IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 29, 2019, accepted December 20, 2019, date of publication December 26, 2019,
date of current version January 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2962543

Polar Coding for the Multiple Access Channel With Confidential Messages

HAOWEI WANG, (Student Member, IEEE), XIAOFENG TAO, (Senior Member, IEEE), NA LI, (Member, IEEE), AND HUICI WU, (Member, IEEE)
National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Xiaofeng Tao (taoxf@bupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61932005, Grant 61901051, and Grant 61941105, in part by the Beijing Municipal Science and Technology Project under Grant Z181100003218005, and in part by the 111 Project of China under Grant B16006.

ABSTRACT The multiple access channel with confidential messages (MAC-CM) generalizes the traditional multiple access channel by allowing both users to receive channel outputs. Achievable secrecy rate region of this model has been established using random coding arguments, whereas practical codes design remains to be further discussed. In this paper, we develop an explicit polar coding scheme that achieves the secrecy rate region of the MAC-CM under strong secrecy. In particular, our scheme mainly relies on monotone chain rules and polar coding techniques for single-user channels. A proper chaining scheme is constructed to align polar indices and to provide strong secrecy. Finally, a rigorous analysis is provided to validate the performance of our scheme.

INDEX TERMS Multiple access channels, monotone chain rules, polar codes, strong secrecy.

I. INTRODUCTION

With the emergence of physical-layer security, fundamental limits of secure transmission over wiretap channels have been studied extensively [1]–[3]. The multiple access channel with confidential messages (MAC-CM) [4], [5] is one of the multiuser wiretap channels, which generalizes the traditional MAC by allowing both users to receive channel outputs. In this model, each user may extract confidential information of the other user from the channel outputs it receives. Hence, each user views the other user as an eavesdropper and intends to keep its confidential information concealed from the other user. The best-known inner bound on the secrecy capacity region of the MAC-CM was obtained in [4] based on random coding arguments. The problem of designing practical codes for this model has not yet been addressed in the literature.

Polar codes, introduced by Arıkan [6], are the first class of provable capacity-achieving codes for binary-input symmetric memoryless channels with low coding complexity. Over the past decade, polar codes have gained significant attention and have been extended to a large variety of scenarios including MACs [7]–[11] and wiretap channels [12]–[18]. In this paper, we are motivated to develop an explicit coding scheme for the MAC-CM using polar codes.

A. RELATED WORKS

Polar coding for MACs was first discussed in [7], in which a MAC polarization approach was proposed for two-user MACs. This approach was later extended to m-user MACs [8] and MACs with input alphabet of arbitrary size [9]. One problem is that it does not always achieve the whole secrecy capacity region of MACs. Along another line, Arıkan [19] introduced a scheme for the Slepian-Wolf problem based on monotone chain rules. This alternate scheme only relies on the polarization of single-user channels, and has been shown to achieve the dominant face of the uniform rate region for two-user MACs [10] and m-user MACs [11]. In this paper, we also adopt monotone chain rules in our scheme for the MAC-CM.

Polar codes that achieve secrecy capacity have been proposed for degraded wiretap channels [12]–[15], general wiretap channels [16]–[18] and other extended wiretap scenarios [20]–[24]. The multiple access wiretap channel (MAC-WT) [25] is the other type of MACs with secrecy constraints, in which the eavesdropper is an external receiver. Polar coding for the MAC-WT can be found in [15], [16], [20]. Specifically, [16] utilizes monotone chain

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Xu.

rules to construct the coding scheme for the MAC-WT satisfying weak secrecy. Another work worth mentioning is [21], which considers the two-way wiretap channel. The coding scheme in [21] also utilizes monotone chain rules in that the eavesdropper sees a MAC in the model.

B. CONTRIBUTIONS

In this paper, we develop an explicit polar coding scheme that achieves the secrecy rate region of the MAC-CM [4]. In particular, we prove strong secrecy for the model. Our main contributions are summarized as follows.

- The secrecy rate region of the MAC-CM mainly consists of three sub-regions, for which two coding schemes are proposed separately. (i) When both users achieve positive secrecy rates, we adopt monotone chain rules to construct the coding scheme that achieves the dominant face of the region directly. (ii) When only one user achieves positive secrecy rate, this user performs wiretap coding scheme, whereas the user of zero secrecy rate performs usual single-user coding scheme.
- In both cases, we do not make any symmetry or degradation assumptions on the channel. Proper chaining schemes are constructed to deal with the general channel setting and to provide strong secrecy.
- A rigorous analysis is finally provided to validate the performance of the proposed scheme. The crucial part of the analysis is to make sure that the distribution induced by the encoder approximates the target distribution from which the polarization sets are defined.

C. ORGANIZATION AND NOTATIONS

The remainder of this paper is organized as follows. In Section II, we introduce the MAC-CM model and recap its best-known achievable secrecy rate region. Preliminaries on polar coding techniques are reviewed in Section III. We present our polar coding scheme for the MAC-CM in Section IV. A rigorous analysis of the proposed scheme is conducted in Section V. Finally, Section VI concludes this paper.

Notations: Uppercase letters indicate random variables, whereas lowercase letters indicate the associated realizations. $[n]$ denotes the index set $\{1, 2, \ldots, n\}$ for $n \in \mathbb{Z}^+$. For any random variable X, $X^{1:n} \triangleq (X^1, \ldots, X^n)$ denotes a vector of n i.i.d. components. For $\mathcal{A} \subset [n]$, we write $X^{1:n}[\mathcal{A}]$ to denote the sequence $\{X^i\}_{i\in\mathcal{A}}$, and $\mathcal{A}^c$ the complement of $\mathcal{A}$ with respect to $[n]$. Let p_X and $p_{\tilde{X}}$ be two distributions defined over the alphabet $\mathcal{X}$. $\mathbb{D}(p_X||p_{\tilde{X}})$ denotes the Kullback-Leibler divergence between two distributions. $\mathbb{V}(p_X, p_{\tilde{X}}) \triangleq \sum_{x\in\mathcal{X}} \left|p_X(x) - p_{\tilde{X}}(x)\right|$ denotes the total variation distance between two distributions. The generator matrix G_n of polar codes is defined as in [6].

II. SYSTEM MODEL

We consider secure transmission over a two-user MAC-CM as depicted in Fig. 1. In this channel model, each user intends to transmit one confidential message to the destination, whereas information leakage happens due to the presence of channel outputs at users, i.e., $Z_1^{1:n}$ and $Z_2^{1:n}$. As a result, each user treats the other user as eavesdropper and tries to keep its message as secure as possible. *Self-interference* is considered in the model, i.e., channel outputs at one user also depend on its own channel inputs, i.e., $Z_1^{1:n}$ can depend on $X_1^{1:n}$, and $Z_2^{1:n}$ can depend on $X_2^{1:n}$. Both users are assumed to be *passive* eavesdroppers in that, channel outputs at one user is only used to extract the other user's information, but not to facilitate its own transmission or disturb the other user's transmission.

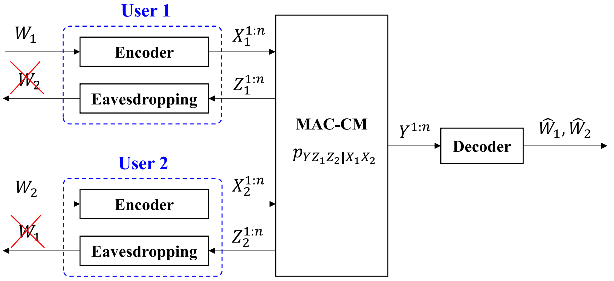

FIGURE 1. Two-user multiple access channel with confidential messages.

Definition 1: A $(2^{nR_1}, 2^{nR_2}, n)$ *code for the two-user MAC-CM* $(\mathcal{X}_1 \times \mathcal{X}_2, p_{YZ_1Z_2|X_1X_2}, \mathcal{Y} \times \mathcal{Z}_1 \times \mathcal{Z}_2)$ *consists of*

- *two message sets* $\mathcal{W}_k = [1, 2^{nR_k}]$, $k = 1, 2$;
- *two encoding functions* $f_k : \mathcal{W}_k \to \mathcal{X}_k^{1:n}$, *which map the messages* w_k *to a codeword* $x_k^{1:n}$, $k = 1, 2$;
- *a decoding function* $g : \mathcal{Y}^{1:n} \to \mathcal{W}_1 \times \mathcal{W}_2$, *which maps the channel output* $y^{1:n}$ *to the messages* $(\hat{w}_1, \hat{w}_2)$.

The code performance is evaluated by reliability and secrecy. Reliability is measured in terms of error probability

$$\mathbb{P}_e = \mathbb{P}[(\hat{W}_1\hat{W}_2) \neq (W_1W_2)]. \tag{1}$$

Secrecy is measured in terms of information leakage

$$\begin{aligned} \mathbb{L}_1 &= I(W_1; Z_2^{1:n}X_2^{1:n}W_2), \\ \mathbb{L}_2 &= I(W_2; Z_1^{1:n}X_1^{1:n}W_1). \end{aligned} \tag{2}$$

Remark 1: Two Markov chains can be obtained from Definition 1, namely, $W_1 \to X_1^{1:n} \to (W_2, Z_1^{1:n})$ *and* $W_2 \to X_2^{1:n} \to (W_1, Z_2^{1:n})$. *Therefore, (2) can be simplified to be*

$$\begin{aligned} \mathbb{L}_1 &= I(W_1; Z_2^{1:n}X_2^{1:n}), \\ \mathbb{L}_2 &= I(W_2; Z_1^{1:n}X_1^{1:n}). \end{aligned} \tag{3}$$

Definition 2: A secrecy rate pair (R_1, R_2) *is said to be achievable if there exists a sequence of* $(2^{nR_1}, 2^{nR_2}, n)$ *codes such that*

$$\lim_{n\to\infty} \mathbb{P}_e = 0 \text{ (reliability)}, \tag{4}$$

$$\lim_{n\to\infty} \mathbb{L}_1 = 0, \quad \lim_{n\to\infty} \mathbb{L}_2 = 0 \text{ (strong secrecy)}. \tag{5}$$

The secrecy capacity region is defined as the supremum of all achievable secrecy rates.

