This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

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

Rémi A. Chou, *Member, IEEE*, and Aylin Yener, *Fellow, IEEE*

***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 an *explicit* and 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, which introduces two virtual transmitters, and cooperative jamming strategies implemented by these virtual transmitters. Specifically, our coding scheme combines 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 block Markov encoding to be able to deal with an arbitrary channel and strong secrecy. Consequently, our coding scheme is the combination of inter-dependent block Markov constructions. We assess reliability and strong secrecy through a detailed analysis of the dependencies between the random variables involved in the scheme.**

I. Introduction

Although [2] provides the fundamental limits of secure communication over a noisy channel tapped by an eavesdropper, it leaves open the problem of designing explicit and low-complexity codes. Recent efforts have been made to construct such coding schemes. Specifically, coding schemes based on low-density parity-check codes [3]–[5], polar codes [6]–[10], and invertible extractors [11]–[13] have been successfully developed for special cases of Wyner's wire-tap channel model, in which the communication channels are at least required to be symmetric. Among those, [4], [7], [9], [11], [12] provide strong secrecy. Explicit wiretap codes with low complexity encoding/decoding for arbitrary channels are reported in [14]–[17], with the caveats that [14] deals with weak secrecy and requires a non-negligible amount of shared randomness between encoder and decoder, no efficient code construction is known for the scheme in [15], and a pre-shared secret with negligible rate is required in [16]. Note that a polar coding scheme is also proposed in [18], however, it relies on existence results from [19] and thus does not provide a scheme that is fully explicit. Additionally, explicit coding schemes have been proposed for the Gaussian wiretap channel in [20], [21].

In this paper, we consider a multi-transmitter setting, the multiple access wiretap channel (MAC-WT) [22]. Our main results can be summarized as follows.

- Any rate pair known to be achievable for the two-user discrete memoryless MAC-WT is also achievable under strong secrecy with an explicit and 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 either.

Similar to polar coding schemes for the point-to-point wiretap channel under strong secrecy [9], [16], [18], our coding scheme requires the transmitters to share secret randomness with the legitimate receiver to be able to deal with strong secrecy and any general discrete memoryless channel model. Fortunately, the shared randomness needed has negligible rate.

Our coding scheme does not involve joint polarization results [23], [24] and relies, instead, on perhaps simpler results for source polarization [25]. We also rely on rate-splitting [26], which consists in splitting one user into two *virtual* users, resulting in a total of three users. Although rate-splitting is well understood for multiple access channels without secrecy constraints [26], some complications arise for the MAC-WT. Indeed, as we will later see, some of the virtual users could be associated with a "negative rate". We deal with this issue as follows. A user associated with a positive rate will code to securely transmit information messages to the legitimate receiver, i.e., messages fixed independently of the coding scheme and containing the information that the user wishes to securely transmit. On the other hand, a user associated with a "negative rate" will code to perform cooperative jamming [22]. In the later case, the user 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. More specifically, our approach consists of an appropriate combination of the polar coding scheme for point-to-point wiretap channel proposed in [16] and three different cooperative jamming coding schemes. To be able to deal with arbitrary channels, each point-to-point wiretap code or cooperative jamming code used in our coding scheme relies on block Markov encoding. Consequently, our scheme is the

Rémi A. Chou is with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS 67260. Part of this work has been performed while the first author was a postdoctoral researcher in the Department of Electrical Engineering, The Pennsylvania State University, University Park, PA 16802. Aylin Yener is with the Department of Electrical Engineering, The Pennsylvania State University, University Park, PA 16802. Part of this work was presented at the 2016 IEEE International Symposium on Information Theory (ISIT) [1]. This work was supported in part by NSF grants CIF-1319338 and CNS-1314719. E-mails: remi.chou@wichita.edu, yener@engr.psu.edu.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

combination of inter-dependent block Markov constructions, and assessing reliability and strong secrecy requires a detailed analysis of the dependencies between the random variables involved in the scheme, which, unfortunately, will not follow from the results for the point-to-point case developed in [16].

The remainder of the paper is organized as follows. We formally describe the problem studied and discuss related works in the literature in Section II. In Section III, we differentiate several cases to achieve the best known achievable region for the MAC-WT, and propose different coding strategies for each case. We propose our encoding and decoding schemes for the MAC-WT in Section IV, and provide their analyses in Section V. We end the paper with concluding remarks in Section VI.

II. Problem Statement and Related Works

A. Notation

Let $[\![a,b]\!]$ denote the integers between $\lfloor a \rfloor$ and $\lceil b \rceil$. For $n \in \mathbb{N}$, let $G_n \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes n}$ be the source polarization transform defined in [25]. The components of a vector, $X^{1:N}$, of size $N \in \mathbb{N}$, are denoted by superscripts, i.e., $X^{1:N} \triangleq (X^1, X^2, \ldots, X^N)$. For two distributions p_X and $p_{X'}$ defined over a finite alphabet $\mathcal{X}$, let $\mathbb{V}(p_X, p_{X'}) \triangleq \sum_{x\in\mathcal{X}} |p_X(x) - p_{X'}(x)|$ denote the variational distance between p_X and $p_{X'}$. Let $\mathbb{D}(\cdot||\cdot)$ denote the divergence between two distributions. For $x \in \mathbb{R}$, define $[x]^+ \triangleq \max(0, x)$. Let the power set of $\mathcal{S}$ be denoted by $2^{\mathcal{S}}$. Finally, unless specified otherwise, capital letters designate random variables, whereas lowercase letters designate realizations of associated random variables, e.g., x is a realization of the random variable X.

B. Model

We consider secure communication between two transmitters and one legitimate receiver over a discrete memoryless MAC in the presence of an eavesdropper, i.e., the two-user MAC-WT, as depicted in Figure 1. That is we have the following setup.

Definition 1. *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 $\mathcal{M}_i \triangleq [\![1, 2^{NR_i}]\!]$, $i \in \{1,2\}$.*
- *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.*
- *One decoder, $g_N : \mathcal{Y}^N \to \mathcal{M}_1 \times \mathcal{M}_2$, which maps a sequence of N channel output observations to an estimate $\left(\widehat{M}_1, \widehat{M}_2\right)$ of the messages (M_1, M_2).*

Definition 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*

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

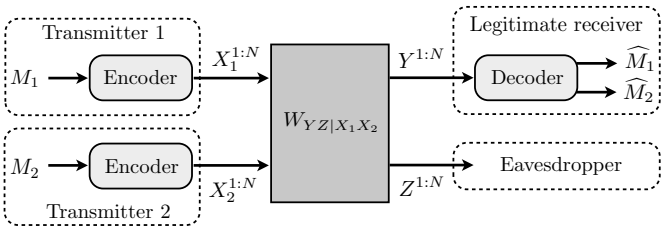

Fig. 1. Discrete memoryless multiple access wiretap channel.

As pointed out in [27], only requiring $\lim_{N\to\infty} \frac{1}{N} I\left(M_1M_2; Z^{1:N}\right) = 0$, i.e., weak secrecy, might not always be satisfactory as it could allow an unbounded, with the code length, number of bits of the confidential messages to be unprotected.

C. Known achievable regions and outerbounds

The following rate-pair region is the best known achievable region for weak secrecy [22] or strong secrecy [28], [29], up to channel prefixing. In this paper, we omit channel prefixing in our coding scheme for clarity, however, it could also be implemented with polar codes as in [16].

Theorem 1. *$\mathcal{R} \triangleq Conv\left(\bigcup_{p_{X_1}p_{X_2}} (\mathcal{R}' \cup \mathcal{R}'' \cup \mathcal{R}''')\right)$ is an achievable rate-pair region, where Conv$(\cdot)$ denotes the convex hull of a set and where*

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

$$\mathcal{R}''(p_{X_1}p_{X_2}) \triangleq \left\{(R_1,0) : R_1 \leqslant [I(X_1;Y|X_2) - I(X_1;Z|X_2)]^+\right\},$$

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

When the context is clear we drop the dependence on $(p_{X_1}p_{X_2})$ in our notation.

The only known upper-bounds are reported in [30], [31]. Specifically, [30] shows that the secrecy sum rate achieved in $\mathcal{R}$ is optimal in the case of degraded Gaussian channels. [31] provides additional n-letter upper-bounds that are shown to be tight, or close to tight, for specific Gaussian channel models.

To simplify notation in the following, we define $\mathcal{M} \triangleq \{1,2\}$, and for a fixed product distribution $p_{X_\mathcal{M}} \triangleq p_{X_1}p_{X_2}$, we define the set function

$$g_{p_{X_\mathcal{M}}} : 2^{\mathcal{M}} \to \mathbb{R}, \mathcal{S} \mapsto I(X_\mathcal{S}; Y|X_{\mathcal{S}^c}) - I(X_\mathcal{S}; Z).$$

Property 1. *A property of $g_{p_{X_\mathcal{M}}}$ that will be useful in our analysis is submodularity, i.e., for any $p_{X_\mathcal{M}} \triangleq p_{X_1}p_{X_2}$, for any $\mathcal{S}, \mathcal{T} \subset \mathcal{M}$,*

$$g_{p_{X_\mathcal{M}}}(\mathcal{S} \cup \mathcal{T}) + g_{p_{X_\mathcal{M}}}(\mathcal{S} \cap \mathcal{T}) \leqslant g_{p_{X_\mathcal{M}}}(\mathcal{S}) + g_{p_{X_\mathcal{M}}}(\mathcal{T}).$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

See Appendix A for a proof of Property 1. When the context is clear we drop the subscript $p_{X_{\mathcal{M}}}$.

D. Related works

[28], [29] provide existence using random coding arguments to achieve the region $\mathcal{R}$ of Theorem 2 under strong secrecy. To the best of our knowledge [8], [14] provide the only explicit and low-complexity coding schemes reported in the literature for the multiple access wiretap channel.

1) Comparison with [8]: [8] shows under weak secrecy, under the assumption of a degraded eavesdropper channel and uniformly distributed inputs, the achievability of the two points described in [8, Corollary 11], and any convex combination by time-sharing.

By comparison, our scheme achieves the region $\mathcal{R}$ in Theorem 2, under strong secrecy, without assuming that the eavesdropper channel is degraded, and without being restricted to uniform input distribution. Finally, for any $(p_{X_1}p_{X_2})$, $\mathcal{R}'(p_{X_1}p_{X_2})$ is achieved without time-sharing.

2) Comparison with [14]: A first difference is that [14, Section VI] provides an achievability scheme under weak secrecy compared to strong secrecy for our coding scheme. Unlike [14], our coding scheme is designed to emulate source resolvability in each block so that the distribution of the constructed random variables and thus the distribution induced by the encoders outputs can be characterized, which is crucial in our analysis. Additionally, unlike [14], we do not make use of deterministic decisions for bits that do not have "low-entropy". To the best of our knowledge, studying the encoder output distribution in this case is an open problem [32].

A second difference is that the coding scheme in [14] requires the encoders and the decoder to share a number of uniform bits that scales linearly with the block length. This requirement appears in the way some sets are "frozen" in [14] by using in the encoding procedure some random bits known by the receiver. A solution proposed in [19, Section III.A] to remove this requirement is to perform an average over the choice of bits in the "frozen sets". However, this solution only provides an existence result compared to an explicit coding scheme. In contrast, we avoid this requirement of non-negligible shared randomness in our coding scheme by repeating some bits in each blocks. However, this operation creates additional dependencies that need to be carefully addressed in the analysis, which we provide in our work.

A third difference is that the coding scheme in [14] relies on the monotone chain rule method for Slepian-Wolf coding [33]. Although it is conjectured in [33, Section IV.E] that known efficient code constructions could be adapted to deal with the additional random variables introduced by the monotone chain rule, to the best of our knowledge, proposing such efficient constructions is still an open problem. By contrast, our coding scheme relies on polarization for source coding with side information [25].

3) Comparison with polar coding schemes for the multiple access channel without secrecy constraints: Our construction is different than existing polar codes construction for the multiple access channel without secrecy constraint [14], [24], [33].

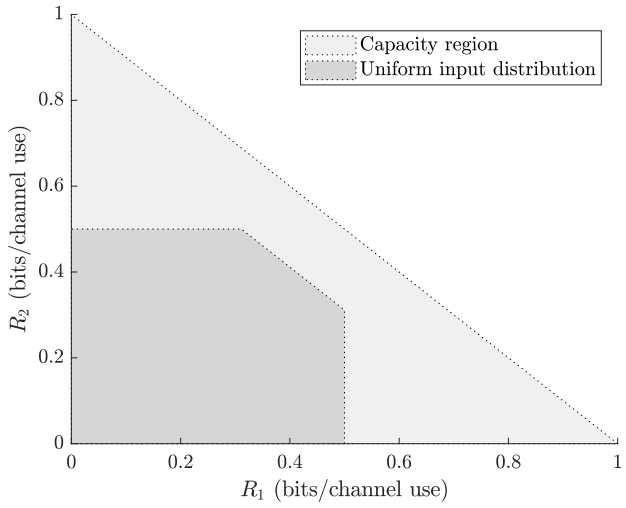

Fig. 2. Comparison of the capacity region and achievable region with a uniform input distribution $(p_{X_1}p_{X_2})$ for a multiple-access channel with binary inputs X_1, X_2, and output $Y = X_1X_2$.

The coding schemes in [24], [33] achieve the dominant face (only part of it for [24]) of the capacity region for uniform input distributions without time-sharing, and could be extended to arbitrary input distributions by extension of the input alphabets [34, P208]. Challenges related to this method are discussed in [19], [35], which also provide alternative solutions to avoid alphabet extension in the point-to-point case. Figure 2 illustrates the benefit of not being restricted by a uniform input distribution.

The coding scheme in [14], if one removes the secrecy constraint, uses a method similar to [19] to avoid alphabet extension and to achieve the capacity region without time sharing. However, [14] requires as in [19] encoders and decoder to share a non-negligible amount of shared randomness.

Our coding scheme, if one removes the secrecy constraint, achieves the capacity region without time-sharing, without alphabet extension, and without the requirement of a non-negligible amount of shared randomness between encoders and decoder. The price paid for removing those requirements is the use of block Markov coding. Another difference with [14] and [33] is that our coding scheme relies on polarization for source coding with side information [25] instead of polarization for Slepian-Wolf coding via monotone chain rules [33].

III. Coding strategies for achieving $\mathcal{R}$

In this section, we describe our coding strategies for achieving $\mathcal{R}$ in Theorem 1. We differentiate several cases, for which we propose a specific coding strategy.

We first consider the achievability of $\mathcal{R}'(p_{X_1}p_{X_2})$ for a fixed choice of $(p_{X_1}p_{X_2})$. If $g(\{1,2\}) \leqslant 0$, then $\mathcal{R}'(p_{X_1}p_{X_2}) = \{(0,0)\}$. We thus assume $g(\{1,2\}) > 0$. Then, we either have the case $g(\{1\})g(\{2\}) > 0$, which is treated in Section III-A, or the case $g(\{1\})g(\{2\}) \leqslant 0$, which is treated in Section III-B. We consider the achievability of $\mathcal{R}''(p_{X_1}p_{X_2})$ and $\mathcal{R}'''(p_{X_1}p_{X_2})$ for a fixed choice of $(p_{X_1}p_{X_2})$ in Section III-C. Finally, we discuss achievability of the entire region $\mathcal{R}$ in Section III-D.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

A. Achievability of the Region $\mathcal{R}'(p_{X_1}p_{X_2})$ when $g(\{1\})g(\{2\}) > 0$

Observe that by submodularity of g, we have $g(\{1,2\}) \leqslant g(\{1\}) + g(\{2\})$, so that, if $g(\{1\})g(\{2\}) > 0$, then $\min(g(\{1\}), g(\{2\})) > 0$ when $g(\{1,2\}) > 0$.

We summarize our strategy to achieve $\mathcal{R}'(p_{X_1}p_{X_2})$ in the following property, which takes advantage of a systematic method to characterize the corner points of $\mathcal{R}'(p_{X_1}p_{X_2})$ in Appendix B.

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

$$\begin{aligned} g(\{1,2\}) - g(\{2\}) &= I(X_1;Y) - I(X_1;Z|X_2), \\ g(\{1\}) &= I(X_1;Y|X_2) - I(X_1;Z), \\ g(\{1,2\} &= I(X_1X_2;Y) - I(X_1X_2;Z). \end{aligned}$$

Proof. See Appendix B. ∎

We next wish to use rate-splitting [26] to achieve the rate pairs described in Property 2 by means of point-to-point codes and without time-sharing, which has been shown to be unnecessary in [28], [29].

Lemma 1. *As in [26, 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*

$$U_{\epsilon=0} = 0 = V_{\epsilon=1}, \tag{1}$$
$$U_{\epsilon=1} = f(U_{\epsilon=1}, V_{\epsilon=1}), \tag{2}$$
$$V_{\epsilon=0} = f(U_{\epsilon=0}, V_{\epsilon=0}). \tag{3}$$

When the context is clear we do not explicitly write the dependence of U and V with respect to ϵ by dropping the subscript ϵ. Then, we have $g(\{1,2\}) = R_U + R_V + R_1$, where we have defined the functions

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

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

Proof. We have

$$\begin{aligned} &I(X_1X_2;Y) - I(X_1X_2;Z) \\ &\overset{(a)}{=} I(X_1UV;Y) - I(X_1X_2;Z) \\ &\overset{(b)}{=} I(X_1UV;Y) - I(X_1UV;Z) \\ &\overset{(c)}{=} I(U;Y) + I(X_1;Y|U) + I(V;Y|UX_1) - I(V;Z) \\ &\quad - I(X_1;Z|V) - I(U;Z|VX_1), \end{aligned}$$

where (a) holds by noting that $I(X_1UV;Y) \geqslant I(X_1X_2;Y)$ since $X_2 = f(U,V)$ and $I(X_1UV;Y) \leqslant I(X_1X_2;Y)$ since $(X_1UV) - (X_1X_2) - (YZ)$, (b) is obtained similar to (a), and (c) holds by the chain rule. Note that (a) is due to [26, Lemma 5].

