Polar Coding for the Multiple Access Wiretap Channel via Rate-Splitting and Cooperative Jamming

Rémi A. Chou and Aylin Yener
Wireless Communications and Networking Laboratory
Department of Electrical Engineering
The Pennsylvania State University, University Park, PA 16802

***Abstract*—We consider strongly secure communication over a discrete memoryless multiple access wiretap channel with two transmitters – no degradation or symmetry assumptions are made on the channel. Our main result is that any rate pair known to be achievable with a random coding like proof, is also achievable with a low-complexity polar coding scheme. Moreover, if the rate pair is known to be achievable without time-sharing, then time-sharing is not needed in our polar coding scheme as well. Our proof technique relies on rate-splitting and different cooperative jamming strategies. Specifically, our coding scheme combines several point-to-point codes that either aim at secretly conveying a message to the legitimate receiver or at performing cooperative jamming. Each point-to-point code relies on a chaining construction to be able to deal with an arbitrary channel and strong secrecy. We assess reliability and strong secrecy through a detailed analysis of the dependencies between the random variables involved in the scheme.**

I. Introduction

Recent efforts have been made to construct coding schemes for the wiretap channel model [1], see, for instance, [2] for a recent review. In this paper, we pursue this line of work by developing a low-complexity coding scheme based on polar codes for discrete memoryless multiple access wiretap channels (MAC-WT) with two transmitters under strong secrecy. Note that this problem has also been considered in [3], and in the independent work [4]. However, in contrast to [3], [4], we deal with strong secrecy instead of weak secrecy. Consequently, our proof for secrecy cannot rely on Fano's inequality and requires a detailed analysis of the dependencies between all the random variables involved in the scheme. Additionally, our coding approach is different from [3], [4], as [3] relies on polar codes for channel coding, and [4] relies on monotone chain rules for Slepian-Wolf coding [5], whereas we rely on (i) rate-splitting, which involves virtual users, and (ii) cooperative jamming, in the sense that one user, potentially virtual, does not transmit information messages to the legitimate receiver but transmits, instead, appropriately chosen codewords that will help the other users to securely transmit their information messages. Our result can be summarized as follows.

- Any rate pair known to be achievable for the two-user MAC-WT is also achievable under strong secrecy with a low-complexity polar coding scheme.
- Moreover, if the rate pair is known to be achievable without time-sharing, then our polar coding scheme does not require time-sharing.

Note that similar to polar coding schemes for the point-to-point wiretap channel under strong secrecy [6], [7], our coding scheme requires the transmitters to share secret randomness with the legitimate receiver to be able to deal with strong secrecy and arbitrary discrete memoryless channels. Fortunately, the amount of shared randomness needed is negligible compared to the blocklength of the coding scheme. Note also that our coding scheme involves Block-Markov encoding, which is critical to ensure (i) strong secrecy, as first remarked in [6] for the wiretap channel, (ii) be able to deal with asymmetric channels, as first remarked in [8]. Finally, note that in our setting, reliability constraints only apply to the legitimate receiver, consequently, complications for rate-splitting in presence of multiple receivers discussed in [9] will not apply.

The remaining of the paper is organized as follows. We formally describe the problem studied in Section II. We detail our coding strategies in Section III. We then provide our coding scheme and its analysis in Section IV. Finally, we propose concluding remarks in Section V. Due to space constraints, we do not detail proofs.

II. Problem Statement

We first introduce some notation. Let $[\![a,b]\!]$ denote the integers between $\lfloor a \rfloor$ and $\lceil b \rceil$. For $n \in \mathbb{N}$ and $N \triangleq 2^n$, let $G_n \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes n}$ be the source polarization transform defined in [10]. The components of a vector, $X^{1:N}$, of size $N \in \mathbb{N}$, are denoted by superscripts, i.e., $X^{1:N} \triangleq (X^1, X^2, \dots, X^N)$. Moreover, for any set $\mathcal{I} \subset [\![1,N]\!]$, define $X^{1:N}[\mathcal{I}] \triangleq \left(X^i\right)_{i \in \mathcal{I}}$. Define also $[x]^+ \triangleq \max(x,0)$. The indicator function $\mathbb{1}\{\omega\}$ is equal to 1 if the predicate ω is true and 0 otherwise. The power set of $\mathcal{S}$ is denoted by $2^{\mathcal{S}}$. Finally, unless specified otherwise, capital letters designate random variables, whereas lowercase

This work was supported in part by NSF grants CIF-1319338 and CNS-1314719.

letters designate realizations of associated random variables, e.g., x is a realization of the random variable X.