Remark 2: The secrecy constraints given by (5) are known as the strong secrecy, whereas the random coding scheme in [4] provides only weak secrecy, which is given by

$$\lim_{n\to\infty} \frac{\mathbb{L}_1}{n} = 0, \quad \lim_{n\to\infty} \frac{\mathbb{L}_2}{n} = 0. \tag{6}$$

Results under weak secrecy can be improved to strong secrecy by using privacy amplification [26]. In this paper, we provide an alternative approach for the MAC-CM using polar codes.

The best-known achievable secrecy rate region for the MAC-CM is given in Theorem 1, which was obtained in [4] under weak secrecy.

Theorem 1: An achievable secrecy rate region for the two-user MAC-CM is given by

$$\mathcal{R}_S \triangleq Conv \bigcup_{\mathcal{P}} \left\{ \mathcal{R}_S^{(1)} \cup \mathcal{R}_S^{(2)} \cup \mathcal{R}_S^{(3)} \right\}, \tag{7}$$

where $Conv(\cdot)$ *denotes the convex hull of a given set,* $\mathcal{P} \triangleq p_{V_1}p_{V_2}p_{X_1|V_1}p_{X_2|V_2}p_{YZ_1Z_2|X_1X_2}$, *and*

$$\mathcal{R}_S^{(1)} \triangleq \left\{ (R_1, R_2) \middle| \begin{array}{l} 0 \le R_1 \le R_A \\ 0 \le R_2 \le R_B \\ R_1 + R_2 \le R_C \end{array} \right\}, \tag{8}$$

$$\mathcal{R}_S^{(2)} \triangleq \left\{ (R_1, 0) \middle| 0 \le R_1 \le R_A \right\}, \tag{9}$$

$$\mathcal{R}_S^{(3)} \triangleq \left\{ (0, R_2) \middle| 0 \le R_2 \le R_B \right\}, \tag{10}$$

where

$$\begin{aligned} R_A &\triangleq I(V_1; Y|V_2) - I(V_1; Z_2|V_2X_2), \\ R_B &\triangleq I(V_2; Y|V_1) - I(V_2; Z_1|V_1X_1), \\ R_C &\triangleq I(V_1V_2; Y) - I(V_1; Z_2|V_2X_2) - I(V_2; Z_1|V_1X_1). \end{aligned} \tag{11}$$

Remark 3: The random coding scheme [4] considers the scenario that both users also have a common message. We omit the common message here such that we focus on the polar coding design for secret messages. The common message can be embedded into our scheme using superposition coding [27].

In this paper, out goal is to develop an explicit polar coding scheme that achieves $\mathcal{R}_S$ in Theorem 1 under strong secrecy.

III. PRELIMINARIES ON POLAR CODES

A. POLAR CODING FOR ASYMMETRIC CHANNELS

We recall the polar coding design for asymmetric channels [18], [28] in this section. Consider a discrete memoryless channel $p_{Y|X}$ with binary input X and output Y. The goal is to approach the rate $I(X; Y)$.

Define $U^{1:n} = X^{1:n}G_n$, and the following polarized sets:

$$\begin{aligned} \mathcal{H}_X &= \{i \in [n] : Z(U^i|U^{1:i-1}) \ge 1 - \delta_n\}, \\ \mathcal{L}_X &= \{i \in [n] : Z(U^i|U^{1:i-1}) \le \delta_n\}, \\ \mathcal{H}_{X|Y} &= \{i \in [n] : Z(U^i|U^{1:i-1}Y^{1:n}) \ge 1 - \delta_n\}, \\ \mathcal{L}_{X|Y} &= \{i \in [n] : Z(U^i|U^{1:i-1}Y^{1:n}) \le \delta_n\}. \end{aligned} \tag{12}$$

where $\delta_n \triangleq 2^{-n^\beta}$, $\beta \in (0, 0.5)$, and $Z(\cdot|\cdot)$ denotes the Bhattacharyya parameter. It is shown [29] that, $\frac{1}{n}|\mathcal{H}_X| \to H(X)$, $\frac{1}{n}|\mathcal{L}_X| \to 1 - H(X)$, $\frac{1}{n}|\mathcal{H}_{X|Y}| \to H(X|Y)$, and $\frac{1}{n}|\mathcal{L}_{X|Y}| \to 1 - H(X|Y)$, for sufficiently large n.

To construct the polar coding scheme, one can partition the index $[n]$ as follows [28]:

$$\begin{aligned} \mathcal{I} &= \mathcal{H}_X \cap \mathcal{L}_{X|Y}, \\ \mathcal{R} &= \mathcal{H}_X \cap (\mathcal{L}_{X|Y})^c, \\ \mathcal{D} &= (\mathcal{H}_X)^c. \end{aligned} \tag{13}$$

1) ENCODING

Let $\tilde{u}^{1:n}$ denote the realization of $U^{1:n}$. The encoder forms $\tilde{u}^{1:n}$ as follows.

- $\tilde{u}^{1:n}[\mathcal{I}]$ stores the information bits. First, $\mathcal{I}$ is suitable to contain uniformly distributed bits since $\mathcal{I} \subseteq \mathcal{H}_X$. Further, $\mathcal{I} \subseteq \mathcal{L}_{X|Y}$ means that those bits within $\mathcal{I}$ can be reliably decoded.
- $\tilde{u}^{1:n}[\mathcal{R}]$ contains uniformly distributed random bits, which are shared between the encoder and the decoder. Let $J \triangleq \tilde{u}^{1:n}[\mathcal{R}]$. Note that, J can be reused over a sufficient number of blocks to make the induced rate loss negligible.
- $\tilde{u}^{1:n}[\mathcal{D}]$ contains almost deterministic bits sampled from the conditional probability $P_{U^i|U^{1:i-1}}$. We use random decisions here like [18].
- Let $\Phi \triangleq \tilde{u}^{1:n}[(\mathcal{H}_X)^c \cap (\mathcal{L}_{X|Y})^c]$. Note that, Φ is transmitted to the receiver separately with some reliable error-correcting codes. This transmission is shown to be negligible in terms of rate, i.e., $|\Phi| = o(n)$ [18].

The encoder computes $\tilde{x}^{1:n} = \tilde{u}^{1:n}G_n$ once $\tilde{u}^{1:n}$ is formed.

2) DECODING

The receiver obtains $\tilde{u}^{1:n}[(\mathcal{L}_{X|Y})^c]$ through (J, Φ). Then the receiver decodes $\tilde{u}^{1:n}$ with the successive cancellation (SC) decoder [29]:

$$\hat{u}^i = \begin{cases} \tilde{u}^i, \text{ if } i \in (\mathcal{L}_{X|Y})^c \\ \arg\max_{u\in\{0,1\}} P_{U^i|U^{1:i-1}Y^{1:n}}(u|\hat{u}^{1:i-1}y^{1:n}), \text{ if } i \in \mathcal{L}_{X|Y} \end{cases} \tag{14}$$

The error probability $\mathbb{P}_e$ can be upper bounded by

$$\mathbb{P}_e \le \sum_{i\in\mathcal{L}_{X|Y}} Z(U^i|U^{1:i-1}Y^{1:n}) = O(\delta_n), \tag{15}$$

with complexity $O(n \log n)$. The information rate is

$$\begin{aligned} \lim_{n\to\infty} \frac{|\mathcal{I}|}{n} &= \lim_{n\to\infty} \frac{|\mathcal{H}_X \cap \mathcal{L}_{X|Y}|}{n} \\ &= \lim_{n\to\infty} \frac{|\mathcal{H}_X \backslash \mathcal{H}_{X|Y}|}{n} \\ &= H(X) - H(X|Y) = I(X; Y). \end{aligned} \tag{16}$$

B. POLAR CODING FOR MACS WITH MONOTONE CHAIN RULES

Monotone chain rules are first introduced for the Slepian-Wolf problem [19], and then extended to two-user MACs [10]. Consider a two-user MAC $p_{Y|X_1X_2}$ with binary inputs X_1, X_2 and output Y. The capacity region is the convex hull of all rate pairs satisfying

$$\begin{aligned} 0 \leq R_1 &\leq I(X_1; Y|X_2), \\ 0 \leq R_2 &\leq I(X_2; Y|X_1), \\ R_1 + R_2 &\leq I(X_1X_2; Y), \end{aligned} \tag{17}$$

for which $R_1+R_2 = I(X_1X_2; Y)$ is referred to as the *dominant face*.

Define $U_1^{1:n} = X_1^{1:n}G_n$, $U_2^{1:n} = X_2^{1:n}G_n$. Denote by $S^{1:2n} \triangleq (S^1, \ldots, S^{2n})$ an arbitrary permutation of $U_1^{1:n}U_2^{1:n}$. $S^{1:2n}$ is said to be monotone if it preserves the relative order of the elements of both $U_1^{1:n}$ and $U_2^{1:n}$. Accordingly, one can expand the mutual information $I(U_1^{1:n}U_2^{1:n}; Y^{1:n})$ as

$$I(U_1^{1:n}U_2^{1:n}; Y^{1:n}) = \sum_{l=1}^{2n} I(S^l; Y^{1:n}|S^{1:l-1}), \tag{18}$$

where each term $I(S^l; Y^{1:n}|S^{1:l-1})$ polarizes to 0 or 1 as n goes to infinity. The rates of two users are defined as

$$R_1' = \frac{1}{n} \sum_{l:S^l \in U_1^{1:n}} I(S^l; Y^{1:n}|S^{1:l-1}), \tag{19}$$

$$R_2' = \frac{1}{n} \sum_{l:S^l \in U_2^{1:n}} I(S^l; Y^{1:n}|S^{1:l-1}). \tag{20}$$

It is shown that (R_1', R_2') can be arbitrarily close to the rate pairs on the dominant face of (17) by using monotone permutations of the type $S^{1:2n} = U_1^{1:i}U_2^{1:n}U_1^{i+1:n}$ $(i \in [n])$.

