslant 1-\delta_n\},\\
&\mathcal{H}_{U|Y_s} \triangleq \{i \in [n] : H(A^i|A^{1:i-1}, Y_s^{1:n}) \geqslant \delta_n\},\\
&\mathcal{V}_{U|Z_s} \triangleq \{i \in [n] : H(A^i|A^{1:i-1}, Z_s^{1:n}) \geqslant 1-\delta_n\}.
\end{aligned} \tag{10}$$

Roughly, (i) $A^{1:n}[\mathcal{H}_{U|Y_s}]$ stores the necessary information for Bob to reconstruct $A^{1:n}$ with the successive cancellation (SC) decoder [39], and (ii) the secret key should be chosen from $A^{1:n}[\mathcal{V}_{U|Z_s}]$ since it is almost uniformly distributed and independent of Eve's observations [38]. In addition, the sets $\mathcal{H}_U$ and $\mathcal{V}_{U|X_s}$ are considered on account of a stochastic encoder in the scheme [38]. It follows from the Markov chain $U \to X_s \to (Y_s, Z_s)$ that $\mathcal{V}_{U|X_s} \subseteq (\mathcal{H}_{U|Y_s} \cap \mathcal{V}_{U|Z_s})$. To handle non-degraded sources, we further define

$$\begin{aligned}
&\mathcal{K} \triangleq (\mathcal{H}_{U|Y_s})^c \cap \mathcal{V}_{U|Z_s},\\
&\mathcal{F}_a \triangleq (\mathcal{H}_{U|Y_s} \cap \mathcal{V}_{U|Z_s}) \backslash \mathcal{V}_{U|X_s},\\
&\mathcal{F}_b \triangleq \mathcal{H}_{U|Y_s} \cap (\mathcal{V}_{U|Z_s})^c,
\end{aligned} \tag{11}$$

which is graphically shown in Figure 2. Based on (11), we have $\mathcal{H}_{U|Y_s} = \mathcal{F}_a \cup \mathcal{F}_b \cup \mathcal{V}_{U|X_s}$ and $\mathcal{V}_{U|Z_s} = \mathcal{F}_a \cup \mathcal{K} \cup \mathcal{V}_{U|X_s}$. Given $A^{1:n}[\mathcal{V}_{U|X_s}]$, (i) Bob requires $A^{1:n}[\mathcal{F}_a]$ and $A^{1:n}[\mathcal{F}_b]$ to extract $A^{1:n}[\mathcal{H}_{U|Y_s}]$ and then reconstructs $A^{1:n}$; (ii) the secret key should be chosen from $A^{1:n}[\mathcal{K}]$. Note that $\mathcal{F}_b \not\subset \mathcal{V}_{U|Z_s}$, the direct transmission of $A^{1:n}[\mathcal{F}_b]$ leaks information about the generated key. Therefore, additional protection is required for $A^{1:n}[\mathcal{F}_b]$. The chaining method [40] can be adopted to handle this task. Let $\mathcal{F}_b'$ be an arbitrary subset of $\mathcal{K}$ with size $|\mathcal{F}_b|$. Note that, the existence of such a subset is ensured by

$$\lim_{n\to\infty} \frac{|\mathcal{K}\backslash\mathcal{F}_b'|}{n} \overset{\text{(a)}}{=} \lim_{n\to\infty} \frac{|\mathcal{K}| - |\mathcal{F}_b|}{n} \overset{\text{(b)}}{=} \lim_{n\to\infty} \frac{|\mathcal{V}_{U|Z_s}| - |\mathcal{H}_{U|Y_s}|}{n} \overset{\text{(c)}}{=} H(U|Z_s) - H(U|Y_s) \overset{\text{(d)}}{=} R_k, \tag{12}$$

where (a) holds by the definition of $\mathcal{F}_b'$, (b) holds by (11), (c) holds by [32, Lemmas 6 and 7], (d) holds by (4). Similarly, we also have

$$\lim_{n\to\infty} \frac{|\mathcal{F}_a| + |\mathcal{F}_b|}{n} = \lim_{n\to\infty} \frac{|\mathcal{H}_{U|Y_s}| - |\mathcal{V}_{U|X_s}|}{n} = H(U|Y_s) - H(U|X_s) = R_m. \tag{13}$$

3.1.2 *Polarization w.r.t. the wiretap channel*

We consider the structure of superposition coding, in which the transmitted message is split into two parts carried by $V_2^{1:n}$ and $V_1^{1:n}$, respectively. First, the polar transform of $V_2^{1:n}$ is defined as $B_2^{1:n} = V_2^{1:n} G_n$. For $\delta_n \triangleq 2^{-n^\beta}$, $\beta \in (0, 0.5)$, we define the following polarized sets:

$$\begin{aligned}
&\mathcal{V}_{V_2} \triangleq \{i \in [n] : H(B_2^i|B_2^{1:i-1}) \geqslant 1-\delta_n\},\\
&\mathcal{H}_{V_2|Y_c} \triangleq \{i \in [n] : H(B_2^i|B_2^{1:i-1}, Y_c^{1:n}) \geqslant \delta_n\}.
\end{aligned} \tag{14}$$

We partition the index set $[n]$ as in point-to-point channels [41]:

$$\begin{aligned}
&\mathcal{I}_2 = \mathcal{V}_{V_2} \cap (\mathcal{H}_{V_2|Y_c})^c,\\
&\mathcal{R}_2 = \mathcal{V}_{V_2} \cap \mathcal{H}_{V_2|Y_c},\\
&\mathcal{D}_2 = (\mathcal{V}_{V_2})^c,
\end{aligned} \tag{15}$$

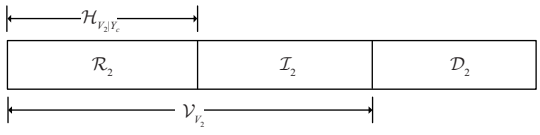

Figure 3 Partition of the index set $[n]$ for $B_2^{1:n}$.

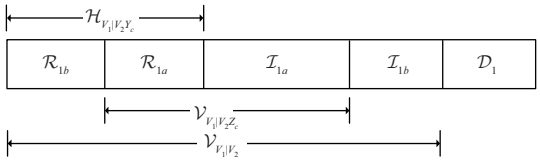

Figure 4 Partition of the index set $[n]$ for $B_1^{1:n}$.

which is graphically shown in Figure 3. It is known that, (i) $B_2^{1:n}[\mathcal{I}_2]$ is suitable to carry information; (ii) $B_2^{1:n}[\mathcal{R}_2]$ stores uniformly distributed random bits which are pre-shared by the encoder and the decoder; and (iii) $B_2^{1:n}[\mathcal{R}_2]$ stores those almost deterministic bits. It is easy to see that

$$\lim_{n\to\infty}\frac{|\mathcal{I}_2|}{n}=\lim_{n\to\infty}\frac{|\mathcal{V}_{V_2}|-|\mathcal{H}_{V_2|Y_c}|}{n}=H(V_2)-H(V_2|Y_c)=I(V_2;Y_c). \tag{16}$$

Next, the polar transform of $V_1^{1:n}$ is defined as $B_1^{1:n}=V_1^{1:n}G_n$, where we view $V_2^{1:n}$ as side information on $V_1^{1:n}$. For $\delta_n\triangleq 2^{-n^\beta}$, $\beta\in(0,0.5)$, we define the following polarized sets:

$$\begin{aligned}
&\mathcal{V}_{V_1|V_2}\triangleq\{i\in[n]:H(B_1^i|B_1^{1:i-1},V_2^{1:n})\geqslant 1-\delta_n\},\\
&\mathcal{H}_{V_1|V_2Y_c}\triangleq\{i\in[n]:H(B_1^i|B_1^{1:i-1},V_2^{1:n},Y_c^{1:n})\geqslant \delta_n\},\\
&\mathcal{V}_{V_1|V_2Z_c}\triangleq\{i\in[n]:H(B_1^i|B_1^{1:i-1},V_2^{1:n},Z_c^{1:n})\geqslant 1-\delta_n\}.
\end{aligned} \tag{17}$$

Roughly, (i) $B_1^{1:n}[\mathcal{H}_{V_1|V_2Y_c}]$ stores the necessary information for Bob to decode $B^{1:n}$ with the SC decoder [39], and (ii) $B_1^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]$ is suitable to carry the secret information since it is almost uniformly distributed and independent of Eve's channel outputs. To handle non-degraded channels, we consider the partition of the index set $[n]$ as follows:

$$\begin{aligned}
&\mathcal{I}_{1a}=\mathcal{V}_{V_1|V_2}\cap(\mathcal{H}_{V_1|V_2Y_c})^c\cap\mathcal{V}_{V_1|V_2Z_c},\\
&\mathcal{I}_{1b}=\mathcal{V}_{V_1|V_2}\cap(\mathcal{H}_{V_1|V_2Y_c})^c\cap(\mathcal{V}_{V_1|V_2Z_c})^c,\\
&\mathcal{R}_{1a}=\mathcal{V}_{V_1|V_2}\cap\mathcal{H}_{V_1|V_2Y_c}\cap\mathcal{V}_{V_1|V_2Z_c},\\
&\mathcal{R}_{1b}=\mathcal{V}_{V_1|V_2}\cap\mathcal{H}_{V_1|V_2Y_c}\cap(\mathcal{V}_{V_1|V_2Z_c})^c,\\
&\mathcal{D}_1=(\mathcal{V}_{V_1|V_2})^c,
\end{aligned} \tag{18}$$

which is graphically shown in Figure 4. Note that, Eq. (18) is a typical partition for general wiretap channels, see [30], for instance. It is known that, (i) $B_1^{1:n}[\mathcal{I}_{1a}]$ is suitable to carry secret information; (ii) $B_1^{1:n}[\mathcal{I}_{1b}]$ stores the confusion message or the private message which does not have to satisfy the security constraint; (iii) $B_1^{1:n}[\mathcal{R}_{1a}]$ stores uniformly distributed random bits which are pre-shared by the encoder and the decoder; (iv) $B_1^{1:n}[\mathcal{R}_{1b}]$ can be properly handled by the chaining method [40]; and (v) $B_1^{1:n}[\mathcal{D}_1]$ stores those almost deterministic bits. Let $\mathcal{R}'_{1b}$ be an arbitrary subset of $\mathcal{I}_{1a}$ with size $|\mathcal{R}_{1b}|$. Similar to (12), the existence of such a subset is ensured by

$$\begin{aligned}
\lim_{n\to\infty}\frac{|\mathcal{I}_{1a}\backslash\mathcal{R}'_{1b}|}{n}&=\lim_{n\to\infty}\frac{|\mathcal{I}_{1a}|-|\mathcal{R}_{1b}|}{n}=\lim_{n\to\infty}\frac{|\mathcal{V}_{V_1|V_2Z_c}|-|\mathcal{H}_{V_1|V_2Y_c}|}{n}\\
&=H(V_1|V_2Z_c)-H(V_1|V_2Y_c)=R_c.
\end{aligned} \tag{19}$$

In addition, we also have

$$\begin{aligned}
\lim_{n\to\infty}\frac{|\mathcal{I}_{1b}|+|\mathcal{R}'_{1b}|}{n}&=\lim_{n\to\infty}\frac{|\mathcal{I}_{1b}|+|\mathcal{R}_{1b}|}{n}=\lim_{n\to\infty}\frac{|\mathcal{V}_{V_1|V_2}|-|\mathcal{V}_{V_1|V_2Z_c}|}{n}\\
&=H(V_1|V_2)-H(V_1|V_2Z_c)=I(V_1;Z_c|V_2).
\end{aligned} \tag{20}$$

3.2 Polar coding scheme

The polar coding scheme for achieving the rate pair (8) is detailed as follows. Recall that $R_m+R_k\geqslant I(V_2;Y_c)+I(V_1;Z_c|V_2)$ in this case.

