Polar Coding for the Wiretap Broadcast Channel with Multiple Messages

Jaume del Olmo Alòs and Javier R. Fonollosa
Universitat Politècnica de Catalunya
Barcelona, Spain
Email: {jaume.del.olmo, javier.fonollosa}@upc.edu

Abstract—**A polar coding scheme is proposed for the Wiretap Broadcast Channel with two legitimate receivers and one eavesdropper. We consider a model in which the transmitter wishes to to reliably send different confidential and private messages to the different legitimate receivers, and the confidential message must also be (strongly) secured from the eavesdropper. There are two different inner-bounds on the achievable region of this model in the literature. Both are characterized by using Marton's coding and the only difference between them is the decoding strategy: one is characterized by using joint decoding, while the other uses successive decoding. In this paper we present a polar coding scheme that achieves the larger inner-bound, and we show that polar-based joint decoding is crucial for this purpose.**

A full version of this paper is accessible at: https://arxiv.org/abs/1909.04898

I. Introduction

Information-theoretic security over noisy channels was introduced by Wyner in [1], which characterized the secrecy-capacity of the degraded wiretap channel. Later, Csiszár and Körner in [2] generalized Wyner's results to the general wiretap channel. In these settings, one transmitter wishes to reliably send one message to a legitimate receiver, while keeping it secret from an eavesdropper, where secrecy is defined based on a condition on some information-theoretic measure that is fully quantifiable. One of these measures is the *information leakage*, defined as the mutual information $I(S; Z^n)$ between a uniformly distributed random message S and the channel observations Z^n at the eavesdropper, n being the number of uses of the channel. Based on this measure, the most common secrecy conditions required to be satisfied by channel codes are the *weak secrecy*, which requires $\lim_{n\to\infty} \frac{1}{n} I(S; Z^n) = 0$, and the *strong secrecy*, requiring $\lim_{n\to\infty} I(S; Z^n) = 0$.

Information-theoretic security has been extended to a large variety of contexts, and polar codes [3] have become increasingly popular in this topic due to their easily provable secrecy capacity achieving property. Secrecy capacity achieving polar codes for the binary symmetric degraded wiretap channel were introduced in [4] and [5], satisfying the weak and the strong secrecy condition, respectively. Recently, polar coding has been extended to the general wiretap channel in [6]–[9] and to different multiuser scenarios (for instance, see [10] and [11]).

This paper presents the main aspects of a polar coding scheme for a model over the Wiretap Broadcast Channel (WTBC) where transmitter wants to reliably send different confidential (and non-confidential) messages to two different legitimate receivers in the presence of an eavesdropper. This model generalizes the one considered in [12], where only common information is intended for both receivers.

There are two different inner-bounds on the achievable region of this model in the literature: [13, Theorem 2] and [14, Theorem 1]. The random coding techniques used to characterize the bounds are almost the same and the only difference is the decoding strategy: joint decoding in the former and successive decoding in the later.

We provide a polar coding scheme that achieves the inner-bound in [13] (which includes the one in [14]). Our polar coding scheme is based in part on the one described in [15] that achieves Marton's region of broadcast channels without secrecy constraints, and the one described in [12]. In Marton's coding we have three different layers: one inner-layer that must be decoded by both legitimate receivers, and two outer-layers such that each one conveys information intended only for one receiver. Due to the non-degradedness condition of channels, the coding scheme requires the use of a chaining which induces bidirectional dependencies between adjacent blocks. We show that joint and successive decoding have their counterpart in polar coding, and jointly decoding allows to enlarge the achievable region for a particular input distribution. Indeed, due to the polar-based jointly decoding, the coding scheme needs to build a chaining that introduces dependencies between different encoding layers of adjacent blocks.