Similar to the single-user case in previous section, one can develop polar codes for two-user MACs. For $k = \{1, 2\}$, assume that U_k^i is mapped to $S^{l(k)}$, where $i \in [n]$ and $l(k) \in [2n]$. Define the following polarized sets:

$$\begin{aligned} \mathcal{H}_{X_k} &= \{i \in [n] : Z(U_k^i|S^{1:l(k)-1}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{X_k|Y} &= \{i \in [n] : Z(U_k^i|S^{1:l(k)-1}Y^n) \leq \delta_n\}. \end{aligned} \tag{21}$$

Partition the index $[n]$ for user k as follows:

$$\begin{aligned} \mathcal{I}^{(k)} &= \mathcal{H}_{X_k} \cap \mathcal{L}_{X_k|Y}, \\ \mathcal{R}^{(k)} &= \mathcal{H}_{X_k} \cap (\mathcal{L}_{X_k|Y})^c, \\ \mathcal{D}^{(k)} &= (\mathcal{H}_{X_k})^c. \end{aligned} \tag{22}$$

Then user k transmits $X_k^{1:n} = U_k^{1:n}G_n$ over the channel. On the other side, the receiver decodes $U_1^{1:n}$ and $U_2^{1:n}$ jointly using a SC decoder with the used permutation $S^{1:2n}$. The encoding and decoding complexity of this scheme are the same as the single-user case, which are $O(n \log n)$. For codes construction, the complexity can be made as low as $O(n)$ using existing methods [10].

IV. POLAR CODING SCHEME FOR THE MAC-CM

In this section, we develop an explicit polar coding scheme that achieves $\mathcal{R}_S$ in Theorem 1 under strong secrecy. Specifically, $\mathcal{R}_S$ mainly consists of three sub-regions, i.e., $\mathcal{R}_S^{(1)}$, $\mathcal{R}_S^{(2)}$, and $\mathcal{R}_S^{(3)}$, for which we aim to consider the achievability separately as follows.

Achievability of $\mathcal{R}_S^{(1)}$: To obtain a nonempty $\mathcal{R}_S^{(1)}$, we assume that $\max\{R_A, R_B\} > 0$ and $R_C > 0$. Then we have three cases to consider, i.e. $\{R_A > 0, R_B > 0\}$, $\{R_A > 0, R_B \leq 0\}$, and $\{R_A \leq 0, R_B > 0\}$. For the first case, $\mathcal{R}_S^{(1)}$ is a polytope of which $R_1 + R_2 = R_C$ is the dominant face. In Section IV-A, we construct the coding scheme using monotone chain rules such that we achieve the dominant face of $\mathcal{R}_S^{(1)}$ directly. For the second case, we have

$$\mathcal{R}_S^{(1)} = \{(R_1, 0) \big| 0 \leq R_1 \leq \min(R_A, R_C)\} \subset \mathcal{R}_S^{(2)}. \tag{23}$$

We similarly have $\mathcal{R}_S^{(1)} \subset \mathcal{R}_S^{(3)}$ for the third case.

Achievability of $\mathcal{R}_S^{(2)}$ and $\mathcal{R}_S^{(3)}$: It suffices to construct the coding scheme to achieve $\mathcal{R}_S^{(2)}$ due to symmetry. In this case, the target rate pair is $(R_A, 0)$, where user 1 achieves a positive secrecy rate and user 2 has a secrecy rate of zero. We develop the coding scheme achieving $(R_A, 0)$ in Section IV-B. In particular, the user with positive secrecy rate preforms usual wiretap coding scheme, whereas the user of zero secrecy rate performs single-user coding scheme.

Finally, the remaining rate pairs within $\mathcal{R}_S$ (obtained by convexification) can be achieved by time-sharing.

A. CODING SCHEME FOR ACHIEVING $\mathcal{R}_S^{(1)}$ WHEN $R_A > 0$, $R_B > 0$

We refer to the channel from both users to the receiver as the main channel. Obviously, the main channel is a typical two-user MAC, which is defined as $p_{Y|V_1V_2}$. Moreover, we refer to the channel from both users to one of the them as the eavesdropper channel. Two eavesdropper channels, which are respectively defined as $p_{Z_1|X_1V_2}$ and $p_{Z_2|V_1X_2}$, can also be viewed as two-user MACs since we take self-interference into consideration. In the following, we construct the coding scheme using monotone chain rules.

1) THE MAIN CHANNEL

The achievable rate region for the main channel is

$$\mathcal{R}_m = \left\{ (R_{m1}, R_{m2}) \middle| \begin{array}{l} 0 \leq R_{m1} \leq I(V_1; Y|V_2) \\ 0 \leq R_{m2} \leq I(V_2; Y|V_1) \\ R_{m1} + R_{m2} \leq I(V_1V_2; Y) \end{array} \right\}, \tag{24}$$

of which the dominant face is $R_{m1} + R_{m2} = I(V_1V_2; Y)$.

Define $U_k^{1:n} = V_k^{1:n}G_n$, for $k = \{1, 2\}$. Consider monotone permutations of the type $S^{1:2n} = U_1^{1:i}U_2^{1:n}U_1^{i+1:n}$. Assume that U_k^i is mapped to $S^{l(k)}$, where $i \in [n]$ and $l(k) \in [2n]$. Define the following polarized sets:

$$\begin{aligned} \mathcal{H}_{V_k} &= \{i \in [n] : Z(U_k^i|S^{1:l(k)-1}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{V_k|Y} &= \{i \in [n] : Z(U_k^i|S^{1:l(k)-1}Y^n) \leq \delta_n\}. \end{aligned} \tag{25}$$

Due to the independence of $U_1^{1:n}$ and $U_2^{1:n}$, one can rewrite $\mathcal{H}_{V_k}$ equivalently as

$$\mathcal{H}_{V_k} = \{i \in [n] : Z(U_k^i|U_k^{1:i-1}) \geq 1 - \delta_n\}. \tag{26}$$

Similar to (13) and (22), we partition the index $[n]$ for user k as follows:

$$\begin{aligned}\mathcal{I}_m^{(k)} &= \mathcal{H}_{V_k} \cap \mathcal{L}_{V_k|Y},\\ \mathcal{R}_m^{(k)} &= \mathcal{H}_{V_k} \cap (\mathcal{L}_{V_k|Y})^c,\\ \mathcal{D}_m^{(k)} &= (\mathcal{H}_{V_k})^c. \end{aligned} \tag{27}$$

The encoder computes $V_k^{1:n} = U_k^{1:n} G_n$ and generates the channel input $X_k^{1:n}$ according to the conditional probability $P_{X_k^{1:n}|V_k^{1:n}}$. Similar to (16), the scheme can achieve the rate pair (R_{m1}, R_{m2}) where

$$\begin{aligned} R_{m1} &= \lim_{n\to\infty} \frac{|\mathcal{I}_m^{(1)}|}{n},\\ R_{m2} &= \lim_{n\to\infty} \frac{|\mathcal{I}_m^{(2)}|}{n}. \end{aligned} \tag{28}$$

According to Section III-B, (R_{m1}, R_{m2}) is on the dominant face of (24), namely, $R_{m1} + R_{m2} = I(V_1V_2; Y)$.

2) THE EAVESDROPPER CHANNELS

User 1 is an eavesdropper who has access to the side information (V_1, X_1), whereas user 2 is an eavesdropper who has access to the side information (V_2, X_2). Let $d = \{1, 2\}\backslash k$, we define the following polarized sets

$$\begin{aligned} &\mathcal{H}_{V_k|V_dX_d}\\ &\quad = \{i \in [n] : Z(U_k^i | U_k^{1:i-1} V_d^{1:n} X_d^{1:n}) \geq 1 - \delta_n\},\\ &\mathcal{H}_{V_k|Y_dV_dX_d}\\ &\quad = \{i \in [n] : Z(U_k^i | U_k^{1:i-1} Z_d^{1:n} V_d^{1:n} X_d^{1:n}) \geq 1 - \delta_n\}, \end{aligned} \tag{29}$$

where $\frac{1}{n}|\mathcal{H}_{V_k|V_dX_d}| \to H(V_k|V_dX_d)$, and $\frac{1}{n}|\mathcal{H}_{V_k|Y_dV_dX_d}| \to H(V_k|Y_dV_dX_d)$, for sufficiently large n. Furthermore, $H_{V_k|V_dX_d}$ is equivalent to $\mathcal{H}_{V_k}$ given by (26), as $U_k^{1:n}$ is independent of $(V_d^{1:n}, X_d^{1:n})$.

Then partition the index $[n]$ as follows:

$$\begin{aligned} \mathcal{I}_e^{(k)} &= \mathcal{H}_{V_k|V_dX_d} \cap (\mathcal{H}_{V_k|Z_dV_dX_d})^c,\\ \mathcal{R}_e^{(k)} &= \mathcal{H}_{V_k|V_dX_d} \cap \mathcal{H}_{V_k|Z_dV_dX_d},\\ \mathcal{D}_e^{(k)} &= (\mathcal{H}_{V_k|V_dX_d})^c. \end{aligned} \tag{30}$$

Compared to (13) and (22), here exists a slight difference. In particular, we use the high-entropy set $\mathcal{H}_{V_k|Z_dV_dX_d}$ in the partition. Similar to (16), we have

$$\begin{aligned} R_{e1} &= \lim_{n\to\infty} \frac{|\mathcal{I}_e^{(1)}|}{n} = I(V_1; Z_2|V_2X_2),\\ R_{e2} &= \lim_{n\to\infty} \frac{|\mathcal{I}_e^{(2)}|}{n} = I(V_2; Z_1|V_1X_1). \end{aligned} \tag{31}$$

Note that, the polar codes defined here can be viewed as polar codes for two-user MACs that achieve the corner points.

For an arbitrary rate pair (R_{m1}, R_{m2}) on the dominant face of $\mathcal{R}_m$, define $R_1 \triangleq R_{m1} - R_{e1}$, and $R_2 \triangleq R_{m2} - R_{e2}$. It is clear that (R_1, R_2) is on the dominant face of $\mathcal{R}_S^{(1)}$, i.e., $R_1 + R_2 = R_C$.