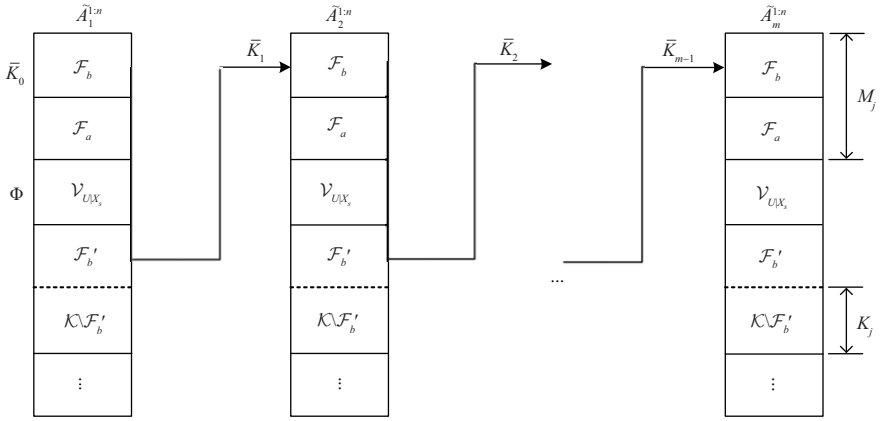

Figure 5 Sketch of the encoding scheme for achieving the rate pair (8). Step 1: source part.

3.2.1 *Encoding scheme*

The encoding scheme operates over m blocks of size n. In each block $j \in [1, m]$, the encoding scheme mainly consists of two steps that handle the correlated sources and the wiretap channel successively. A graphic summary of the encoding scheme is given by Figures 5 and 6.

Step 1 (source part)**.** Alice quantizes its source sequence $X_{sj}^{1:n}$ and extracts a public message that contains the side information necessary for Bob to reconstruct the quantized sequence, and a secret key that will be used later as a one-time pad to encrypt the secret message. The work of Chou et al. [38, Model 2] can be adopted to fulfill the task.

Let Φ be a sequence of $|\mathcal{V}_{U|X_s}|$ uniformly distributed random bits known to all terminals including Eve. Alice forms a vector quantized version $\tilde{A}_j^{1:n}$ of $X_{sj}^{1:n}$ as follows:

- $\tilde{A}_j^{1:n}[\mathcal{V}_{U|X_s}]$ store Φ;
- $\tilde{A}_j^{1:n}[(\mathcal{V}_{U|X_s})^c]$ are drawn from the conditional probability

$$p_{\tilde{A}_j^i|\tilde{A}_j^{1:i-1}X_{sj}^{1:n}}(a_j^i|\tilde{A}_j^{1:i-1}X_{sj}^{1:n}) = \begin{cases} p_{A^i|A^{1:i-1}X_s^{1:n}}(a_j^i|\tilde{A}_j^{1:i-1}X_{sj}^{1:n}), & \text{if } i \in \mathcal{H}_U\backslash\mathcal{V}_{U|X_s}, \\ p_{A^i|A^{1:i-1}}(a_j^i|\tilde{A}_j^{1:i-1}), & \text{if } i \in \mathcal{H}_U^c. \end{cases} \tag{21}$$

Define $K_j \triangleq \tilde{A}_j^{1:n}[\mathcal{K}\backslash\mathcal{F}_b']$, $\bar{K}_j \triangleq \tilde{A}_j^{1:n}[\mathcal{F}_b']$, $F_j \triangleq \tilde{A}_j^{1:n}[\mathcal{F}_a]$, and $\bar{F}_j \triangleq \tilde{A}_j^{1:n}[\mathcal{F}_b]$. Let $\bar{K}_0$ be a secret seed of size $|\mathcal{F}_b|$ privately shared by Alice and Bob. The public message M_j is defined as

$$M_j \triangleq (F_j, \bar{F}_j \oplus \bar{K}_{j-1}), \tag{22}$$

where $\bar{K}_{j-1}$ is a secret seed of block $j-1$ and used as a one-time pad to protect $\bar{F}_j$. We further split the public message M_j and the secret key K_j into

$$M_j \triangleq (M_j^{1a}, M_j^{1b}, M_j^2), \quad K_j \triangleq (K_j^{1a}, K_j^{1b}, K_j^2), \tag{23}$$

which satisfy $|M_j^2| + |K_j^2| = |\mathcal{I}_2|$ and $|M_j^{1b}| + |K_j^{1b}| = |\mathcal{I}_{1b} \cup \mathcal{R}_{1b}'|$. The justification for this operation is given in Remark 3.

Step 2 (channel part)**.** Alice encodes the public message M_j and the secret message into the channel codeword, in which the secret key is used as a one-time pad to encrypt part of the secret message. Let S_j be a sequence of uniformly distributed bits representing the secret message. We further split S_j into

$$S_j \triangleq (S_j^{1a}, S_j^{1b}, S_j^2), \tag{24}$$

which satisfy $|S_j^2| = |K_j^2|$, $|S_j^{1b}| = |K_j^{1b}|$ and $|S_j^{1a}| = |\mathcal{I}_{1a}\backslash\mathcal{R}_{1b}'| - |M_j^{1a}|$. For convenience, define $\bar{S}_j^{1b} \triangleq S_j^{1b} \oplus K_j^{1b}$ and $\bar{S}_j^2 \triangleq S_j^2 \oplus K_j^2$.

Let Ψ_2 be a sequence of $|\mathcal{R}_2|$ uniformly distributed random bits known to all terminals including Eve. Alice forms $\tilde{B}_{2j}^{1:n}$ as follows:

- $\tilde{B}_{2j}^{1:n}[\mathcal{I}_2]$ stores $(\bar{S}_j^2, M_j^2)$;

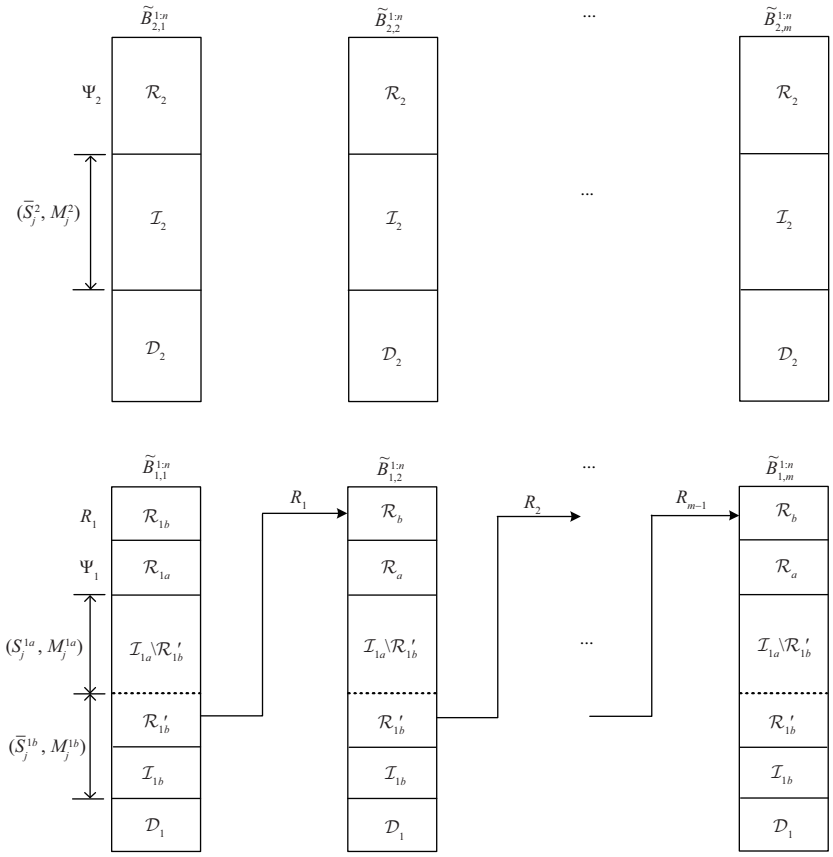

Figure 6 Sketch of the encoding scheme for achieving the rate pair (8). Step 2: channel part.

- $\tilde{B}^{1:n}_{2j}[\mathcal{R}_2]$ stores Ψ_2;
- $\tilde{B}^{1:n}_{2j}[\mathcal{D}_2]$ is drawn from the condition probability

$$p_{\tilde{B}^i_{2j}|\tilde{B}^{1:i-1}_{2j}}(b^i_{2j}|\tilde{B}^{1:i-1}_{2j}) = p_{B^i_2|B^{1:i-1}_2}(b^i_{2j}|\tilde{B}^{1:i-1}_{2j}). \tag{25}$$

In particular, Alice sends $\tilde{B}^{1:n}_{2j}[\mathcal{H}_{V_2|Y_c}\backslash\mathcal{V}_{V_2}]$ separately to Bob, which only incurs a negligible rate cost since $|\mathcal{H}_{V_2|Y_c}\backslash\mathcal{V}_{V_2}| = o(n)$. Then Alice computes $\tilde{V}^{1:n}_{2j} = \tilde{B}^{1:n}_{2j}G_n$.