II. Channel model and achievable region

A WTBC $(\mathcal{X}, p_{Y_{(1)}Y_{(2)}Z|X}, \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z})$ with 2 legitimate receivers and an external eavesdropper is characterized by the probability transition function $p_{Y_{(1)}Y_{(2)}Z|X}$, where $X \in \mathcal{X}$ denotes the channel input, $Y_{(k)} \in \mathcal{Y}_{(k)}$ denotes the channel output corresponding to the legitimate receiver $k \in [1, 2]$, and $Z \in \mathcal{Z}$ denotes the channel output corresponding to the eavesdropper. Now, we consider a model, namely *Multiple Information over the WTBC* (MI-WTBC), in which the transmitter wishes to send two private messages W_1 and W_2, and two confidential messages S_1 and S_2, where W_1 and S_1 are intended to legitimate Receiver 1, and W_2 and S_2 are intended to legitimate Receiver 2. A code $\big(\lceil 2^{nR_{W_{(1)}}} \rceil, \lceil 2^{nR_{S_{(1)}}} \rceil, \lceil 2^{nR_{W_{(2)}}} \rceil, \lceil 2^{nR_{S_{(2)}}} \rceil, n\big)$ for the MI-WTBC consists of two private message sets $\mathcal{W}_{(1)}$ and $\mathcal{W}_{(2)}$ where $\mathcal{W}_{(k)} \triangleq \big[1, \lceil 2^{nR_{W_{(k)}}} \rceil\big]$ for $k \in [1, 2]$, two confidential message sets $\mathcal{S}_{(1)}$ and $\mathcal{S}_{(2)}$ where $\mathcal{S}_{(k)} \triangleq \big[1, \lceil 2^{nR_{S_{(k)}}} \rceil\big]$ for

$k \in [1,2]$, an encoding function $f : \mathcal{W}_{(1)} \times \mathcal{S}_{(1)} \times \mathcal{W}_{(2)} \times \mathcal{S}_{(2)} \to \mathcal{X}^n$ that maps $(w_{(1)}, w_{(2)}, s_{(1)}, s_{(2)})$ to a codeword x^n, and two decoding functions $g_{(1)}$ and $g_{(2)}$ such that $g_{(k)} : \mathcal{Y}_{(k)}^n \to \mathcal{W}_{(k)} \times \mathcal{S}_{(k)}$ ($k \in [1,2]$) maps the k-th legitimate receiver observations $y_{(k)}^n$ to the estimates $(\hat{w}_{(k)}, \hat{s}_{(k)})$. The reliability condition to be satisfied by this code is given by

$$\lim_{n\to\infty} \mathbb{P}\left[(W_{(k)}, S_{(k)}) \neq (\hat{W}_{(k)}, \hat{S}_{(k)})\right] = 0, \quad k \in [1,2]. \quad (1)$$

The *strong* secrecy condition is measured in terms of the information leakage and is given by

$$\lim_{n\to\infty} I\left(S_{(1)} S_{(2)}; Z^n\right) = 0. \quad (2)$$

A tuple of rates $(R_{W_{(1)}}, R_{S_{(1)}}, R_{W_{(2)}}, R_{S_{(2)}}) \in \mathbb{R}_+^4$ is achievable for the MI-WTBC if a sequence of $\left(\lceil 2^{nR_{W_{(1)}}} \rceil, \lceil 2^{nR_{S_{(1)}}} \rceil, \lceil 2^{nR_{W_{(2)}}} \rceil, \lceil 2^{nR_{S_{(2)}}} \rceil, n\right)$ codes that satisfy the reliability and secrecy conditions (1) and (2) respectively exists. This model is represented in Fig. 1.

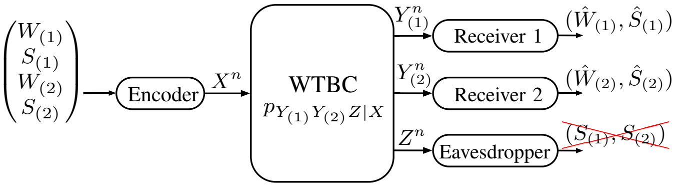

Fig. 1: Channel model: MI-WTBC.

References [13, Theorem 2] and [14, Theorem 1] define two different inner-bounds on the capacity region of this model. Indeed, the inner-bound in [13] only consider the case where $R_{W_{(1)}} = R_{W_{(2)}} \triangleq 0$. In this situation, for a particular input distribution, the inner-bound in [13] is strictly larger than the one in [14]. However, in general we cannot affirm that the inner-bound in [13] is strictly larger than the one in [14] because the rate tuples that are included only in [13] for a particular input distribution may be in [14] under another distribution. Moreover, the region in [14] imposes $I(V;Z) \leq I(V;Y_{(k)})$ for any $k \in [1,2]$, V being an auxiliary input random variable, while this condition is not imposed in [13]. The coding techniques used in [13] and [14] are Marton's coding and rate splitting in conjunction with superposition and binning, and the only difference is the decoding strategy: joint decoding in [13] and successive decoding in [14].

For compactness of notation, let $k \in [1,2]$ and $\bar{k} \triangleq [1,2] \setminus k$. The following proposition defines an inner-bound on the achievable region for the MI-WTBC.