Similar to [26, Example 3] for fixed (x,v), $p_{f(U,V)|V}(x,v)$ is a continuous function of ϵ and similar to [26, Lemma 6], $I(X_1;ZV)$ is a continuous function of ϵ. We also know by [26, Lemma 6] that $I(X_1;YU)$ is a continuous function of ϵ, hence so is

$$R_1 = I(X_1;Y|U) - I(X_1;Z|V) = I(X_1;YU) - I(X_1;ZV),$$

where we have used independence between X_1 and U, and between X_1 and V.

Then, $(g(\{1,2\}) - g(\{2\}))$ and $g(\{1\})$ are in the image of R_1 by (1)-(3), hence, using $g(\{1,2\}) \leqslant g(\{1\}) + g(\{2\})$ by submodularity of g, $[g(\{1,2\}) - g(\{2\}), g(\{1\})]$ is also in the image of R_1 by continuity. ∎

The complication with rate-splitting for the MAC-WT, compared to multiple access channels without secrecy constraints [26], is as follows. 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 $R_1(\epsilon_0) \in [[g(\{1,2\}) - g(\{2\})]^+, \min(g(\{1\}), g(\{1,2\}))]$ does not necessarily imply that $R_U(\epsilon_0) \geqslant 0$ and $R_V(\epsilon_0) \geqslant 0$; this is a possible event though. 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 approach to take care of this issue can be summarized at a high level as follows. When the rate associated with one of the three inputs 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 appropriate cooperative jamming.

B. Achievability of the Region $\mathcal{R}'(p_{X_1}p_{X_2})$ when $g(\{1\})g(\{2\}) \leqslant 0$

Without loss of generality, we assume $g(\{1\}) > 0$ and $g(\{2\}) \leqslant 0$. We first observe by submodularity of g that $g(\{1,2\}) \leqslant g(\{1\}) + g(\{2\}) \leqslant g(\{1\})$. Hence, $R_1 \leqslant \min(g(\{1\}), g(\{1,2\})) = g(\{1,2\})$. Next, we observe that

$$\begin{aligned} &g(\{1,2\}) \\ &= I(X_1;YX_2) - I(X_1;ZX_2) + I(X_2;Y) - I(X_2;Z) \\ &\leqslant I(X_1;YX_2) - I(X_1;ZX_2) + I(X_2;YX_1) - I(X_2;Z) \\ &= I(X_1;YX_2) - I(X_1;ZX_2) + g(\{2\}) \\ &\leqslant I(X_1;YX_2) - I(X_1;ZX_2). \end{aligned}$$

Consequently,

$$g(\{1\})g(\{2\}) \leqslant 0 \implies \mathcal{R}'(p_{X_1}p_{X_2}) \subset \mathcal{R}''(p_{X_1}p_{X_2}).$$

C. Achievability of the Regions $\mathcal{R}''(p_{X_1}p_{X_2})$ and $\mathcal{R}'''(p_{X_1}p_{X_2})$

It is sufficient to consider achievability of $\mathcal{R}''(p_{X_1}p_{X_2})$. Achievability of $\mathcal{R}'''(p_{X_1}p_{X_2})$ is obtained by exchanging the role of X_1 and X_2. Our approach will follow the same idea as the one in Section III-A. The transmitter with a secret communication rate of zero performs cooperative jamming, while the other transmitter makes use of a point-to-point wiretap code.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

D. Achievability of the entire Region $\mathcal{R}$

The remaining rate-pairs in $\mathcal{R}$ can be achieved with time-sharing using density of $\{\alpha \in [0,1] : \exists p,q \in \mathbb{N}, \alpha = \frac{p}{2^q}\}$ in $[0,1]$ which can be shown similar to density of $\mathbb{Q}$ in $\mathbb{R}$. Observe, however, that any rate-pair achieved without time-sharing in Theorem 1, is also achieved without time-sharing with the coding strategies described in Sections III-A, III-B, and III-C.

IV. Coding Scheme for the MAC-WT

In this section, we propose a coding scheme based on source polarization [25] that achieves the region $\mathcal{R}$ defined in Theorem 1 using the strategies proposed in Section III. Specifically, in Section IV-B, we propose a coding scheme to achieve $\mathcal{R}'(p_{X_1}p_{X_2})$ for any (p_{X_1}, p_{X_2}) such that $\min(g(\{1\}), g(\{2\})) > 0$. We then propose a coding scheme to achieve $\mathcal{R}''(p_{X_1}p_{X_2})$ in Section IV-C.

Our encoding schemes in Section IV-B, IV-C rely on an appropriate combination of (i) point-to-point wiretap encoding schemes, and (ii) point-to-point cooperative jamming encoding schemes. To simplify the description of our encoding schemes, we describe in Section IV-A a generic point-to-point wiretap encoding scheme and three generic point-to-point cooperative jamming encoding schemes, which will be used in Section IV-B, IV-C by doing appropriate substitutions of the generic random variables. The reader can directly go to Section IV-B and Section IV-C and refer to the detailed description of the generic encoding schemes when needed.

For each point-to-point code we use block Markov encoding to be able to deal with a reliability constraint over asymmetric channels by means of source coding with side information as in [36]. However, unlike [36], we do not use deterministic decisions in the encoding to simplify the study of the distribution of our encoders output [32], which is crucial to ensure reliability and secrecy in our scheme. We also use the encoding scheme described in [37] for the point-to-point wiretap codes. However, because our encoding scheme for the MAC-WT is a combination of interdependent block Markov constructions, we will not be able to reuse the reliability and secrecy analysis of [37].

A. Generic encoding schemes

In Section IV-A1, we describe a generic encoding scheme for a point-to-point wiretap channel, referred to as encoding scheme E^{WT}. In Sections IV-A2, IV-A3, IV-A4, we introduce three generic cooperative jamming encoding schemes referred to as encoding schemes E^{CJ1}, E^{CJ2}, and E^{CJ3}, respectively.

The four generic coding schemes operate over L blocks of length $N \triangleq 2^n$, $n \in \mathbb{N}$. For each of them we consider a discrete memoryless source with joint probability distribution p_{XYZ} over $\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$ with $|\mathcal{X}|= 2$. Define $A^{1:N} \triangleq X^{1:N}G_n$, and for $\delta_N \triangleq 2^{-N^\beta}$ with $\beta \in]0, 1/2[$, the sets

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

$$\mathcal{V}_{X|Z} \triangleq \left\{i \in [\![1,N]\!] : H(A^i|A^{1:i-1}Z^{1:N}) > 1-\delta_N\right\}, \quad (5)$$

$$\mathcal{H}_{X|Y} \triangleq \left\{i \in [\![1,N]\!] : H(A^i|A^{1:i-1}Y^{1:N}) > \delta_N\right\}, \quad (6)$$

$$\mathcal{V}_{X|Y} \triangleq \left\{i \in [\![1,N]\!] : H(A^i|A^{1:i-1}Y^{1:N}) > 1-\delta_N\right\}. \quad (7)$$

Moreover, for any set of indices $\mathcal{I} \subset [\![1,N]\!]$, we define $A^{1:N}[\mathcal{I}] \triangleq \left(A^i\right)_{i\in\mathcal{I}}$. An interpretation of these sets that will be used in our analysis can be summarized in the following two lemmas.

Lemma 2 (Source coding with side information [25])**.** *Given $A^{1:N}[\mathcal{H}_{X|Y}]$ and $Y^{1:N}$, it is possible to form $\widehat{A}^{1:N}$ by the successive cancellation decoder of [25] such that $\lim_{N\to\infty}\mathbb{P}[\widehat{A}^{1:N} \neq A^{1:N}] = 0$. Moreover, $\lim_{N\to\infty}|\mathcal{H}_{X|Y}|/N = H(X|Y)$.*

Lemma 3 (Privacy amplification [38])**.** *$A^{1:N}[\mathcal{V}_{X|Z}]$ is almost uniform and independent from $Z^{1:N}$ in the sense $\lim_{N\to\infty}\mathbb{V}(p_{A^{1:N}[\mathcal{V}_{X|Z}]Z^{1:N}}, p_U p_{Z^{1:N}}) = 0$, where p_U is the uniform distribution over $\{0,1\}^{|\mathcal{V}_{X|Z}|}$. Moreover, $\lim_{N\to\infty}|\mathcal{V}_{X|Z}|/N = H(X|Z)$.*

We use in the following the notation constructed random variable $\widetilde{A}^{1:N}$ with distribution $\widetilde{p}_{A^{1:N}}$. Moreover, random variables constructed in Block $i \in [\![1,L]\!]$ are indexed by the subscript i, and we use the notation $\widetilde{A}_{1:i}^{1:N} \triangleq \left(\widetilde{A}_j^{1:N}\right)_{j\in[\![1,i]\!]}$.

1) Encoding scheme E^{WT} : We describe the encoding scheme for the point-to-point wiretap channel proposed in [37, Section V, §*Confidential message encoding*]. We provide this encoding scheme for completeness and to clarify the case $I(X;Y) - I(X;Z) = 0$. Although the case $I(X;Y) - I(X;Z) = 0$ is irrelevant for the point-to-point setting, handling this case is needed in our treatment of the MAC-WT.

Assume $I(X;Y) - I(X;Z) \geqslant 0$ and let $\mathcal{A}_{X|Y}$ be a fixed subset of $\mathcal{V}_{X|Z}$ with size $|\mathcal{H}_{X|Y} \cap \mathcal{V}_{X|}|$. When $I(X;Y) - I(X;Z) = 0$, if $|\mathcal{V}_{X|Z}| < |\mathcal{H}_{X|Y}\cap\mathcal{V}_X|$, choose $\mathcal{A}_{X|Y} = \mathcal{V}_{X|Z}$. In Block $i \in [\![1,L]\!]$, let S_i denote the secret message to be transmitted and T_i denote the sequence of local randomness used by the encoder. The block Markov encoding procedure is summarized in Figure 3 and formally described in Algorithm 1.

Remark 1. *When $I(X;Y) - I(X;Z) = 0$, if $|\mathcal{V}_{X|Z}| < |\mathcal{H}_{X|Y} \cap \mathcal{V}_X|$, then in Algorithm 1 we add to Φ_i the bits of Ψ_{i-1} that did not fit in $\widetilde{A}_i^{1:N}[\mathcal{A}_{X|Y}] = \widetilde{A}_i^{1:N}[\mathcal{V}_{X|Z}]$. The rate of these bits is negligible since $H(X|Z) - H(X|Y) = I(X;Y) - I(X;Z) = 0$.*

2) Encoding scheme E^{CJ1}: We let T_i denote the sequence of local randomness used by the encoder in Block $i \in [\![1,L]\!]$. The encoding procedure is described in Algorithm 2.

3) Encoding scheme E^{CJ2} : Assume $I(X;Z) - I(X;Y) > 0$. Let K_i, $i \in [\![1, L-1]\!]$, denote the sequence of randomness shared with the legitimate transmitter that is used in Block i and T_i denote the sequence of local randomness used by the encoder in Block $i \in [\![1,L]\!]$. Let $\mathcal{C}_{XYZ}$ be a subset of $\mathcal{V}_{X|Y} \cap \mathcal{V}^c_{X|Z}$ with size $|\mathcal{V}^c_{X|Y} \cap \mathcal{V}_{X|Z}|$, and define the set $\mathcal{K}_{XYZ} \triangleq (\mathcal{V}_{X|Y} \cap \mathcal{V}^c_{X|Z})\backslash\mathcal{C}_{XYZ}$, whose size is $|\mathcal{V}_{X|Y} \cap \mathcal{V}^c_{X|Z}| - |\mathcal{V}^c_{X|Y} \cap \mathcal{V}_{X|Z}| = |\mathcal{V}_{X|Y}| - |\mathcal{V}_{X|Z}|$. The block Markov encoding procedure is summarized in Figure 4 and formally described in Algorithm 3.

4) Encoding scheme E^{CJ3}: Let T_i be a vector of $|\mathcal{V}_X\backslash\mathcal{V}_{X|Y}|$ uniformly distributed bits that represent a random-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

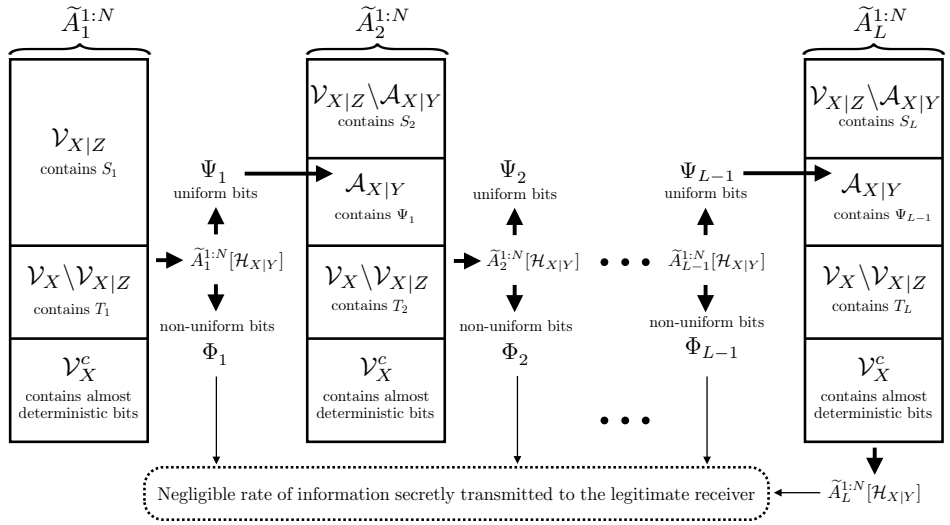

Fig. 3. Encoding scheme E^{WT}. In Block $i \in [\![1, L]\!]$, $\widetilde{A}_i^{1:N}$ is constructed from the secret message S_i, the local randomness T_i, and the subsequence Ψ_{i-1} of the previous block $\widetilde{A}_{i-1}^{1:N}$. The remaining symbols of $\widetilde{A}_i^{1:N}$ are almost deterministic given (S_i, T_i, Ψ_{i-1}). Note that (Ψ_i, Φ_i) is the information necessary to the legitimate receiver to recover $\widetilde{A}_i^{1:N}$. Note also that Ψ_i is uniform and repeated in Block $i+1$, whereas Φ_i, whose rate is negligible, is non-uniform and secretly transmitted to the legitimate receiver with a one-time pad. Finally, $\widetilde{A}_L^{1:N}[\mathcal{H}_{X|Y}]$ is also secretly transmitted to the legitimate receiver with a one-time pad, and the rate of this transmission vanishes to zero as the number of blocks L increases.

Algorithm 1 Generic Encoding Scheme E^{WT}

Require: S_1 a vector of $|\mathcal{V}_{X|Z}|$ uniformly distributed bits, and $L-1$ vectors $\{S_i\}_{i\in[\![2,L]\!]}$ of $|\mathcal{V}_{X|Z}\backslash\mathcal{A}_{X|Y}|$ uniformly distributed bits that represent secret messages.
L vectors $\{T_i\}_{i\in[\![1,L]\!]}$ of $|\mathcal{V}_X\backslash\mathcal{V}_{X|Z}|$ uniformly distributed bits that represent randomization sequences.

1: **for** Block $i = 1$ to L **do**
2: **if** i=1 **then**
3: $\widetilde{A}_1^{1:N}[\mathcal{V}_{X|Z}] \leftarrow S_1$
4: **else**
5: $\widetilde{A}_i^{1:N}[\mathcal{V}_{X|Z}\backslash\mathcal{A}_{X|Y}] \leftarrow S_i$
6: $\widetilde{A}_i^{1:N}[\mathcal{A}_{X|Y}] \leftarrow \Psi_{i-1}$
7: **end if**
8: $\widetilde{A}_i^{1:N}[\mathcal{V}_X\backslash\mathcal{V}_{X|Z}] \leftarrow T_i$
9: Successively draw the remaining components of $\widetilde{A}_i^{1:N}$, i.e., the components in $\mathcal{V}_X^c$, according to

$$\widetilde{p}_{A_i^j|A_i^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \triangleq p_{A^j|A^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \text{ if } j \in \mathcal{V}_X^c.$$

10: $\Psi_i \leftarrow \widetilde{A}_i^{1:N}[\mathcal{H}_{X|Y} \cap \mathcal{V}_X]$
11: $\Phi_i \leftarrow \widetilde{A}_i^{1:N}[\mathcal{H}_{X|Y} \cap \mathcal{V}_X^c]$
12: $\widetilde{X}_i^{1:N} \leftarrow \widetilde{A}_i^{1:N} G_n$
13: **end for**
14: The transmitter securely shares $(\Psi_L, \Phi_{1:L})$ with the legitimate receiver by means of a one-time pad.

Algorithm 2 Generic Encoding Scheme E^{CJ1}

Require: L vectors $\{T_i\}_{i\in[\![1,L]\!]}$ of $|\mathcal{V}_X|$ uniformly distributed bits that represent randomization sequences.

1: **for** Block $i = 1$ to L **do**
2: $\widetilde{A}_i^{1:N}[\mathcal{V}_X] \leftarrow T_i$
3: Successively draw the remaining components of $\widetilde{A}_i^{1:N}$, i.e., the components in $\mathcal{V}_X^c$, according to

$$\widetilde{p}_{A_i^j|A_i^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \triangleq p_{A^j|A^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \text{ if } j \in \mathcal{V}_X^c.$$

4: $\widetilde{X}_i^{1:N} \leftarrow \widetilde{A}_i^{1:N} G_n$
5: **end for**

ization sequence used by the encoder in Block $i \in [\![1, L]\!]$. The block Markov encoding procedure is summarized in Figure 5 and formalized in Algorithm 4.

B. Coding scheme for achieving $\mathcal{R}'(p_{X_1}p_{X_2})$ when $\min(g(\{1\}), g(\{2\})) > 0$

The coding scheme operates over L blocks of length N. $M_{1:L}^{(1)}$ and $\left(M_{1:L}^{(U)}, M_{1:L}^{(V)}\right)$ are the binary, uniformly distributed, and mutually independent secret messages to be transmitted over the L blocks by Transmitters 1 and 2, respectively.