The model considered is as follows. Let $N \in \mathbb{N}$. A $(2^{NR_1}, 2^{NR_2}, N)$ code $\mathcal{C}_N$ for a discrete memoryless MAC-WT $(\mathcal{X}_1 \times \mathcal{X}_2, W_{YZ|X_1X_2}, \mathcal{Y} \times \mathcal{Z})$ consists of two message sets $\mathcal{M}_i \triangleq [\![1, 2^{nR_i}]\!]$ associated with two stochastic encoders, $f_N^{(i)} : \mathcal{M}_i \to \mathcal{X}_i^N$, $i \in \{1,2\}$, which maps a uniformly distributed message $M_i \in \mathcal{M}_i$ to a codeword of length N, and one decoder, $g_N : \mathcal{Y}^N \to \mathcal{M}_1 \times \mathcal{M}_2$, which maps a sequence of N channel outputs to an estimate $\left(\widehat{M}_1, \widehat{M}_2\right)$ of (M_1, M_2). A rate pair (R_1, R_2) is achievable, if there exists a sequence of $(2^{NR_1}, 2^{NR_2}, N)$ codes $\{\mathcal{C}_N\}_{N \in \mathbb{N}^*}$, such that

$$\lim_{N\to\infty} \mathbb{P}\left[\left(\widehat{M}_1, \widehat{M}_2\right) \neq (M_1, M_2)\right] = 0 \text{ (\textbf{Reliability})},$$
$$\lim_{N\to\infty} I\left(M_1M_2; Z^{1:N}\right) = 0 \text{ (\textbf{Strong Secrecy})}.$$

It is known from [11] that the convex hull of the rate-pair region $\mathcal{R}$ is achievable, where $\mathcal{R} \triangleq \bigcup_{p_{X_1}p_{X_2}} (\mathcal{R}' \cup \mathcal{R}'' \cup \mathcal{R}''')$, with

$$\mathcal{R}' \triangleq \begin{Bmatrix} (R_1,R_2): & \\ R_1 & \leqslant [I(X_1;Y|X_2) - I(X_1;Z)]^+ \\ R_2 & \leqslant [I(X_2;Y|X_1) - I(X_2;Z)]^+ \\ R_1+R_2 & \leqslant [I(X_1X_2;Y) - I(X_1X_2;Z)]^+ \end{Bmatrix},$$
$$\mathcal{R}'' \triangleq \left\{(R_1,0) : R_1 \leqslant [I(X_1;Y|X_2) - I(X_1;Z|X_2)]^+\right\},$$
$$\mathcal{R}''' \triangleq \left\{(0,R_2) : R_2 \leqslant [I(X_2;Y|X_1) - I(X_2;Z|X_1)]^+\right\}.$$

III. Achievability of $\mathcal{R}$

In this section, we describe our coding strategies to achieve any rate of $\mathcal{R}$. We will use the following result.

Lemma 1. *For a fixed $p \triangleq (p_{X_1}, p_{X_2})$, define the set functions*

$$g_p : 2^{\{1,2\}} \to \mathbb{R}, \mathcal{S} \mapsto I(X_\mathcal{S}; Y|X_{\mathcal{S}^c}) - I(X_\mathcal{S}; Z),$$
$$g_p^{*+} : 2^{\{1,2\}} \to \mathbb{R}_+, \mathcal{S} \mapsto \min_{\substack{\mathcal{A}\subset\mathcal{M} \\ \text{s.t. } \mathcal{A}\supset\mathcal{S}}} [g_p(\mathcal{A})]^+.$$

When the context is clear, we will drop the dependence on p in our notation. We have the following properties.

(i) g is submodular.
(ii) $\mathcal{P}(g^{*+}) \triangleq \left\{(R_1,R_2) : g^{*+}(\mathcal{S}) \leqslant \sum_{i\in\mathcal{S}} R_i, \forall \mathcal{S} \subset \mathcal{M}\right\}$ is a polymatroid [12, Definition 3.1], [13].
(iii) $\mathcal{R}' = \mathcal{P}(g^{*+})$.

Fix $p \triangleq (p_{X_1}, p_{X_2})$. Achievability of $\mathcal{R}''$ and $\mathcal{R}'''$ is similar to the one of $\mathcal{R}'$ and is thus omitted due to space constraints – see Remark 1. Moreover, we only need to consider achievability of $\mathcal{R}'$ when $\min(g(\{1\}), g(\{2\})) \geqslant 0$, since if $g(\{1,2\}) \leqslant 0$, then $\mathcal{R}' = \{(0,0)\}$, and if $g(\{1\})g(\{2\}) \leqslant 0$, then it can be shown with (i) of Lemma 1 that $\mathcal{R}' \subset \mathcal{R}''$. We thus assume in the following $\min(g(\{1\}), g(\{2\})) \geqslant 0$.

We propose in Lemma 2 a rate-splitting strategy [14] to achieve any rate pair of $\mathcal{R}'$ using Property 1. The latter can be obtained with Lemma 1 and [12, Lemma 3.2], [13].

Property 1. *Fix $p \triangleq (p_{X_1}, p_{X_2})$. To achieve $\mathcal{R}'$, it is sufficient to achieve for any $R_1 \in \mathcal{I}_p$, the rate pair $[R_1, g(\{1,2\}) - R_1]$, where*

$$\mathcal{I}_p \triangleq [[g(\{1,2\}) - g(\{2\})]^+, \min(g(\{1\}), g(\{1,2\}))].$$

Lemma 2. *As in [14, Example 3], we choose $f : \mathcal{X}_2 \times \mathcal{X}_2 \to \mathcal{X}_2, (u,v) \mapsto \max(u,v)$, and split $(\mathcal{X}_2, p_{X_2})$ to form $(\mathcal{X}_2 \times \mathcal{X}_2, p_{U_\epsilon}p_{V_\epsilon})$, $\epsilon \in [0,1]$, such that for any $\epsilon > 0$, $p_{f(U_\epsilon,V_\epsilon)} = p_{X_2}$, for fixed (x,u), $p_{f(U_\epsilon,V_\epsilon)|U}(x|u)$ is a continuous function of ϵ, and $U_{\epsilon=0} = 0 = V_{\epsilon=1}$, $U_{\epsilon=1} = f(U_{\epsilon=1}, V_{\epsilon=1})$, $V_{\epsilon=0} = f(U_{\epsilon=0}, V_{\epsilon=0})$.*[1]