Let Ψ_1 be a sequence of $|\mathcal{R}_{1a}|$ uniformly distributed random bits known to all terminals including Eve. Let R_0 and $\tilde{K}_j$ be two secret seeds of size $|\mathcal{R}_{1b}|$ and $|\mathcal{H}_{V_1|V_2Y_c}\backslash\mathcal{V}_{V_1|V_2}|$, respectively, privately shared by Alice and Bob. Alice forms $\tilde{B}^{1:n}_{1j}$ as follows:

- $\tilde{B}^{1:n}_{1j}[\mathcal{I}_{1a}\backslash\mathcal{R}'_{1b}]$ stores (S^{1a}_j, M^{1a}_j);
- $\tilde{B}^{1:n}_{1j}[\mathcal{I}_{1b}\cup\mathcal{R}'_{1b}]$ stores $(\bar{S}^{1b}_j, M^{1b}_j)$;
- $\tilde{B}^{1:n}_{1j}[\mathcal{R}_{1a}]$ stores Ψ_1;
- $\tilde{B}^{1:n}_{1j}[\mathcal{R}_{1b}]$ is equal to $R_{j-1} \triangleq \tilde{B}^{1:n}_{1,j-1}[\mathcal{R}'_{1b}]$, for $j \in [2,m]$. In block 1, $\tilde{B}^{1:n}_{1,1}[\mathcal{R}_{1b}]$ stores R_0;
- $\tilde{B}^{1:n}_{1j}[\mathcal{D}_1]$ is drawn from the condition probability

$$p_{\tilde{B}^i_{1j}|\tilde{B}^{1:i-1}_{1j}\tilde{V}^{1:n}_{2j}}(b^i_{1j}|\tilde{B}^{1:i-1}_{1j}\tilde{V}^{1:n}_{2j}) = p_{B^i_1|B^{1:i-1}_1V^{1:n}_2}(b^i_{1j}|\tilde{B}^{1:i-1}_{1j}V^{1:n}_2). \tag{26}$$

In particular, Alice sends $\tilde{B}^{1:n}_{1j}[\mathcal{H}_{V_1|V_2Y_c}\backslash\mathcal{V}_{V_1|V_2}] \oplus \tilde{K}_j$ separately to Bob, which only incurs a negligible rate cost since $|\mathcal{H}_{V_1|V_2Y_c}\backslash\mathcal{V}_{V_1|V_2}| = o(n)$. Then Alice computes $\tilde{V}^{1:n}_{1j} = \tilde{B}^{1:n}_{1j}G_n$. Finally, the codeword $\tilde{X}^{1:n}_{cj}$ is determined according to the conditional probability $p_{X^{1:n}_c|V^{1:n}_1}(\tilde{X}^{1:n}_{cj}|\tilde{V}^{1:n}_{1j})$. The corresponding channel outputs are denoted by $\tilde{Y}^{1:n}_{cj}$ and $\tilde{Z}^{1:n}_{cj}$.

In each block $j \in [1,m]$, (K^{1a}_j, M^{1a}_j) is the final secret-key shared by Alice and Bob. Intuitively, K^{1a}_j is the unused part of K_j, while M^{1a}_j is stored into $\tilde{B}^{1:n}_{1j}[\mathcal{I}_{1a}\backslash\mathcal{R}'_{1b}]$ which is almost independent of Eve's

observations. Since $M_1 \triangleq (F_1, \bar{F}_1 \oplus \bar{K}_0)$, as a subvector of M_1, M_1^{1a} contains a part of the secret seed $\bar{K}_0$. But this has negligible impact on the overall key rate for a sufficient number of blocks.

Remark 3. From (12), (13) and the definition of K_j and M_j, we know that $\frac{1}{n}|K_j| \to R_k$ and $\frac{1}{n}|M_j| \to R_m$ as $n \to \infty$. Moreover, we have (16) and (20) that $\frac{1}{n}|\mathcal{I}_2| \to I(V_2; Y_c)$ and $\frac{1}{n}|\mathcal{I}_{1b} \cup \mathcal{R}'_{1b}| \to I(V_1; Z_c|V_2)$ as $n \to \infty$. Thus, it is possible to split M_j and K_j as in (23), since we have assumed that $R_m + R_k \geqslant I(V_2; Y_c) + I(V_1; Z_c|V_2)$ for case 1.

Remark 4. The randomization sequences $\{\Phi, \Psi_2, \Psi_1\}$ are reused over m blocks to make the induced rate cost vanish. Along with the chaining vectors $\{\bar{K}_j, R_j\}$ for $j \in [1, m-1]$, the reused sequences causes additional dependencies between random variables from adjacent blocks. In Section 4, we show that the reuse does not harm strong secrecy.

Remark 5. The secret seeds $\{\bar{K}_0, R_0, \tilde{K}_{1:m}\}$ are required by the scheme. $\{\bar{K}_0, R_0\}$ are used to protect the insecure parts of block 1, which completes the chaining process. $\tilde{K}_j$ is used to protect a small portion of those almost deterministic bits $\tilde{B}_{1j}^{1:n}[\mathcal{H}_{V_1|V_2Y_c} \backslash \mathcal{V}_{V_1|V_2}]$, which is needed by Bob. It was noted in [32,38] that these secret seeds are necessary for ensuing reliability and strong secrecy simultaneously. The rate of the secret seeds is negligible for sufficiently large m and n.

3.2.2 *Decoding scheme*

Bob decodes the m blocks in a natural order, i.e., from block 1 to block m. In each block $j \in [1, m]$, Bob decodes $\tilde{B}_{2j}^{1:n}$, $\tilde{B}_{1j}^{1:n}$, and $\tilde{A}_j^{1:n}$ in order.

• Given Ψ_2 and $\tilde{B}_{2j}^{1:n}[\mathcal{H}_{V_2|Y_c} \backslash \mathcal{V}_{V_2}]$, Bob knows $\tilde{B}_{2j}^{1:n}[\mathcal{H}_{V_2|Y_c}]$ by construction. Then Bob runs the SC decoder [39] to form $\hat{B}_{2j}^{1:n}$ using $\tilde{B}_{2j}^{1:n}[\mathcal{H}_{V_2|Y_c}]$ and $\tilde{Y}_{cj}^{1:n}$. Define $\hat{V}_{2j}^{1:n} = \hat{B}_{2j}^{1:n} G_n$.

• Given Ψ_1, $\hat{R}_{j-1}$, and $\tilde{B}_{1j}^{1:n}[\mathcal{H}_{V_1|V_2Y_c} \backslash \mathcal{V}_{V_2}]$, Bob knows $\tilde{B}_{1j}^{1:n}[\mathcal{H}_{V_1|V_2Y_c}]$ by construction. Note that, $\hat{R}_0 = R_0$. Then Bob runs the SC decoder [39] to estimate $\tilde{B}_{1j}^{1:n}$ using $\tilde{B}_{1j}^{1:n}[\mathcal{H}_{V_1|V_2Y_c}]$, $\hat{V}_{2j}^{1:n}$, and $\tilde{Y}_{cj}^{1:n}$. Then Bob can extract $\hat{M}_j$ from $\hat{B}_{2j}^{1:n}$ and $\hat{B}_{1j}^{1:n}$.

• Given Φ, $\hat{\bar{K}}_{j-1}$, and $\hat{M}_j$, Bob can extract $\hat{A}_j^{1:n}[\mathcal{H}_{U|Y_s}]$. Note that, $\hat{\bar{K}}_0 = \bar{K}_0$. Then Bob runs the SC decoder [39] to form $\hat{A}_j^{1:n}$ using $\tilde{A}_j^{1:n}[\mathcal{H}_{U|Y_s}]$ and $Y_{sj}^{1:n}$.

Remark 6. Finally, we show how to achieve the rate pair (9) in case 2. Recall that $R_m + R_k < I(V_2; Y_c) + I(V_1; Z_c|V_2)$ in this case. Similarly as in Remark 3, the condition of this case results in $|M_j| + |K_j| < |\mathcal{I}_2| + |\mathcal{I}_{1b} \cup \mathcal{R}'_{1b}|$ for sufficiently large n. Thus, K_j and M_j can be entirely contained in $\tilde{B}_{2j}^{1:n}[\mathcal{I}_2]$ and $\tilde{B}_{1j}^{1:n}[\mathcal{I}_{1b} \cup \mathcal{R}'_{1b}]$. Then we can set $|S_j^{1a}| = |\mathcal{I}_{1a} \backslash \mathcal{R}'_{1b}|$ and $M_j^{1a} = K_j^{1a} = \emptyset$ in the aforementioned scheme. Note that, the remaining bits of $\tilde{B}_{2j}^{1:n}[\mathcal{I}_2]$ and $\tilde{B}_{1j}^{1:n}[\mathcal{I}_{1b} \cup \mathcal{R}'_{1b}]$ are chosen uniformly at random.

4 Analysis of the polar coding scheme

In this section, we mainly present the detailed analysis of the scheme for achieving the rate pair (8) in case 1. Only in Subsection 4.1, we analyze the achievable rate pair for case 2. The remaining analysis for case 2 can be similarly obtained and thus omitted for brevity.

4.1 Achievable rate pair

In case 1, Alice shares the secret message S_j and the secret key (K_j^{1a}, M_j^{1a}) with Bob in each block $j \in [1, m]$. The secret-message rate is

$$\begin{aligned} R_{\mathrm{SM}} &= \lim_{n\to\infty} \frac{|S_j^{1a}| + |S_j^{1b}| + |S_j^2|}{n} \overset{\text{(a)}}{=} \lim_{n\to\infty} \frac{|S_j^{1a}| + |K_j^{1b}| + |K_j^2|}{n} \\ &\overset{\text{(b)}}{=} \lim_{n\to\infty} \frac{|\mathcal{I}_{1a} \cup \mathcal{I}_{1b}| + |\mathcal{I}_2| - |M_j|}{n} \overset{\text{(c)}}{=} I(V_1; Y_c|V_2) + I(V_2; Y_c) - R_m \\ &\overset{\text{(d)}}{=} I(V_1; Y_c) - R_m, \end{aligned} \tag{27}$$

where (a) and (b) hold by the encoding scheme, (c) holds by (13), (19) and (20), (d) holds by the Markov chain $V_2 \to V_1 \to Y_c$. The secret-key rate is

$$\begin{aligned} R_{\mathrm{SK}} &= \lim_{n\to\infty} \frac{|K_j^{1a}| + |M_j^{1a}|}{n} \\ &\overset{\text{(a)}}{=} \lim_{n\to\infty} \frac{|K_j| + |M_j| - (|K_j^{1b}| + |M_j^{1b}|) - (|K_j^2| + |M_j^2|)}{n} \\ &\overset{\text{(b)}}{=} \lim_{n\to\infty} \frac{|K_j| + |M_j| - |\mathcal{I}_{1b} \cup \mathcal{R}'_{1b}| - |\mathcal{I}_2|}{n} \\ &\overset{\text{(c)}}{=} R_k + R_m - (I(V_1; Z_c|V_2) + I(V_2; Y_c)), \end{aligned} \tag{28}$$

where (a) and (b) hold by the encoding scheme, (c) holds by (12), (13), (16) and (20). Therefore, the rate pair (8) is achieved.

In case 2, Alice sends the secret message S_j to Bob in each block $j \in [1, m]$. The secret-message rate is

$$\begin{aligned} R_{\mathrm{SM}} &= \lim_{n\to\infty} \frac{|S_j^{1a}| + |S_j^{1b}| + |S_j^2|}{n} \overset{\text{(a)}}{=} \lim_{n\to\infty} \frac{|S_j^{1a}| + |K_j|}{n} \\ &= \lim_{n\to\infty} \frac{|\mathcal{I}_{1a} \backslash \mathcal{R}'_{1b}| + |\mathcal{K} \backslash \mathcal{F}'_b|}{n} \overset{\text{(b)}}{=} R_c + R_k, \end{aligned} \tag{29}$$

where (a) holds because K_j is entirely used to encrypt S_j^{1b} and S_j^2 in case 2, (b) holds by (12) and (19).