Fix (p_{X_1}, p_{X_2}) and denote the joint distribution of the random variables (U, V, X_1, X_2, Y, Z) by $p_{UVX_1X_2YZ}$. By Property 2, it is sufficient to achieve for any $R_1 \in [[g(\{1,2\}) - g(\{2\})]^+, \min(g(\{1\}), g(\{1,2\}))]$ the rate pair $[R_1, g(\{1,2\}) - R_1]$. We thus fix $R_1 \in [[g(\{1,2\}) - g(\{2\})]^+, \min(g(\{1\}), g(\{1,2\}))]$. Observing that $\min(g(\{1\}), g(\{1,2\})) \leqslant g(\{1\})$ and $[g(\{1,2\}) - g(\{2\})]^+ \geqslant g(\{1,2\}) - g(\{2\})$, by Lemma 1, there exists

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

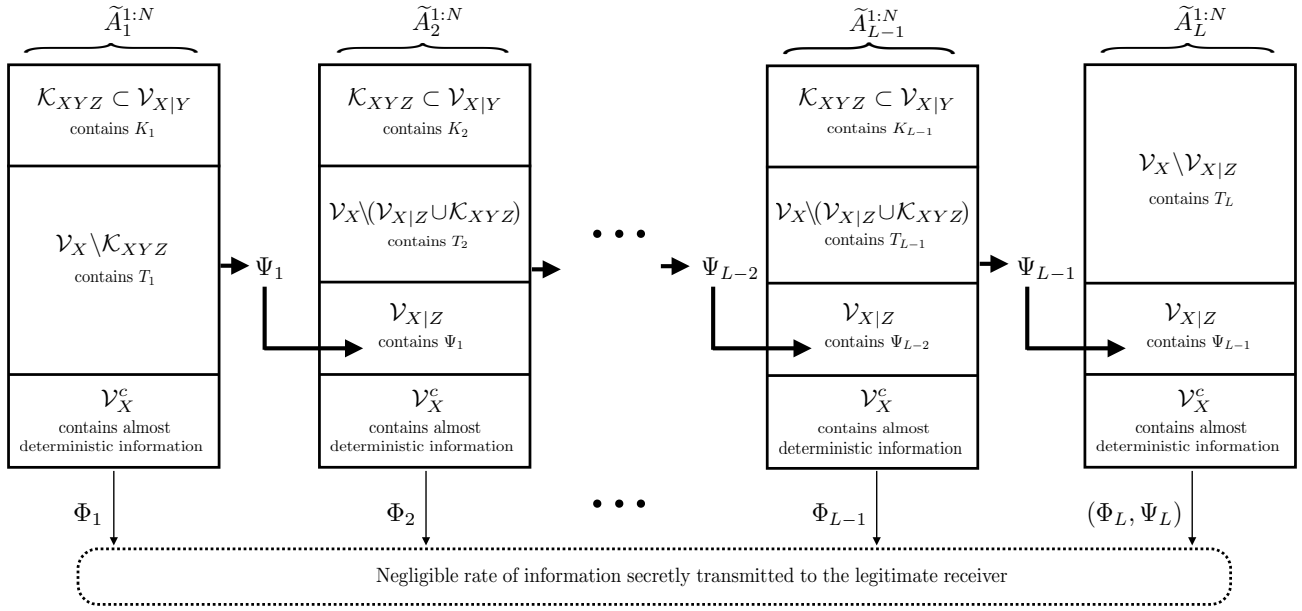

Fig. 4. Encoding scheme E^{CJ2}. In Block $i \in [\![1, L]\!]$, $\widetilde{A}_i^{1:N}$ is constructed from the randomness K_i shared with the transmitter, the local randomness T_i, and the subsequence Ψ_{i-1} of the previous block $\widetilde{A}_{i-1}^{1:N}$. The remaining symbols of $\widetilde{A}_i^{1:N}$ are almost deterministic given (K_i, T_i, Ψ_{i-1}). Note that (Ψ_i, K_i, Φ_i) is the information necessary to the legitimate receiver to recover $\widetilde{A}_i^{1:N}$. Note also that Ψ_i, which will be shown to be concealed from the eavesdropper, is uniform and repeated in Block $i+1$, whereas Φ_i, whose rate is negligible, is non-uniform and secretly transmitted to the legitimate receiver with a one-time pad. Finally, $\widetilde{A}_L^{1:N}[\mathcal{H}_{X|Y}]$ is also secretly transmitted to the legitimate receiver with a one-time pad, and the rate of this transmission vanishes to zero as the number of blocks L increases.

$\epsilon_0 \in [0, 1]$ such that $R_1 = I(X_1; Y|U) - I(X_1; Z|V)$ and $R_U + R_V = g(\{1, 2\}) - R_1 \geqslant 0$. We then have the three possible cases ($R_U \geqslant 0$ and $R_V \geqslant 0$) , ($R_U > 0$ and $R_V \leqslant 0$), and ($R_U < 0$ and $R_V \geqslant 0$), which will lead to three different coding strategies.

1) Encoding: Define $A^{1:N} \triangleq U^{1:N} G_n$, $B^{1:N} \triangleq V^{1:N} G_n$, and $C^{1:N} \triangleq (X_1)^{1:N} G_n$. The functional dependence graphs for the three cases $\min(R_U, R_V) \geqslant 0$, ($R_U > 0$ and $R_V \leqslant 0$), and ($R_U < 0$ and $R_V \geqslant 0$) are depicted in Figures 6, 7, and 8, respectively. The encoding procedure for Transmitters 1 and 2 is as follows.

- Transmitter 2:
  - Assume $\min(R_U, R_V) \geqslant 0$. As described in Section III, our strategy is to make each virtual user use the encoding scheme for a point-to-point wiretap channel E^{WT} in Algorithm 1.
    (i) Apply the encoding scheme E^{WT} by doing the substitutions $X \leftarrow U$, $Z \leftarrow ZVX_1$, $S_{1:L} \leftarrow M_{1:L}^{(U)}$ to encode the secret messages $M_{1:L}^{(U)}$ and let $U_{1:L}^{1:N}$ denote the outputs of this encoding step. For $i \in [\![1, L]\!]$, we add the superscript (U) to Φ_i and Ψ_i defined in E^{WT}.
    (ii) Apply the encoding scheme E^{WT} by doing the substitutions, $X \leftarrow V$, $Y \leftarrow YUX_1$, $S_{1:L} \leftarrow M_{1:L}^{(V)}$ to encode the secret messages $M_{1:L}^{(V)}$ and let $V_{1:L}^{1:N}$ 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}.
  - Assume $R_U > 0$ and $R_V \leqslant 0$. As described in Section III, our strategy is to make the virtual user associated with $R_U > 0$ use the encoding scheme for a point-to-point wiretap code E^{WT} in Algorithm 1, and to make the other virtual user use the cooperative jamming encoding scheme E^{CJ1} in Algorithm 2. The aim of E^{CJ1} is to approximate a target distribution at the input of a channel, and can be understood as performing source resolvability [39] for each encoding block.
    (i) Encode the secret messages $M_{1:L}^{(U)}$ as in the case $\min(R_U, R_V) \geqslant 0$.
    (ii) Apply the encoding scheme E^{CJ1} by doing the substitution $X \leftarrow V$. Let $\widetilde{V}_{1:L}^{1:N}$ denote the outputs of this encoding step. Hence, the virtual user associated with the input V does not transmit information messages via $\widetilde{V}_{1:L}^{1:N}$.
  - Assume $R_U < 0$ and $R_V \geqslant 0$. As described in Section III, the strategy is for the virtual user associated with $R_V \geqslant 0$ to use the encoding scheme for a point-to-point wiretap code E^{WT} in Algorithm 1, and for the other virtual user to perform cooperative jamming with the encoding scheme E^{CJ2} in Algorithm 3. Here, cooperative jamming is aided by secret information with rate $-R_U$, that has been secretly transmitted to the legitimate receiver via the virtual user associated with rate R_V. More specifically, in Algorithm 3 provided that the transmitter and the legitimate receiver share $(L-1)(|\mathcal{V}_{U|Y}| - |\mathcal{V}_{U|ZVX_1}|)$ uniformly distributed bits, E^{CJ2} aims at making available at the legitimate receiver the codewords sent at the input of the channel while concealing in each block $|\mathcal{V}_{U|ZVX_1}|$ bits from the eavesdropper.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

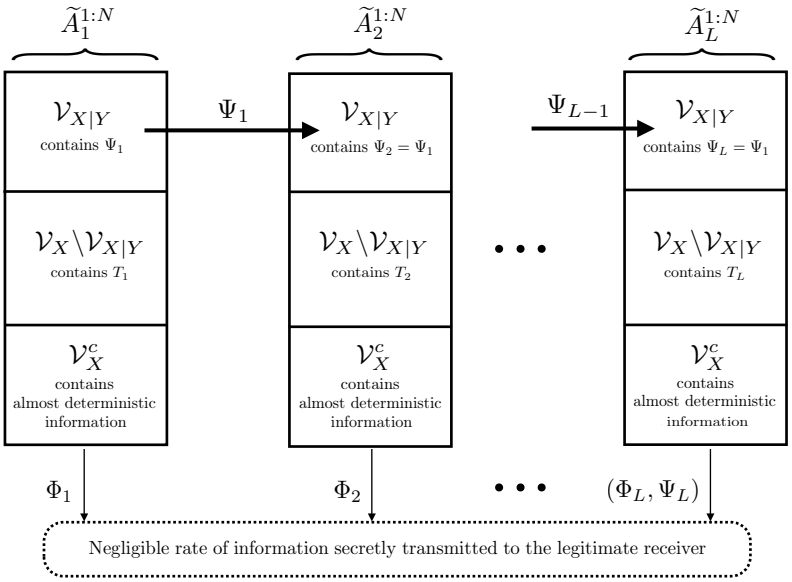

Fig. 5. Encoding scheme E^{CJ3}. In Block $i \in [\![1, L]\!]$, $\widetilde{A}_i^{1:N}$ is constructed from the local randomness T_i, and the subsequence Ψ_{i-1} of the previous block $\widetilde{A}_{i-1}^{1:N}$. The remaining symbols of $\widetilde{A}_i^{1:N}$ are almost deterministic given (T_i, Ψ_{i-1}). Note that (Ψ_i, Φ_i) is the information necessary to the legitimate receiver to recover $\widetilde{A}_i^{1:N}$. Note also that Ψ_i is uniform and repeated in Block $i+1$, whereas Φ_i, whose rate is negligible, is non-uniform and secretly transmitted to the legitimate receiver with a one-time pad. Finally, $\widetilde{A}_L^{1:N}[\mathcal{H}_{X|Y}]$ is also secretly transmitted to the legitimate receiver with a one-time pad, and the rate of this transmission vanishes to zero as the number of blocks L increases.

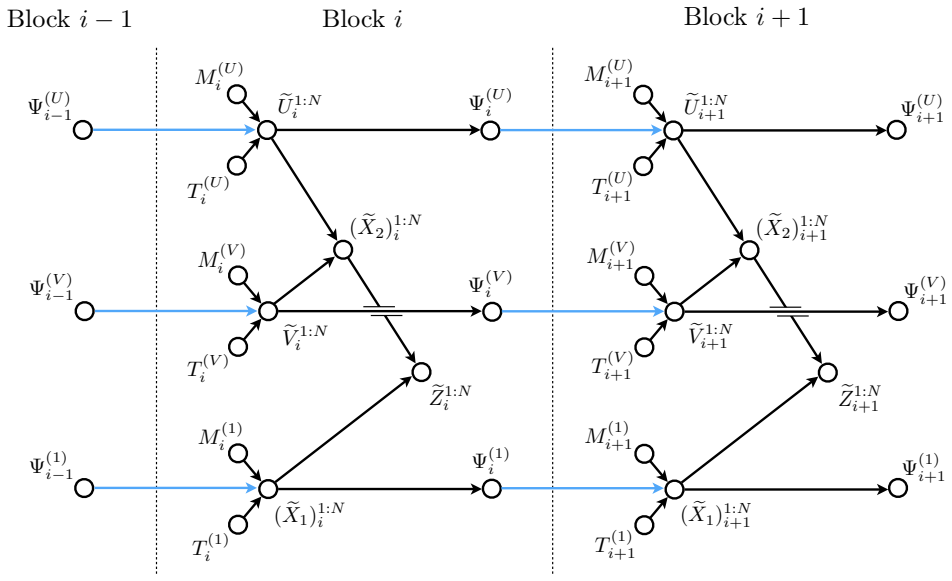

Fig. 6. Functional dependence graph of the block encoding scheme when $\min(R_U, R_V) \geqslant 0$. In Block $i \in [\![1, L]\!]$, $\widetilde{U}_i^{1:N}$ is constructed with the message $M_i^{(U)}$, the randomization sequence $T_i^{(U)}$, and the subsequence $\Psi_{i-1}^{(U)}$ of $\widetilde{U}_{i-1}^{1:N}$. $\widetilde{V}_i^{1:N}$ is constructed with the messages $M_i^{(V)}$ and $\overline{M}_i^{(V)}$, the randomization sequence $T_i^{(V)}$, and the subsequence $\Psi_{i-1}^{(V)}$ of $\widetilde{V}_{i-1}^{1:N}$. $(\widetilde{X}_2)_i^{1:N}$ is constructed from $(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N})$ and is sent over the channel by User 2. User 1 sends $(\widetilde{X}_1)_i^{1:N}$ over the channel, where $(\widetilde{X}_1)_i^{1:N}$ is constructed from the message $M_i^{(1)}$, the randomization sequence $T_i^{(1)}$, and the subsequence $\Psi_{i-1}^{(1)}$ of $(\widetilde{X}_1)_{i-1}^{1:N}$. We have represented in blue the dependencies between consecutive blocks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

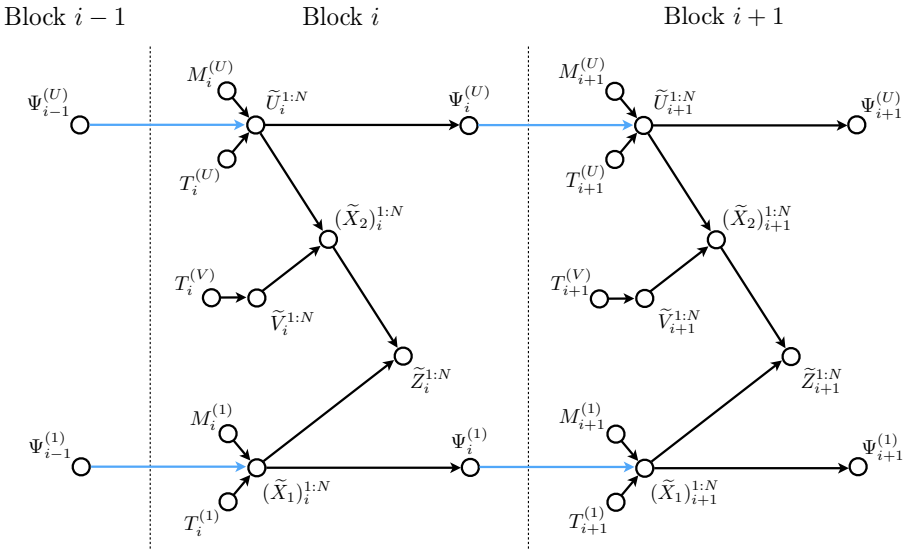

Fig. 7. Functional dependence graph of the block encoding scheme when $R_U > 0$ and $R_V \leqslant 0$. The description of this figure is similar to the one of Figure 6, except that $\widetilde{V}_i^{1:N}$ is here only constructed with the randomization sequence $T_i^{(V)}$ as $M_i^{(V)} = \emptyset$, $i \in [\![1, L]\!]$. Note also that $\Psi_{1:L}^{(V)} = \emptyset$.

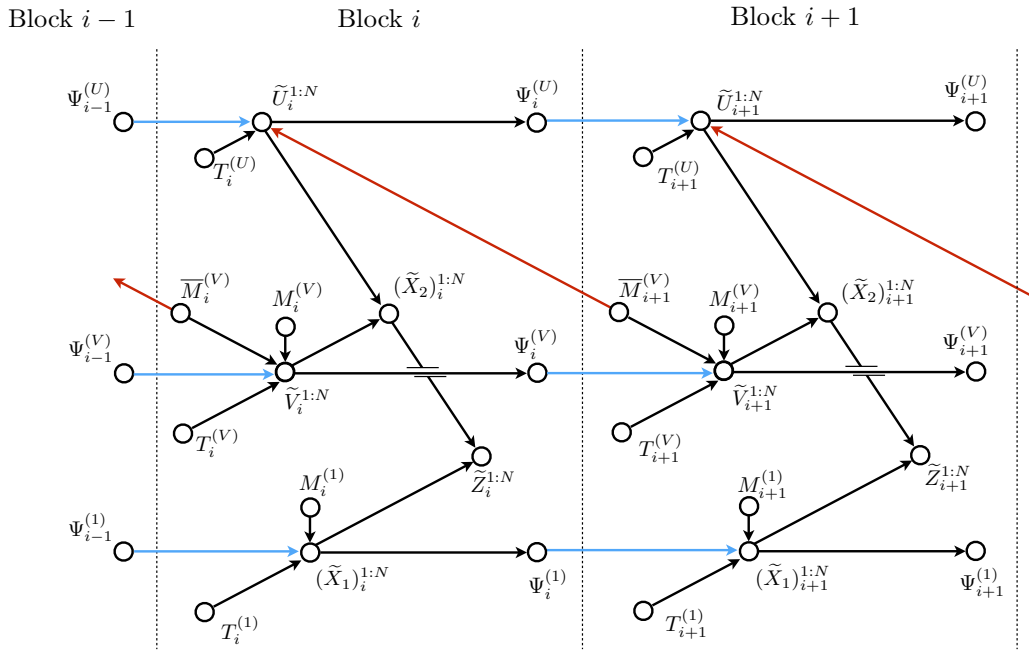

Fig. 8. Functional dependence graph of the block encoding scheme when $R_U < 0$ and $R_V \geqslant 0$. The description of this figure is similar to the one of Figure 6, except that the construction of $\widetilde{V}_i^{1:N}$ requires in addition the message $\overline{M}_i^{(V)}$, and the construction of $\widetilde{U}_i^{1:N}$ requires the message $\overline{M}_{i+1}^{(V)}$. Hence, note that additional inter-block dependencies, depicted in red, exist.