Proposition 1: $\mathfrak{R}_{\text{MI-WTBC}} \triangleq Conv\big(\mathfrak{R}_{\text{MI-WTBC}}^{(1)} \cup \mathfrak{R}_{\text{MI-WTBC}}^{(2)}\big)$ defines an inner-bound on the achievable region of the MI-WTBC, where for $k \in [1,2]$:

$$\mathfrak{R}_{\text{MI-WTBC}}^{(k)} \triangleq \bigcup_{\mathcal{P}} \left\{ \begin{aligned} &R_{S_{(k)}} \leq I(VU_{(k)};Y_{(k)}) - I(VU_{(k)};Z) \\ &R_{S_{(\bar{k})}} \leq I(VU_{(\bar{k})};Y_{(\bar{k})}) - I(U_{(\bar{k})};U_{(k)}|V) \\ &\qquad\qquad -I(U_{(\bar{k})};Z|VU_{(k)}) - I^\dagger \\ &R_{S_{(k)}} + R_{W_{(k)}} \leq I(VU_{(k)};Y_{(k)}) \\ &R_{S_{(\bar{k})}} + R_{W_{(\bar{k})}} \leq I(VU_{(\bar{k})};Y_{(\bar{k})}) - I(U_{(\bar{k})};U_{(k)}|V) \\ &\qquad\qquad -I^\dagger + I(V;Z), \end{aligned} \right\},$$

where $\mathcal{P}$ contains all distributions $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$ such that $(VU_{(1)}U_{(2)}) - X - (Y_{(1)}, Y_{(2)}, Z)$ forms a Markov chain and $I(U_{(1)};Y_{(1)}|V) + I(U_{(2)};Y_{(2)}|V) \geq I(U_{(1)};U_{(2)}|V)$; and

$$I^\dagger \triangleq \max\{I(V;Y_{(1)}), I(V;Y_{(2)}), I(V;Z)\}$$

Remark 1: Since the previous inner-bound on the achievable region of the MI-WTBC cannot be enlarged by considering general distributions $p_{X|VU_{(1)}U_{(2)}}$, the channel input X can be restricted to be any deterministic function of $(VU_{(1)}U_{(2)})$.

The region in Prop. 1 is based on the one in [13]. Indeed, if we assume an input distribution such that $I(V;Y_{(1)}) \leq I(V;Y_{(2)})$, then the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ is not achievable in [14]. Moreover, $\mathfrak{R}_{\text{MI-WTBC}}$ does not restrict the input distribution to satisfy $I(V;Z) \leq I(V;Y_{(k)})$ for any $k \in [1,2]$.

In Section III we describe the main aspects of the polar coding scheme when it operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ for $I(V;Y_{(1)}) \leq I(V;Y_{(2)})$. In Section IV we show that polar-based joint decoding is crucial for this purpose.

III. Polar coding scheme

Under the assumption $I(V;Y_{(1)}) \leq I(V;Y_{(2)})$, the polar coding scheme must contemplate three different situations:

Situation 1: when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$,
Situation 2: when $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_{(2)})$,
Situation 3: when $I(V;Y_{(1)}) \leq I(V;Y_{(2)}) < I(V;Z)$.

Due to space constraints, we consider the Situation 1 only, and we describe a polar code that achieves the corner point $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ of Prop. 1, where

$$R_{S_{(2)}}^{\star 2} \triangleq H(VU_{(2)}|Z) - H(VU_{(2)}|Y_{(2)}), \quad (3)$$

$$R_{S_{(1)}}^{\star 2} \triangleq H(U_{(1)}|VU_{(2)}Z) - H(U_{(1)}|VY_{(1)}) \quad (4)$$

$$R_{W_{(2)}}^{\star 2} \triangleq H(VU_{(2)}) - H(VU_{(2)}|Z), \quad (5)$$

$$R_{W_{(1)}}^{\star 1} \triangleq H(U_{(1)}|VU_{(2)}) - H(U_{(1)}|VU_{(2)}Z). \quad (6)$$

Notice that $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2})$ corresponds to the case where, for a given distribution $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$, we set the maximum rate for the confidential and private messages intended for Receiver 2, and then we set the maximum possible rates of the remaining messages associated to Receiver 1.