The rate of the randomization sequences $\{\Phi, \Psi_1, \Psi_2\}$ is

$$\begin{aligned} &\lim_{m,n\to\infty} \frac{|\Phi| + |\Psi_1| + |\Psi_2|}{mn} \\ &\overset{\text{(a)}}{=} \lim_{m,n\to\infty} \frac{|\mathcal{V}_{U|X_s}| + |\mathcal{R}_{1a}| + |\mathcal{R}_2|}{mn} \\ &\overset{\text{(b)}}{\leqslant} \lim_{m,n\to\infty} \frac{|\mathcal{V}_{U|X_s}| + |\mathcal{H}_{V_1|V_2Y_c}| + |\mathcal{H}_{V_2|Y_c}|}{mn} \\ &\overset{\text{(c)}}{=} \lim_{m\to\infty} \frac{H(U|Z_s) + H(V_1|V_2Y_c) + H(V_2|Y_c)}{m} = 0, \end{aligned} \tag{30}$$

where (a) holds by the encoding scheme, (b) holds by (15) and (18), (c) holds by [32, Lemma 6,7]. Similarly, the rate of the secret seeds $\{\bar{K}_0, R_0, \tilde{K}_{1:m}\}$ is

$$\begin{aligned} &\lim_{m,n\to\infty} \frac{|\bar{K}_0| + |R_0| + |\tilde{K}_{1:m}|}{mn} \\ &= \lim_{m,n\to\infty} \frac{|\mathcal{F}_b| + |\mathcal{R}_{1b}|}{mn} + \lim_{n\to\infty} \frac{|\mathcal{H}_{V_1|V_2Y_c} \backslash \mathcal{V}_{V_1|V_2}|}{n} \\ &\leqslant \lim_{m,n\to\infty} \frac{|\mathcal{H}_{U|Y_s}| + |\mathcal{H}_{V_1|V_2Y_c}|}{mn} + \lim_{n\to\infty} \frac{|\mathcal{H}_{V_1|V_2Y_c} \backslash \mathcal{V}_{V_1|V_2}|}{n} \\ &= \lim_{m\to\infty} \frac{H(U|Y_s) + H(V_1|V_2Y_c)}{m} = 0. \end{aligned} \tag{31}$$

4.2 Total variation distance

In the encoding scheme, Alice generates the sequence $\tilde{A}_j^{1:n}$ according to the distribution $p_{\tilde{A}_j^{1:n} X_{sj}^{1:n}}$. Take $Z_{sj}^{1:n}$ into consideration and denote the induced joint distribution by $p_{\tilde{A}_j^{1:n} X_{sj}^{1:n} Z_{sj}^{1:n}}$. We have Lemma 1 showing that $p_{\tilde{A}_j^{1:n} X_{sj}^{1:n} Z_{sj}^{1:n}}$ is a close approximation of the target joint distribution $p_{A^{1:n} X_s^{1:n} Z_s^{1:n}}$.

Lemma 1. For each block $j \in [1, m]$, we have

$$V(p_{\tilde{A}_j^{1:n} X_{sj}^{1:n} Z_{sj}^{1:n}}, p_{A^{1:n} X_s^{1:n} Z_s^{1:n}}) \leqslant \sqrt{2 \ln 2} \sqrt{n \delta_n}.$$

Proof. From [38, Lemma 6], we know that

$$V(p_{\tilde{A}_j^{1:n}X_{sj}^{1:n}}, p_{A^{1:n}X_s^{1:n}}) \leqslant \sqrt{2\ln 2}\sqrt{n\delta_n}. \tag{32}$$

Then we have

$$\begin{aligned}
&V(p_{\tilde{A}_j^{1:n}X_{sj}^{1:n}Z_{sj}^{1:n}}, p_{A^{1:n}X_s^{1:n}Z_s^{1:n}})\\
&= V(p_{\tilde{A}_j^{1:n}X_{sj}^{1:n}}p_{Z_{sj}^{1:n}|\tilde{A}_j^{1:n}X_{sj}^{1:n}}, p_{A^{1:n}X_s^{1:n}}p_{Z_s^{1:n}|A^{1:n}X_s^{1:n}})\\
&\overset{\text{(a)}}{=} V(p_{\tilde{A}_j^{1:n}X_{sj}^{1:n}}p_{Z_{sj}^{1:n}|X_{sj}^{1:n}}, p_{A^{1:n}X_s^{1:n}}p_{Z_s^{1:n}|X_s^{1:n}})\\
&\overset{\text{(b)}}{=} V(p_{\tilde{A}_j^{1:n}X_{sj}^{1:n}}, p_{A^{1:n}X_s^{1:n}}),
\end{aligned} \tag{33}$$

where (a) holds by the Markov chain $U \to X_s \to Z_s$, (b) holds by [42, Lemma 17].

From Lemma 1, we derive the following lemmas, which will be useful subsequently. Specifically, Lemma 3 indicates that the public message M_j is nearly uniform, which is crucial for the channel codes.

Lemma 2. Let $\mathcal{T}$ denote an arbitrary subset of $\mathcal{V}_{U|Z_s}$. For each block $j \in [1, m]$, we have

$$|\mathcal{T}| - H(\tilde{A}_j^{1:n}[\mathcal{T}]|Z_{sj}^{1:n}) \leqslant O(n\sqrt{n\delta_n}).$$

Proof. See Appendix A.

Lemma 3. Recall that $M_j \triangleq (F_j, \bar{F}_j \oplus \bar{K}_{j-1})$. For each block $j \in [1, m]$, we have

$$|M_j| - H(M_j) \leqslant O(n\sqrt{n\delta_n}).$$

Proof. See Appendix B.

Lemma 4. For each block $j \in [1, m]$, we have

$$I(K_j\bar{K}_j; M_j\Phi Z_{sj}^{1:n}) \leqslant O(n\sqrt{n\delta_n}), \quad I(M_j; K_j\bar{K}_j\Phi Z_{sj}^{1:n}) \leqslant O(n\sqrt{n\delta_n}).$$

Proof. See Appendix C.

Finally, we prove in the following lemma that the induced joint distribution $p_{\tilde{V}_{2j}^{1:n}\tilde{V}_{1j}^{1:n}\tilde{X}_{cj}^{1:n}\tilde{Y}_{cj}^{1:n}\tilde{Z}_{cj}^{1:n}}$ is close to the target joint distribution $p_{V_2^{1:n}V_1^{1:n}X_c^{1:n}Y_c^{1:n}Z_c^{1:n}}$ for sufficiently large n.

Lemma 5. For each block $j \in [1, m]$, we have

$$V(p_{\tilde{V}_{2j}^{1:n}\tilde{V}_{1j}^{1:n}\tilde{X}_{cj}^{1:n}\tilde{Y}_{cj}^{1:n}\tilde{Z}_{cj}^{1:n}}, p_{V_2^{1:n}V_1^{1:n}X_c^{1:n}Y_c^{1:n}Z_c^{1:n}}) \leqslant O\left(\sqrt{n\sqrt{n\delta_n}}\right).$$

Proof. See Appendix D.

4.3 Key uniformity

Denote the generated key by $T_j \triangleq (K_j^{1a}, M_j^{1a})$ for $j \in [1, m]$, which is a subvector of (K_j, M_j). First, we derive the following lemma, which shows key uniformity in a single block.

Lemma 6. In each block $j \in [1, m]$, (K_j, M_j) is nearly uniform because

$$|K_j| + |M_j| - H(K_jM_j) \leqslant O(n\sqrt{n\delta_n}).$$

Proof. Recall that, $M_j \triangleq (F_j, \bar{F}_j \oplus \bar{K}_{j-1})$. Define $M_j' \triangleq (K_jF_j, \bar{F}_j \oplus \bar{K}_{j-1})$. Following the proof of Lemma 3 with the substitution $F_j \leftarrow K_jF_j$, we have $|M_j'| - H(M_j') \leqslant O(n\sqrt{n\delta_n})$.

Next, we have

$$H(T_{1:m}) = \sum_{j=m}^{1} H(T_j|T_{j+1:m}) \overset{\text{(a)}}{\geqslant} \sum_{j=m}^{1} H(T_j|T_{j+1:m}\Phi\bar{K}_j)$$

$$\begin{aligned}
&\overset{\text{(b)}}{=} \sum_{j=m}^{1} H(T_j|\Phi\bar{K}_j) = \sum_{j=m}^{1} (H(T_j) - I(T_j;\Phi\bar{K}_j)) \\
&\overset{\text{(c)}}{\geqslant} \sum_{j=m}^{1} (|T_j| - O(n\sqrt{n\delta_n}) - I(T_j;\Phi\bar{K}_j)) \\
&\overset{\text{(d)}}{\geqslant} \sum_{j=m}^{1} (|T_j| - O(n\sqrt{n\delta_n})) = |T_{1:m}| - O(mn\sqrt{n\delta_n}),
\end{aligned} \tag{34}$$

where (a) holds because condition reduces entropy, (b) holds by the Markov chain $T_j \to \Phi\bar{K}_j \to T_{j+1:m}$, (c) holds by Lemma 6, (d) holds by Lemma 4, i.e., $I(T_j;\Phi\bar{K}_j) \leqslant I(K_jM_j;\Phi\bar{K}_j)$. Hence, the overall key $T_{1:m}$ is nearly uniform because

$$\boldsymbol{U}(T_{1:m}) = |T_{1:m}| - H(T_{1:m}) \leqslant O(mn\sqrt{n\delta_n}). \tag{35}$$

4.4 Reliability

First, we show that Bob can decode $\tilde{V}_{2j}^{1:n}$ with a small error probability. Define the error event:

$$\mathcal{E}_j \triangleq \{(\tilde{V}_{2j}^{1:n}\tilde{Y}_{cj}^{1:n}) \neq (V_2^{1:n}Y_c^{1:n})\}.$$

By optimal coupling [43, Lemma 3.6] and Lemma 5, we have $P(\mathcal{E}_j) = V(p_{\tilde{V}_{2j}^{1:n}\tilde{Y}_{cj}^{1:n}}, p_{V_2^{1:n}Y_c^{1:n}}) \leqslant O(\sqrt{n\sqrt{n\delta_n}})$. Denote $\delta_n^{(*)} \triangleq O(\sqrt{n\sqrt{n\delta_n}})$. Then we have

$$\begin{aligned}
P(\tilde{V}_{2j}^{1:n} \neq \hat{V}_{2j}^{1:n}) &= P(\tilde{V}_{2j}^{1:n} \neq \hat{V}_{2j}^{1:n}|\mathcal{E}_j)P(\mathcal{E}_j) + P(\tilde{V}_{2j}^{1:n} \neq \hat{V}_{2j}^{1:n}|\mathcal{E}_j^c)P(\mathcal{E}_j^c) \\
&\leqslant P(\mathcal{E}_j) + P(\tilde{V}_{2j}^{1:n} \neq \hat{V}_{2j}^{1:n}|\mathcal{E}_j^c) \\
&\overset{\text{(a)}}{\leqslant} P(\mathcal{E}_j) + n\delta_n \\
&\overset{\text{(b)}}{\leqslant} \delta_n^{(*)} + n\delta_n,
\end{aligned} \tag{36}$$

where (a) holds by the error probability of SC decoder [39], (b) follows from optimal coupling and Lemma 5.