These codewords do not contain information but will help the other users (virtual and real) to communicate their secret information messages with the legitimate receiver.

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

$$|\overline{M}_i^{(V)}| \triangleq |\mathcal{V}_{U|Y}| - |\mathcal{V}_{U|ZVX_1}|,$$

$$|M_i^{(V)}| \triangleq |\mathcal{V}_{V|Z} \backslash \mathcal{A}_{V|YUX_1}| - |\overline{M}_i^{(V)}|,$$

such that $|\overline{M}_i^{(V)}| + |M_i^{(V)}| = |\mathcal{V}_{V|Z} \backslash \mathcal{A}_{V|YUX_1}|$. 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^{CJ2} with the substitutions $X \leftarrow U$, $Z \leftarrow ZVX_1$, for $i \in [\![1, B-1]\!]$, $K_i \leftarrow \overline{M}_{i+1}^{(V)}$. Let $\widetilde{U}_{1:L}^{1:N}$ denote the outputs of this encoding step. For $i \in [\![1, L]\!]$, we add the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

Algorithm 3 Generic Encoding Scheme E^{CJ2}

Require: $L-1$ vectors $\{K_i\}_{i\in[\![1,L-1]\!]}$ of $|\mathcal{K}_{XYZ}|$ uniformly distributed bits that represent shared randomness between encoder and decoder.
T_1 a vector of $|\mathcal{V}_X\backslash\mathcal{K}_{XYZ}|$ uniformly distributed bits, T_L a vector of $|\mathcal{V}_X\backslash\mathcal{V}_{X|Z}|$ uniformly distributed bits, and $L-2$ vectors $\{T_i\}_{i\in[\![2,L-1]\!]}$ of $|\mathcal{V}_X\backslash(\mathcal{V}_{X|Z}\cup\mathcal{K}_{XYZ})|$ uniformly distributed bits that represent randomization sequences.

for Block $i=1$ to L **do**
  if $i=1$ **then**
    $\widetilde{A}_1^{1:N}[\mathcal{K}_{XYZ}]\leftarrow K_1$
    $\widetilde{A}_1^{1:N}[\mathcal{V}_X\backslash\mathcal{K}_{XYZ}]\leftarrow T_1$
  else if $i\in[\![2,L]\!]$ **then**
    $\widetilde{A}_i^{1:N}[\mathcal{K}_{XYZ}]\leftarrow K_i$
    $\widetilde{A}_i^{1:N}[\mathcal{V}_{X|Z}]\leftarrow\Psi_{i-1}$
    $\widetilde{A}_i^{1:N}[\mathcal{V}_X\backslash(\mathcal{V}_{X|Z}\cup\mathcal{K}_{XYZ})]\leftarrow T_i$
  else if $i=L$ **then**
    $\widetilde{A}_L^{1:N}[\mathcal{V}_{X|Z}]\leftarrow\Psi_{L-1}$
    $\widetilde{A}_L^{1:N}[\mathcal{V}_X\backslash\mathcal{V}_{X|Z}]\leftarrow T_L$
  end if
  Successively draw the remaining components of $\widetilde{A}_i^{1:N}$, i.e., the components in $\mathcal{V}_X^c$, according to

$$\widetilde{p}_{A_i^j|A_i^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \triangleq p_{A^j|A^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \text{ if } j\in\mathcal{V}_X^c.$$

  if $i=L$ **then**
    $\Psi_L\leftarrow\widetilde{A}_L^{1:N}[\mathcal{V}_{X|Y}]$
  else
    $\Psi_i\leftarrow\widetilde{A}_i^{1:N}[\mathcal{C}_{XYZ}\cup(\mathcal{V}_{X|Y}\cap\mathcal{V}_{X|Z})]$
  end if
  $\Phi_i\leftarrow\widetilde{A}_i^{1:N}[\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Y}^c]$
  $\widetilde{X}_i^{1:N}\leftarrow\widetilde{A}_i^{1:N}G_n$
end for
The transmitter securely shares $(\Psi_L,\Phi_{1:L})$ with the legitimate receiver by means of a one-time pad.

superscript (U) to Φ_i and Ψ_i defined in E^{CJ2}. Note that the virtual user associated with input U does not transmit information messages.

Finally, in all cases do (iii).

(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 $i\in[\![1,L]\!]$, where f is defined as in Lemma 1.

- Transmitter 1: As described in Section III, Transmitter1 is associated with a positive secrecy rate and uses the encoding scheme for a point-to-point wiretap code E^{WT} in Algorithm 1.

(i) Apply the encoding scheme E^{WT} by doing the substitutions $X\leftarrow X_1$, $Z\leftarrow ZV$, $Y\leftarrow YU$, $S_{1:L}\leftarrow M_{1:L}^{(1)}$ 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 $i\in[\![1,L]\!]$.

Algorithm 4 Generic Encoding Scheme E^{CJ3}

Require: Ψ_1 a vector of $|\mathcal{V}_{X|Y}|$ uniformly distributed bits.
L vectors $\{T_i\}_{i\in[\![1,L]\!]}$ of $|\mathcal{V}_X\backslash\mathcal{V}_{X|Y}|$ uniformly distributed bits that represent randomization sequences.

for Block $i=1$ to L **do**
  $\widetilde{A}_i^{1:N}[\mathcal{V}_{X|Y}]\leftarrow\Psi_1$
  $\widetilde{A}_i^{1:N}[\mathcal{V}_X\backslash\mathcal{V}_{X|Y}]\leftarrow T_i$
  Successively draw the remaining components of $\widetilde{A}_i^{1:N}$, i.e., the components in $\mathcal{V}_X^c$, according to

$$\widetilde{p}_{A_i^j|A_i^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \triangleq p_{A^j|A^{1:j-1}}(a_i^j|\widetilde{A}_i^{1:j-1}) \text{ if } j\in\mathcal{V}_X^c.$$

  $\Psi_i\leftarrow\widetilde{A}_i^{1:N}[\mathcal{V}_{X|Y}]$
  $\Phi_i\leftarrow\widetilde{A}_i^{1:N}[\mathcal{H}_{X|Y}\backslash\mathcal{V}_{X|Y}]$
  $\widetilde{X}_i^{1:N}\leftarrow\widetilde{A}_i^{1:N}G_n$
end for
The transmitter securely shares $(\Psi_L,\Phi_{1:L})$ with the legitimate receiver by means of a one-time pad.

In Block $i\in[\![1,L]\!]$, the channel observations of the legitimate receiver and the eavesdropper are denoted by $\widetilde{Y}_i^{1:N}$ and $\widetilde{Z}_i^{1:N}$, respectively.

2) Decoding:

For each Block $i\in[\![1,L]\!]$, the receiver decodes as follows.

- Assume $R_U<0$ and $R_V\geqslant 0$.
The receiver decodes as follows. Define

$$\begin{aligned}\widehat{\Psi}_L^{(U)}&\triangleq\Psi_L^{(U)},\\ \widehat{\Psi}_L^{(V)}&\triangleq\Psi_L^{(V)},\\ \widehat{\Psi}_L^{(1)}&\triangleq\Psi_L^{(1)},\\ \widehat{\widehat{M}}_{L+1}^{(V)}&\triangleq\emptyset,\\ \widehat{A}_L^{1:N}[\mathcal{H}_{U|Y}]&\triangleq\widetilde{A}_L^{1:N}[\mathcal{H}_{U|Y}],\\ \widehat{C}_L^{1:N}[\mathcal{H}_{X_1|YU}]&\triangleq\widetilde{C}_L^{1:N}[\mathcal{H}_{X_1|YU}],\\ \widehat{B}_L^{1:N}[\mathcal{H}_{V|YUX_1}]&\triangleq\widetilde{B}_L^{1:N}[\mathcal{H}_{V|YUX_1}].\end{aligned}$$

Then, for i from L to 1, given $\widetilde{Y}_i^{1:N}$ and $\left(\widehat{\Psi}_i^{(U)},\Phi_i^{(U)},\widehat{\widehat{M}}_{i+1}^{(V)}\right)=\widehat{A}_i^{1:N}[\mathcal{H}_{U|Y}]$, use the successive cancellation (SC) decoder for source coding with side information of [25] to form an estimate $\widehat{A}_i^{1:N}$ of $\widetilde{A}_i^{1:N}$. The decoder thus obtains an estimate $\widehat{\Psi}_{i-1}^{(U)}$ of $\Psi_{i-1}^{(U)}$, and form $\widehat{U}_i^{1:N}\triangleq\widehat{A}_i^{1:N}G_n$. Then, given $(\widetilde{Y}_i^{1:N},\widehat{U}_i^{1:N})$ and $\left(\widehat{\Psi}_i^{(1)},\Phi_i^{(1)}\right)=\widehat{C}_i^{1:N}[\mathcal{H}_{X_1|YU}]$, use the SC decoder of [25] to form an estimate $\widehat{C}_i^{1:N}$ of $\widetilde{C}_i^{1:N}$. The decoder thus obtains an estimate $\widehat{\Psi}_{i-1}^{(1)}$ of $\Psi_{i-1}^{(1)}$, and form $(\widehat{X}_1)_i^{1:N}\triangleq\widehat{C}_i^{1:N}G_n$. Then, given $\left(\widetilde{Y}_i^{1:N},\widehat{U}_i^{1:N},(\widehat{X}_1)_i^{1:N}\right)$ and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

$\left(\widehat{\Psi}_i^{(V)}, \Phi_i^{(V)}\right) = \widehat{B}_i^{1:N}[\mathcal{H}_{V|YUX_1}]$, use the SC decoder of [25] to form an estimate $\widehat{B}_i^{1:N}$ of $\widetilde{B}_i^{1:N}$. The decoder thus obtains an estimate $\widehat{\Psi}_{i-1}^{(V)}$ of $\Psi_{i-1}^{(V)}$. Define $\widehat{V}_i^{1:N} \triangleq \widehat{B}_i^{1:N} G_n$ and let $\widehat{\overline{M}}_i^{(V)}$ denote an estimate of $\overline{M}_i^{(V)}$.
Finally, from $\left((\widehat{X}_1)_{1:L}^{1:N}, \widehat{V}_{1:L}^{1:N}\right)$ the decoder obtains estimates of $M_{1:L}^{(V)}$, and $M_{1:L}^{(1)}$.

- Assume $R_U \geqslant 0$ and $R_V \geqslant 0$.
The decoder operates as in the case $R_U < 0$ and $R_V \geqslant 0$, with $\overline{M}_{1:L}^{(V)} = \emptyset$. Moreover, the decoder estimates $M_{1:L}^{(U)}$ from $\widehat{U}_{1:L}^{1:N}$.
- Assume $R_U > 0$ and $R_V \leqslant 0$.
The decoder operates as in the case $R_U < 0$ and $R_V \geqslant 0$, with $\widehat{V}_{1:L}^{1:N} = \emptyset$ and $\overline{M}_{1:L}^{(V)} = \emptyset$. Remark indeed that $\widehat{V}_{1:L}^{1:N}$ is not needed to form the estimates $\widehat{U}_{1:L}^{1:N}$ and $(\widehat{X}_1)_{1:L}^{1:N}$. Moreover, the decoder obtains estimates of $M_{1:L}^{(U)}$ from $\widehat{U}_{1:L}^{1:N}$.

Remark 2. *Depending on the sign of R_U and R_V, observe that $\Psi_{1:L}^{(U)}$, $\Phi_{1:L}^{(U)}$, $\Psi_{1:L}^{(V)}$, and $\Phi_{1:L}^{(V)}$ do not have the same definition. Note also that depending on the sign of R_U the messages $M_{1:L}^{(V)}$ do not have the same size.*

Remark 3. *Observe that the cooperative jamming scheme for the case ($R_U > 0$ and $R_V \leqslant 0$) is simpler than for the case ($R_U < 0$ and $R_V \geqslant 0$) because, in the former case, reconstruction of $\widetilde{V}_{1:L}^{1:N}$ at the legitimate user is not necessary in the decoding procedure.*

C. Coding scheme for achieving $\mathcal{R}''(p_{X_1}p_{X_2})$

In this section, $M_{1:L}^{(1)}$ and $M_{1:L}^{(2)}$ are the binary, uniformly distributed, and mutually independent secret messages to be transmitted over the L blocks by Transmitters 1 and 2, respectively.

1) Encoding: Define $A^{1:N} \triangleq (X_1)^{1:N} G_n$ and $B^{1:N} \triangleq (X_2)^{1:N} G_n$. The functional dependence graph is depicted in Figure 9 and the encoding for Transmitters 1 and 2 is as follows.

- Transmitter 2: As described in Section III, Transmitter 2 performs cooperative jamming with the encoding scheme E^{CJ3} in Algorithm 4, which aims at making available at the legitimate receiver the codewords sent at the input of the channel without any secrecy constraint. The codewords sent do not contain information but will help the other user to secretly transmit his messages. Moreover, although the scheme sends codewords only the distribution of the channel input is critical.
  (i) Apply the encoding scheme E^{CJ3} by doing the substitutions $X \leftarrow X_2$, and let $(\widetilde{X}_2)_{1:L}^{1:N}$ denote the outputs of this encoding step. For $i \in [\![1, L]\!]$, we add the superscript (2) to Φ_i and Ψ_i defined in E^{CJ3}. Note that Transmitter 2 does not transmit information messages.
  (ii) Send over the channel $(\widetilde{X}_2)_i^{1:N}$ for each encoding Block $i \in [\![1, L]\!]$.
- Transmitter 1: As described in Section III, Transmitter 1 is associated with a positive secrecy rate and use the encoding scheme for a point-to-point wiretap code E^{WT} in Algorithm 1.
  (i) Apply the encoding scheme E^{WT} by doing the substitutions $X \leftarrow X_1$, $Z \leftarrow ZX_2$, $Y \leftarrow YX_2$, $S_{1:L} \leftarrow M_{1:L}^{(1)}$ to encode the secret messages $M_{1:L}^{(1)}$ and let $(\widetilde{X}_1)_{1:L}^{1:N}$ denote the result 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: The receiver decodes as follows. Define

$$\begin{aligned}
\widehat{\Psi}_L^{(2)} &\triangleq \Psi_L^{(2)}, \\
\widehat{\Psi}_L^{(1)} &\triangleq \Psi_L^{(1)}, \\
\widehat{B}_L^{1:N}[\mathcal{H}_{X_2|Y}] &\triangleq \widetilde{B}_L^{1:N}[\mathcal{H}_{X_2|Y}], \\
\widehat{A}_L^{1:N}[\mathcal{H}_{X_1|YX_2}] &\triangleq \widetilde{A}_L^{1:N}[\mathcal{H}_{X_1|YX_2}].
\end{aligned}$$

Then, for i from L to 1 given $\widetilde{Y}_i^{1:N}$ and $\left(\widehat{\Psi}_i^{(2)}, \Phi_i^{(2)}\right) = \widehat{B}_i^{1:N}[\mathcal{H}_{X_2|Y}]$, use the SC decoder for source coding with side information of [25] to form an estimate $\widehat{B}_i^{1:N}$ of $\widetilde{B}_i^{1:N}$. The decoder thus obtains an estimate $\widehat{\Psi}_{i-1}^{(2)}$ of $\Psi_{i-1}^{(2)}$ and form $(\widehat{X}_2)_i^{1:N} \triangleq \widehat{B}_i^{1:N} G_n$. Then, given $\left(\widetilde{Y}_i^{1:N}, (\widehat{X}_2)_i^{1:N}\right)$ and $\left(\widehat{\Psi}_i^{(1)}, \Phi_i^{(1)}\right) = \widehat{A}_i^{1:N}[\mathcal{H}_{X_1|YX_2}]$, use the SC decoder of [25] to form an estimate $\widehat{A}_i^{1:N}$ of $\widetilde{A}_i^{1:N}$. The decoder thus obtains an estimate $\widehat{\Psi}_{i-1}^{(1)}$ of $\Psi_{i-1}^{(1)}$ and forms $(\widehat{X}_1)_i^{1:N} \triangleq \widehat{A}_i^{1:N} G_n$. Finally, from $(\widehat{X}_1)_{1:L}^{1:N}$ the decoder obtains an estimate of $M_{1:L}^{(1)}$.

V. Main result and Scheme analysis

The analysis for the coding schemes of Sections IV-B, IV-C are provided in Sections V-A, V-B, respectively. Our main result is summarized as follows.