Consider a Discrete Memoryless Source (DMS)

$$(\mathcal{V} \times \mathcal{U}_{(1)} \times \mathcal{U}_{(2)} \times \mathcal{X} \times \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z}, p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z})$$

that represents the input $(V, U_{(1)}, U_{(2)}, X)$ and output $(Y_{(1)}, Y_{(2)}, Z)$ random variables of the MI-WTBC, where $|\mathcal{V}| = |\mathcal{U}_{(1)}| = |\mathcal{U}_{(2)}| = |\mathcal{X}| \triangleq 2$. Associated to V, we define the polar transform $A^n \triangleq V^n G_n$ and the sets

$$\mathcal{H}_V^{(n)} \triangleq \left\{j \in [1,n] : H\big(A(j) \big| A^{1:j-1}\big) \geq 1 - \delta_n\right\},$$

$$\mathcal{L}_V^{(n)} \triangleq \left\{j \in [1,n] : H\big(A(j) \big| A^{1:j-1}\big) \leq \delta_n\right\},$$

$$\mathcal{H}_{V|Z}^{(n)} \triangleq \left\{j \in [1,n] : H\big(A(j) \big| A^{1:j-1} Z^n\big) \geq 1 - \delta_n\right\},$$

$$\mathcal{L}_{V|Y_{(k)}}^{(n)} \triangleq \left\{j \in [1,n] : H\big(A(j) \big| A^{1:j-1} Y_{(k)}^n\big) \leq \delta_n\right\},$$

where $k \in [1,2]$. For the random variable $U_{(k)}$, being $k \in [1,2]$, we define the polar transform $T_{(k)}^n \triangleq U_{(k)}^n G_n$. In order to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$, we define

$$\mathcal{H}_{U_{(2)}|V}^{(n)} \triangleq \{j \in [1,n] : H(T_{(2)}(j)|T_{(2)}^{1:j-1}V^n) \geq 1-\delta_n\},$$
$$\mathcal{L}_{U_{(2)}|V}^{(n)} \triangleq \{j \in [1,n] : H(T_{(2)}(j)|T_{(2)}^{1:j-1}V^n) \leq \delta_n\},$$
$$\mathcal{H}_{U_{(2)}|VZ}^{(n)} \triangleq \{j \in [1,n] : H(T_{(2)}(j)|T_{(2)}^{1:j-1}V^n Z^n) \geq 1-\delta_n\},$$
$$\mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)} \triangleq \{j \in [1,n] : H\big(T_{(2)}(j)\big|T_{(2)}^{1:j-1}V^n Y_{(2)}^n\big) \leq \delta_n\}.$$

associated to $U_{(2)}$; and associated to $U_{(1)}$, we define

$$\mathcal{H}_{U_{(1)}|VU_{(2)}}^{(n)} \triangleq \{j \in [n] : H\big(T_{(1)}(j)\big|T_{(1)}^{1:j-1}V^n U_{(2)}^n\big) \geq 1-\delta_n\},$$
$$\mathcal{L}_{U_{(1)}|VU_{(2)}}^{(n)} \triangleq \{j \in [n] : H\big(T_{(1)}(j)\big|T_{(1)}^{1:j-1}V^n U_{(2)}^n\big) \leq \delta_n\},$$
$$\mathcal{H}_{U_{(1)}|VU_{(2)}Z}^{(n)} \triangleq \{j \in [n] : H\big(T_{(1)}(j)\big|T_{(1)}^{1:j-1}V^n U_{(2)}^n Z^n\big) \geq 1-\delta_n\},$$
$$\mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)} \triangleq \{j \in [n] : H\big(T_{(1)}(j)\big|T_{(1)}^{1:j-1}V^n Y_{(1)}^n\big) \leq \delta_n\}.$$

Consider that the encoding takes place over L blocks indexed by $i \in [1,L]$. At Block $i \in [1,L]$, the encoder will construct $\tilde{A}_i^n$, which will carry part of the confidential and private message that is intended for legitimate Receiver 2. Then, the encoder first constructs $\tilde{T}_{(2),i}^n$, which will depend on $\tilde{V}_i^n = \tilde{A}_i^n G_n$ and will carry the remaining parts of the confidential and private messages intended for Receiver 2. Then, the encoder forms $\tilde{T}_{(1),i}^n$, which depends on $\big(\tilde{V}_i^n, \tilde{T}_{(2),i}^n\big)$. Finally, it will obtain $\tilde{U}_{(k),i}^n = \tilde{T}_{(k),i}^n G_n$ for $k \in [1,2]$ and deterministically form $\tilde{X}_i^n$. The codeword $\tilde{X}^n$ then is transmitted over the WTBC inducing $(\tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n)$.