Next, we show that Bob can decode $\tilde{V}_{1j}^{1:n}$ with a small error probability. Define the error events:

$$\begin{aligned}
&\mathcal{E}_j^{(1)} \triangleq \{(\tilde{V}_{2j}^{1:n}\tilde{V}_{1j}^{1:n}\tilde{Y}_{cj}^{1:n}) \neq (V_2^{1:n}V_1^{1:n}Y_c^{1:n})\}, \\
&\mathcal{E}_j^{(2)} \triangleq \{\tilde{V}_{2j}^{1:n} \neq \hat{V}_{2j}^{1:n}\}, \\
&\mathcal{E}_j^{(3)} \triangleq \{R_{j-1} \neq \hat{R}_{j-1}\}, \\
&\mathcal{E}_j \triangleq \mathcal{E}_j^{(1)} \cup \mathcal{E}_j^{(2)} \cup \mathcal{E}_j^{(3)}.
\end{aligned}$$

Note that, $\mathcal{E}_0^{(3)} \triangleq \emptyset$. By optimal coupling [43, Lemma 3.6], we have $P(\mathcal{E}_j^{(1)}) = V(p_{\tilde{V}_{2j}^{1:n}\tilde{V}_{1j}^{1:n}\tilde{Y}_{cj}^{1:n}}, p_{V_2^{1:n}V_1^{1:n}Y_c^{1:n}})$. Then we have

$$\begin{aligned}
P(\tilde{V}_{1j}^{1:n} \neq \hat{V}_{1j}^{1:n}) &= P(\tilde{V}_{1j}^{1:n} \neq \hat{V}_{1j}^{1:n}|\mathcal{E}_j)P(\mathcal{E}_j) + P(\tilde{V}_{1j}^{1:n} \neq \hat{V}_{1j}^{1:n}|\mathcal{E}_j^c)P(\mathcal{E}_j^c) \\
&\leqslant P(\mathcal{E}_j) + P(\tilde{V}_{1j}^{1:n} \neq \hat{V}_{1j}^{1:n}|\mathcal{E}_j^c) \\
&\overset{\text{(a)}}{\leqslant} P(\mathcal{E}_j) + n\delta_n \\
&\leqslant P(\mathcal{E}_j^{(1)}) + P(\mathcal{E}_j^{(2)}) + P(\mathcal{E}_j^{(3)}) + n\delta_n \\
&\overset{\text{(b)}}{\leqslant} \delta_n^{(*)} + P(\mathcal{E}_j^{(2)}) + P(\mathcal{E}_j^{(3)}) + n\delta_n \\
&\overset{\text{(c)}}{\leqslant} 2(\delta_n^{(*)} + n\delta_n) + P(\mathcal{E}_j^{(3)})
\end{aligned}$$

$$\begin{aligned}
&\leqslant 2(\delta_n^{(*)}+n\delta_n)+P(\tilde{V}_{1,j-1}^{1:n}\neq\hat{V}_{1,j-1}^{1:n})\\
&\overset{\text{(d)}}{\leqslant} 2(j-1)(\delta_n^{(*)}+n\delta_n)+P(\tilde{V}_{1,1}^{1:n}\neq\hat{V}_{1,1}^{1:n})\\
&\overset{\text{(e)}}{\leqslant} 2j(\delta_n^{(*)}+n\delta_n),
\end{aligned}\tag{37}$$

where (a) holds by the error probability of SC decoder [39], (b) follows from optimal coupling and Lemma 5, (c) holds by (36), (d) holds by induction, (e) holds by similarly bounding the error probability of decoding block 1.

From $\tilde{V}_{2j}^{1:n}$ and $\tilde{V}_{1j}^{1:n}$, Bob can recover $\bar{S}_j^2$, $\bar{S}_j^{1b}$, S_j^{1a}, and M_j. Finally, we show that Bob can decode $\tilde{A}_j^{1:n}$ with small error probability. Thus, Bob can recover the secret-key K_j with which he can recover S_j^2 and S_j^{1b}. Define the error events:

$$\begin{aligned}
&\mathcal{E}_j^{(1)}\triangleq\{\tilde{A}_j^{1:n}\neq A^{1:n}\},\quad \mathcal{E}_j^{(2)}\triangleq\{M_j\neq\hat{M}_j\},\\
&\mathcal{E}_j^{(3)}\triangleq\{\bar{K}_{j-1}\neq\hat{\bar{K}}_{j-1}\},\quad \mathcal{E}_j\triangleq\mathcal{E}_j^{(1)}\cup\mathcal{E}_j^{(2)}\cup\mathcal{E}_j^{(3)}.
\end{aligned}$$

Note that, $\mathcal{E}_0^{(3)}\triangleq\emptyset$. By optimal coupling [43, Lemma 3.6], we have $\mathbb{P}(\mathcal{E}_j^{(1)})=\mathbb{V}(p_{\tilde{A}_j^{1:n}},p_{A^{1:n}})$. According to the encoding scheme, we have $P(\mathcal{E}_j^{(2)})\leqslant(2j+1)(\delta_n^{(*)}+n\delta_n)$ by (36) and (37). Similarly to (37), we have

$$\begin{aligned}
P(\tilde{A}_j^{1:n}\neq\hat{A}_j^{1:n}) &= P(\tilde{A}_j^{1:n}\neq\hat{A}_j^{1:n}|\mathcal{E}_j)P(\mathcal{E}_j)+P(\tilde{A}_j^{1:n}\neq\hat{A}_j^{1:n}|\mathcal{E}_j^c)P(\mathcal{E}_j^c)\\
&\leqslant P(\mathcal{E}_j)+P(\tilde{A}_j^{1:n}\neq\hat{A}_j^{1:n}|\mathcal{E}_j^c)\\
&\overset{\text{(a)}}{\leqslant} P(\mathcal{E}_j)+n\delta_n\\
&\leqslant P(\mathcal{E}_j^{(1)})+P(\mathcal{E}_j^{(2)})+P(\mathcal{E}_j^{(3)})+n\delta_n\\
&\overset{\text{(b)}}{\leqslant} \sqrt{2\ln 2}\sqrt{n\delta_n}+P(\mathcal{E}_j^{(2)})+P(\mathcal{E}_j^{(3)})+n\delta_n\\
&\overset{\text{(c)}}{\leqslant} \sqrt{2\ln 2}\sqrt{n\delta_n}+(2j+1)(\delta_n^{(*)}+n\delta_n)+P(\mathcal{E}_j^{(3)})+n\delta_n\\
&\leqslant \sqrt{2\ln 2}\sqrt{n\delta_n}+(2j+1)(\delta_n^{(*)}+n\delta_n)+P(\tilde{A}_{j-1}^{1:n}\neq\hat{A}_{j-1}^{1:n})+n\delta_n\\
&\overset{\text{(d)}}{\leqslant} (j-1)(\sqrt{2\ln 2}\sqrt{n\delta_n}+n\delta_n)+\sum_{k=2}^{j}(2k+1)(\delta_n^{(*)}+n\delta_n)+P(\tilde{A}_1^{1:n}\neq\hat{A}_1^{1:n})\\
&\overset{\text{(e)}}{\leqslant} j(\sqrt{2\ln 2}\sqrt{n\delta_n}+n\delta_n)+j(j+2)(\delta_n^{(*)}+n\delta_n),
\end{aligned}\tag{38}$$

where (a) holds by the error probability of SC decoder [39], (b) follows from optimal coupling and Lemma 1, (c) holds by (36) and (37), (d) holds by induction, (e) holds by similarly bounding the error probability of decoding block 1.

With (36)–(38) and the union bound, the overall error probability is bounded by

$$\begin{aligned}
\boldsymbol{P}_e(S_{1:m}K_{1:m}^{1a}M_{1:m}^{1a}) &\leqslant \sum_{j=1}^{m}P[(S_jK_j^{1a}M_j^{1a})\neq(\hat{S}_j\hat{K}_j^{1a}\hat{M}_j^{1a})]\\
&\leqslant \sum_{j=1}^{m}P[(S_jK_jM_j)\neq(\hat{S}_j\hat{K}_j\hat{M}_j)]\\
&\leqslant \sum_{j=1}^{m}[P(\tilde{V}_{2j}^{1:n}\neq\hat{V}_{2j}^{1:n})+P(\tilde{V}_{1j}^{1:n}\neq\hat{V}_{1j}^{1:n})+P(\tilde{A}_j^{1:n}\neq\hat{A}_j^{1:n})]\\
&\leqslant \sum_{j=1}^{m}[(2j+1)(\delta_n^{(*)}+n\delta_n)+j(\sqrt{2\ln 2}\sqrt{n\delta_n}+n\delta_n)+j(j+2)(\delta_n^{(*)}+n\delta_n)]
\end{aligned}$$

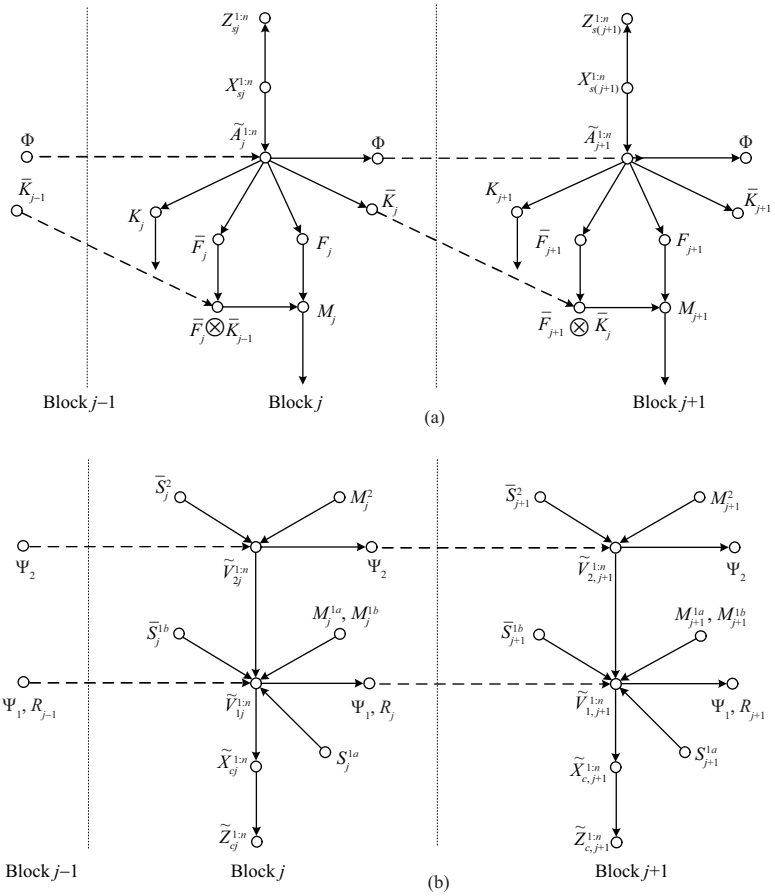

Figure 7 Functional dependence graph of the encoding scheme for achieving the rate pair (8). We split the graph into the source and channel parts for clarity. The dashed lines represent the dependencies between adjacent blocks. In each block $j \in [1, m]$, $K_j \triangleq (K_j^{1a}, K_j^{1b}, K_j^2)$ and $M_j \triangleq (M_j^{1a}, M_j^{1b}, M_j^2)$ are the random variables connecting the two parts. Also note that $\bar{S}_j^2 \triangleq S_j^2 \oplus K_j^2$ and $\bar{S}_j^{1b} \triangleq S_j^{1b} \oplus K_j^{1b}$. (a) Source part; (b) channel part.