Theorem 2. *Consider a discrete memoryless MAC-WT $(\mathcal{X}_1 \times \mathcal{X}_2, W_{YZ|X_1X_2}, \mathcal{Y}, \mathcal{Z})$, where $|\mathcal{X}_1| = |\mathcal{X}_2| = 2$. The coding schemes of Section IV, which operate over L encoding blocks of length N and whose complexities are $O(LN \log N)$, achieve the region $\mathcal{R}$ defined in Theorem 1.*

Remark 4. *In Theorem 2, the case of prime alphabet sizes for $\mathcal{X}_1$, $\mathcal{X}_2$ can be addressed as in [16].*

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

Example 1. *Assume $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y} = \mathcal{Z} = \{0, 1\}$. Consider X_1, X_2, independent and uniformly distributed, B independent of (X_1, X_2) following a Bernoulli distribution with parameter α, i.e., $p_B(1) = \alpha$. Consider the channel defined by $Y \triangleq X_1 \oplus X_2$, $Z \triangleq Y \oplus B$. Define for $\epsilon \in [0, 1]$, $v_0 \triangleq \frac{1}{2-\epsilon}$, $\bar{v}_0 \triangleq 1 - v_0$, $u_0 \triangleq 1 - \frac{\epsilon}{2}$, $\bar{u}_0 \triangleq 1 - u_0$. We also define $\bar{\alpha} = 1 - \alpha$. After some computations and following the rate-splitting method described in Section III-A, one can*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

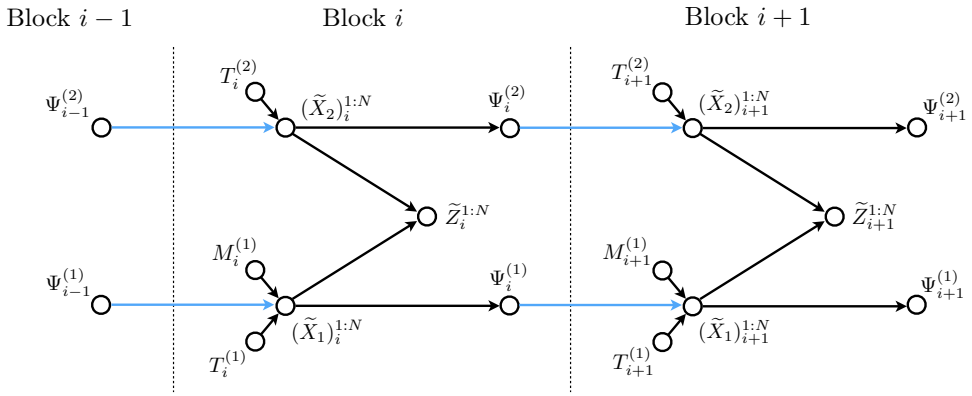

Fig. 9. Functional dependence graph of the block encoding scheme. In Block $i \in [\![1, L]\!]$, $(\widetilde{X}_2)_i^{1:N}$ is constructed with the randomization sequence $T_i^{(2)}$, and the subsequence $\Psi_{i-1}^{(2)}$ of $(\widetilde{X}_2)_{i-1}^{1:N}$, and is sent over the channel by User 2. User 1 sends $(\widetilde{X}_1)_i^{1:N}$ over the channel, where $(\widetilde{X}_1)_i^{1:N}$ is constructed from the information message $M_i^{(1)}$, the randomization sequence $T_i^{(1)}$, and the subsequence $\Psi_{i-1}^{(1)}$ of $(\widetilde{X}_1)_{i-1}^{1:N}$.

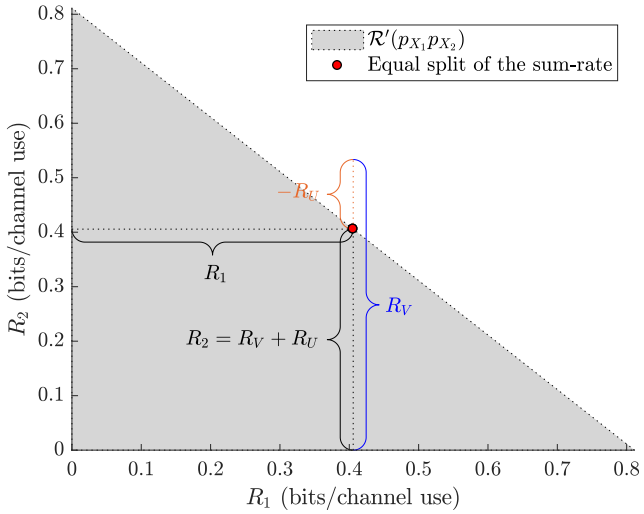

Fig. 10. Representation of $\mathcal{R}'(p_{X_1}p_{X_2})$ for the setting described in Example 1. We fix $\alpha = 1/4$. The point that corresponds to an equal split of the sum rate between both transmitters (with precision 10^{-4}) is obtained with $\epsilon = 0.674024$, $R_U \in [-0.1279, -0.1278]$, $R_V \in [0.5334, 0.5335]$, $R_1 \in [0.4056, 0.4057]$.

show that

$$\begin{aligned} R_U(\epsilon) &= v_0 \left[H_b(\alpha) - H_b\left(\bar{\alpha}u_0 + \alpha\bar{u}_0\right)\right], \\ R_V(\epsilon) &= u_0 H_b\left(v_0\right), \\ R_1(\epsilon) &= v_0 H_b\left(\bar{\alpha}u_0 + \alpha\bar{u}_0\right) + \bar{v}_0 H_b(\alpha) - u_0 H_b\left(v_0\right), \\ R_1(\epsilon) + R_U(\epsilon) + R_V(\epsilon) &= H_b(\alpha), \end{aligned}$$

where H_b denotes the binary entropy. We have represented $\mathcal{R}'(p_{X_1}p_{X_2})$ in Figure 10 for $\alpha = 1/4$ and precised the choice of ϵ to equally split the sum-rate among both transmitters.

A. Scheme analysis for the achievability of $\mathcal{R}'(p_{X_1}p_{X_2})$ when $\min(g(\{1\}), g(\{2\})) > 0$

1) Induced distribution: A crucial step to assess reliability and secrecy for our coding scheme, as we will later see, is the study of the distribution induced by our encoders. We first review the following result whose proof follows from [16], see also [19], [38], [40], [41].

Lemma 4. *Consider a binary memoryless source $(\mathcal{X}, p_X)$ and define $A^{1:N} \triangleq X^{1:N}G_n$. Assume that $\widetilde{A}^{1:N}$, whose distribution is denoted by $\widetilde{p}_{A^{1:N}}$, is constructed as follows. The bits of $\widetilde{A}^{1:N}$ indexed by $\mathcal{V}_X$ are uniformly distributed and the remaining bits of $\widetilde{A}^{1:N}$ indexed by $j \in \mathcal{V}_X^c$ follow the distribution $p_{A^j|A^{1:j-1}}$, $j \in \mathcal{V}_X^c$. Then, $\mathbb{V}(\widetilde{p}_{A^{1:N}}, p_{A^{1:N}}) \leqslant \delta(N)$.*

We can now prove the following lemma.

Lemma 5. *Let $\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_1)_i^{1:N}(X_2)_i^{1:N}Y_i^{1:N}Z_i^{1:N}}$ 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*

$$\begin{aligned} \mathbb{V}\Big(&\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_1)_i^{1:N}(X_2)_i^{1:N}Y_i^{1:N}Z_i^{1:N}}, \\ &p_{U^{1:N}V^{1:N}(X_1)^{1:N}(X_2)^{1:N}Y^{1:N}Z^{1:N}}\Big) \leqslant \delta(N). \end{aligned}$$

Proof. Since $(\widetilde{U}_i^{1:N}\widetilde{V}_i^{1:N}) - (\widetilde{X}_1)_i^{1:N}(\widetilde{X}_2)_i^{1:N} - \widetilde{Y}_i^{1:N}\widetilde{Z}_i^{1:N}$, we have

$$\begin{aligned} &\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_1)_i^{1:N}(X_2)_i^{1:N}Y_i^{1:N}Z_i^{1:N}} \\ &= p_{Y^{1:N}Z^{1:N}|X_1^{1:N}X_2^{1:N}}\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_1)_i^{1:N}(X_2)_i^{1:N}}, \end{aligned}$$

hence, by redefining $\delta(N)$ when necessary,

$$\begin{aligned} &\mathbb{V}\Big(\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_1)_i^{1:N}(X_2)_i^{1:N}Y_i^{1:N}Z_i^{1:N}}, \\ &\qquad p_{U^{1:N}V^{1:N}X_1^{1:N}X_2^{1:N}Y^{1:N}Z^{1:N}}\Big) \\ &= \mathbb{V}\left(\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_1)_i^{1:N}(X_2)_i^{1:N}}, p_{U^{1:N}V^{1:N}X_1^{1:N}X_2^{1:N}}\right) \\ &\overset{(a)}{=} \mathbb{V}\left(\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_2)_i^{1:N}}\widetilde{p}_{(X_1)_i^{1:N}}, p_{U^{1:N}V^{1:N}X_2^{1:N}}p_{X_1^{1:N}}\right) \\ &\overset{(b)}{\leqslant} \mathbb{V}\left(\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_2)_i^{1:N}}, p_{U^{1:N}V^{1:N}X_2^{1:N}}\right) \\ &\qquad + \mathbb{V}\left(\widetilde{p}_{(X_1)_i^{1:N}}, p_{X_1^{1:N}}\right) \\ &\overset{(c)}{\leqslant} \mathbb{V}\left(\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_2)_i^{1:N}}, p_{U^{1:N}V^{1:N}X_2^{1:N}}\right) + \delta(N) \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

$$\begin{aligned}
&\overset{(d)}{=} \mathbb{V}\left(\widetilde{p}_{(X_2)_i^{1:N}|U_i^{1:N}V_i^{1:N}}\widetilde{p}_{U_i^{1:N}}\widetilde{p}_{V_i^{1:N}}, \right.\\
&\qquad \left. p_{X_2^{1:N}|U^{1:N}V^{1:N}}p_{U^{1:N}}p_{V^{1:N}}\right) + \delta(N)\\
&\overset{(e)}{=} \mathbb{V}\left(\widetilde{p}_{U_i^{1:N}}\widetilde{p}_{V_i^{1:N}}, p_{U^{1:N}}p_{V^{1:N}}\right) + \delta(N)\\
&\overset{(f)}{\leqslant} \mathbb{V}\left(\widetilde{p}_{U_i^{1:N}}, p_{U^{1:N}}\right) + \mathbb{V}\left(\widetilde{p}_{V_i^{1:N}}, p_{V^{1:N}}\right) + \delta(N)\\
&\overset{(g)}{\leqslant} \delta(N),
\end{aligned}$$

where (a) holds by independence between $(\widetilde{X}_1)_i^{1:N}$ and $(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N}, (\widetilde{X}_2)_i^{1:N})$ and between $X_1^{1:N}$ and $(U^{1:N}, V^{1:N}, (X_2)^{1:N})$, (b) holds by the triangle inequality, (c) holds by Lemma 4, (d) holds by independence between $\widetilde{U}_i^{1:N}$ and $\widetilde{V}_i^{1:N}$ and between $U^{1:N}$ and $V^{1:N}$, (e) holds because $(\widetilde{X}_2)_i^{1:N} = f(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N})$ and $X_2^{1:N} = f(U^{1:N}, V^{1:N})$, (f) holds by the triangle inequality, (g) holds by Lemma 4. ∎

2) Communication rates: We now determine the different communication rates. In all cases, the rate of $M_{1:L}^{(1)}$ is

$$\begin{aligned}
\frac{1}{NL}\sum_{i=1}^{L}|M_i^{(1)}| &= \frac{|\mathcal{V}_{X_1|ZV}|+(L-1)|\mathcal{V}_{X_1|ZV}\backslash\mathcal{A}_{X_1|YU}|}{NL}\\
&\geqslant \frac{|\mathcal{V}_{X_1|ZV}\backslash\mathcal{A}_{X_1|YU}|}{N}\\
&\overset{(a)}{\geqslant} \frac{|\mathcal{V}_{X_1|ZV}|-|\mathcal{H}_{X_1|YU}|}{N}\\
&\xrightarrow{N\to\infty} H(X_1|ZV) - H(X_1|YU)\\
&= I(X_1;YU) - I(X_1;ZV)\\
&\overset{(b)}{=} R_1
\end{aligned}$$

where (a) holds because $\mathcal{A}_{X_1|YU} \subset \mathcal{V}_{X_1|ZV}$ and $|\mathcal{A}_{X_1|YU}|= |\mathcal{H}_{X_1|YU} \cap \mathcal{V}_{X_1}|$, (b) holds by independence between X_1 and U and between X_1 and V, the limit holds by Lemmas 2, 3.

Assume first that $R_U \geqslant 0$ and $R_V \geqslant 0$. Similar to the rate of $M_{1:L}^{(1)}$, the rate of of $M_{1:L}^{(U)}$ is

$$\begin{aligned}
\frac{1}{NL}\sum_{i=1}^{L}|M_i^{(U)}| &= \frac{|\mathcal{V}_{U|ZVX_1}|+(L-1)|\mathcal{V}_{U|ZVX_1}\backslash\mathcal{A}_{U|Y}|}{NL}\\
&\geqslant \frac{|\mathcal{V}_{U|ZVX_1}|-|\mathcal{H}_{U|Y}|}{N}\\
&\xrightarrow{N\to\infty} H(U|ZVX_1) - H(U|Y)\\
&= I(U;Y) - I(U;ZVX_1)\\
&= I(U;Y) - I(U;Z|VX_1)\\
&= R_U,
\end{aligned}$$

and the rate of of $M_{1:L}^{(V)}$ is

$$\begin{aligned}
\frac{1}{NL}\sum_{i=1}^{L}|M_i^{(V)}| &= \frac{|\mathcal{V}_{V|Z}|+(L-1)|\mathcal{V}_{V|Z}\backslash\mathcal{A}_{V|YUX_1}|}{NL}\\
&\geqslant \frac{|\mathcal{V}_{V|Z}|-|\mathcal{H}_{V|YUX_1}|}{N}\\
&\xrightarrow{N\to\infty} H(V|Z) - H(V|YUX_1)\\
&= I(V;YUX_1) - I(V;Z)\\
&= I(V;Y|UX_1) - I(V;Z)\\
&= R_V.
\end{aligned}$$

Assume now that $R_U > 0$ and $R_V \leqslant 0$, then the rate of $M_{1:L}^{(V)}$ is equal to zero and the rate of $M_{1:L}^{(U)}$ is derived as in the case $R_U \geqslant 0$ and $R_V \geqslant 0$. We thus obtain a rate $R_U \geqslant R_U + R_V$ for Transmitter 2.

Finally, assume that $R_U < 0$ and $R_V \geqslant 0$. The rate of $M_{1:L}^{(U)}$ is equal to zero and the rate of $M_{1:L}^{(V)}$ is

$$\begin{aligned}
&\frac{1}{NL}\sum_{i=1}^{L}|M_i^{(V)}|\\
&= \frac{|\mathcal{V}_{V|Z}|+\sum_{i=2}^{L}|M_i^{(V)}|}{NL}\\
&= \frac{|\mathcal{V}_{V|Z}|+(L-1)(|\mathcal{V}_{V|Z}\backslash\mathcal{A}_{V|YUX_1}|-|\overline{M}_2^{(V)}|)}{NL}\\
&\overset{(a)}{=} \frac{|\mathcal{V}_{V|Z}|+(L-1)(|\mathcal{V}_{V|Z}|-|\mathcal{H}_{V|YUX_1}\cap\mathcal{V}_V|-|\overline{M}_2^{(V)}|)}{NL}\\
&\geqslant \frac{|\mathcal{V}_{V|Z}|-|\mathcal{H}_{V|YUX_1}|-|\overline{M}_2^{(V)}|}{N}\\
&\overset{(b)}{=} \frac{|\mathcal{V}_{V|Z}|-|\mathcal{H}_{V|YUX_1}|-|\mathcal{V}_{U|Y}|+|\mathcal{V}_{U|ZVX_1}|}{N}\\
&\xrightarrow{N\to\infty} H(V|Z) - H(V|YUX_1) - H(U|Y) + H(U|ZVX_1)\\
&= I(V;YUX_1) - I(V;Z) + I(U;Y) - I(U;ZVX_1)\\
&\overset{(c)}{=} I(V;Y|UX_1) - I(V;Z) + I(U;Y) - I(U;Z|VX_1)\\
&= R_U + R_V,
\end{aligned}$$

where (a) holds because $\mathcal{A}_{V|YUX_1} \subset \mathcal{V}_{V|Z}$ and $|\mathcal{A}_{V|YUX_1}|= |\mathcal{H}_{V|YUX_1} \cap \mathcal{V}_V|$, (b) holds by definition of $|\overline{M}_2^{(V)}|$, the limit holds by Lemmas 2, 3, (c) holds by mutual independence between X_1, U, and V.