3) CODING SCHEME FOR ACHIEVING $\mathcal{R}_S^{(1)}$

By combining (27) and (30), the index $[n]$ for user k can be partitioned as follows:

$$\begin{aligned} \mathcal{I}_a^{(k)} &= \mathcal{H}_{V_k} \cap \mathcal{L}_{V_k|Y} \cap \mathcal{H}_{V_k|Z_dV_dX_d},\\ \mathcal{I}_b^{(k)} &= \mathcal{H}_{V_k} \cap \mathcal{L}_{V_k|Y} \cap (\mathcal{H}_{V_k|Z_dV_dX_d})^c,\\ \mathcal{R}_a^{(k)} &= \mathcal{H}_{V_k} \cap (\mathcal{L}_{V_k|Y})^c \cap \mathcal{H}_{V_k|Z_dV_dX_d},\\ \mathcal{R}_b^{(k)} &= \mathcal{H}_{V_k} \cap (\mathcal{L}_{V_k|Y})^c \cap (\mathcal{H}_{V_k|Z_dV_dX_d})^c,\\ \mathcal{D}^{(k)} &= (\mathcal{H}_{V_k})^c. \end{aligned} \tag{32}$$

Due to symmetry, we mainly describe the coding scheme for user 1 in the following. A graphical representation of the partition for user 1 is illustrated in Fig. 2. The partition defined by (32) results into five distinct subsets as follows.

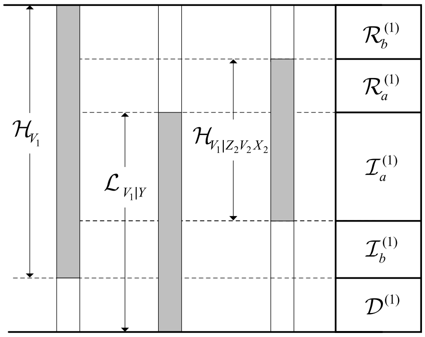

FIGURE 2. **Partition of the index [*n*] for user 1.**

- $\mathcal{I}_a^{(1)}$ is the subset good for user 1 but bad for user 2, which makes it suitable to store user 1's secret message.
- $\mathcal{I}_b^{(1)}$ is the subset good for both users. Uniformly distributed random bits are assigned to $\mathcal{I}_b^{(1)}$ such that user 2 cannot extract any useful information.
- $\mathcal{R}_a^{(1)}$ is the subset bad for both users. Uniformly distributed random bits are also assigned to $\mathcal{R}_a^{(1)}$. Further, these bits are assumed to be shared among all terminals.
- $\mathcal{R}_b^{(1)}$ is the subset bad for user 1 but good for user 2. In existing literature, chaining construction is a useful technique to deal with this subset.
- $\mathcal{D}^{(1)}$ contains the almost deterministic bits.

A chaining scheme is proposed as follows (see Fig. 3). Let $\mathcal{B}^{(1)}$ be an arbitrary subset of $\mathcal{I}_a^{(1)}$ with the size of $\mathcal{R}_b^{(1)}$. We can verify the existence of $\mathcal{B}^{(1)}$ by

$$\begin{aligned} \lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)} \backslash \mathcal{B}^{(1)}|}{n} &= \lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)}| - |\mathcal{R}_b^{(1)}|}{n}\\ &= \lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)} \cup \mathcal{I}_b^{(1)}| - |\mathcal{R}_b^{(1)} \cup \mathcal{I}_b^{(1)}|}{n}\\ &= \lim_{n\to\infty} \frac{|\mathcal{I}_m^{(1)}| - |\mathcal{I}_e^{(1)}|}{n} = R_1 > 0. \end{aligned} \tag{33}$$

Assume that the encoding scheme operates over m blocks and the notation $j \in [1, m]$ indicates the jth block. The encoding chain is formed in that, for $j \in [2, m]$, uniformly distributed random bits are placed in $\mathcal{B}^{(1)}$ in Block $(j - 1)$, and repeated

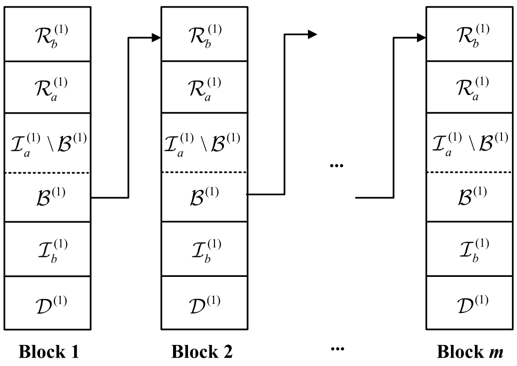

FIGURE 3. *m*-block chaining construction for user 1.

in $\mathcal{R}_b^{(1)}$ in Block j. The bits in $\mathcal{R}_b^{(1)}$ of Block 1 are secretly shared between user 1 and the receiver.

a: ENCODING SCHEME FOR USER 1

Let W_1^j be a vector of $|\mathcal{I}_a^{(1)} \setminus \mathcal{B}^{(1)}|$ uniformly distributed random bits, which represents the secret message. Let J_1 be a vector of $|\mathcal{R}_a^{(1)}|$ uniformly distributed random bits, which represents a source of common randomness available to all terminals. Let K_1 be a vector of $|\mathcal{R}_b^{(1)}|$ uniformly distributed random bits, which represents a secret seed shared by user 1 and the receiver. Let $\tilde{u}_1^{1:n}$ denote the realization of $U_1^{1:n}$ in Block j. Then user 1 forms $\tilde{u}_1^{1:n}$ as follows.

- $\tilde{u}_1^{1:n}[\mathcal{I}_a^{(1)} \setminus \mathcal{B}^{(1)}]$ stores the secret message W_1^j;
- $\tilde{u}_1^{1:n}[\mathcal{I}_b^{(1)} \cup \mathcal{B}^{(1)}]$ stores uniformly distributed random bits;
- $\tilde{u}_1^{1:n}[\mathcal{R}_a^{(1)}]$ stores the random vector J_1. We can reuse J_1 over blocks since $\mathcal{R}_a^{(1)} \subseteq \mathcal{H}_{V_1}$.
- $\tilde{u}_1^{1:n}[\mathcal{D}^{(1)}]$ are sampled from the conditional probability $P_{U_1^i|U_1^{1:i-1}}(u_1^i|u_1^{1:i-1})$.
- Let $\Phi_j \triangleq \tilde{u}_1^{1:n}[(\mathcal{H}_{V_1})^c \cap (\mathcal{L}_{V_1|Y})^c]$. We assume that Φ_j is secretly shared by user 1 and the receiver. Also note that, $|\Phi_j| = o(n)$.

The remaining $\mathcal{R}_b^{(1)}$ in Block j is determined by chaining construction:

- If $j = 1$, $\tilde{u}_1^{1:n}[\mathcal{R}_b^{(1)}]$ stores the secret seed K_1;
- Otherwise, $\tilde{u}_1^{1:n}[\mathcal{R}_b^{(1)}]$ is equal to $\tilde{u}_1^{1:n}[\mathcal{B}^{(1)}]$ of Block $(j-1)$.

Once $\tilde{u}_1^{1:n}$ is formed, user 1 computes $\tilde{v}_1^{1:n} = \tilde{u}_1^{1:n} G_n$. Finally, user 1 generates the channel input $\tilde{x}_1^{1:n}$ by transmitting $\tilde{v}_1^{1:n}$ through a virtual channel with conditional probability $p_{X_1^{1:n}|V_1^{1:n}}(\tilde{x}_1^{1:n}|\tilde{v}_1^{1:n})$.

Remark 4: The encoding scheme requires an amount of shared randomness, which includes J_1, K_1, and $\Phi^m \triangleq (\Phi_1, \ldots, \Phi_m)$. Specifically, J_1 is a source of common randomness available to all terminals, K_1 and Φ^m are known only to user 1 and the receiver. We will prove in Section V that the rate loss induced by the shared randomness is negligible as m, n goes to infinity. Moreover, we will show that reusing J_1 over different blocks does not harm strong secrecy.

b: ENCODING SCHEME FOR USER 2

The encoding scheme for user 2 is obtained by replacing the subscript 1 by 2. The shared randomness required by user 2 is similarly defined as J_2, K_2, and $\Psi^m \triangleq (\Psi_1, \ldots, \Psi_m)$.

c: DECODING

The receiver jointly decodes $\tilde{u}_1^{1:n}$ and $\tilde{u}_2^{1:n}$ starting from Block 1 and going forward to Block m. Let Y_j^n denote the channel outputs of Block j, and $S_j^{1:2n}$ denote the monotone permutation used in Block j. Recall that, U_k^i is mapped to $S^{l(k)}$, where $l(k) \in [2n]$.

The receiver decodes $\tilde{u}_1^{1:n}$ as follows. In Block 1, the receiver obtains $\tilde{u}_1^{1:n}[(\mathcal{L}_{V_1|Y})^c]$ via (J_1, K_1, Φ_1). Otherwise, the receiver obtains $\tilde{u}_1^{1:n}[(\mathcal{L}_{V_1|Y})^c]$ via (J_1, Φ_j) and $\hat{u}_1^{1:n}[\mathcal{B}^{(1)}]$ from Block $(j-1)$. The receiver then forms an estimate $\hat{u}_1^{1:n}$, and extracts $\hat{W}_1^j$ using the following SC decoder:

$$\hat{u}_1^i = \begin{cases} \tilde{u}_1^i, \text{ if } i \in (\mathcal{L}_{V_1|Y})^c \\ \arg \max\limits_{u \in \{0,1\}} P_{U_1^i|S^{1:l(1)-1}Y^{1:n}}(u|\hat{s}^{1:l(1)-1}y^{1:n}), \\ \qquad \text{if } i \in \mathcal{L}_{V_1|Y} \end{cases} \tag{34}$$

The receiver decodes $\tilde{u}_2^{1:n}$ using a similar SC decoder by replacing the subscript 1 by 2.