Then, we have $g(\{1,2\}) = R_U + R_V + R_1$, where we have defined the functions

$$R_U : \epsilon \mapsto I(U;Y) - I(U;Z|VX_1), \text{ from } [0,1] \text{ to } \mathbb{R},$$
$$R_V : \epsilon \mapsto I(V;Y|UX_1) - I(V;Z), \text{ from } [0,1] \text{ to } \mathbb{R},$$
$$R_1 : \epsilon \mapsto I(X_1;Y|U) - I(X_1;Z|V), \text{ from } [0,1] \text{ to } \mathbb{R}.$$

Moreover, $\epsilon \mapsto R_1(\epsilon)$ is continuous and $[g(\{1,2\}) - g(\{2\}), g(\{1\})]$ is contained in its image.

Although rate-splitting is well understood for models without secrecy constraints [14], some complications arise for the MAC-WT: While $\forall\epsilon \in [0,1], (R_U + R_V + R_1)(\epsilon) = g(\{1,2\}) > 0$, choosing $\epsilon_0 \in [0,1]$ such that $R_1(\epsilon_0) \in \mathcal{I}_p$ does not necessarily imply that $R_U(\epsilon_0) \geqslant 0$ and $R_V(\epsilon_0) \geqslant 0$. We indeed have $(R_U + R_V)(\epsilon_0) \geqslant 0$ but we might also have $\min(R_U(\epsilon_0), R_V(\epsilon_0)) < 0$ for some values of ϵ_0; see Example 1.

Our coding approach, which is detailed in Section IV-B, can be summarized as follows. When the rate associated with one of the three variables X_1, U, or V, is positive, we use the encoding procedure of a point-to-point wiretap code, whereas for a "negative rate", we perform cooperative jamming. In the following, due to space constraints, we only treat the case ($R_U < 0$ and $R_V \geqslant 0$). All other cases can be treated similarly or more easily. In particular, because the codewords associated with V are not needed to decode the ones associated with U and X_1, the eventuality ($R_V \leqslant 0$ and $R_U \geqslant 0$) can be handled with a relatively simple cooperative jamming scheme, compared to the one of Section IV-A.

Remark 1. *Achievability of $\mathcal{R}''$ or $\mathcal{R}'''$ follows the same idea as the one described above. The transmitter with a secret communication rate of zero performs cooperative jamming, whereas the other transmitter makes use of a point-to-point wiretap code.*

Example 1. *Assume $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y} = \mathcal{Z} = \{0,1\}$, and X_1, X_2, independent and uniformly distributed. Assume $Y \triangleq X_1 \oplus X_2$ and $Z \triangleq Y \oplus B$, where B is independent of (X_1, X_2) and follows a Bernoulli distribution with parameter α. Define $v_0 \triangleq (2-\epsilon)^{-1}$, $v_1 = 1 - v_0$, $u_0 \triangleq 1 - \epsilon/2$, $u_1 = 1 - u_0$, and*

[1] When the context is clear we do not explicitly write the dependence of U and V with respect to ϵ.

$\overline{\alpha} = 1 - \alpha$. *After some computations, one can show*

$$\begin{aligned} H_b(\alpha) &= \min(g(\{1,2\}, g(\{1\})), \\ 0 &= [g(\{1,2\} - g(\{2\})]^+, \\ R_U &= v_0 \left[H_b(\alpha) - H_b\left(\overline{\alpha}u_0 + \alpha u_1\right)\right], \\ R_V &= u_0 H_b\left(v_0\right), \\ R_1 &= v_0 H_b\left(\overline{\alpha}u_0 + \alpha u_1\right) + v_1 H_b(\alpha) - u_0 H_b\left(v_0\right), \\ H_b(\alpha) &= R_1 + R_U + R_V. \end{aligned}$$

We fix $\alpha = 1/4$ *and choose* $\epsilon = 0.674$ *to equally split the sum rate between Transmitters* 1 *and* 2. *We obtain*

$$\begin{aligned} &R_U \in [-0.128, -0.127],\ R_V \in [0.533, 0.534], \\ &R_1 \in [0.405, 0.406],\ R_U + R_V - R_1 \leqslant 10^{-4}, \\ &\min(g(\{1,2\}, g(\{1\})) \in [0.811, 0.812]. \end{aligned}$$

IV. Coding scheme for MAC-WT

Our coding scheme for the MAC-WT is presented in Section IV-B. It makes use of the encoding scheme for the point-to-point wiretap channel described in [7, Section V, §*Confidential message encoding*], which will be referred to as encoding scheme E^{WT}. It also makes use of the generic cooperative jamming encoding scheme presented in Section IV-A, which will be referred to as encoding scheme E^{CJ}.