Finally, we verify that the rates of the secret seeds required to be shared between the transmitters and the legitimate receiver are negligible. For Transmitter 2 this rate is at most

$$\begin{aligned}
&\frac{|\Psi_L^{(U)}|+|\Psi_L^{(V)}|+\sum_{i=1}^{L}\left(|\Phi_i^{(U)}|+|\Phi_i^{(V)}|\right)}{NL}\\
&= \frac{|\Psi_L^{(U)}|+|\Psi_L^{(V)}|+L\left(|\Phi_1^{(U)}|+|\Phi_1^{(V)}|\right)}{NL}\\
&\leqslant \frac{|\mathcal{H}_{U|Y}|+|\mathcal{H}_{V|YUX_1}|}{NL}\\
&\quad + \frac{|\mathcal{H}_{U|Y}|-|\mathcal{V}_{U|Y}|+|\mathcal{H}_{V|YUX_1}|-|\mathcal{V}_{V|YUX_1}|}{N}\\
&\xrightarrow{N\to\infty,} \frac{H(U|Y)+H(V|YUX_1)}{L}\\
&\xrightarrow{L\to\infty} 0,
\end{aligned}$$

where the first inequality holds by considering the signs of R_U and R_V, and where we have used Lemmas 2, 3 for the limits. For Transmitter 1 the secret seed rate is

$$\frac{|\Psi_L^{(1)}|+\sum_{i=1}^{L}|\Phi_1^{(U)}|}{NL} \leqslant \frac{|\mathcal{H}_{X_1|YU}|}{NL} + \frac{|\mathcal{H}_{X_1|YU}|-|\mathcal{V}_{X_1|YU}|}{N}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

$$\xrightarrow{N\to\infty} \frac{H(X_1|YU)}{L}$$
$$\xrightarrow{L\to\infty} 0.$$

3) Reliability: It will now become clear that Lemma 5 is crucial to ensure reliability. Let $i \in [\![1, L]\!]$, consider a coupling [42, Lemma 3.6] between $\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_1)_i^{1:N}Y_i^{1:N}}$ and $p_{U^{1:N}V^{1:N}(X_1)^{1:N}Y^{1:N}}$ such that

$$\mathbb{P}[\mathcal{E}_i] = \mathbb{V}(\widetilde{p}_{U_i^{1:N}V_i^{1:N}(X_1)_i^{1:N}Y_i^{1:N}}, p_{U^{1:N}V^{1:N}(X_1)^{1:N}Y^{1:N}}),$$

where

$$\mathcal{E}_i \triangleq \{(\widetilde{U}_i^{1:N}, \widetilde{V}_i^{1:N}, (\widetilde{X}_1)_i^{1:N}, \widetilde{Y}_i^{1:N}) \neq (U^{1:N}, V^{1:N}, (X_1)^{1:N}, Y^{1:N})\}.$$

Define also for $i \in [\![1, L]\!]$,

$$\mathcal{E}_{\widetilde{A}_i} \triangleq \left\{\widehat{A}_i^{1:N}[\mathcal{H}_{U|Y}] \neq \widetilde{A}_i^{1:N}[\mathcal{H}_{U|Y}]\right\},$$
$$\mathcal{E}_{\widetilde{B}_i} \triangleq \left\{\widehat{B}_i^{1:N}[\mathcal{H}_{V|YUX_1}] \neq \widetilde{B}_i^{1:N}[\mathcal{H}_{V|YUX_1}]\right\} \cup \left\{\widehat{U}_i^{1:N} \neq \widetilde{U}_i^{1:N}\right\} \cup \left\{(\widehat{X}_1)_i^{1:N} \neq (\widetilde{X}_1)_i^{1:N}\right\},$$
$$\mathcal{E}_{\widetilde{C}_i} \triangleq \left\{\widehat{C}_i^{1:N}[\mathcal{H}_{X_1|YU}] \neq \widetilde{C}_i^{1:N}[\mathcal{H}_{X_1|YU}]\right\} \cup \left\{\widehat{U}_i^{1:N} \neq \widetilde{U}_i^{1:N}\right\}.$$

We consider the case $R_U < 0$ and $R_V \geqslant 0$. The other cases can be treated similarly. For $i \in [\![1, L-1]\!]$, we have, by redefining $\delta(N)$ when necessary,

$$\begin{aligned}
&\mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N}\right] \\
&= \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N} | \mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{A}_i}^c\right] \mathbb{P}\left[\mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{A}_i}^c\right] \\
&\quad + \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N} | \mathcal{E}_i \cup \mathcal{E}_{\widetilde{A}_i}\right] \mathbb{P}\left[\mathcal{E}_i \cup \mathcal{E}_{\widetilde{A}_i}\right] \\
&\leqslant \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N} | \mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{A}_i}^c\right] + \mathbb{P}\left[\mathcal{E}_i \cup \mathcal{E}_{\widetilde{A}_i}\right] \\
&\overset{(a)}{\leqslant} \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N} | \mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{A}_i}^c\right] + \delta(N) + \mathbb{P}\left[\mathcal{E}_{\widetilde{A}_i}\right] \\
&\overset{(b)}{\leqslant} \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N} | \mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{A}_i}^c\right] + \delta(N) + \mathbb{P}\left[\widehat{A}_{i+1}^{1:N} \neq \widetilde{A}_{i+1}^{1:N}\right] \\
&\quad + \mathbb{P}\left[\widehat{B}_{i+1}^{1:N} \neq \widetilde{B}_{i+1}^{1:N}\right] \\
&\overset{(c)}{\leqslant} \delta(N) + \mathbb{P}\left[\widehat{A}_{i+1}^{1:N} \neq \widetilde{A}_{i+1}^{1:N}\right] + \mathbb{P}\left[\widehat{B}_{i+1}^{1:N} \neq \widetilde{B}_{i+1}^{1:N}\right], \qquad (8)
\end{aligned}$$

where (a) holds by the union bound, and by the coupling and Lemma 5, (b) holds by the union bound because $\mathcal{E}_{\widetilde{A}_i} = \left\{\widehat{\Psi}_i^{(U)} \neq \Psi_i^{(U)}\right\} \cup \left\{\widehat{\overline{M}}_{i+1}^{(V)} \neq \overline{M}_{i+1}^{(V)}\right\}$, (c) holds by Lemma 2.

We then have, by redefining $\delta(N)$ when necessary,

$$\begin{aligned}
&\mathbb{P}\left[\widehat{C}_i^{1:N} \neq \widetilde{C}_i^{1:N}\right] \\
&\leqslant \mathbb{P}\left[\widehat{C}_i^{1:N} \neq \widetilde{C}_i^{1:N} | \mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{C}_i}^c\right] + \mathbb{P}\left[\mathcal{E}_i \cup \mathcal{E}_{\widetilde{C}_i}\right] \\
&\overset{(a)}{\leqslant} \mathbb{P}\left[\widehat{C}_i^{1:N} \neq \widetilde{C}_i^{1:N} | \mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{C}_i}^c\right] + \mathbb{P}\left[\mathcal{E}_i\right] + \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N}\right] \\
&\quad + \mathbb{P}\left[\widehat{C}_{i+1}^{1:N} \neq \widetilde{C}_{i+1}^{1:N}\right] \\
&\overset{(b)}{\leqslant} \delta(N) + \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N}\right] + \mathbb{P}\left[\widehat{C}_i^{1:N} \neq \widetilde{C}_i^{1:N}\right] \\
&\quad + \mathbb{P}\left[\widehat{B}_{i+1}^{1:N} \neq \widetilde{B}_{i+1}^{1:N}\right] \\
&\overset{(c)}{\leqslant} \delta(N) + \mathbb{P}\left[\widehat{A}_{i+1}^{1:N} \neq \widetilde{A}_{i+1}^{1:N}\right] + \mathbb{P}\left[\widehat{B}_{i+1}^{1:N} \neq \widetilde{B}_{i+1}^{1:N}\right] \\
&\quad + \mathbb{P}\left[\widehat{C}_{i+1}^{1:N} \neq \widetilde{C}_{i+1}^{1:N}\right], \qquad (9)
\end{aligned}$$

where (a) holds by the union bound because $\mathcal{E}_{\widetilde{C}_i} = \left\{\widehat{\Psi}_i^{(1)} \neq \Psi_i^{(1)}\right\} \cup \left\{\widehat{U}_i^{1:N} \neq \widetilde{U}_i^{1:N}\right\}$, (b) holds by the coupling and Lemma 5, and by Lemma 2, (c) holds by (8).

Finally, we have, by redefining $\delta(N)$ when necessary,

$$\begin{aligned}
&\mathbb{P}\left[\widehat{B}_i^{1:N} \neq \widetilde{B}_i^{1:N}\right] \\
&\leqslant \mathbb{P}\left[\widehat{B}_i^{1:N} \neq \widetilde{B}_i^{1:N} | \mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{B}_i}^c\right] + \mathbb{P}\left[\mathcal{E}_i \cup \mathcal{E}_{\widetilde{B}_i}\right] \\
&\overset{(a)}{\leqslant} \mathbb{P}\left[\widehat{B}_i^{1:N} \neq \widetilde{B}_i^{1:N} | \mathcal{E}_i^c \cap \mathcal{E}_{\widetilde{B}_i}^c\right] + \mathbb{P}\left[\mathcal{E}_i\right] + \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N}\right] \\
&\quad + \mathbb{P}\left[\widehat{C}_i^{1:N} \neq \widetilde{C}_i^{1:N}\right] + \mathbb{P}\left[\widehat{B}_{i+1}^{1:N} \neq \widetilde{B}_{i+1}^{1:N}\right] \\
&\overset{(b)}{\leqslant} \delta(N) + \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N}\right] + \mathbb{P}\left[\widehat{C}_i^{1:N} \neq \widetilde{C}_i^{1:N}\right] \\
&\quad + \mathbb{P}\left[\widehat{B}_{i+1}^{1:N} \neq \widetilde{B}_{i+1}^{1:N}\right] \\
&\overset{(c)}{\leqslant} \delta(N) + 2\mathbb{P}\left[\widehat{A}_{i+1}^{1:N} \neq \widetilde{A}_{i+1}^{1:N}\right] + 3\mathbb{P}\left[\widehat{B}_{i+1}^{1:N} \neq \widetilde{B}_{i+1}^{1:N}\right] \\
&\quad + \mathbb{P}\left[\widehat{C}_{i+1}^{1:N} \neq \widetilde{C}_{i+1}^{1:N}\right], \qquad (10)
\end{aligned}$$

where (a) holds by the union bound because

$$\mathcal{E}_{\widetilde{B}_i} = \left\{\widehat{\Psi}_i^{(V)} \neq \Psi_i^{(V)}\right\} \cup \left\{\widehat{U}_i^{1:N} \neq \widetilde{U}_i^{1:N}\right\} \cup \left\{(\widehat{X}_1)_i^{1:N} \neq (\widetilde{X}_1)_i^{1:N}\right\},$$

(b) holds by the coupling and Lemma 5, and by Lemma 2, (c) holds by (9).

Combining (8), (9), and (10) we obtain, by redefining $\delta(N)$ when necessary,

$$\begin{aligned}
&\mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N}\right] + \mathbb{P}\left[\widehat{B}_i^{1:N} \neq \widetilde{B}_i^{1:N}\right] + \mathbb{P}\left[\widehat{C}_i^{1:N} \neq \widetilde{C}_i^{1:N}\right] \\
&\leqslant \delta(N) + 5\left(\mathbb{P}\left[\widehat{A}_{i+1}^{1:N} \neq \widetilde{A}_{i+1}^{1:N}\right] + \mathbb{P}\left[\widehat{B}_{i+1}^{1:N} \neq \widetilde{B}_{i+1}^{1:N}\right]\right. \\
&\quad \left. + \mathbb{P}\left[\widehat{C}_{i+1}^{1:N} \neq \widetilde{C}_{i+1}^{1:N}\right]\right) \\
&\leqslant 5^{L-i}\delta(N) + 5^{L-i}\left(\mathbb{P}\left[\widehat{A}_L^{1:N} \neq \widetilde{A}_L^{1:N}\right]\right. \\
&\quad \left. + \mathbb{P}\left[\widehat{B}_L^{1:N} \neq \widetilde{B}_L^{1:N}\right] + \mathbb{P}\left[\widehat{C}_L^{1:N} \neq \widetilde{C}_L^{1:N}\right]\right) \\
&\leqslant 5^{L-i}\delta(N),
\end{aligned}$$

hence,

$$\begin{aligned}
&\mathbb{P}\left[(\widehat{M}_{1:L}^{(U)}, \widehat{M}_{1:L}^{(V)}, \widehat{M}_{1:L}^{(1)}) \neq (M_{1:L}^{(U)}, M_{1:L}^{(V)}, M_{1:L}^{(1)})\right] \\
&\leqslant \mathbb{P}\left[(\widehat{A}_{1:L}^{1:N}, \widehat{B}_{1:L}^{1:N}, \widehat{C}_{1:L}^{1:N}) \neq (\widetilde{A}_{1:L}^{1:N}, \widetilde{B}_{1:L}^{1:N}, \widetilde{C}_{1:L}^{1:N})\right] \\
&\leqslant \sum_{i=1}^{L} \mathbb{P}\left[\widehat{A}_i^{1:N} \neq \widetilde{A}_i^{1:N}\right] + \mathbb{P}\left[\widehat{B}_i^{1:N} \neq \widetilde{B}_i^{1:N}\right] \\
&\quad + \mathbb{P}\left[\widehat{C}_i^{1:N} \neq \widetilde{C}_i^{1:N}\right] \\
&\leqslant \delta(N) \sum_{i=1}^{L} 5^{L-i} \\
&= \delta(N)(5^L - 1)/4. \qquad (11)
\end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

4) Strong secrecy: We provide a unified proof for all the cases considered in the encoding scheme. In the following, do the substitution $M_{1:L}^{(U)} \leftarrow \emptyset$, $\widetilde{L}_{1:L}^{(U)} \leftarrow \emptyset$ for the case ($R_U < 0$ and $R_V \geqslant 0$), the substitution $\overline{M}_{1:L}^{(V)} \leftarrow \emptyset$ for the case ($R_U \geqslant 0$ and $R_V \geqslant 0$), and the substitution $\Psi_{1:L}^{(V)} \leftarrow \emptyset$, $\overline{M}_{1:L}^{(V)} \leftarrow \emptyset$, $M_{1:L}^{(V)} \leftarrow \emptyset$, $\widetilde{L}_{1:L}^{(V)} \leftarrow \emptyset$ for the case ($R_U > 0$ and $R_V \leqslant 0$).

It is tempting to state that the following security constraints hold by the proof in [16],

$$I\left(M_{1:L}^{(U)}\Psi_{1:L}^{(U)}; \widetilde{Z}_{1:L}^{1:N}(X_1)_{1:L}^{1:N}\widetilde{V}_{1:L}^{1:N}\right) \leqslant \delta(N),$$
$$I\left(M_{1:L}^{(V)}\overline{M}_{1:L}^{(V)}\Psi_{1:L}^{(V)}; \widetilde{Z}_{1:L}^{1:N}\right) \leqslant \delta(N),$$
$$I\left(M_{1:L}^{(1)}\Psi_{1:L}^{(1)}; \widetilde{Z}_{1:L}^{1:N}\widetilde{V}_{1:L}^{1:N}\right) \leqslant \delta(N),$$

this assertion would, however, be incorrect. The proof in [16] can only be applied to show block wise strong secrecy and does not apply to show secrecy over all blocks jointly, due to the fact that the functional dependence graphs that describe dependencies between random variables across all blocks differ from [16] – see Figures 6, 7, and 8. In particular, additional dependencies exist because of our combination of three point-to-point wiretap and cooperative jamming codes.

We first show blockwise strong secrecy in the following lemma.

Lemma 6. *For any Block $i \in [\![1, L]\!]$ strong secrecy holds. Specifically,*

$$I\left(\Psi_{i-1}^{(U)}\Psi_{i-1}^{(V)}\Psi_{i-1}^{(1)}M_i^{(U)}\overline{M}_i^{(V)}M_i^{(V)}M_i^{(1)}; \widetilde{Z}_i^{1:N}\right) \leqslant \delta(N),$$

where $\Psi_0^{(U)} = \Psi_0^{(V)} = \Psi_0^{(1)} = \emptyset$.

Remark 5. *Note that one only needs $I\left(M_i^{(U)}M_i^{(V)}M_i^{(1)}; \widetilde{Z}_i^{1:N}\right) \leqslant \delta(N)$, to have blockwise strong secrecy. We prove a stronger result in Lemma 6 to be able to study strong secrecy over consecutive blocks in Lemma 7.*

Remark 6. *When $R_U \leqslant 0$, although the virtual user does not transmit secret information messages to the legitimate receiver, it is critical, for Lemma 6 to hold, that $\Psi_i^{(U)}$, $i \in [\![1, L]\!]$, is almost independent from $(\widetilde{Z}_i^{1:N}, (X_1)_i^{1:N}, \widetilde{V}_i^{1:N})$, i.e., $I\left(\Psi_{i-1}^{(U)}; \widetilde{Z}_i^{1:N}(X_1)_i^{1:N}\widetilde{V}_i^{1:N}\right) \leqslant \delta(N)$. This remark justifies a posteriori the design of the coding scheme E^{CJ2}. Note also that when $R_V \leqslant 0$, we simply have $(M_i^{(V)}, \overline{M}_i^{(V)}, \Psi_{i-1}^{(V)}) = \emptyset$.*

Proof. Following the proof of [16, Lemma 8] with Lemmas 3, 5, one can show that for any $i \in [\![1, L]\!]$,

$$I\left(M_i^{(U)}\Psi_{i-1}^{(U)}; \widetilde{Z}_i^{1:N}(X_1)_i^{1:N}\widetilde{V}_i^{1:N}\right) \leqslant \delta(N),$$
$$I\left(M_i^{(V)}\overline{M}_i^{(V)}\Psi_{i-1}^{(V)}; \widetilde{Z}_i^{1:N}\right) \leqslant \delta(N),$$
$$I\left(M_i^{(1)}\Psi_{i-1}^{(1)}; \widetilde{Z}_i^{1:N}\widetilde{V}_i^{1:N}\right) \leqslant \delta(N).$$

We then have

$$\begin{aligned}
&I\left(\Psi_{i-1}^{(U)}\Psi_{i-1}^{(V)}\Psi_{i-1}^{(1)}M_i^{(U)}\overline{M}_i^{(V)}M_i^{(V)}M_i^{(1)}; \widetilde{Z}_i^{1:N}\right)\\
&= I\left(\Psi_{i-1}^{(V)}\overline{M}_i^{(V)}M_i^{(V)}; \widetilde{Z}_i^{1:N}\right)\\
&\quad + I\left(\Psi_{i-1}^{(1)}M_i^{(1)}; \widetilde{Z}_i^{1:N}|\Psi_{i-1}^{(V)}\overline{M}_i^{(V)}M_i^{(V)}\right)\\
&\quad + I\left(\Psi_{i-1}^{(U)}M_i^{(U)}; \widetilde{Z}_i^{1:N}|\Psi_{i-1}^{(V)}\overline{M}_i^{(V)}M_i^{(V)}\Psi_{i-1}^{(1)}M_i^{(1)}\right)\\
&\leqslant I\left(\Psi_{i-1}^{(V)}\overline{M}_i^{(V)}M_i^{(V)}; \widetilde{Z}_i^{1:N}\right) + I\left(\Psi_{i-1}^{(1)}M_i^{(1)}; \widetilde{Z}_i^{1:N}\widetilde{V}_i^{1:N}\right)\\
&\quad + I\left(\Psi_{i-1}^{(U)}M_i^{(U)}; \widetilde{Z}_i^{1:N}\widetilde{V}_i^{1:N}(X_1)_i^{1:N}\right)\\
&\leqslant \delta(N).
\end{aligned}$$

■

We now study strong secrecy across two consecutive blocks in the following lemma.