As discussed in Section III, the encoding and decoding complexity of the proposed scheme are $O(n \log n)$, and the construction complexity is $O(n)$.

B. CODING SCHEME FOR ACHIEVING $\mathcal{R}_S^{(2)}$

The target rate pair is $(R_A, 0)$, in which user 1 achieves a positive secrecy rate and user 2 has a secrecy rate of zero. We construct the coding scheme as follows. Instead of remaining silent, user 2 performs the coding scheme for single-user channels as described in Section III. The signals transmitted by user 2 do not store any secret message. User 1 treats user 2 as an eavesdropper, and perform the usual wiretap coding scheme. Note that, a similar scheme was proposed for the MAWC in [20], where user 2's transmission is termed as cooperative jamming.

a: ENCODING SCHEME FOR USER 2

Define $U_2^{1:n} = V_2^{1:n} G_n$. Consider the following polarized sets:

$$\begin{aligned} \mathcal{H}_{V_2} &= \{i \in [n] : Z(U_2^i|U_2^{1:i-1}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{V_2|Y} &= \{i \in [n] : Z(U_2^i|U_2^{1:i-1}Y^n) \leq \delta_n\}. \end{aligned} \tag{35}$$

We partition the index $[n]$ as follows:

$$\begin{aligned} \mathcal{I}^{(2)} &= \mathcal{H}_{V_2} \cap \mathcal{L}_{V_2|Y}, \\ \mathcal{R}^{(2)} &= \mathcal{H}_{V_2} \cap (\mathcal{L}_{V_2|Y})^c, \\ \mathcal{D}^{(2)} &= (\mathcal{H}_{V_2})^c. \end{aligned} \tag{36}$$

User 2 aims to transmit the codeword to the receiver which does not store any secret message. Let J_2 be a vector of $|\mathcal{R}^{(2)}|$ uniformly distributed random bits shared by user 2 and the receiver. The encoding scheme operates over m blocks.

Let $\tilde{u}_2^{1:n}$ denote the realization of $U_2^{1:n}$ in Block j. The encoder forms $\tilde{u}_2^{1:n}$ as follows.

- $\tilde{u}_2^{1:n}[\mathcal{I}]$ stores uniformly distributed random bits.
- $\tilde{u}_2^{1:n}[\mathcal{R}]$ stores the vector J_2. Note that we reuse J_2 over different blocks. The rate loss is made negligible by sufficiently large m.
- $\tilde{u}_2^{1:n}[\mathcal{D}]$ contains almost deterministic bits sampled from the conditional probability $P_{U_2^i|U_2^{1:i-1}}(u_2^i|u_2^{1:i-1})$.
- Let $\Psi_j \triangleq \tilde{u}_2^{1:n}[(\mathcal{H}_{V_2})^c \cap (\mathcal{L}_{V_2|Y})^c]$. User 2 transmits Ψ_j additionally to the receiver with some reliable error-correcting codes. Note that $|\Psi_j| = o(n)$.

Once $\tilde{u}_2^{1:n}$ is formed, user 2 computes $\tilde{v}_2^{1:n} = \tilde{u}_2^{1:n}G_n$, and generates the channel inputs $\tilde{x}_2^{1:n}$ according to the conditional probability $p_{X_2^{1:n}|V_2^{1:n}}(\tilde{x}_2^{1:n}|\tilde{v}_2^{1:n})$.

b: ENCODING SCHEME FOR USER 1

Define $U_1^{1:n} = V_1^{1:n}G_n$. Consider the following polarized sets:

$$\begin{aligned}
\mathcal{H}_{V_1|V_2} &= \{i \in [n] : Z(U_1^i|U_1^{1:i-1}V_2^{1:n}) \geq 1-\delta_n\},\\
\mathcal{L}_{V_1|YV_2} &= \{i \in [n] : Z(U_1^i|U_1^{1:i-1}Y^{1:n}V_2^{1:n}) \leq \delta_n\},\\
\mathcal{H}_{V_1|Z_2V_2X_2} &= \{i \in [n] : Z(U_1^i|U_1^{1:i-1}Z_2^{1:n}V_2^{1:n}X_2^{1:n}) \geq 1-\delta_n\}.
\end{aligned} \tag{37}$$

We partition the index $[n]$ as follows:

$$\begin{aligned}
\mathcal{I}_a^{(1)} &= \mathcal{H}_{V_1|V_2} \cap \mathcal{L}_{V_1|YV_2} \cap \mathcal{H}_{V_1|Z_2V_2X_2},\\
\mathcal{I}_b^{(1)} &= \mathcal{H}_{V_1|V_2} \cap \mathcal{L}_{V_1|YV_2} \cap (\mathcal{H}_{V_1|Z_2V_2X_2})^c,\\
\mathcal{R}_a^{(1)} &= \mathcal{H}_{V_1|V_2} \cap (\mathcal{L}_{V_1|YV_2})^c \cap \mathcal{H}_{V_1|Z_2V_2X_2},\\
\mathcal{R}_b^{(1)} &= \mathcal{H}_{V_1|V_2} \cap (\mathcal{L}_{V_1|YV_2})^c \cap (\mathcal{H}_{V_1|Z_2V_2X_2})^c,\\
\mathcal{D}^{(1)} &= (\mathcal{H}_{V_1|V_2})^c.
\end{aligned} \tag{38}$$

Similar to (16), we obtain the following results.

$$\begin{aligned}
\lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)} \cup \mathcal{I}_b^{(1)}|}{n} &= \lim_{n\to\infty} \frac{|\mathcal{H}_{V_1|V_2} \cap \mathcal{L}_{V_1|YV_2}|}{n}\\
&= I(V_1; Y|V_2), \qquad (39)\\
\lim_{n\to\infty} \frac{|\mathcal{I}_b^{(1)} \cup \mathcal{R}_b^{(1)}|}{n} &= \lim_{n\to\infty} \frac{|\mathcal{H}_{V_1} \cap (\mathcal{H}_{V_1|Z_2V_2X_2})^c|}{n}\\
&= I(V_1; Z_2V_2X_2)\\
&= I(V_1; V_2X_2) + I(V_1; Z_2|V_2X_2)\\
&= I(V_1; Z_2|V_2X_2), \qquad (40)
\end{aligned}$$

where (40) holds by the independence of V_1 and (V_2, X_2).

Assume that the encoding scheme operates over m blocks. Chaining construction is applied to deal with $\mathcal{R}_b^{(1)}$. Let $\mathcal{B}^{(1)}$ be an arbitrary subset of $\mathcal{I}_a^{(1)}$ with the size of $\mathcal{R}_b^{(1)}$. Similar to (33), the existence of $\mathcal{B}^{(1)}$ is ensured by

$$\begin{aligned}
\lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)} \backslash \mathcal{B}^{(1)}|}{n} &= \lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)}| - |\mathcal{R}_b^{(1)}|}{n}\\
&= \lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)} \cup \mathcal{I}_b^{(1)}| - |\mathcal{R}_b^{(1)} \cup \mathcal{I}_b^{(1)}|}{n}\\
&= I(V_1; Y|V_2) - I(V_1; Z_2|V_2X_2).
\end{aligned} \tag{41}$$

The encoding procedure is similar to that described in Section IV-A, which we omit here for conciseness.

c: DECODING

The receiver first decodes $\tilde{u}_2^{1:n}$ using a similar SC decoder as described in Section III-A. The receiver then computes $\hat{v}_2^{1:n} = \hat{u}_2^{1:n}G_n$, and proceeds to decode $\tilde{u}_1^{1:n}$ using a similar SC decoder as described in Section IV-A.

V. ANALYSIS OF THE PROPOSED SCHEME

We provide in this section an analysis of the coding scheme described in Section IV, which leads to the following theorem.

Theorem 2: For a discrete memoryless MAC-CM given by $(\mathcal{X}_1 \times \mathcal{X}_2, p_{YZ_1Z_2|X_1X_2}, \mathcal{Y} \times \mathcal{Z}_1 \times \mathcal{Z}_2)$, where $|\mathcal{X}_1| = 2$, $|\mathcal{X}_2| = 2$, the polar coding scheme described in Section IV *achieves the secrecy rate region $\mathcal{R}_S$ given in Theorem 1 satisfying strong secrecy.*

A. ANALYSIS OF THE SCHEME ACHIEVING $\mathcal{R}_S^{(1)}$

1) TRANSMISSION RATES

For user k, the secret message W_k^j is assigned to $|\mathcal{I}_a^{(k)} \backslash \mathcal{B}^{(k)}|$ in Block j. According to (33), we have

$$\begin{aligned}
\lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)} \backslash \mathcal{B}^{(1)}|}{n} &= R_1,\\
\lim_{n\to\infty} \frac{|\mathcal{I}_a^{(2)} \backslash \mathcal{B}^{(2)}|}{n} &= R_2,
\end{aligned} \tag{42}$$

where (R_1, R_2) is on the dominant face of $\mathcal{R}_S^{(1)}$.

The rate of the shared randomness for user 1 is

$$\begin{aligned}
\frac{|(J_1, K_1, \Phi^m)|}{nm} &= \frac{|\mathcal{R}_a^{(1)} \cup \mathcal{R}_b^{(1)}| + m|\Phi_j|}{nm}\\
&= \frac{|\mathcal{H}_{V_1} \cap (\mathcal{L}_{V_1|Y})^c|}{nm} + \frac{o(n)}{n}\\
&\xrightarrow{n\to\infty} \frac{|\mathcal{H}_{V_1|Y}|}{m}\\
&\xrightarrow{m\to\infty} 0.
\end{aligned} \tag{43}$$

Similarly for user 2, we have $\frac{|(J_2,K_2,\Psi^m)|}{nm} \xrightarrow{m,n\to\infty} 0$. Overall, the rate of shared randomness is negligible as m, n goes to infinity.

2) VARIATION DISTANCE

The joint distribution induced by the coding scheme is not exactly the same as the target joint distribution. The following lemma provides an upper bound on the total variation distance between these two distributions.