A. Generic encoding scheme E^{CJ}

In this section, we propose a generic cooperative jamming scheme which operates over L blocks of length N; we will make the appropriate subsitutions of random variables in Section IV-B. Consider a discrete memoryless source with joint probability p_{XYZ} over $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ with $|\mathcal{X}| = 2$, and such that $I(X;Z) - I(X;Y) > 0$. Define the polar transform of $X^{1:N}$ as $A^{1:N} \triangleq X^{1:N} G_n$, and for $\delta_N \triangleq 2^{-N^\beta}$ with $\beta \in]0, 1/2[$, the "very high entropy" and "high entropy" sets (we refer to [7] and [15] for an interpretation of these sets)

$$\mathcal{V}_X \triangleq \left\{i \in [\![1,N]\!] : H(A^i|A^{1:i-1}) > 1 - \delta_N\right\}, \quad (1)$$

$$\mathcal{V}_{X|Z} \triangleq \left\{i \in [\![1,N]\!] : H(A^i|A^{1:i-1}Z^{1:N}) > 1 - \delta_N\right\}, \quad (2)$$

$$\mathcal{H}_{X|Y} \triangleq \left\{i \in [\![1,N]\!] : H(A^i|A^{1:i-1}Y^{1:N}) > \delta_N\right\}, \quad (3)$$

$$\mathcal{V}_{X|Y} \triangleq \left\{i \in [\![1,N]\!] : H(A^i|A^{1:i-1}Y^{1:N}) > 1 - \delta_N\right\}. \quad (4)$$

The idea of the encoding scheme E^{CJ} is as follows. Provided that the transmitter and the legitimate receiver share $(L-1)(|\mathcal{V}_{X|Y}| - |\mathcal{V}_{X|Z}|)$ uniformly distributed bits, the scheme aims at making available at the legitimate receiver the codewords sent at the input of the channel while concealing in each block $|\mathcal{V}_{X|Z}|$ bits from the eavesdropper. These codewords do not contain information but will help the other users to secretly share their information messages with the legitimate receiver. Note that in Section IV-B, we combine in an appropriate manner for two virtual users, the encoding schemes E^{CJ} and E^{WT}, so that the shared randomness required by E^{CJ} can be transmitted using E^{WT}.

In Block $i \in [\![1, L]\!]$, let K_i be a sequence of randomness shared with the legitimate transmitter, and T_i be the sequence of local randomness used by the encoder.

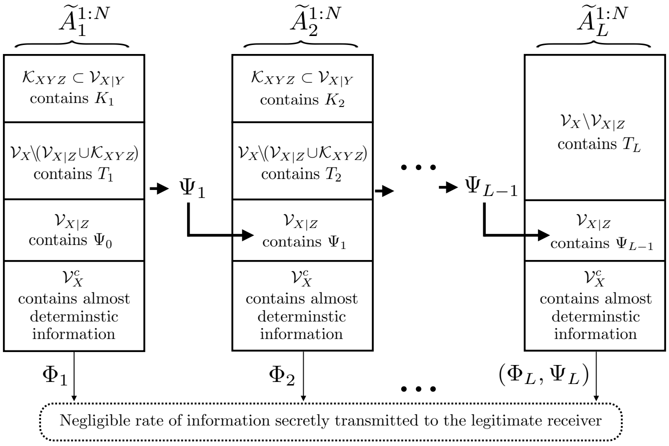
$\widetilde{A}_1^{1:N}$
$\widetilde{A}_2^{1:N}$
$\widetilde{A}_L^{1:N}$
$\mathcal{K}_{XYZ} \subset \mathcal{V}_{X|Y}$ contains K_1
$\mathcal{V}_X \backslash (\mathcal{V}_{X|Z} \cup \mathcal{K}_{XYZ})$ contains T_1
$\mathcal{V}_{X|Z}$ contains Ψ_0
$\mathcal{V}_X^c$ contains almost determinstic information
Ψ_1
$\mathcal{K}_{XYZ} \subset \mathcal{V}_{X|Y}$ contains K_2
$\mathcal{V}_X \backslash (\mathcal{V}_{X|Z} \cup \mathcal{K}_{XYZ})$ contains T_2
$\mathcal{V}_{X|Z}$ contains Ψ_1
$\mathcal{V}_X^c$ contains almost determinstic information
Ψ_{L-1}
$\mathcal{V}_X \backslash \mathcal{V}_{X|Z}$ contains T_L
$\mathcal{V}_{X|Z}$ contains Ψ_{L-1}
$\mathcal{V}_X^c$ contains almost determinstic information
Φ_1
Φ_2
(Φ_L, Ψ_L)
Negligible rate of information secretly transmitted to the legitimate receiver

Fig. 1. Chaining construction for the encoding scheme E^{CJ}.

We define $\mathcal{C}_{XYZ}$ to be a subset of $\mathcal{V}_{X|Y} \cap \mathcal{V}_{X|Z}^c$ with size $|\mathcal{V}_{X|Y}^c \cap \mathcal{V}_{X|Z}|$, and the set

$$\mathcal{K}_{XYZ} \triangleq (\mathcal{V}_{X|Y} \cap \mathcal{V}_{X|Z}^c) \backslash \mathcal{C}_{XYZ},$$

whose size is

$$|\mathcal{V}_{X|Y} \cap \mathcal{V}_{X|Z}^c| - |\mathcal{V}_{X|Y}^c \cap \mathcal{V}_{X|Z}| = |\mathcal{V}_{X|Y}| - |\mathcal{V}_{X|Z}|.$$

The encoding procedure is depicted in Figure 1.