$$= O\left(m^3\sqrt{n\sqrt{n\delta_n}}\right). \tag{39}$$

4.5 Strong secrecy

For brevity, let $\Psi \triangleq (\Psi_2, \Psi_1)$ and $\tilde{Z}_j^{1:n} \triangleq (Z_{sj}^{1:n}, \tilde{Z}_{cj}^{1:n})$ for $j \in [1, m]$. Note that, the randomization sequences $\{\Phi, \Psi_2, \Psi_1\}$ are known to all terminals including Eve. Hence, we need to bound $I(S_{1:m}T_{1:m}; \Phi\Psi\tilde{Z}_{1:m}^{1:n})$ to prove strong secrecy. A functional dependence graph of the encoding scheme is illustrated in Figure 7, which is adapted from [32] and [38]. First, we prove Lemma 7.

Lemma 7. For each block $j \in [1, m]$, we have

$$I(S_j^{1a}M_j^{1a}R_j; \Psi\tilde{Z}_{cj}^{1:n}) \leqslant O\left(n\sqrt{n\sqrt{n\delta_n}}\right).$$

Proof. First, it follows from Lemma 5 that

$$\begin{aligned} V(p_{\tilde{B}_{1j}^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]\tilde{V}_{2j}^{1:n}\tilde{Z}_{cj}^{1:n}}, p_{B_1^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]V_2^{1:n}Z_c^{1:n}}) &\leqslant V(p_{\tilde{B}_{1j}^{1:n}\tilde{V}_{2j}^{1:n}\tilde{Z}_{cj}^{1:n}}, p_{B_1^{1:n}V_2^{1:n}Z_c^{1:n}}) \\ &= V(p_{\tilde{V}_{1j}^{1:n}\tilde{V}_{2j}^{1:n}\tilde{Z}_{cj}^{1:n}}, p_{V_1^{1:n}V_2^{1:n}Z_c^{1:n}}) \leqslant O\left(\sqrt{n\sqrt{n\delta_n}}\right). \end{aligned} \tag{40}$$

Let $V(p_{\tilde{B}_{1j}^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]\tilde{V}_{2j}^{1:n}\tilde{Z}_{cj}^{1:n}}, p_{B_1^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]V_2^{1:n}Z_c^{1:n}}) \triangleq V_0$. Then, similar to (A1) in Appendix A, we have

$$|H(\tilde{B}_{1j}^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]|\tilde{V}_{2j}^{1:n}Z_{cj}^{1:n}) - H(B_1^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]|V_2^{1:n}Z_c^{1:n})|$$

$$\begin{aligned}
&\overset{(a)}{\leqslant} V_0 \log \frac{2^{2n}|\mathcal{Z}_c|^n}{V_0} \\
&\leqslant V_0(n(2+\log_2|\mathcal{Z}_c|) - \log V_0) \\
&\overset{(b)}{\leqslant} \delta_n^{(*)}(n(2+\log|\mathcal{Z}_c|) - \log_2 \delta_n^{(*)}) = O\left(n\sqrt{n\sqrt{n\delta_n}}\right),
\end{aligned} \tag{41}$$

where (a) holds by [44, Theorem 17.3.3] and $|\mathcal{Z}_c|$ denotes the alphabet size for a single observation of Eve, (b) holds by (40) and that $f(x) \triangleq x(a - \log_2 x)$ is increasing for x close enough to zero. Then we have

$$\begin{aligned}
&|\mathcal{V}_{V_1|V_2Z_c}| - H(\tilde{B}_{1j}^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]|\tilde{V}_{2j}^{1:n}\tilde{Z}_{cj}^{1:n}) \\
&\leqslant |\mathcal{V}_{V_1|V_2Z_c}| - H(B_1^{1:n}[\mathcal{T}]|V_2^{1:n}Z_c^{1:n}) + O\left(n\sqrt{n\sqrt{n\delta_n}}\right) \\
&\leqslant |\mathcal{V}_{V_1|V_2Z_c}| - \sum_{i\in\mathcal{V}_{V_1|V_2Z_c}} H(B_1^i|B_1^{1:i-1}V_2^{1:n}Z_c^{1:n}) + O\left(n\sqrt{n\sqrt{n\delta_n}}\right) \\
&\overset{(a)}{\leqslant} |\mathcal{V}_{V_1|V_2Z_c}| - \sum_{i\in\mathcal{V}_{V_1|V_2Z_c}} (1-\delta_n) + O\left(n\sqrt{n\sqrt{n\delta_n}}\right) \\
&= |\mathcal{V}_{V_1|V_2Z_c}|\delta_n + O\left(n\sqrt{n\sqrt{n\delta_n}}\right) = O\left(n\sqrt{n\sqrt{n\delta_n}}\right),
\end{aligned} \tag{42}$$

where (a) follows from the definition of $\mathcal{V}_{V_1|V_2Z_c}$.

Finally, we bound $I(S_j^{1a}M_j^{1a}R_j;\Psi\tilde{Z}_{cj}^{1:n})$ as follows:

$$\begin{aligned}
I(S_j^{1a}M_j^{1a}R_j;\Psi\tilde{Z}_{cj}^{1:n}) &= I(S_j^{1a}M_j^{1a}R_j;\Psi_1) + I(S_j^{1a}M_j^{1a}R_j;\Psi_2\tilde{Z}_{cj}^{1:n}|\Psi_1) \\
&\overset{(a)}{=} I(S_j^{1a}M_j^{1a}R_j;\Psi_2\tilde{Z}_{cj}^{1:n}|\Psi_1) \\
&\leqslant I(S_j^{1a}M_j^{1a}R_j\Psi_1;\Psi_2\tilde{Z}_{cj}^{1:n}) \\
&\overset{(b)}{\leqslant} I(\tilde{B}_{1j}^{1:n}[\mathcal{V}_{V_1|V_2Z_c}];\tilde{V}_{2j}^{1:n}\tilde{Z}_{cj}^{1:n}) \\
&= H(\tilde{B}_{1j}^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]) - H(\tilde{B}_{1j}^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]|\tilde{V}_{2j}^{1:n}\tilde{Z}_{cj}^{1:n}) \\
&\leqslant |\mathcal{V}_{V_1|V_2Z_c}| - H(\tilde{B}_{1j}^{1:n}[\mathcal{V}_{V_1|V_2Z_c}]|\tilde{V}_{2j}^{1:n}\tilde{Z}_{cj}^{1:n}) \overset{(c)}{\leqslant} O\left(n\sqrt{n\sqrt{n\delta_n}}\right),
\end{aligned} \tag{43}$$

where (a) holds because Ψ_1 is independent of $S_j^{1a}M_j^{1a}R_j$, (b) holds by the encoding scheme, (c) holds by (42).

Based on Lemmas 4 and 7, we derive Lemma 8, which shows block-wise strong secrecy.

Lemma 8. For each block $j \in [1,m]$, we have

$$I(S_jT_j\bar{K}_jR_j;\Phi\Psi\tilde{Z}_j^{1:n}) \leqslant O\left(n\sqrt{n\sqrt{n\delta_n}}\right).$$

Proof. Recall that, $S_j \triangleq (S_j^{1a}, S_j^{1b}, S_j^2)$, $T_j \triangleq (K_j^{1a}, M_j^{1a})$, $\Psi \triangleq (\Psi_2, \Psi_1)$ and $\tilde{Z}_j^{1:n} \triangleq (Z_{sj}^{1:n}, \tilde{Z}_{cj}^{1:n})$. First, we have

$$\begin{aligned}
I(S_j^{1a}M_j^{1a}R_j;\Phi Z_{sj}^{1:n}|\Psi\tilde{Z}_{cj}^{1:n}) &\leqslant I(S_j^{1a}\bar{S}_j^{1b}\bar{S}_j^2M_jR_{j-1};\Phi Z_{sj}^{1:n}|\Psi\tilde{Z}_{cj}^{1:n}) \\
&\overset{(a)}{\leqslant} I(S_j^{1a}\bar{S}_j^2\bar{S}_j^{1b}M_jR_{j-1};\Phi Z_{sj}^{1:n}) \\
&\overset{(b)}{\leqslant} I(S_j^{1a}\bar{S}_j^2\bar{S}_j^{1b}M_j\bar{S}_{j-1}^{1b}M_{j-1}^{1b};\Phi Z_{sj}^{1:n}) \\
&\overset{(c)}{=} I(M_jM_{j-1}^{1b};\Phi Z_{sj}^{1:n}) \\
&\leqslant I(M_jM_{j-1};\Phi Z_{sj}^{1:n})
\end{aligned}$$

$$
\begin{aligned}
&= I(M_j;\Phi Z_{sj}^{1:n}) + I(M_{j-1};\Phi Z_{sj}^{1:n}|M_j)\\
&\overset{\text{(d)}}{\leqslant} O(n\sqrt{n\delta_n}) + I(M_{j-1};\Phi Z_{sj}^{1:n}|M_j)\\
&\leqslant O(n\sqrt{n\delta_n}) + I(M_{j-1};\Phi Z_{sj}^{1:n}M_j\bar{K}_{j-1})\\
&= O(n\sqrt{n\delta_n}) + I(M_{j-1};\Phi\bar{K}_{j-1}) + I(M_{j-1};Z_{sj}^{1:n}M_j|\Phi\bar{K}_{j-1})\\
&\overset{\text{(e)}}{=} O(n\sqrt{n\delta_n}) + I(M_{j-1};\Phi\bar{K}_{j-1}) \overset{\text{(f)}}{\leqslant} O(n\sqrt{n\delta_n}),
\end{aligned}
\tag{44}
$$

where (a) holds because $\Phi Z_{sj}^{1:n} \to S_j^{1a}\bar{S}_j^2\bar{S}_j^{1b}M_jR_{j-1} \to \Psi\tilde{Z}_{cj}^{1:n}$, (b) holds because R_{j-1} is a subvector of $(\bar{S}_{j-1}^{1b}, M_{j-1}^{1b})$, (c) holds by the uniformity of $\{S_{j-1}, S_j\}$ and the independence between $\{S_{j-1}, S_j\}$ and $M_jM_{j-1}^{1b}\Phi Z_{sj}^{1:n}$, (d) holds by Lemma 4, (e) holds because $M_{j-1} \to \Phi\bar{K}_{j-1} \to Z_{sj}^{1:n}M_j$, (f) holds by Lemma 4. By combining Lemma 7 and (44) with the chain rule, we have

$$
I(S_j^{1a}M_j^{1a}R_j;\Phi\Psi\tilde{Z}_j^{1:n}) \leqslant O\left(n\sqrt{n\sqrt{n\delta_n}}\right). \tag{45}
$$