Lemma 7. *Define for $i \in [\![1, L]\!]$,*

$$\widetilde{L}_i^{(V)} \triangleq I\left(M_{1:L}^{(V)}; \widetilde{Z}_{1:i}^{1:N}\right),$$
$$\widetilde{L}_i^{(U)} \triangleq I\left(M_{1:L}^{(U)}; \widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)}\right),$$
$$\widetilde{L}_i^{(1)} \triangleq I\left(M_{1:L}^{(1)}; \widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}\right),$$

and $\widetilde{L}_0^{(V)} = \widetilde{L}_0^{(U)} = \widetilde{L}_0^{(1)} = 0$.

For $i \in [\![0, L-1]\!]$, we have

$$\max\left(\widetilde{L}_{i+1}^{(V)} - \widetilde{L}_i^{(V)}, \widetilde{L}_{i+1}^{(U)} - \widetilde{L}_i^{(U)}, \widetilde{L}_{i+1}^{(1)} - \widetilde{L}_i^{(1)}\right) \leqslant \delta(N).$$

Proof. For $i \in [\![0, L-1]\!]$, we have

$$\begin{aligned}
&\widetilde{L}_{i+1}^{(U)} - \widetilde{L}_i^{(U)}\\
&= I\left(M_{1:L}^{(U)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}|\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)}\right)\\
&\overset{(a)}{=} I\left(M_{1:i+1}^{(U)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}|\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)}\right)\\
&\leqslant I\left(M_{1:i+1}^{(U)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}\right)\\
&= I\left(M_{i+1}^{(U)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}\right)\\
&\quad + I\left(M_{1:i}^{(U)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}|M_{i+1}^{(U)}\right)\\
&\overset{(b)}{\leqslant} I\left(M_{1:i}^{(U)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}|M_{i+1}^{(U)}\right)\\
&\quad + \delta(N)\\
&\leqslant I\Big(\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}M_{1:i}^{(U)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)}\\
&\qquad ; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}M_{i+1}^{(U)}\Big) + \delta(N)\\
&\overset{(c)}{=} I\left(\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}M_{i+1}^{(U)}\right) + \delta(N)\\
&= I\left(\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}; \widetilde{Z}_{i+1}^{1:N}|M_{i+1}^{(V)}M_{i+1}^{(1)}M_{i+1}^{(U)}\right) + \delta(N)\\
&\leqslant I\left(\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}M_{i+1}^{(V)}M_{i+1}^{(1)}M_{i+1}^{(U)}; \widetilde{Z}_{i+1}^{1:N}\right) + \delta(N)\\
&\overset{(d)}{\leqslant} \delta(N),
\end{aligned}$$

where (a) holds by the chain rule and because

$$\begin{aligned}
&I\left(M_{i+2:L}^{(U)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}|\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)}M_{1:i+1}^{(U)}\right)\\
&\quad \leqslant I\left(M_{i+2:L}^{(U)}; \widetilde{Z}_{1:i+1}^{1:N}M_{1:i+1}^{(V)}M_{1:i+1}^{(1)}M_{1:i+1}^{(U)}\right) = 0,
\end{aligned}$$

(b) holds by the proof of Lemma 6 because $I\left(M_{i+1}^{(U)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}\right) \leqslant I\left(M_{i+1}^{(U)}; \widetilde{Z}_{i+1}^{1:N}(X_1)_{i+1}^{1:N}\widetilde{V}_{i+1}^{1:N}\right)$, (c) holds by the chain

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

rule and as one can check with the dependence graphs depicted in Figures 6, 7,[1] because the following Markov chain holds $M_{1:i}^{(U)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)} - \Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)} - \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}M_{i+1}^{(U)}$, (d) holds by Lemma 6.

Then we have

$$\begin{aligned}
&\widetilde{L}_{i+1}^{(1)} - \widetilde{L}_i^{(1)}\\
&= I\left(M_{1:L}^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}|\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}\right)\\
&\overset{(a)}{=} I\left(M_{1:i+1}^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}|\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}\right)\\
&\leqslant I\left(M_{1:i+1}^{(1)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}\right)\\
&= I\left(M_{i+1}^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}\right)\\
&\quad + I\left(M_{1:i}^{(1)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}|M_{i+1}^{(1)}\right)\\
&\overset{(b)}{\leqslant} I\left(M_{1:i}^{(1)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}|M_{i+1}^{(1)}\right) + \delta(N)\\
&\leqslant I\Big(\overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}M_{1:i}^{(1)}\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}\Big)\\
&\quad + \delta(N)\\
&\overset{(c)}{=} I\left(\overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)}\right) + \delta(N)\\
&= I\left(\overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}; \widetilde{Z}_{i+1}^{1:N}|M_{i+1}^{(V)}M_{i+1}^{(1)}\right) + \delta(N)\\
&\leqslant I\left(\overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}M_{i+1}^{(V)}M_{i+1}^{(1)}; \widetilde{Z}_{i+1}^{1:N}\right) + \delta(N)\\
&\overset{(d)}{\leqslant} \delta(N),
\end{aligned}$$

where (a) holds because

$$\begin{aligned}
&I\left(M_{i+2:L}^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}|\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i+1}^{(1)}\right)\\
&\leqslant I\left(M_{i+2:L}^{(1)}; \widetilde{Z}_{1:i+1}^{1:N}M_{1:i+1}^{(V)}M_{1:i+1}^{(1)}\right) = 0,
\end{aligned}$$

(b) holds by the proof of Lemma 6 because $I\left(M_{i+1}^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}\right) \leqslant I\left(M_{i+1}^{(1)}; \widetilde{Z}_{i+1}^{1:N}\widetilde{V}_{i+1}^{1:N}\right)$, (c) holds by the chain rule and as one can check with the dependence graph depicted in Figures 6, 7, 8, because the following Markov chain holds

$$\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)}M_{1:i}^{(1)} - \overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)} - \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}M_{i+1}^{(1)},$$

(d) holds by Lemma 6.

Finally, we have,

$$\begin{aligned}
&\widetilde{L}_{i+1}^{(V)} - \widetilde{L}_i^{(V)}\\
&= I\left(M_{1:L}^{(V)}; \widetilde{Z}_{i+1}^{1:N}|\widetilde{Z}_{1:i}^{1:N}\right)\\
&\overset{(a)}{=} I\left(M_{1:i+1}^{(V)}; \widetilde{Z}_{i+1}^{1:N}|\widetilde{Z}_{1:i}^{1:N}\right)\\
&\leqslant I\left(M_{1:i+1}^{(V)}\widetilde{Z}_{1:i}^{1:N}; \widetilde{Z}_{i+1}^{1:N}\right)\\
&= I\left(M_{i+1}^{(V)}; \widetilde{Z}_{i+1}^{1:N}\right) + I\left(M_{1:i}^{(V)}\widetilde{Z}_{1:i}^{1:N}; \widetilde{Z}_{i+1}^{1:N}|M_{i+1}^{(V)}\right)\\
&\overset{(b)}{\leqslant} I\left(M_{1:i}^{(V)}\widetilde{Z}_{1:i}^{1:N}; \widetilde{Z}_{i+1}^{1:N}|M_{i+1}^{(V)}\right) + \delta(N)\\
&\leqslant I\left(\overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}M_{1:i}^{(V)}\widetilde{Z}_{1:i}^{1:N}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}\right) + \delta(N)\\
&\overset{(c)}{=} I\left(\overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}; \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)}\right) + \delta(N)\\
&= I\left(\overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}; \widetilde{Z}_{i+1}^{1:N}|M_{i+1}^{(V)}\right) + \delta(N)\\
&\leqslant I\left(\overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)}M_{i+1}^{(V)}; \widetilde{Z}_{i+1}^{1:N}\right) + \delta(N)\\
&\overset{(d)}{\leqslant} \delta(N),
\end{aligned}$$

where (a) holds because

$$\begin{aligned}
&I\left(M_{i+2:L}^{(V)}; \widetilde{Z}_{i+1}^{1:N}|\widetilde{Z}_{1:i}^{1:N}M_{1:i+1}^{(V)}\right)\\
&\leqslant I\left(M_{i+2:L}^{(V)}; \widetilde{Z}_{1:i+1}^{1:N}M_{1:i+1}^{(V)}\right) = 0,
\end{aligned}$$

(b) holds by Lemma 6, (c) holds by the chain rule and as one can check with the dependence graphs depicted in Figure 6, 8,[2] because the following Markov chain holds

$$\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(V)} - \overline{M}_{i+1}^{(V)}\Psi_i^{(U)}\Psi_i^{(V)}\Psi_i^{(1)} - \widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(V)},$$

(d) holds by Lemma 6. ∎

We can now study strong secrecy over all blocks jointly. Observe first that

$$\begin{aligned}
&I\left(M_{1:L}^{(U)}; \widetilde{Z}_{1:L}^{1:N}M_{1:L}^{(V)}M_{1:L}^{(1)}\right)\\
&= \sum_{i=1}^{L-1}\left(\widetilde{L}_{i+1}^{(U)} - \widetilde{L}_i^{(U)}\right) + \widetilde{L}_1^{(U)} \leqslant L\delta(N),
\end{aligned}$$

where the last inequality holds by Lemma 7.

Similarly, $I\left(M_{1:L}^{(V)}; \widetilde{Z}_{1:L}^{1:N}\right) \leqslant L\delta(N)$ and $I\left(M_{1:L}^{(1)}; \widetilde{Z}_{1:L}^{1:N}M_{1:L}^{(V)}\right) \leqslant L\delta(N)$. We thus obtain strong secrecy as follows.

$$\begin{aligned}
&I\left(M_{1:L}^{(U)}M_{1:L}^{(V)}M_{1:L}^{(1)}; \widetilde{Z}_{1:L}^{1:N}\right)\\
&= I\left(M_{1:L}^{(V)}; \widetilde{Z}_{1:L}^{1:N}\right) + I\left(M_{1:L}^{(U)}; \widetilde{Z}_{1:L}^{1:N}|M_{1:L}^{(V)}\right)\\
&\quad + I\left(M_{1:L}^{(1)}; \widetilde{Z}_{1:L}^{1:N}|M_{1:L}^{(U)}M_{1:L}^{(V)}\right)\\
&= I\left(M_{1:L}^{(V)}; \widetilde{Z}_{1:L}^{1:N}\right) + I\left(M_{1:L}^{(U)}; \widetilde{Z}_{1:L}^{1:N}M_{1:L}^{(V)}\right)\\
&\quad + I\left(M_{1:L}^{(1)}; \widetilde{Z}_{1:L}^{1:N}M_{1:L}^{(U)}M_{1:L}^{(V)}\right)\\
&\leqslant L\delta(N). \qquad (12)
\end{aligned}$$

B. Scheme analysis for the achievability of $\mathcal{R}''(p_{X_1}p_{X_2})$

1) Induced distribution: As in Section V-A, a crucial step to assess reliability and secrecy is the study of the distribution induced by the encoder. One can show a similar to Lemma 5, for all $i \in [\![1, L]\!]$,

$$\begin{aligned}
&\mathbb{V}\left(\widetilde{p}_{(X_1)_i^{1:N}(X_2)_i^{1:N}Y_i^{1:N}Z_i^{1:N}}, p_{(X_1)^{1:N}(X_2)^{1:N}Y^{1:N}Z^{1:N}}\right)\\
&\qquad \leqslant \delta(N), \qquad (13)
\end{aligned}$$

where $\widetilde{p}_{(X_1)_i^{1:N}(X_2)_i^{1:N}Y_i^{1:N}Z_i^{1:N}}$ is the joint distribution of $\left((\widetilde{X}_1)_i^{1:N}(\widetilde{X}_2)_i^{1:N}, \widetilde{Y}_i^{1:N}, \widetilde{Z}_i^{1:N}\right)$.

[1]Recall that $\widetilde{L}_i^{(U)}$ is not defined when $R_U \leqslant 0$.

[2]Recall that $\widetilde{L}_i^{(V)}$ is not defined when $R_V \leqslant 0$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

2) Communication rate: Similar to Section V-A2, the rate of $M_{1:L}^{(1)}$ can be shown to satisfy, as N goes to infinity,

$$\frac{1}{NL}\sum_{i=1}^{L}|M_i^{(1)}|\geqslant I(X_1;Y|X_2)-I(X_1;Z|X_2),$$

and one can verify that the rates of the secret seeds that need to be shared between the transmitters and the legitimate receiver are negligible.

3) Reliability: Similar to Section V-A3, one can show using (13),

$$\mathbb{P}\left[\widehat{M}_{1:L}^{(1)},\neq M_{1:L}^{(1)}\right]\leqslant \delta(N)L(L-1)(2L-1)/6.$$

4) Strong secrecy: Although only one user is transmitting secret information to the legitimate receiver, one still cannot reuse the security proof for the point-to-point wiretap channel [16] to show security over the L encoding blocks jointly. We can though, similar to [16], show that blockwise secrecy holds by using (13) and Lemma 3. We now show strong secrecy for two consecutive encoding blocks.

Lemma 8. *Define*

$$\widetilde{L}_i^{(1)}\triangleq I\left(M_{1:L}^{(1)};\widetilde{Z}_{1:i}^{1:N}\Psi_1^{(2)}\right),\ \textit{for } i\in[\![1,L]\!],$$
$$\widetilde{L}_0^{(1)}\triangleq 0.$$

For $i\in[\![0,L-1]\!]$, we have $\widetilde{L}_{i+1}^{(1)}-\widetilde{L}_i^{(1)}\leqslant\delta(N)$.

Remark 7. *Observe that unlike in Lemma 7, here, $\Psi_1^{(2)}$ might not be concealed from the eavesdropper. Consequently, the proof of Lemma 7 cannot be reused to prove Lemma 8.*

Proof. For $i\in[\![0,L-1]\!]$, we have

$$\begin{aligned}
&\widetilde{L}_{i+1}^{(1)}-\widetilde{L}_i^{(1)}\\
&=I\left(M_{1:L}^{(1)};\widetilde{Z}_{i+1}^{1:N}|\widetilde{Z}_{1:i}^{1:N}\Psi_1^{(2)}\right)\\
&\overset{(a)}{=}I\left(M_{1:i+1}^{(1)};\widetilde{Z}_{i+1}^{1:N}|\widetilde{Z}_{1:i}^{1:N}\Psi_1^{(2)}\right)\\
&\leqslant I\left(M_{1:i+1}^{(1)}\widetilde{Z}_{1:i}^{1:N};\widetilde{Z}_{i+1}^{1:N}|\Psi_1^{(2)}\right)\\
&=I\left(M_{i+1}^{(1)};\widetilde{Z}_{i+1}^{1:N}|\Psi_1^{(2)}\right)+I\left(M_{1:i}^{(1)}\widetilde{Z}_{1:i}^{1:N};\widetilde{Z}_{i+1}^{1:N}|\Psi_1^{(2)}M_{i+1}^{(1)}\right)\\
&\overset{(b)}{\leqslant} I\left(M_{1:i}^{(1)}\widetilde{Z}_{1:i}^{1:N};\widetilde{Z}_{i+1}^{1:N}|\Psi_1^{(2)}M_{i+1}^{(1)}\right)+\delta(N)\\
&\leqslant I\left(\Psi_i^{(1)}M_{1:i}^{(1)}\widetilde{Z}_{1:i}^{1:N};\widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(1)}|\Psi_1^{(2)}\right)+\delta(N)\\
&\overset{(c)}{=} I\left(\Psi_i^{(1)};\widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(1)}|\Psi_1^{(2)}\right)+\delta(N)\\
&=I\left(\Psi_i^{(1)};\widetilde{Z}_{i+1}^{1:N}|\Psi_1^{(2)}M_{i+1}^{(1)}\right)+\delta(N)\\
&\leqslant I\left(\Psi_i^{(1)}M_{i+1}^{(1)};\widetilde{Z}_{i+1}^{1:N}\Psi_1^{(2)}\right)+\delta(N)\\
&\overset{(d)}{\leqslant}\delta(N),
\end{aligned}$$

where (a) holds because

$$I\left(M_{i+2:L}^{(1)};\widetilde{Z}_{i+1}^{1:N}|\widetilde{Z}_{1:i}^{1:N}\Psi_1^{(2)}M_{1:i+1}^{(1)}\right)\leqslant I\left(M_{i+2:L}^{(1)};\widetilde{Z}_{1:i+1}^{1:N}\Psi_1^{(2)}M_{1:i+1}^{(1)}\right)=0,$$

(b) holds by blockwise secrecy because $I\left(M_{i+1}^{(1)};\widetilde{Z}_{i+1}^{1:N}\Psi_1^{(2)}\right)\leqslant I\left(M_{i+1}^{(1)};\widetilde{Z}_{i+1}^{1:N}(\widetilde{X}_2)_{i+1}^{1:N}\right)$, (c) holds by the chain rule and as one can check with the dependence graph depicted in Figure 9 because

$$\widetilde{Z}_{1:i}^{1:N}M_{1:i}^{(1)}-\Psi_i^{(1)}\Psi_i^{(2)}-\widetilde{Z}_{i+1}^{1:N}M_{i+1}^{(1)}$$

forms a Markov chain (d) holds by blockwise secrecy. ∎

From Lemma 8, we deduce $I\left(M_{1:L}^{(1)};\widetilde{Z}_{1:L}^{1:N}\right)\leqslant L\delta(N)$, i.e., strong secrecy holds over all blocks jointly.

VI. Concluding remarks

Polar codes [43] are the subject of intense research both on the theoretical and practical level because of their potential for low-complexity implementation and provable performances. While polar codes are already candidates for error-control coding in 5G communication systems [44], recent results have also demonstrated their potential for securing the physical layer.

In this paper, we have considered polar codes for communication over a MAC-WT with two transmitters under strong secrecy. We have seen that rate-splitting for the multiple access channel (MAC) without secrecy constraint [26] can be adapted to the MAC wiretap channel, 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 have, consequently, been able to provide low-complexity polar coding achievable strategies for the achievability proof of Theorem 1. Moreover, for a given rate pair, if time-sharing is not needed in the achievability scheme of Theorem 1, then time-sharing is not needed in our coding scheme.