In Block $i \in [\![1, L-1]\!]$, the encoder forms $\widetilde{X}_i^{1:N}$ as follows. Let K_i be a vector of $|\mathcal{V}_{X|Y}| - |\mathcal{V}_{X|Z}|$ uniformly distributed bits and T_i be a vector of $|\mathcal{V}_X \backslash (\mathcal{V}_{X|Z} \cup \mathcal{K}_{XYZ})|$ uniformly distributed bits that represent randomness shared with the legitimate receiver and a randomization sequence, respectively. Define ψ_0 as a local randomization sequence of $|\mathcal{V}_{X|Z}|$ uniformly distributed bits. Given k_i, t_i, ψ_{i-1}, the encoder draws $\widetilde{a}_i^{1:N}$ from the distribution $\widetilde{p}_{A_i^{1:N}}$ defined by

$$\begin{aligned} &\widetilde{p}_{A_i^j|A_i^{1:j-1}}(a_i^j|a_i^{1:j-1}) \\ &\triangleq \begin{cases} \mathbb{1}\left\{a_i^j = k_i^j\right\} & \text{if } j \in \mathcal{K}_{XYZ} \\ \mathbb{1}\left\{a_i^j = \psi_{i-1}^j\right\} & \text{if } j \in \mathcal{V}_{X|Z} \\ \mathbb{1}\left\{a_i^j = t_i^j\right\} & \text{if } j \in \mathcal{V}_X \backslash (\mathcal{V}_{X|Z} \cup \mathcal{K}_{XYZ}) \\ p_{A^j|A^{1:j-1}}(a_i^j|a_i^{1:j-1}) & \text{if } j \in \mathcal{V}_X^c \end{cases} \end{aligned}$$

where the components of k_i, ψ_{i-1}, and t_i have been indexed by the set of indices $\mathcal{K}_{XYZ}$, $\mathcal{V}_{X|Z}$, and $\mathcal{V}_X \backslash (\mathcal{V}_{X|Z} \cup \mathcal{K}_{XYZ})$ respectively, so that

$$\begin{aligned} K_i &= \widetilde{A}_i^{1:N}[\mathcal{K}_{XYZ}], \\ \Psi_{i-1} &= \widetilde{A}_i^{1:N}[\mathcal{V}_{X|Z}], \\ T_i &= \widetilde{A}_i^{1:N}[\mathcal{V}_X \backslash (\mathcal{V}_{X|Z} \cup \mathcal{K}_{XYZ})]. \end{aligned}$$

We then define $\widetilde{X}_i^{1:N} \triangleq \widetilde{A}_i^{1:N} G_n$ and

$$\begin{aligned} \Psi_i &\triangleq \widetilde{A}_i^{1:N}[\mathcal{C}_{XYZ} \cup (\mathcal{V}_{X|Y} \cap \mathcal{V}_{X|Z})], \\ \Phi_i &\triangleq \widetilde{A}_i^{1:N}[\mathcal{H}_{X|Y} \cap \mathcal{V}_{X|Y}^c]. \end{aligned}$$

The following remark is formally justified by Section IV-C.

Remark 2. *Observe that $|\Psi_i| = |\mathcal{V}_{X|Z}|$ and that $(\Psi_i, K_i, \Phi_i) = \widetilde{A}_i^{1:N}[\mathcal{H}_{X|Y}]$ will allow reconstruction of $\widetilde{A}_i^{1:N}$ given $\widetilde{Y}_i^{1:N}$. Note also that Ψ_i is uniformly distributed but Φ_i is not. Consequently, we reuse Ψ_i in the next block but we will not reuse Φ_i. We instead share Φ_i secretly between the transmitter and the legitimate receiver, and one can show that this may be accomplished with negligible rate cost.*

In Block L, the encoder forms $\widetilde{X}_L^{1:N}$ as follows. Let T_L be a vector of $|\mathcal{V}_X \backslash \mathcal{V}_{X|Z}|$ uniformly distributed bits that represents a randomization sequence. Given t_L, ψ_{L-1}, the encoder draws $\widetilde{a}_L^{1:N}$ from the distribution $\widetilde{p}_{A_L^{1:N}}$ defined by

$$\widetilde{p}_{A_L^j | A_L^{1:j-1}}(a_L^j | a_L^{1:j-1}) \triangleq \begin{cases} \mathbb{1}\left\{a_L^j = \psi_{L-1}^j\right\} & \text{if } j \in \mathcal{V}_{X|Z} \\ \mathbb{1}\left\{a_L^j = t_L^j\right\} & \text{if } j \in \mathcal{V}_X \backslash \mathcal{V}_{X|Z} \\ p_{A^j|A^{1:j-1}}(a_L^j | a_L^{1:j-1}) & \text{if } j \in \mathcal{V}_X^c \end{cases}$$

where the components of ψ_{L-1}, and t_L have been indexed by the set of indices $\mathcal{V}_{X|Z}$, and $\mathcal{V}_X \backslash \mathcal{V}_{X|Z}$ respectively, so that

$$\Psi_{L-1} = \widetilde{A}_L^{1:N}[\mathcal{V}_{X|Z}], \quad T_L = \widetilde{A}_L^{1:N}[\mathcal{V}_X \backslash \mathcal{V}_{X|Z}].$$

We then define $\widetilde{X}_L^{1:N} \triangleq \widetilde{A}_L^{1:N} G_n$ and

$$\Psi_L \triangleq \widetilde{A}_L^{1:N}[\mathcal{V}_{X|Y}], \quad \Phi_L \triangleq \widetilde{A}_L^{1:N}[\mathcal{H}_{X|Y} \cap \mathcal{V}_{X|Y}^c].$$

Finally, in Block L, the transmitter securely shares $(\Psi_L, \Phi_{1:L})$ with the legitimate receiver by means of a one-time pad.