Note that,

$$
\begin{aligned}
I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\bar{S}_j^{1b}\bar{S}_j^2) &= H(\bar{S}_j^{1b}\bar{S}_j^2) - H(\bar{S}_j^{1b}\bar{S}_j^2|S_j^{1b}S_j^2K_j^{1a}\bar{K}_j)\\
&= H(\bar{S}_j^{1b}\bar{S}_j^2) - H(K_j^{1b}K_j^2|S_j^{1b}S_j^2K_j^{1a}\bar{K}_j)\\
&\overset{\text{(a)}}{=} H(\bar{S}_j^{1b}\bar{S}_j^2) - H(K_j^{1b}K_j^2|K_j^{1a}\bar{K}_j)\\
&\leqslant |K_j^{1b}| + |K_j^2| - H(K_j^{1b}K_j^2|K_j^{1a}\bar{K}_j)\\
&\overset{\text{(b)}}{\leqslant} |K_j^{1b}| + |K_j^2| - H(K_j\bar{K}_j) + H(K_j^{1a}\bar{K}_j)\\
&\overset{\text{(c)}}{\leqslant} |K_j| + |\bar{K}_j| - H(K_j\bar{K}_j)\\
&\leqslant |\bar{K}_j| + |K_j| - H(\bar{K}_jK_j|Z_{sj}^{1:n}) \overset{\text{(d)}}{\leqslant} O(n\sqrt{n\delta_n}),
\end{aligned}
\tag{46}
$$

where (a) holds by the independence between S_j and $\bar{K}_jK_j$, (b) and (c) hold because $K_j \triangleq (K_j^{1a}, K_j^{1b}, K_j^2)$, (d) holds by Lemma 2. Next, we show that

$$
\begin{aligned}
&I(S_jT_j\bar{K}_jR_j;\Phi\Psi\tilde{Z}_j^{1:n}) - I(S_j^{1a}M_j^{1a}R_j;\Phi\Psi\tilde{Z}_j^{1:n})\\
&= I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Phi\Psi\tilde{Z}_j^{1:n}|S_j^{1a}M_j^{1a}R_j)\\
&\leqslant I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Phi\Psi\tilde{Z}_j^{1:n}S_j^{1a}M_j^{1a}R_j)\\
&\leqslant I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Phi\Psi\tilde{Z}_j^{1:n}S_j^{1a}M_j\bar{S}_j^{1b}\bar{S}_j^2)\\
&= I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Phi Z_{sj}^{1:n}M_j\bar{S}_j^{1b}\bar{S}_j^2) + I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Psi\tilde{Z}_{cj}^{1:n}S_j^{1a}|\Phi Z_{sj}^{1:n}M_j\bar{S}_j^{1b}\bar{S}_j^2)\\
&\overset{\text{(a)}}{=} I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Phi Z_{sj}^{1:n}M_j\bar{S}_j^{1b}\bar{S}_j^2)\\
&= I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\bar{S}_j^{1b}\bar{S}_j^2) + I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Phi Z_{sj}^{1:n}M_j|\bar{S}_j^{1b}\bar{S}_j^2)\\
&\overset{\text{(b)}}{\leqslant} O(n\sqrt{n\delta_n}) + I(S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Phi Z_{sj}^{1:n}M_j|\bar{S}_j^{1b}\bar{S}_j^2)\\
&\leqslant O(n\sqrt{n\delta_n}) + I(\bar{S}_j^{1b}\bar{S}_j^2S_j^{1b}S_j^2K_j^{1a}\bar{K}_j;\Phi Z_{sj}^{1:n}M_j)\\
&= O(n\sqrt{n\delta_n}) + I(S_j^{1b}S_j^2K_j\bar{K}_j;\Phi Z_{sj}^{1:n}M_j)\\
&\overset{\text{(c)}}{=} O(n\sqrt{n\delta_n}) + I(K_j\bar{K}_j;\Phi Z_{sj}^{1:n}M_j) \overset{\text{(d)}}{\leqslant} O(n\sqrt{n\delta_n}),
\end{aligned}
\tag{47}
$$

where (a) holds because $S_j^{1b}S_j^2K_j^{1a}\bar{K}_j \to \Phi Z_{sj}^{1:n}M_j\bar{S}_j^{1b}\bar{S}_j^2 \to \Psi\tilde{Z}_{cj}^{1:n}S_j^{1a}$, (b) holds by (46), (c) holds by the independence between $S_j^{1b}S_j^2$ and $\bar{K}_jK_j\Phi Z_{sj}^{1:n}M_j$, (d) holds by Lemma 4. Finally, we conclude by combining (45) and (47).

The following lemma shows strong secrecy across two adjacent blocks.

Lemma 9. For each block $j \in [1, m]$, define $L_e^j \triangleq I(S_{1:j}T_{1:j}\bar{K}_j R_j; \Phi\Psi\tilde{Z}_{1:j}^{1:n})$. For $j \in [2, m]$, we have

$$L_e^j - L_e^{j-1} \leqslant O(jn\sqrt{n\delta_n}) + O\left(n\sqrt{n\sqrt{n\delta_n}}\right).$$

Proof. For brevity, we further define $Q_j \triangleq (S_j, T_j)$. Part of the proof is adapted from [38, Lemma 12]. By the chain rule for mutual information, we have

$$I(Q_{1:j}\bar{K}_j R_j; \Phi\Psi\tilde{Z}_{1:j}^{1:n}) = \omega_1 + \omega_2 + \omega_3, \tag{48}$$

where

$$\begin{aligned}
&\omega_1 \triangleq I(Q_j\bar{K}_j R_j; \Phi\Psi\tilde{Z}_j^{1:n}),\\
&\omega_2 \triangleq I(Q_{1:j-1}; \Phi\Psi\tilde{Z}_j^{1:n}|Q_j\bar{K}_j R_j),\\
&\omega_3 \triangleq I(Q_{1:j}\bar{K}_j R_j; \tilde{Z}_{1:j-1}^{1:n}|\Phi\Psi\tilde{Z}_j^{1:n}).
\end{aligned}$$

Immediately, ω_1 is bounded by Lemma 8. We continue to bound ω_2 and ω_3 as follows.

First, we have

$$\begin{aligned}
\omega_3 &\leqslant I(Q_{1:j}\bar{K}_j R_j\tilde{Z}_j^{1:n}; \tilde{Z}_{1:j-1}^{1:n}|\Phi\Psi)\\
&\leqslant I(Q_{1:j}\bar{K}_{j-1:j}R_{j-1:j}\tilde{Z}_j^{1:n}; \tilde{Z}_{1:j-1}^{1:n}|\Phi\Psi)\\
&= I(Q_{1:j-1}\bar{K}_{j-1}R_{j-1}; \tilde{Z}_{1:j-1}^{1:n}|\Phi\Psi) + I(Q_j\bar{K}_j R_j\tilde{Z}_j^{1:n}; \tilde{Z}_{1:j-1}^{1:n}|\Phi\Psi Q_{1:j-1}\bar{K}_{j-1}R_{j-1})\\
&\overset{(a)}{=} I(Q_{1:j-1}\bar{K}_{j-1}R_{j-1}; \tilde{Z}_{1:j-1}^{1:n}|\Phi\Psi)\\
&\leqslant I(Q_{1:j-1}\bar{K}_{j-1}R_{j-1}; \Phi\Psi\tilde{Z}_{1:j-1}^{1:n}) = L_e^{j-1},
\end{aligned} \tag{49}$$

where (a) holds because $\tilde{Z}_{1:j-1}^{1:n} \to \Phi\Psi Q_{1:j-1}\bar{K}_{j-1}R_{j-1} \to Q_j\bar{K}_j R_j\tilde{Z}_j^{1:n}$.

Next, we have

$$\begin{aligned}
\omega_2 &\leqslant I(Q_{1:j-1}; \Phi\Psi\tilde{Z}_j^{1:n}\bar{K}_{j-1}R_{j-1}|Q_j\bar{K}_j R_j)\\
&= I(Q_{1:j-1}; \Phi\Psi\bar{K}_{j-1}R_{j-1}|Q_j\bar{K}_j R_j) + I(Q_{1:j-1}; \tilde{Z}_j^{1:n}|\Phi\Psi Q_j\bar{K}_{j-1:j}R_{j-1:j})\\
&\overset{(a)}{=} I(Q_{1:j-1}; \Phi\Psi\bar{K}_{j-1}R_{j-1}|Q_j\bar{K}_j R_j)\\
&\overset{(b)}{\leqslant} I(Q_{1:j-1}; \Phi\Psi\bar{K}_{j-1}R_{j-1})\\
&\overset{(c)}{=} I(T_{1:j-1}; \Phi\bar{K}_{j-1}R_{j-1}),
\end{aligned} \tag{50}$$

where (a) holds by $Q_{1:j-1} \to \Phi\Psi Q_j\bar{K}_{j-1:j}R_{j-1:j} \to \tilde{Z}_j^{1:n}$, (b) holds because $Q_{1:j-1} \to \Phi\Psi\bar{K}_{j-1}R_{j-1} \to Q_j\bar{K}_j R_j$, (c) holds because $S_{1:j-1}$ and Ψ are mutually independent and also independent of the remaining random variables. Before we bound the last term of (50), we derive the following result:

$$\begin{aligned}
I(T_j; \Phi\bar{K}_j R_j) &\leqslant I(T_j; \Phi\bar{K}_j M_j^{1b}\bar{S}_j^{1b})\\
&\leqslant I(T_j; \Phi\bar{K}_j M_j^{1b}\bar{S}_j^{1b}K_j^{1b})\\
&\overset{(a)}{=} I(T_j; \Phi\bar{K}_j K_j^{1b}M_j^{1b})\\
&= I(T_j; K_j^{1b}M_j^{1b}) + I(T_j; \Phi\bar{K}_j|K_j^{1b}M_j^{1b})\\
&\overset{(b)}{\leqslant} O(n\sqrt{n\delta_n}) + I(T_j; \Phi\bar{K}_j|K_j^{1b}M_j^{1b})\\
&\leqslant O(n\sqrt{n\delta_n}) + I(T_jK_j^{1b}M_j^{1b}; \Phi\bar{K}_j)\\
&\leqslant O(n\sqrt{n\delta_n}) + I(K_jM_j; \Phi\bar{K}_j) \overset{(c)}{\leqslant} O(n\sqrt{n\delta_n}),
\end{aligned} \tag{51}$$

where (a) holds because $T_j\Phi\bar{K}_jM_j^{1b}\to K_j^{1b}\to\bar{S}_j^{1b}$, (b) holds by Lemma 6 and let $T_j'\triangleq(K_j^{1b},M_j^{1b})$,

$$\begin{aligned}I(T_j;T_j')&=H(T_j)+H(T_j')-H(T_jT_j')\\&\leqslant|T_j|+|T_j'|-H(T_jT_j')\\&\leqslant|K_j|+|M_j|-H(K_jM_j)\leqslant O(n\sqrt{n\delta_n}),\end{aligned}\tag{52}$$

finally (c) holds by Lemma 4.