Lemma 1: Let $p_{(\tilde{V}_1^{1:n}\tilde{V}_2^{1:n}\tilde{X}_1^{1:n}\tilde{X}_2^{1:n}\tilde{Y}^{1:n}\tilde{Z}_1^{1:n}\tilde{Z}_2^{1:n})_j}$ denote the induced joint distribution in Block $j \in [1, m]$. We have

$$\begin{aligned}
\mathbb{V}(&p_{V_1^{1:n}V_2^{1:n}X_1^{1:n}X_2^{1:n}Y^{1:n}Z_1^{1:n}Z_2^{1:n}},\\
&\qquad p_{(\tilde{V}_1^{1:n}\tilde{V}_2^{1:n}\tilde{X}_1^{1:n}\tilde{X}_2^{1:n}\tilde{Y}^{1:n}\tilde{Z}_1^{1:n}\tilde{Z}_2^{1:n})_j}) \leq \eta_n,
\end{aligned}$$

where $\eta_n \triangleq 4\sqrt{\ln 2}\sqrt{n\delta_n}$.

Proof: For conciseness, we omit the subscript j in the induced joint distribution. Following similar steps as [23], we can bound $\mathbb{D}(p_{V_1^{1:n}}||p_{\tilde{V}_1^{1:n}})$ as follows.

$$\begin{aligned}
\mathbb{D}(p_{V_1^{1:n}}||p_{\tilde{V}_1^{1:n}}) &\overset{(a)}{=} \mathbb{D}(p_{U_1^{1:n}}||p_{\tilde{U}_1^{1:n}}) \\
&\overset{(b)}{=} \sum_{i=1}^{n} \mathbb{D}(p_{U_1^i|U_1^{1:i-1}}||p_{\tilde{U}_1^i|\tilde{U}_1^{1:i-1}}) \\
&\overset{(c)}{=} \sum_{i\in\mathcal{H}_{V_1}} \left[1 - H(U_1^i|U_1^{1:i-1})\right] \\
&\overset{(d)}{\leq} \sum_{i\in\mathcal{H}_{V_1}} \left[1 - Z^2(U_1^i|U_1^{1:i-1})\right] \\
&\overset{(e)}{\leq} 2|\mathcal{H}_{V_1}|\delta_n \leq 2n\delta_n, \qquad (44)
\end{aligned}$$

where (a) holds by the polar transform $U_1^{1:n} = V_1^{1:n}G_n$ and the invertibility of G_n, (b) holds by the chain rule for the divergence, (c) holds by the uniformity of the bits stored in $\mathcal{H}_{V_1}$, (d) holds by the relationship between the entropy and Bhattacharyya parameter, (e) holds by the definition of $\mathcal{H}_{V_1}$.

Similarly, we have

$$\mathbb{D}(p_{V_2^{1:n}}||p_{\tilde{V}_2^{1:n}}) \leq 2n\delta_n. \qquad (45)$$

For the considered model, we have

$$\begin{aligned}
p_{X_1^{1:n}|V_1^{1:n}}p_{X_2^{1:n}|V_2^{1:n}} &= p_{\tilde{X}_1^{1:n}|\tilde{V}_1^{1:n}}p_{\tilde{X}_2^{1:n}|\tilde{V}_2^{1:n}}, \\
p_{Y^{1:n}Z_1^{1:n}Z_2^{1:n}|X_1^{1:n}X_2^{1:n}} &= p_{\tilde{Y}^{1:n}\tilde{Z}_1^{1:n}\tilde{Z}_2^{1:n}|\tilde{X}_1^{1:n}\tilde{X}_2^{1:n}}. \qquad (46)
\end{aligned}$$

Now we bound the total variation distance between two joint distributions as follows.

$$\begin{aligned}
&\mathbb{V}(p_{V_1^{1:n}V_2^{1:n}X_1^{1:n}X_2^{1:n}Y^{1:n}Z_1^{1:n}Z_2^{1:n}}, \\
&\qquad p_{\tilde{V}_1^{1:n}\tilde{V}_2^{1:n}\tilde{X}_1^{1:n}\tilde{X}_2^{1:n}\tilde{Y}^{1:n}\tilde{Z}_1^{1:n}\tilde{Z}_2^{1:n}}) \\
&\overset{(a)}{=} \mathbb{V}(p_{V_1^{1:n}}p_{V_2^{1:n}}, p_{\tilde{V}_1^{1:n}}p_{\tilde{V}_2^{1:n}}) \\
&\overset{(b)}{\leq} \mathbb{V}(p_{V_1^{1:n}}p_{V_2^{1:n}}, p_{\tilde{V}_1^{1:n}}p_{V_2^{1:n}}) \\
&\quad + \mathbb{V}(p_{\tilde{V}_1^{1:n}}p_{V_2^{1:n}}, p_{\tilde{V}_1^{1:n}}p_{\tilde{V}_2^{1:n}}) \\
&\overset{(c)}{=} \mathbb{V}(p_{V_1^{1:n}}, p_{\tilde{V}_1^n 1:n}) + \mathbb{V}(p_{V_2^{1:n}}, p_{\tilde{V}_2^{1:n}}) \\
&\overset{(d)}{\leq} 4\sqrt{\ln 2}\sqrt{n\delta_n}, \qquad (47)
\end{aligned}$$

where (a) follows from (46) and [30, Lemma 17], (b) follows from the triangle inequality, (c) follows from [30, Lemma 17], (d) follows from Pinsker's inequality and (44), (45). ■

3) ERROR PROBABILITY

Let $\mathbb{P}_j^{(k)}$ denotes the error probability of decoding the secret message W_k^j in Block j. We first bound $\mathbb{P}_j^{(1)}$ in the following.

Define the error event:

$$\mathcal{E}_{V_1Y,j} \triangleq \{(V_1^{1:n}Y^{1:n}) \neq (\tilde{V}_1^{1:n}\tilde{Y}^{1:n})_j\}.$$

By using the coupling approach [31, Lemma 3.6] and Lemma 1, we can bound $\mathbb{P}(\mathcal{E}_{V_1Y,j})$ by

$$\mathbb{P}(\mathcal{E}_{V_1Y,j}) = \mathbb{V}(p_{V_1^{1:n}Y^{1:n}}, p_{(\tilde{V}_1 1:n\tilde{Y}^{1:n})_j}) \leq \eta_n. \qquad (48)$$

Define the error event:

$$\mathcal{E}_{c,j} \triangleq \{(\tilde{U}_1^{1:n}[\mathcal{B}^{(1)}])_{j-1} \neq (\hat{U}_1^{1:n}[\mathcal{B}^{(1)}])_{j-1}\}.$$

Note that $\mathcal{E}_{c,1} = \varnothing$. Obviously, we have

$$\mathbb{P}(\mathcal{E}_{c,j}) \leq \mathbb{P}[(\tilde{U}_1^{1:n})_{j-1} \neq (\hat{U}_1^{1:n})_{j-1}]. \qquad (49)$$

Define $\mathcal{E}_j \triangleq \mathcal{E}_{V_1Y,j} \cup \mathcal{E}_{c,j}$. We bound $\mathbb{P}_j^{(1)}$ as follows.

$$\begin{aligned}
\mathbb{P}_j^{(1)} &\leq \mathbb{P}[(\tilde{U}_1^{1:n})_j \neq (\hat{U}_1^{1:n})_j] \\
&= \mathbb{P}[(\tilde{U}_1^{1:n})_j \neq (\hat{U}_1^{1:n})_j|\mathcal{E}_j]\mathbb{P}(\mathcal{E}_j) \\
&\quad + \mathbb{P}[(\tilde{U}_1^{1:n})_j \neq (\hat{U}_1^{1:n})_j|\mathcal{E}_j^c]\mathbb{P}(\mathcal{E}_j^c) \\
&\leq \mathbb{P}(\mathcal{E}_j) + \mathbb{P}[(\tilde{U}_1^{1:n})_j \neq (\hat{U}_1^{1:n})_j|\mathcal{E}_j^c] \\
&\overset{(a)}{\leq} \mathbb{P}(\mathcal{E}_j) + n\delta_n \\
&\leq \mathbb{P}(\mathcal{E}_{V_1Y,j}) + \mathbb{P}(\mathcal{E}_{c,j}) + n\delta_n \\
&\overset{(b)}{\leq} \eta_n + \mathbb{P}[(\tilde{U}_1^{1:n})_{j-1} \neq (\hat{U}_1^{1:n})_{j-1}] + n\delta_n \\
&\overset{(c)}{\leq} (j-1)(\eta_n + n\delta_n) + \mathbb{P}[(\tilde{U}_1^{1:n})_1 \neq (\hat{U}_1^{1:n})_1], \qquad (50)
\end{aligned}$$

where (a) follows from the error probability of a standard SC decoder, (b) follows from (48) and (49), (c) follows from induction. The last term in (50) can be similarly bounded as follows.

$$\begin{aligned}
&\mathbb{P}[(\tilde{U}_1^{1:n})_1 \neq (\hat{U}_1^{1:n})_1] \\
&\quad = \mathbb{P}[(\tilde{U}_1^{1:n})_1 \neq (\hat{U}_1^{1:n})_1|\mathcal{E}_1]\mathbb{P}(\mathcal{E}_1) \\
&\qquad + \mathbb{P}[(\tilde{U}_1^{1:n})_1 \neq (\hat{U}_1^{1:n})_1|\mathcal{E}_1^c]\mathbb{P}(\mathcal{E}_1^c) \\
&\quad \leq \mathbb{P}(\mathcal{E}_1) + \mathbb{P}[(\tilde{U}_1^{1:n})_1 \neq (\hat{U}_1^{1:n})_1|\mathcal{E}_1^c]\mathbb{P}(\mathcal{E}_1^c) \\
&\quad = \mathbb{P}(\mathcal{E}_{V_1Y,1}) + \mathbb{P}[(\tilde{U}_1^{1:n})_1 \neq (\hat{U}_1^{1:n})_1|\mathcal{E}_1^c]\mathbb{P}(\mathcal{E}_1^c) \\
&\quad \leq \eta_n + n\delta_n. \qquad (51)
\end{aligned}$$

Substituting (51) into (50), we obtain

$$\mathbb{P}_j^{(1)} \leq j(\eta_n + n\delta_n). \qquad (52)$$

Similarly, we can bound $\mathbb{P}_j^{(2)} \leq j(\eta_n + n\delta_n)$. Finally, we bound the overall error probability $\mathbb{P}_e$ as follows.

$$\begin{aligned}
\mathbb{P}_e \leq \sum_{j=1}^{m}[\mathbb{P}_j^{(1)} + \mathbb{P}_j^{(2)}] &\leq 2\sum_{j=1}^{m} j(\eta_n + n\delta_n) \\
&= m(m+1)(\eta_n + n\delta_n). \qquad (53)
\end{aligned}$$

Hence, the receiver can decode the secret messages with arbitrarily small error probability.