B. Coding scheme for achieving $\mathcal{R}'$

Fix (p_{X_1}, p_{X_2}). As explained in Section IV, one can assume $g(\{1\})g(\{2\}) > 0$. We fix $R_1 \in \mathcal{I}_p$. Observing that $[g(\{1,2\}) - g(\{2\})]^+ \geqslant g(\{1,2\}) - g(\{2\})$ and $\min(g(\{1\}), g(\{1,2\})) \leqslant g(\{1,2\})$, by Lemma 2, there exists $\epsilon_0 \in [0,1]$ such that

$$R_1 = I(X_1; Y|U) - I(X_1; Z|V),$$
$$R_U + R_V = g(\{1,2\}) - R_1 \geqslant 0.$$

By Property 1 and Lemma 2, it is sufficient to achieve $(R_1, R_U + R_V)$ to show achievability of $\mathcal{R}'$. Let $p_{UVX_1X_2YZ}$ denote the joint distribution of the random variables (U, V, X_1, X_2, Y, Z). As explained in Section III, we assume $R_U < 0$ and $R_V \geqslant 0$. Our coding scheme operates over L blocks of length N as follows.

1) Encoding:
$M_{1:L}^{(1)}$ and $M_{1:L}^{(V)}$ are the binary, uniformly distributed, and mutually independent secret messages to be transmitted over L blocks by Transmitters 1 and 2, respectively. Define $A^{1:N} \triangleq U^{1:N} G_n$, $B^{1:N} \triangleq V^{1:N} G_n$, $C^{1:N} \triangleq (X_1)^{1:N} G_n$. The encoding procedure, whose functional dependence graph is depicted in Figure 2, is as follows.

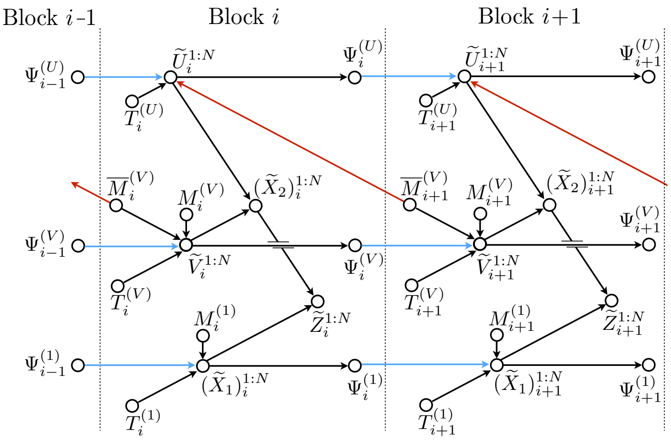

Fig. 2. Functional dependence graph of the block encoding scheme when $R_U < 0$ and $R_V \geqslant 0$.

Transmitter 2:
The approach for Transmitter 2 is to securely transmit at rate R_V for the virtual user associated with input V, and to perform cooperative jamming for the virtual user associated with input U. More specifically, cooperative jamming is aided by secret information with rate $-R_U$, that has been secretly transmitted to the legitimate receiver via the input V.

(i) Apply the encoding scheme E^{WT} by doing the substitutions $Y \leftarrow YUX_1$, $S_{1:L} \leftarrow (M_{1:L}^{(V)}, \overline{M}_{1:L}^{(V)})$ to encode a secret message $(M_{1:L}^{(V)}, \overline{M}_{1:L}^{(V)})$, where for all $i \in [\![2, L]\!]$,

$$|\overline{M}_i^{(V)}| \triangleq |\mathcal{V}_{U|Y}| - |\mathcal{V}_{U|ZVX_1}|,$$
$$|M_i^{(V)}| \triangleq |\mathcal{V}_{V|Z} \backslash \mathcal{A}_{V|YUX_1}| - |\overline{M}_i^{(V)}|,$$
$$|\overline{M}_i^{(V)}| + |M_i^{(V)}| = |\mathcal{V}_{V|Z} \backslash \mathcal{A}_{V|YUX_1}|.$$

We also define $|\overline{M}_1^{(V)}| \triangleq 0$, and $|M_1^{(V)}| \triangleq |\mathcal{V}_{V|Z}|$. Let $\widetilde{V}_{1:L}^{1:N}$ denote the outputs of this encoding step. For $i \in [\![1, L]\!]$, we add the superscript (V) to Φ_i and Ψ_i defined in E^{WT}.