Now, we bound the last term of (50) as follows:

$$\begin{aligned}I(T_{1:j-1};\Phi\bar{K}_{j-1}R_{j-1})&=I(T_{j-1};\Phi\bar{K}_{j-1}R_{j-1})+I(T_{1:j-2};\Phi\bar{K}_{j-1}R_{j-1}|T_{j-1})\\&\overset{(a)}{\leqslant}O(n\sqrt{n\delta_n})+I(T_{1:j-2};\Phi\bar{K}_{j-1}R_{j-1}|T_{j-1})\\&\leqslant O(n\sqrt{n\delta_n})+I(T_{1:j-2};\Phi\bar{K}_{j-1}R_{j-1}T_{j-1})\\&\leqslant O(n\sqrt{n\delta_n})+I(T_{1:j-2};\Phi\bar{K}_{j-2:j-1}R_{j-2:j-1}T_{j-1})\\&=O(n\sqrt{n\delta_n})+I(T_{1:j-2};\Phi\bar{K}_{j-2}R_{j-2})+I(T_{1:j-2};\bar{K}_{j-1}R_{j-1}T_{j-1}|\Phi\bar{K}_{j-2}R_{j-2})\\&\overset{(b)}{=}O(n\sqrt{n\delta_n})+I(T_{1:j-2};\Phi\bar{K}_{j-2}R_{j-2})\\&\overset{(c)}{\leqslant}(j-2)O(n\sqrt{n\delta_n})+I(T_1;\Phi\bar{K}_1R_1)\\&\overset{(d)}{\leqslant}(j-1)O(n\sqrt{n\delta_n}),\end{aligned}\tag{53}$$

where (a) holds by (51), (b) holds by the Markov chain $T_{1:j-2}\to\Phi\bar{K}_{j-2}R_{j-2}\to\bar{K}_{j-1}R_{j-1}T_{j-1}$, (c) holds by induction, (d) holds by (51). By combining (48)–(50), (53) and applying Lemma 8, we finally obtain

$$L_e^j-L_e^{j-1}\leqslant O(jn\sqrt{n\delta_n})+O\left(n\sqrt{n\sqrt{n\delta_n}}\right).$$

Finally, applying Lemmas 8 and 9, we obtain

$$\begin{aligned}\boldsymbol{L}(S_{1:m}T_{1:m})&=I(S_{1:m}T_{1:m};\Phi\Psi\tilde{Z}_{1:m}^{1:n})\\&\leqslant L_e^m\\&=\sum_{j=2}^{m}(L_e^j-L_e^{j-1})+L_e^1\\&\leqslant O(m^2n\sqrt{n\delta_n})+O\left(mn\sqrt{n\sqrt{n\delta_n}}\right).\end{aligned}\tag{54}$$

In summary, the proposed scheme achieves the tradeoff region (5) established in [11] for general sources and channels satisfying strong secrecy criterion.

5 Conclusion

In this paper, we studied the polar coding design for the joint source-channel model. We proposed an explicit polar coding scheme that achieves the tradeoff region [11] for general sources and channels under strong secrecy criterion. This work provides an example of practical code design that fully exploits the advantages of both correlated sources and the wiretap channel. A generalization of the joint source-channel model is the wiretap channel with generalized feedback studied in [25], where novel lower bounds on the secrecy capacity and secret-key capacity were established. It is of interest to see whether the present work can be extended to achieve those lower bounds.

Acknowledgements This work was supported in part by National Key R&D Program of China (Grant No. 2018YFB1801101), in part by National Natural Science Foundation of China (Grant Nos. 61932005, 61941114, 61901051).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387
2 Csiszár I, Körner J. Broadcast channels with confidential messages. IEEE Trans Inform Theory, 1978, 24: 339–348
3 Maurer U M. Secret key agreement by public discussion from common information. IEEE Trans Inform Theory, 1993, 39: 733–742
4 Ahlswede R, Csiszár I. Common randomness in information theory and cryptography. I. Secret sharing. IEEE Trans Inform Theory, 1993, 39: 1121–1132
5 Csiszár I, Narayan P. Common randomness and secret key generation with a helper. IEEE Trans Inform Theory, 2000, 46: 344–366
6 Bloch M, Barros J. Physical-Layer Security: from Information Theory to Security Engineering. Cambridge: Cambridge University Press, 2011
7 Wu Y P, Khisti A, Xiao C S, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J Sel Areas Commun, 2018, 36: 679–695
8 Hamamreh J M, Furqan H M, Arslan H. Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey. IEEE Commun Surv Tut, 2019, 21: 1773–1828
9 Ji X S, Huang K Z, Jin L, et al. Overview of 5G security technology. Sci China Inf Sci, 2018, 61: 081301
10 You X H, Wang C X, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci, 2021, 64: 110301
11 Prabhakaran V M, Eswaran K, Ramchandran K. Secrecy via sources and channels. IEEE Trans Inform Theory, 2012, 58: 6747–6765
12 Khisti A, Diggavi S N, Wornell G W. Secret-key generation using correlated sources and channels. IEEE Trans Inform Theory, 2012, 58: 652–670
13 Eswaran K, Prabhakaran V M, Ramchandran K. Secret communication using sources and channels. In: Proceedings of the 42nd Asilomar Conference on Signals, Systems and Computers, 2008. 671–675
14 Chen Y L, Cai N, Sezgin A. Wiretap channel with correlated sources. In: Proceedings of IEEE International Conference on Cloud Engineering, 2014. 472–477
15 Chen Y, Vogt H, Sezgin A. Gaussian wiretap channels with correlated sources: approaching capacity region within a constant GAP. In: Proceedings of IEEE International Conference on Communications Workshops (ICC), 2014. 794–799
16 Bunin A, Piantanida P, Shitz S S. The gaussian wiretap channel with correlated sources at the terminals: secret communication and key generation. In: Proceedings of IEEE International Conference on the Science of Electrical Engineering (ICSEE), 2016. 1–5
17 Ahlswede R, Cai N. Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder. Electron Notes Discrete Math, 2005, 21: 155–159
18 Gunduz D, Brown D R, Poor H V. Secret communication with feedback. In: Proceedings of International Symposium on Information Theory and Its Applications (ISITA), 2008. 1–6
19 Ardestanizadeh E, Franceschetti M, Javidi T, et al. Wiretap channel with secure rate-limited feedback. IEEE Trans Inform Theory, 2009, 55: 5353–5361
20 Dai B, Vinck A H, Luo Y, et al. Capacity region of non-degraded wiretap channel with noiseless feedback. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), 2012. 244–248
21 Chia Y K, Gamal A E. Wiretap channel with causal state information. IEEE Trans Inform Theory, 2012, 58: 2838–2849
22 Czap L, Prabhakaran V M, Fragouli C, et al. Secret communication over broadcast erasure channels with state-feedback. IEEE Trans Inform Theory, 2015, 61: 4788–4808
23 Cohen A, Cohen A. Wiretap channel with causal state information and secure rate-limited feedback. IEEE Trans Commun, 2016, 64: 1192–1203
24 Han T S, Sasaki M. Wiretap channels with causal state information: strong secrecy. IEEE Trans Inform Theory, 2019, 65: 6750–6765
25 Bassi G, Piantanida P, Shamai S. The wiretap channel with generalized feedback: secure communication and key generation. IEEE Trans Inform Theory, 2019, 65: 2213–2233
26 Yamamoto H. Rate-distortion theory for the Shannon cipher system. IEEE Trans Inform Theory, 1997, 43: 827–835
27 Merhav N. Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels. IEEE Trans Inform Theory, 2008, 54: 2723–2734
28 Kang W, Liu N Q. Wiretap channel with shared key. In: Proceedings of IEEE Information Theory Workshop (ITW), 2010. 1–5
29 Arikan E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Trans Inform Theory, 2009, 55: 3051–3073
30 Wei Y P, Ulukus S. Polar coding for the general wiretap channel with extensions to multiuser scenarios. IEEE J Sel Areas Commun, 2016, 34: 278–291
31 Gulcu T C, Barg A. Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component. IEEE Trans Inform Theory, 2017, 63: 1311–1324
32 Chou R A, Bloch M R. Polar coding for the broadcast channel with confidential messages: a random binning analogy. IEEE Trans Inform Theory, 2016, 62: 2410–2429
33 Wang H W, Tao X F, Li N, et al. Polar coding for the wiretap channel with shared key. IEEE Trans Inform Foren Secur, 2018, 13: 1351–1360
34 Zheng M F, Chen W, Ling C. Polar coding for the cognitive interference channel with confidential messages. IEEE J Sel Areas Commun, 2018, 36: 762–774
35 Alos J O, Fonollosa J R. Polar coding for common message only wiretap broadcast channel. 2019. ArXiv:1901.07649

36 Maurer U, Wolf S. Information-theoretic key agreement: from weak to strong secrecy for free. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, 2000. 351–368
37 Chou R A, Bloch M R, Abbe E. Polar coding for secret-key generation. In: Proceedings of IEEE Information Theory Workshop (ITW), 2013. 1–5
38 Chou R A, Bloch M R, Abbe E. Polar coding for secret-key generation. IEEE Trans Inform Theory, 2015, 61: 6213–6237
39 Arikan E. Source polarization. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), 2010. 899–903
40 Hassani S H, Urbanke R. Universal polar codes. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), 2014. 1451–1455
41 Honda J, Yamamoto H. Polar coding without alphabet extension for asymmetric models. IEEE Trans Inform Theory, 2013, 59: 7829–7838
42 Cuff P W. Communication in Networks for Coordinating Behavior. Stanford: Stanford University Press, 2009
43 Aldous D. Random walks on finite groups and rapidly mixing Markov chains. In: Séminaire de Probabilités XVII 1981/82. Berlin: Springer, 1983. 243–297
44 Cover T M, Thomas J A, Wiley, J. Elements of Information Theory. Beijing: Tsinghua University Press, 2003