Regarding our proof for reliability and secrecy, we stress that polar codes should be handled with care when channels are not symmetric and when block Markov encoding is used, for at least two reasons. First, as already noticed in [16], 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. Consequently, although our coding scheme relies on several point-to-point wiretap codes, secrecy and reliability do not follow from [16]. In our coding scheme, several block Markov constructions are combined together and a detailed analysis of the dependencies of the involved random variables is essential to assess reliability and strong secrecy.

Appendix A
Proof of Property 1

We fix $p_{X_{\mathcal{M}}}$ and drop the subscript on $g_{p_{X_{\mathcal{M}}}}$. To show that g is submodular it is sufficient to show that $g_1:2^{\mathcal{M}}\to\mathbb{R}_+,\mathcal{S}\mapsto -I(X_{\mathcal{S}};Z)$ is submodular, since $g_2:2^{\mathcal{M}}\to\mathbb{R}_+,\mathcal{S}\mapsto I(X_{\mathcal{S}};Y|X_{\mathcal{S}^c})$ is known to be submodular [45].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2018.2865741, IEEE Transactions on Information Theory

For any $\mathcal{S}, \mathcal{T} \in 2^{\mathcal{M}}$, we have for $\mathcal{U} \triangleq \mathcal{S} \cup \mathcal{T}$ and $\mathcal{I} \triangleq \mathcal{S} \cap \mathcal{T}$

$$\begin{aligned}
&g_1(\mathcal{U}) + g_1(\mathcal{I}) \\
&= -H(X_{\mathcal{U}}) - H(X_{\mathcal{I}}) + H(X_{\mathcal{U}}|Z) + H(X_{\mathcal{I}}|Z) \\
&\overset{(a)}{=} -H(X_{\mathcal{S}}) - H(X_{\mathcal{T}}) + H(X_{\mathcal{S}}|Z) + H(X_{\mathcal{T}\setminus\mathcal{S}}|ZX_{\mathcal{S}}) \\
&\qquad + H(X_{\mathcal{I}}|Z) \\
&\overset{(b)}{\leqslant} -H(X_{\mathcal{S}}) - H(X_{\mathcal{T}}) + H(X_{\mathcal{S}}|Z) + H(X_{\mathcal{T}\setminus\mathcal{S}}|ZX_{\mathcal{I}}) \\
&\qquad + H(X_{\mathcal{I}}|Z) \\
&= g_1(\mathcal{S}) + g_1(\mathcal{T}),
\end{aligned}$$

where (a) holds by independence between the X_i's, (b) holds because conditioning reduces entropy.

Appendix B
Systematic method to characterize the corner points and dominant face of $\mathcal{R}'$

We use the notion of polymatroid to characterize in a *systematic manner* the corner points and the dominant face of $\mathcal{R}'$. Although the notion of polymatroid has previously been utilized in the context of multiple access channels without secrecy constraints, e.g., [45], [46], we will see that some complications exist for the MAC-WT.

Remark 8. *Despite our focus on the two-user MAC-WT, we remark that the result presented in this section is valid for any $m \in \mathbb{N}$, which is of independent interest.*

For any subset $\mathcal{S}$ of $\mathcal{M} \triangleq [\![1, m]\!]$, $m \in \mathbb{N}$, define $R_{\mathcal{S}} \triangleq \sum_{i\in\mathcal{S}} R_i$. We first recall the definition of a polymatroid.

Definition 3 ([46], [47])**.** *Let $f : 2^{\mathcal{M}} \to \mathbb{R}$. The polyhedron*

$$\mathcal{P}(f) \triangleq \left\{(R_i)_{i\in\mathcal{M}} \in \mathbb{R}_+^m : R_{\mathcal{S}} \leqslant f(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{M}\right\}$$

associated with the function f, is a polymatroid if

(i) f is normalized, i.e., $f(\emptyset) = 0$,
(ii) f is non-decreasing, i.e., $\forall \mathcal{S}, \mathcal{T} \subset \mathcal{M}, \mathcal{S} \subset \mathcal{T} \implies f(\mathcal{S}) \leqslant f(\mathcal{T})$,
(iii) f is submodular.

Observe that for any $p_{X_{\mathcal{M}}} \triangleq \prod_{i\in\mathcal{M}} p_{X_i}$, we have $\mathcal{R}'(p_{X_{\mathcal{M}}}) = \mathcal{P}(g_{p_{X_{\mathcal{M}}}})$. As shown in Property 1, $g_{p_{X_{\mathcal{M}}}}$ is submodular, however, in general, $g_{p_{X_{\mathcal{M}}}}$ is not non-decreasing. We transform $g_{p_{X_{\mathcal{M}}}}$ into a non-decreasing function, while preserving submodularity and normalization in the following lemma, whose proof can be found in Appendix C.

Lemma 9. *For a fixed $p_{X_{\mathcal{M}}} \triangleq \prod_{i=1}^m p_{X_i}$ such that $g_{p_{X_{\mathcal{M}}}}$ is positive, define*

$$g^*_{p_{X_{\mathcal{M}}}} : 2^{\mathcal{M}} \to \mathbb{R}_+, \mathcal{S} \mapsto \min_{\substack{\mathcal{A}\subset\mathcal{M} \\ \text{s.t. } \mathcal{A}\supset\mathcal{S}}} g_{p_{X_{\mathcal{M}}}}(\mathcal{A}).$$

The set function $g^*_{p_{X_{\mathcal{M}}}}$ is normalized, non-decreasing, and submodular.

We deduce the following result from Lemma 9.

Corollary 1. *For a fixed $p_{X_{\mathcal{M}}} \triangleq \prod_{i=1}^m p_{X_i}$ such that $g_{p_{X_{\mathcal{M}}}}$ is positive, $\mathcal{P}\left(g^*_{p_{X_{\mathcal{M}}}}\right)$ is a polymatroid, moreover,*

$$\mathcal{P}\left(g^*_{p_{X_{\mathcal{M}}}}\right) = \mathcal{P}\left(g_{p_{X_{\mathcal{M}}}}\right) = \mathcal{R}'(p_{X_{\mathcal{M}}}).$$

We obtain the following corollary.

Corollary 2 ([47])**.** *Fix $p_{X_{\mathcal{M}}} \triangleq \prod_{i=1}^m p_{X_i}$ such that $g_{p_{X_{\mathcal{M}}}}$ is positive. For $\pi \in$ Sym(m), where Sym(m) is the symmetric group on $\mathcal{M}$, for $i, j \in \mathcal{M}$, define $\pi^{i:j} \triangleq (\pi(k))_{k\in[\![i,j]\!]}$. Since $\mathcal{P}\left(g^*_{p_{X_{\mathcal{M}}}}\right)$ is a polymatroid by Corollary 1,*

(i) Any point in $\mathcal{R}'(p_{X_{\mathcal{M}}})$ is dominated, with respect to the natural partial order on $\mathbb{R}^m$, by a point in

$$\mathcal{D}(p_{X_{\mathcal{M}}}) \triangleq \left\{(R_i)_{i\in\mathcal{M}} \in \mathcal{R}'(p_{X_{\mathcal{M}}}) : R_{\mathcal{M}} = g^*_{p_{X_{\mathcal{M}}}}(\mathcal{M})\right\}.$$

(ii) We have

$$\mathcal{D}(p_{X_{\mathcal{M}}}) = \textit{Conv}\left(\left\{(C_{\pi(i)})_{i\in[\![1,m]\!]} : \pi \in \textit{Sym}(m)\right\}\right),$$

where for $\pi \in$ Sym(m), for $i \in [\![1, m]\!]$, $C_{\pi(i)} = g^*\left(\{\pi^{i:m}\}\right) - g^*\left(\{\pi^{i+1:m}\}\right)$.

Example 2. *For $m = 2$, and when $g_{p_{X_{\mathcal{M}}}}$ is positive, the dominant face of $\mathcal{R}'(p_{X_1}p_{X_2})$ is $\mathcal{D}(p_{X_1}p_{X_2}) = Conv(\mathcal{V}[\mathcal{R}'(p_{X_1}p_{X_2})])$, where the set of vertices $\mathcal{V}[\mathcal{R}'(p_{X_1}p_{X_2})]$ of $\mathcal{R}'(p_{X_1}p_{X_2})$ is*

$$\begin{aligned}
\mathcal{V}[\mathcal{R}'(p_{X_1}p_{X_2})] \triangleq &\{(g^*(\{1\}), g^*(\{1,2\}) - g^*(\{1\})), \\
&(g^*(\{1,2\}) - g^*(\{2\}), g^*(\{2\}))\}.
\end{aligned}$$

Note that by submodularity and normalization of g^*, $g^*(\{1,2\}) - g^*(\{2\}) \leqslant g^*(\{1\})$. Hence, the range of values taken by R_1 in $\mathcal{D}(p_{X_1}p_{X_2})$ is

$$\begin{aligned}
&[g^*(\{1,2\}) - g^*(\{2\}), g^*(\{1\})] \\
&= [[g(\{1,2\}) - g(\{2\})]^+, \min(g(\{1\}), g(\{1,2\}))],
\end{aligned}$$

where the equality holds by noting that for $i \in \{1,2\}$, $g^*(\{1,2\}) = g(\{1,2\})$, and $g^*(\{i\}) = \min(g(\{i\}), g(\{1,2\}))$. Then, by definition of $\mathcal{D}(p_{X_1}p_{X_2})$, R_2 is determined by $R_2 = g(\{1,2\}) - R_1 \geqslant 0$.

Appendix C
Proof of Lemma 9

We first show monotonicity. Let $\mathcal{S}, \mathcal{T} \subset \mathcal{M}$ such that $\mathcal{S} \subset \mathcal{T}$. Let $\mathcal{T}^* \subset \mathcal{M}$ be such that $g^*(\mathcal{T}) = g(\mathcal{T} \cup \mathcal{T}^*)$, we have $g^*(\mathcal{S}) = \min_{\substack{\mathcal{A}\subset\mathcal{M} \\ \text{s.t. } \mathcal{A}\supset\mathcal{S}}} g(\mathcal{A}) \leqslant g(\mathcal{T} \cup \mathcal{T}^*) = g^*(\mathcal{T})$, where the inequality holds because $\mathcal{T} \cup \mathcal{T}^* \supset \mathcal{S}$. We now show submodularity of g^*. Let $\mathcal{S}, \mathcal{T}$ be any subsets of $\mathcal{M}$. Let $\mathcal{S}^*, \mathcal{T}^* \subset \mathcal{M}$ be such that $g^*(\mathcal{S}) = g(\mathcal{S} \cup \mathcal{S}^*)$ and $g^*(\mathcal{T}) = g(\mathcal{T} \cup \mathcal{T}^*)$. Define $\mathcal{U} \triangleq \mathcal{S} \cup \mathcal{T}$ and $\mathcal{I} \triangleq \mathcal{S} \cap \mathcal{T}$. We have

$$\begin{aligned}
&g^*(\mathcal{U}) + g^*(\mathcal{I}) \\
&\overset{(a)}{\leqslant} g(\mathcal{U} \cup (\mathcal{S}^* \cup \mathcal{T}^*)) + g(\mathcal{I} \cup ((\mathcal{S} \cap \mathcal{T}^*) \cup (\mathcal{S}^* \cap (\mathcal{T} \cup \mathcal{T}^*)))) \\
&= g((\mathcal{S} \cup \mathcal{S}^*) \cup (\mathcal{T} \cup \mathcal{T}^*)) + g((\mathcal{S} \cup \mathcal{S}^*) \cap (\mathcal{T} \cup \mathcal{T}^*)) \\
&\overset{(b)}{\leqslant} g(\mathcal{S} \cup \mathcal{S}^*) + g(\mathcal{T} \cup \mathcal{T}^*) \\
&= g^*(\mathcal{S}) + g^*(\mathcal{T}),
\end{aligned}$$

where (a) holds by definition of g^*, (b) holds by submodularity of g. Finally, normalization of g^* follows from normalization of g.

REFERENCES

[1] R. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2016, pp. 983–987.

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

[3] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[4] A. Subramanian, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 585–594, 2011.

[5] V. Rathi, R. Urbanke, M. Andersson, and M. Skoglund, "Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2011, pp. 2393–2397.

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

[7] 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, 2011.

[8] 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.

[9] 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.

[10] M. Andersson, R. Schaefer, T. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1901–1908, 2013.

[11] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, 2011.

[12] M. Bellare and S. Tessaro, "Polynomial-time, semantically-secure encryption achieving the secrecy capacity," *arXiv preprint arXiv:1201.3160*, 2012.

[13] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Advances in Cryptology–CRYPTO 2012*. Springer, 2012, pp. 294–311.

[14] Y. 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, 2016.

[15] J. M. Renes, R. Renner, and D. Sutter, "Efficient one-way secret-key agreement and private channel coding via polarization," in *Advances in Cryptology-ASIACRYPT 2013*. Springer, 2013, pp. 194–213.

[16] R. Chou and M. 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, 2016.

[17] R. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2018, pp. 476–480.

[18] 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, 2017.

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

[20] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," in *IEEE Int. Symp. Inf. Theory*, 2010.

[21] H. Tyagi and A. Vardy, "Explicit capacity-achieving coding scheme for the Gaussian wiretap channel," in *IEEE Int. Symp. Inf. Theory*, 2014, pp. 956–960.

[22] 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, 2008.

[23] 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, 2012.

[24] 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, 2013.

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

[26] 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.

[27] U. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *Lecture Notes in Computer Science*. Springer-Verlag, 2000, pp. 351–368.

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

[29] A. Pierrot and M. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 595–605, 2011.

[30] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

[31] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. of the Annual Allerton Conf. on Communication Control and Computing*, 2008, pp. 1014–1021.

[32] R. Chou and M. Bloch, "Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes," in *Proc. of the Annual Allerton Conf. on Communication Control and Computing*, 2015, pp. 1380–1385.

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

[34] R. Gallager, *Information Theory and Reliable Communication*. John Wiley and Sons, New York, 1968.

[35] D. Sutter, J. Renes, F. Dupuis, and R. Renner, "Achieving the capacity of any DMC using only polar codes," in *IEEE Inf. Theory Workshop*, 2012, pp. 114–118.

[36] M. Mondelli, S. H. Hassani, I. Sason, and R. L. Urbanke, "Achieving Martons region for broadcast channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 783–800, 2015.

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

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

[39] T. Han, *Information-Spectrum Methods in Information Theory*. Springer, 2002, vol. 50.

[40] S. Korada and R. Urbanke, "Polar Codes are Optimal for Lossy Source Coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, 2010.

[41] R. Chou, M. Bloch, and J. Kliewer, "Polar coding for empirical and strong coordination via distribution approximation," in *IEEE Int. Symp. Inf. Theory*, 2015, pp. 1512–1516.

[42] D. Aldous, "Random walks on finite groups and rapidly mixing Markov chains," in *Séminaire de Probabilités XVII 1981/82*. Springer, 1983, pp. 243–297.

[43] 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, 2009.

[44] W. Tong, "Bringing 5G into reality," *Huawei, Mar*, 2016.

[45] T. Han, "The capacity region of general multiple-access channel with certain correlated sources," *Information and Control*, vol. 40, pp. 37–60, 1979.

[46] D. Tse and S. Hanly, "Multiaccess fading channels-Part I: Polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2796–2815, 1998.

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

Rémi A. Chou (M'17) is an Assistant Professor in the Electrical Engineering and Computer Science Department at Wichita State University. He received the Engineering degree from Supélec, Gif-sur-Yvette, France, in 2011, and the Ph.D. degree in Electrical Engineering from the Georgia Institute of Technology, Atlanta, in 2015. From 2015 to 2017, he was a Postdoctoral Scholar at The Pennsylvania State University, University Park.

Aylin Yener (S'91–M'01–SM'14–F'15) received the B.Sc. degree in electrical and electronics engineering and the B.Sc. degree in physics from Bogazici University, Istanbul, Turkey, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Wireless Information Network Laboratory (WINLAB), Rutgers University, New Brunswick, NJ, USA. She is a Professor of Electrical Engineering at The Pennsylvania State University, University Park, PA, USA, since 2010, where she joined the faculty as an assistant professor in 2002, and was an associate professor 2006-2010. Since 2017, she is a Dean's Fellow in the College of Engineering at The Pennsylvania State University. She was a visiting professor of Electrical Engineering at Stanford University in 2016-2018 and a visiting associate professor in the same department in 2008-2009. Her current research interests are in caching systems, information security, green communications, and more generally in the fields of communication theory, information theory and network science. She received the NSF CAREER Award in 2003, the Best Paper Award in Communication Theory from the IEEE International Conference on Communications in 2010, the Penn State Engineering Alumni Society (PSEAS) Outstanding Research Award in 2010, the IEEE Marconi Prize Paper Award in 2014, the PSEAS Premier Research Award in 2014, and the Leonard A. Doggett Award for Outstanding Writing in Electrical Engineering at Penn State in 2014. She is a distinguished lecturer for the IEEE Communications Society(2018-2020) and the IEEE Vehicular Technology Society (2017-2019).

Dr. Yener is a member of the Board of Governors of the IEEE Information Theory Society (2015-2020), where she was previously the Treasurer from 2012 to 2014. She served as the Student Committee Chair for the IEEE Information Theory Society from 2007 to 2011, and was the co-Founder of the Annual School of Information Theory in North America in 2008. She was a Technical (Co)-Chair for various symposia/tracks at the IEEE ICC, PIMRC, VTC, WCNC, and Asilomar in 2005, 2008-2014 and 2018. She served as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS from 2009 to 2012, an Editor and an Editorial Advisory Board Member for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2001 to 2012, and a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY in 2011, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS in 2015. Currently, she serves on the Editorial Board of the IEEE TRANSACTIONS ON MOBILE COMPUTING and as a Senior Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.