(ii) Apply the encoding scheme E^{CJ} with the substitutions $X \leftarrow U$, $Z \leftarrow ZVX_1$, for $i \in [\![1, L-1]\!]$, $K_i \leftarrow \overline{M}_{i+1}^{(V)}$. For $i \in [\![1, L]\!]$, we add the superscript (U) to Φ_i and Ψ_i defined in E^{CJ}. Let $\widetilde{U}_{1:L}^{1:N}$ denote the outputs of this encoding step. Note that the virtual user associated with input U does not transmit information messages.

(iii) Send over the channel $(\widetilde{X}_2)_i^{1:N} \triangleq f(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N})$ for each encoding block $i \in [\![1, L]\!]$.

Transmitter 1:

(i) Apply the encoding scheme E^{WT} by doing the substitutions $V \leftarrow X_1$, $Z \leftarrow ZV$, $Y \leftarrow YU$, $S_{1:L} \leftarrow M_{1:L}^{(1)}$ to encode the secret messages $M_{1:L}^{(1)}$ and let $(\widetilde{X}_1)_{1:L}^{1:N}$ denote the outputs of this encoding step. For $i \in [\![1, L]\!]$, we add the superscript (1) to Φ_i and Ψ_i defined in E^{WT}.

(ii) Send over the channel $(\widetilde{X}_1)_i^{1:N}$ for each encoding block $i \in [\![1, L]\!]$.

2) Decoding:
For $i \in [\![1, L]\!]$, define $\widehat{U}_i^{1:N} \triangleq \widehat{A}_i^{1:N} G_n$, $\widehat{V}_i^{1:N} \triangleq \widehat{B}_i^{1:N} G_n$,

$(\widehat{X}_1)_i^{1:N} \triangleq \widehat{C}_i^{1:N} G_n$, where $\widehat{A}_i^{1:N}$, $\widehat{B}_i^{1:N}$, and $\widehat{C}_i^{1:N}$ are estimates of $\widetilde{A}_i^{1:N}$, $\widetilde{B}_i^{1:N}$, and $\widetilde{C}_i^{1:N}$, respectively, obtained using the successive cancellation decoder for source coding with side information [10] as follows. Set $\widehat{\overline{M}}_{L+1}^{(V)} \triangleq \emptyset$, $\widehat{\Psi}_L^{(U)} \triangleq \Psi_L^{(U)}$, $\widehat{\Psi}_L^{(V)} \triangleq \Psi_L^{(V)}$, $\widehat{\Psi}_L^{(1)} \triangleq \Psi_L^{(1)}$, $\widehat{A}_L^{1:N}[\mathcal{H}_{U|Y}] \triangleq \widetilde{A}_L^{1:N}[\mathcal{H}_{U|Y}]$, $\widehat{B}_L^{1:N}[\mathcal{H}_{V|YUX_1}] \triangleq \widetilde{B}_L^{1:N}[\mathcal{H}_{V|YUX_1}]$, $\widehat{C}_L^{1:N}[\mathcal{H}_{X_1|YU}] \triangleq \widetilde{C}_L^{1:N}[\mathcal{H}_{X_1|YU}]$, and iterate over i from L to 1. Form $\widehat{A}_i^{1:N}$ from $(\widehat{\Psi}_i^{(U)}, \Phi_i^{(U)}, \widehat{\overline{M}}_{i+1}^{(V)}) = \widehat{A}_i^{1:N}[\mathcal{H}_{U|Y}]$, and $\widetilde{Y}_i^{1:N}$. The decoder thus obtains an estimate $\widehat{\Psi}_{i-1}^{(U)}$ of $\Psi_{i-1}^{(U)}$. Then, form $\widehat{C}_i^{1:N}$ from $(\widehat{\Psi}_i^{(1)}, \Phi_i^{(1)}) = \widehat{C}_i^{1:N}[\mathcal{H}_{X_1|YU}]$, and $(\widetilde{Y}_i^{1:N}, \widehat{U}_i^{1:N})$. The decoder thus obtains an estimate $\widehat{\Psi}_{i-1}^{(1)}$ of $\Psi_{i-1}^{(1)}$. Then, form $\widehat{B}_i^{1:N}$ from $(\widehat{\Psi}_i^{(V)}, \Phi_i^{(V)}) = \widehat{B}_i^{1:N}[\mathcal{H}_{V|YUX_1}]$, and $(\widetilde{Y}_i^{1:N}, \widehat{U}_i^{1:N}, (\widehat{X}_1)_i^{1:N})$. The decoder thus obtains an estimate $\widehat{\Psi}_{i-1}^{(V)}$ of $\Psi_{i-1}^{(V)}$, and an estimate $\widehat{\overline{M}}_i^{(V)}$ of $\overline{M}_i^{(V)}$. Finally, from $(\widehat{X}_1)_{1:L}^{1:N}$ and $\widehat{V}_{1:L}^{1:N}$ the decoder obtains estimates of $M_{1:L}^{(1)}$, and $M_{1:L}^{(V)}$, respectively.

C. Scheme analysis

In the following, we let $\delta(N)$ be a generic function of N such that $\lim_{N\to\infty} 2^{N^\alpha}\delta(N) = 0$ for any $\alpha < \beta$.

1) Induced distribution: A crucial step to assess reliability and secrecy for our coding scheme is the study of the distribution induced by the encoder of Section IV-B.