4) INFORMATION LEAKAGE

Without loss of generality, we consider the information leakage of user 1. First, we introduce some necessary notations. Let $W_1^{1:m} \triangleq (W_1^1, \ldots, W_1^m)$, $\boldsymbol{X}_2^{1:m} \triangleq [(X_2^n)_1, \ldots, (X_2^n)_m]$ and $\boldsymbol{Z}_2^{1:m} \triangleq [(Z_2^n)_1, \ldots, (Z_2^n)_m]$. Recall that J_1 is the common randomness available to all terminals. Then the information leakage of $W_1^{1:m}$ is measured by

$$\mathbb{L}_1 = I(W_1^{1:m}; \boldsymbol{Z}_2^{1:m}\boldsymbol{X}_2^{1:m}J_1). \qquad (54)$$

Lemma 2: For $j \in [1, m]$, we define

$$(\mathbb{L}_1)_j = I(W_1^{1:m}; \boldsymbol{Z}_2^{j:m}\boldsymbol{X}_2^{j:m}J_1).$$

Let $\theta_n \triangleq 2n\delta_n + \eta_n(n - \log \eta_n)$.

- If $j \in [1, m-1]$, we have $(\mathbb{L}_1)_j - (\mathbb{L}_1)_{j+1} \leq 2\theta_n$;
- If $j = m$, we have $(\mathbb{L}_1)_m \leq \theta_n$.

Proof: See Appendix. ■

By using Lemma 2, we can bound (54) as follows.

$$\begin{aligned} \mathbb{L}_1 &= (\mathbb{L}_1)_m + \sum_{j=1}^{m-1}[(\mathbb{L}_1)_j - (\mathbb{L}_1)_{j+1}] \\ &\leq \theta_n + 2(m-1)\theta_n \\ &= (2m-1)\theta_n. \end{aligned} \tag{55}$$

The information leakage vanishes as n goes to infinity, such that strong secrecy (5) is satisfied.

B. ANALYSIS OF THE SCHEME ACHIEVING $\mathcal{R}_S^{(2)}$

1) TRANSMISSION RATES

User 2 achieves a secrecy rate of zero, whereas the rate of user 1's secret message is given by (41)

$$\lim_{n\to\infty} \frac{|\mathcal{I}_a^{(1)} \backslash \mathcal{B}^{(1)}|}{n} = R_A. \tag{56}$$

Similar to (43), the rate of shared randomness is negligible as n, m goes to infinity.

2) VARIATION DISTANCE

Since user 2 does not transmit any secret message, we set $Z_1 = \varnothing$. Then we have the following result similar to Lemma 1, namely, for $j \in [1, m]$,

$$\mathbb{V}(p_{V_1^{1:n}V_2^{1:n}X_1^{1:n}X_2^{1:n}Y^{1:n}Z_2^{1:n}}, p_{(\tilde{V}_1^{1:n}\tilde{V}_2^{1:n}\tilde{X}_1^{1:n}\tilde{X}_2^{1:n}\tilde{Y}^{1:n}\tilde{Z}_2^{1:n})_j}) \leq \eta_n. \tag{57}$$

3) ERROR PROBABILITY

The receiver decodes first user 2's codeword, and then user 1's secret message. Similar to (53), we can show that

$$\mathbb{P}_e \leq \sum_{j=1}^{m} \mathbb{P}_j^{(1)} \leq \frac{m(m+1)}{2}\left(\eta_n + n\delta_n\right). \tag{58}$$

4) INFORMATION LEAKAGE

User 1 transmits the secret message to the receiver while user 2 being the eavesdropper. With notations unchanged, we can show by Lemma 2 that

$$\begin{aligned} \mathbb{L}_1 &= I(W_1^{1:m}; \boldsymbol{Z}_2^{1:m}\boldsymbol{X}_2^{1:m}J_1) \\ &\leq (2m-1)\theta_n. \end{aligned} \tag{59}$$

VI. CONCLUSION

In this paper, we proposed an explicit polar coding scheme for the MAC-CM based on monotone chain rules. We proved that the best-known achievable secrecy rate region for the MAC-CM can be achieved by polar codes satisfying strong secrecy. In this paper, feedback signals are only considered as the cause of information leakage. In fact, they can also be leveraged for user cooperation. The interaction between cooperation and secrecy in the MAC-CM has been studied in [32], which introduced an achievable scheme based on compress-and-forward. Polar coding design for this scenario is left for future work.

APPENDIX

PROOF OF LEMMA 1

We start by proving the following lemma. Recall that $\mathcal{B}^{(1)}$ in Block j is chained to $\mathcal{R}_b^{(1)}$ in Block $(j+1)$. For notational convenience, we define $F^j \triangleq \tilde{\boldsymbol{U}}_1^j[\mathcal{R}_b^{(1)}]$ for $j \in [1, m]$.

Lemma 3: For $j \in [1, m]$, we have

$$I(W_1^j F^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j | J_1) \leq \theta_n,$$

where $\theta_n \triangleq 2n\delta_n + \eta_n(n - \log \eta_n)$.

Proof:

$$\begin{aligned} I(W_1^j F^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j | J_1) &\overset{(a)}{\leq} I(W_{1,j}F_{j+1}J_1; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j) \\ &\overset{(b)}{\leq} I(\tilde{\boldsymbol{U}}_1^j[\mathcal{H}_{V_1|Z_2V_2X_2}]; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j) \\ &= H(\tilde{\boldsymbol{U}}_1^j[\mathcal{H}_{V_1|Z_2V_2X_2}]) \\ &\quad - H(\tilde{\boldsymbol{U}}_1^j[\mathcal{H}_{V_1|Z_2V_2X_2}] | \boldsymbol{Z}_2^j\boldsymbol{X}_2^j), \end{aligned} \tag{60}$$

where (a) holds by the chain rule for mutual information, (b) holds by the encoding scheme, and the fact that $\mathcal{I}_a^{(1)} \cup \mathcal{R}_b^{(1)} = \mathcal{H}_{V_1|Y_2V_2X_2}$.

We bound the last term in (60) as follows.

$$\begin{aligned} &|H(\boldsymbol{U}_1^j[\mathcal{H}_{V_1|Z_2V_2X_2}] | \boldsymbol{Z}_2^j\boldsymbol{X}_2^j) - H(\tilde{\boldsymbol{U}}_1^j[\mathcal{H}_{V_1|Z_2V_2X_2}] | \boldsymbol{Z}_2^j\boldsymbol{X}_2^j)| \\ &\overset{(a)}{\leq} \mathbb{V}(p_{V_1^nV_2^nX_2^nZ_2^n}, p_{(\tilde{V}_1^n\tilde{V}_2^nX_2^nZ_2^n)_j}) \\ &\qquad \times \log \frac{2^n}{\mathbb{V}(p_{V_1^nV_2^nX_2^nZ_2^n}, p_{(\tilde{V}_1^n\tilde{V}_2^nX_2^nZ_2^n)_j})} \\ &\overset{(b)}{\leq} \eta_n(n - \log \eta_n), \end{aligned} \tag{61}$$

where (a) holds by [33, Theorem 17.3.3], (b) holds by Lemma 1 and the fact that $f(x) \overset{\Delta}{=} x(n - \log x)$ is an increasing function for $x \in (0, 1)$.

Let $\gamma_n \triangleq \eta_n(n - \log \eta_n)$. By (61), we have

$$\begin{aligned} &H(\tilde{\boldsymbol{U}}_1^j[\mathcal{H}_{V_1|Z_2V_2X_2}] | \boldsymbol{Z}_2^j\boldsymbol{X}_2^j) \\ &\geq H(\boldsymbol{U}_1^j[\mathcal{H}_{V_1|Z_2V_2X_2}] | \boldsymbol{Z}_2^j\boldsymbol{X}_2^j) - \gamma_n \\ &\overset{(a)}{\geq} \sum_{i \in \mathcal{H}_{V_1|Z_2V_2X_2}} H[(U_1^i)_j | (U_1^{1:i-1})_j \boldsymbol{Z}_2^j\boldsymbol{X}_2^j] - \gamma_n \\ &\overset{(b)}{\geq} \sum_{i \in \mathcal{H}_{V_1|Z_2V_2X_2}} Z^2[(U_1^i)_j | (U_1^{1:i-1})_j \boldsymbol{Z}_2^j\boldsymbol{X}_2^j] - \gamma_n \\ &\geq |\mathcal{H}_{V_1|Z_2V_2X_2}|(1 - 2\delta_n) - \gamma_n, \end{aligned} \tag{62}$$

where (a) holds by the fact that conditioning reduces entropy, and (b) holds by the inequality $H(X|Y) \geq Z^2(X|Y)$ [29, Proposition 2].