Lemma 3. *Let $\widetilde{p}$ denote the distribution induced by the encoding scheme in Block $i \in [\![1, L]\!]$, i.e., the joint distribution of $\left(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N}, (\widetilde{X}_1)_i^{1:N}(\widetilde{X}_2)_i^{1:N}, \widetilde{Y}_i^{1:N}, \widetilde{Z}_i^{1:N}\right)$. We have*

$$\mathbb{V}\left(\widetilde{p}, p_{U^{1:N}V^{1:N}(X_1)^{1:N}(X_2)^{1:N}Y^{1:N}Z^{1:N}}\right) \leqslant \delta(N),$$

where $\mathbb{V}(\cdot,\cdot)$ denotes the variational distance.

2) Reliability: Using Lemma 3 and appropriate optimal couplings [16, Lemma 3.6], one can show

$$\mathbb{P}\left[(\widehat{M}_{1:L}^{(V)}, \widehat{M}_{1:L}^{(1)}) \neq (M_{1:L}^{(V)}, M_{1:L}^{(1)})\right] \leqslant 5^L \delta(N).$$

3) Communication rates: Using [10] and [15, Lemma 1], one can show that the rates of $M_{1:L}^{(1)}$ and $M_{1:L}^{(V)}$ are R_1 and $R_U + R_V$, respectively. Moreover, one can also show that the rates of the secret seeds shared by Transmitters 1, 2, and the legitimate receiver – whose lengths are $|\Psi_L^{(1)}| + \sum_{i=1}^L |\Phi_i^{(1)}|$ and $|\Psi_L^{(V)}| + \sum_{i=1}^L |\Phi_i^{(V)}|$, respectively – vanish to zero as $N \to \infty, L \to \infty$.

4) Strong secrecy: It is tempting to state that the following security conditions hold by the result in [7],

$$\max\left[I\left(M_{1:L}^{(V)}\overline{M}_{1:L}^{(V)}; \widetilde{Z}_{1:L}^{1:N}\right), I\left(M_{1:L}^{(1)}; \widetilde{Z}_{1:L}^{1:N}\widetilde{V}_{1:L}^{1:N}\right)\right] \leqslant \delta(N).$$

This assertion would, however, be incorrect. The result from [7] does not apply due to the fact that the functional dependence graphs that describes dependencies between random variables across all blocks are different. In particular, additional dependencies exist here because of our combination of two point-to-point wiretap codes and one cooperative jamming code. Fortunately, using the functional dependence graph depicted in Figure 2, one can show blockwise strong secrecy, from which one can study strong secrecy across two consecutive blocks, to finally obtain strong secrecy over all blocks jointly, specifically,

$$I\left(M_{1:L}^{(V)} M_{1:L}^{(1)}; \widetilde{Z}_{1:L}^{1:N}\right) \leqslant L\delta(N).$$

V. Concluding remarks

In this paper, we have shown that rate-splitting for the multiple access channel (MAC) without secrecy constraint [14] can be adapted to the MAC wiretap channel, though, with the caveat that a "negative rate" can be associated with a virtual input. We have shown that such case can be handled with appropriate cooperative jamming strategies that we have implemented with polar codes.

We highlight two important technical points. First, the induced distribution of the coding scheme should match the distribution for which the very high entropy and high entropy sets are defined. In our scheme, this point is critical to assess reliability and secrecy. Second, block Markov encoding creates dependencies between random variables. In our coding scheme, several chaining constructions are combined together and a precise analysis of the dependencies of the involved random variables is essential to assess reliability and strong secrecy.

References

[1] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, 2015.

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

[4] Y. Wei and S. Ulukus, "Polar coding for the general wiretap channel with extensions to multiuser scenarios," *to appear in IEEE Jour. on Selected Areas in Communications*, 2016.

[5] E. Arikan, "Polar coding for the slepian-wolf problem based on monotone chain rules," in *IEEE Int. Symp. Inf. Theory*, 2012.

[6] E. Şaşoğlu and A. Vardy, "A New Polar Coding Scheme for Strong Security on Wiretap Channels," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2013, pp. 1117–1121.

[7] R. Chou and M. Bloch, "Polar coding for the broadcast channel with confidential messages," in *IEEE Inf. Theory Workshop*, 2015, pp. 1–5.

[8] M. Mondelli, R. Urbanke, and S. H. Hassani, "How to achieve the capacity of asymmetric channels," in *52nd Annual Allerton Conference*, 2014, pp. 789–796.

[9] O. Fawzi and I. Savov, "Rate-splitting in the presence of multiple receivers," *arXiv preprint arXiv:1207.0543*, 2012.

[10] E. Arikan, "Source Polarization," in *IEEE Int. Symp. Inf. Theory*, 2010, pp. 899–903.

[11] M. Yassaee and M. Aref, "Multiple access wiretap channels with strong secrecy," in *IEEE Inf. Theory Workshop*, 2010, pp. 1–5.

[12] D. Tse and S. Hanly, "Multiaccess fading channels. i. polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2796–2815, 1998.

[13] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," *Combinatorial structures and their applications*, pp. 69–87, 1970.

[14] A. Grant, B. Rimoldi, R. Urbanke, and P. Whiting, "Rate-splitting multiple access for discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 873–890, 2001.

[15] R. Chou, M. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, no. 11, p. 6213, 2015.

[16] D. Aldous, "Random walks on finite groups and rapidly mixing markov chains," in *Séminaire de Probabilités XVII*. Springer, 1983.