Substituting (62) into (60), we finally have

$$\begin{aligned} I(W_1^jF^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|J_1) &\leq 2|\mathcal{H}_{U|Z_2VX_2}|\delta_n + \gamma_n \\ &\leq 2n\delta_n + \gamma_n. \end{aligned} \tag{63}$$

■

For $j \in [1, m-1]$, we bound $(\mathbb{L}_1)_j - (\mathbb{L}_1)_{j+1}$ as follows.

$$\begin{aligned} (\mathbb{L}_1)_j - (\mathbb{L}_1)_{j+1} &= I(W_1^{1:m}; \boldsymbol{Z}_2^{j:m}\boldsymbol{X}_2^{j:m}J_1) \\ &\quad - I(W_1^{1:m}; \boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}J_1) \\ &\overset{(a)}{=} I(W_1^{1:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}J_1) \\ &\overset{(b)}{=} I(W_1^{1:j-1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}W_1^{j:m}J_1) \\ &\quad + I(W_1^{j:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}J_1) \\ &\overset{(c)}{\leq} I(W_1^{1:j-1}; \boldsymbol{Z}_2^{j:m}\boldsymbol{X}_2^{j:m}W_1^{j:m}|J_1) \\ &\quad + I(W_1^{j:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|J_1) \\ &\overset{(d)}{=} I(W_1^{j:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|J_1) \\ &= I(W_1^{j+1:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|W_1^jJ_1) \\ &\quad + I(W_1^j; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|J_1) \\ &\overset{(e)}{\leq} I(W_1^{j+1:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|W_1^jJ_1) \\ &\quad + \theta_n, \end{aligned} \tag{64}$$

where (a), (b) and (c) hold by the chain rule for mutual information, (d) holds by the independence of $W_1^{1:j-1}$ and $(\boldsymbol{Z}_2^{j:m}\boldsymbol{X}_2^{j:m}W_1^{j:m}J_1)$, (e) follows from Lemma 3.

We bound the first term in (64) as follows.

$$\begin{aligned} &I(W_1^{j+1:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|W_1^jJ_1) \\ &\overset{(a)}{\leq} I(W_1^{j+1:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^jW_1^j|J_1) \\ &\overset{(b)}{\leq} I(W_1^{j+1:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}F^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^jW_1^j|J_1) \\ &\overset{(c)}{=} I(W_1^{j+1:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^jW_1^j|F^{j+1}J_1) \\ &\quad + I(F^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^jW_1^j|J_1) \\ &\overset{(d)}{=} I(F^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^jW_1^j|J_1) \\ &= I(F^{j+1}; W_1^j|J_1) + I(F^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|W_1^jJ_1) \\ &\overset{(e)}{=} I(F^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|W_1^jJ_1) \\ &\leq I(W_1^jF^{j+1}; \boldsymbol{Z}_2^j\boldsymbol{X}_2^j|J_1) \\ &\overset{(f)}{\leq} \theta_n, \end{aligned} \tag{65}$$

where (a), (b) and (c) holds by the chain rule for mutual information, (d) holds by the fact that the chaining construction induces the Markov chain $(\boldsymbol{Z}_2^j\boldsymbol{X}_2^jW_1^j) \rightarrow (F^{j+1}J_1) \rightarrow (W_1^{j+1:m}\boldsymbol{Z}_2^{j+1:m}\boldsymbol{X}_2^{j+1:m})$, (e) holds since F^{j+1} is independent of $(W_1^jJ_1)$, (f) holds by Lemma 3.

Substituting (65) ino (64), we have

$$(\mathbb{L}_1)_j - (\mathbb{L}_1)_{j+1} \leq 2\theta_n. \tag{66}$$

Similarly, we bound $(\mathbb{L}_1)_m$ as follows.

$$\begin{aligned} (\mathbb{L}_1)_m &= I(W_1^{1:m}; \boldsymbol{Z}_2^m\boldsymbol{X}_2^mJ_1) \\ &= I(W_1^{1:m-1}; \boldsymbol{Z}_2^m\boldsymbol{X}_2^mJ_1|W_1^m) \\ &\quad + I(W_1^m; \boldsymbol{Z}_2^m\boldsymbol{X}_2^mJ_1) \\ &\overset{(a)}{=} I(W_1^m; \boldsymbol{Z}_2^m\boldsymbol{X}_2^mJ_1) \overset{(b)}{\leq} \theta_n, \end{aligned} \tag{67}$$

where (a) holds since $W_1^{1:m-1}$ is independent of $(\boldsymbol{Z}_2^m\boldsymbol{X}_2^m W_1^mJ_1)$, and (b) holds by Lemma 3.

REFERENCES

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[2] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. Mclaughlin, and J. Barros, "Coding for secrecy: An overview of error–control coding techniques for physical–layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Select. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[4] Y. Liang and H. V. Poor, "Multiple–access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[5] R. Liu, Y. Liang, and H. V. Poor, "Fading cognitive multiple–access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4992–5005, Aug. 2011.

[6] E. Arikan, "Channel polarization: A method for constructing capacity–achieving codes for symmetric binary–input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[7] E. Sasoglu, E. Telatar, and E. M. Yeh, "Polar codes for the two–user multiple–access channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6583–6592, Oct. 2013.

[8] E. Abbe and E. Telatar, "Polar codes for the m-user multiple access channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5437–5448, Aug. 2012.

[9] R. Nasser and E. Telatar, "Polar codes for arbitrary DMCs and arbitrary MACs," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 2917–2936, Jun. 2016.

[10] S. Önay, "Successive cancellation decoding of polar codes for the two-user binary-input MAC," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 1122–1126.

[11] H. Mahdavifar, M. El-Khamy, J. Lee, and I. Kang, "Achieving the uniform rate region of general multiple access channels by polar coding," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 467–478, Feb. 2016.

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

[13] E. Hof and S. Shamai (Shitz), "Secrecy-achieving polar-coding," in *Proc. IEEE Inf. Theory Workshop*, Dublin, Ireland, Aug. 2010, pp. 1–5.

[14] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[15] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. Inf. Forensics Security.*, vol. 7, no. 5, pp. 1472–1483, Oct. 2012.

[16] Y.-P. Wei and S. Ulukus, "Polar coding for the general wiretap channel with extensions to multiuser scenarios," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 2, pp. 278–291, Feb. 2016.

[17] T. C. Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," *IEEE Trans. Inf. Theory*, vol. 63, no. 2, pp. 1311–1324, Feb. 2017.

[18] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.

[19] E. Arıkan, "Polar coding for the Slepian-Wolf problem based on monotone chain rules," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 566–570.

[20] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7903–7921, Dec. 2018.

[21] M. Zheng, M. Tao, W. Chen, and C. Ling, "Secure polar coding for the two-way wiretap channel," *IEEE Access*, vol. 6, pp. 21731–21744, Mar. 2018.

[22] M. Zheng, W. Chen, and C. Ling, "Polar coding for the cognitive interference channel with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 762–774, Apr. 2018.

[23] H. Wang, X. Tao, N. Li, and Z. Han, "Polar coding for the wiretap channel with shared key," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1351–1360, Jun. 2018.

[24] J. D. O. Alos and J. R. Fonollosa, "Polar coding for common message only wiretap broadcast channel," 2019, *arXiv:1901.07649*. [Online]. Available: https://arxiv.org/abs/1901.07649

[25] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[26] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology* (Lecture Notes in Computer Science). Bruges, Belgium: Springer-Verlag, 2000, pp. 351–368.

[27] M. Mondelli, S. H. Hassani, I. Sason, and R. L. Urbanke, "Achieving Marton's region for broadcast channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 783–800, Feb. 2014.

[28] J. Honda and H. Yamamoto, "Polar coding without alphabet extension for asymmetric models," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7829–7838, Dec. 2013.

[29] E. Arıkan, "Source polarization," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 899–903.

[30] P. W. Cuff, "Communications in networks for coordinating behavior," Ph.D. dissertation, Dept. Elect. Eng., Stanford Univ., Stanford, CA, USA, 2009.

[31] D. Aldous, "Random walks on finite groups and rapidly mixing Markov chains," in *Séminaire de Probabilités XVII*. Strasbourg, France: Springer, 1983, pp. 243–297.

[32] E. Ekrem and S. Ulukus, "Effects of cooperation on the secrecy of multiple access channels with generalized feedback," in *Proc. 42nd Annu. Conf. Inf. Sci. Syst.*, Mar. 2008, pp. 791–796.

[33] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.

HAOWEI WANG received the B.E. degree in communication engineering from the Harbin Institute of Technology (HIT), Weihai, China, in 2014. He is currently pursuing the Ph.D. degree in information and communication engineering with the Beijing University of Posts and Telecommunications (BUPT), Beijing, China. His research interests include information theory and information theoretic security.

XIAOFENG TAO (Senior Member, IEEE) received the B.S. degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 1993, and the M.S.E.E. and Ph.D. degrees in telecommunication engineering from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 1999 and 2002, respectively. He is currently a Professor and the Director of the National Engineering Laboratory, BUPT. He has authored or coauthored over 200 articles and two books, in wireless communication areas, and holds 80 patents. He currently focuses on 5G research. He is a Fellow of the IET. He was a recipient of the Honored Mention Award at the ACM MobiCom 2009, the Best Paper Awards at ISCIT 2012 and WCNC 2014, and the Chinese National Invention Awards, in 2008 and 2013. He is the Chair of the IEEE ComSoc Beijing Chapter.

NA LI (Member, IEEE) received the B.S. degree in electronic information science and technology and the M.S. degree in communications and information systems from the Ocean University of China, Qingdao, China, in 2009 and 2012, respectively, and the Ph.D. degree in communications and information systems from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2015. She is currently a Lecturer with BUPT. Her research interests include the area of wireless communications and networks, with current emphasis on physical layer security, cooperation, and resource allocation in future wireless networks.

HUICI WU (Member, IEEE) received the B.S. degree in communication engineering from the Communication University of China, Beijing, China, in 2013, and the Ph.D. degree in information and communication engineering from the Beijing University of Posts and Telecommunications (BUPT), Beijing, in 2018. From September 2016 to August 2017, she is visiting the Broadband Communications Research (BBCR) Group, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. She is currently an Assistant Professor with BUPT. Her research interests include the area of wireless communications and networks, with current emphasis on the collaborative transmission in air-to-ground integrated networks and wireless access security. She served as the Publication Co-Chair of APCC 2018 and a TPC member of the IEEE ICC 2019 and IEEE ICC 2020. She also served as a Guest Editor for *Science China Information Sciences*.