A. Construction of the inner-layer

The method of forming $\tilde{A}_{1:L}^n$ is very similar to the one described in [12]. Thus, we define $\mathcal{G}^{(n)} \triangleq \mathcal{H}_{V|Z}^{(n)}$ and $\mathcal{C}^{(n)} \triangleq \mathcal{H}_V^{(n)} \cap \big(\mathcal{H}_{V|Z}^{(n)}\big)^{\mathrm{C}}$, which form a partition of $\mathcal{H}_V^{(n)}$. Moreover, we also define the following partition of the set $\mathcal{G}^{(n)}$:

$$\mathcal{G}_0^{(n)} \triangleq \mathcal{G}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{7}$$
$$\mathcal{G}_1^{(n)} \triangleq \mathcal{G}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{8}$$
$$\mathcal{G}_2^{(n)} \triangleq \mathcal{G}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{9}$$
$$\mathcal{G}_{1,2}^{(n)} \triangleq \mathcal{G}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{10}$$

and the following partition of the set $\mathcal{C}^{(n)}$:

$$\mathcal{C}_0^{(n)} \triangleq \mathcal{C}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{11}$$
$$\mathcal{C}_1^{(n)} \triangleq \mathcal{C}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{12}$$
$$\mathcal{C}_2^{(n)} \triangleq \mathcal{C}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{13}$$
$$\mathcal{C}_{1,2}^{(n)} \triangleq \mathcal{C}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}. \tag{14}$$

Recall that $\tilde{A}_i[\mathcal{H}_V^{(n)}]$, $i \in [1,L]$, is suitable for storing uniformly distributed random sequences, and $\tilde{A}_i[\mathcal{G}^{(n)}]$ is suitable for storing information to be secured from the eavesdropper. Also, sets with subscript $k \in [1,2]$ form $\mathcal{H}_V^{(n)} \setminus \mathcal{L}_{V|Y_{(k)}}^{(n)}$, and the elements of $\tilde{A}_i^n$ corresponding to this set of indices are required by Receiver k to reliably reconstruct $\tilde{A}_i^n$ entirely.

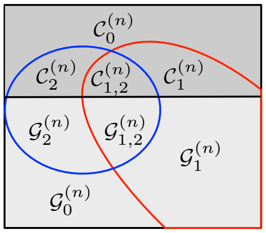

Fig. 2: Graphical representation of the sets in (7)–(14). The indices inside the soft and dark gray area form $\mathcal{G}^{(n)}$ and $\mathcal{C}^{(n)}$ respectively. The indices that form $\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}$ are those inside the red curve, while those inside the blue curve form $\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}$.

In Situation 1 we have the condition $I(V;Z) \leq I(V;Y_1) \leq I(V;Y_2)$. As seen in [12], for n sufficiently large this condition imposes the following restriction on the size of previous sets:

$$\big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| \geq \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| \geq \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|,$$

which entails having to consider four different cases. In this paper we consider the Case A only, where $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| \geq |\mathcal{C}_{1,2}^{(n)}|$.

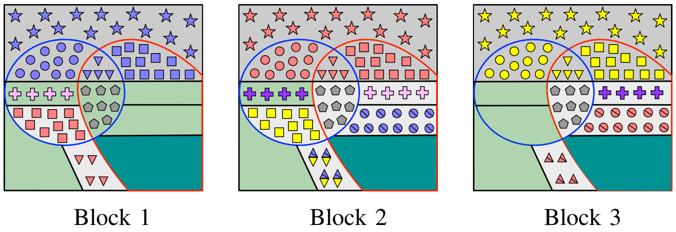

Fig. 3: Representation of the encoding of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ ($L = 3$), which carries the private and confidential messages intended for Receiver 2.

The encoding of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ is as follows. At Block $i \in [1,L]$, the encoder stores part of the private message intended for Receiver 2 in $\tilde{A}_i[\mathcal{C}^{(n)}]$ (red symbols at Block 2 in Fig. 3). Then, it repeats entries of *bad* indices (only) for Receiver 1 in some *good* entries of Block $i-1$ (red squares). Similarly, it repeats entries of *bad* indices (only) for Receiver 2 in some entries of Block $i+1$ (red circles). These entries are not repeated directly, but they are previously encrypted by using a secret-key that is reused in all blocks (circles with a line through them). Moreover, it also repeats entries of *bad* indices for both receivers in Block $i-1$ and Block $i+1$ (red triangles). Indeed, for $i \in [2, L-1]$, these elements are repeated after modulo-2 addition with ones from Block $i-2$ and $i+2$ respectively. Consequently, at Block $i \in [1,L]$, some indices suitable for confidential information must be used also to allocate repetitions of private information of adjacent blocks. As in [12], at Block $i \in [2, L-1]$ the confidential information intended for Receiver 2 is placed into those elements good for Receiver 1 that are still available (bright green shaded regions at Block 2). Then, those that correspond to the *bad* indices for Receiver 2 will be repeated to the next block (purple crosses). In [12], the remaining entries store a sequence that is replicated in all blocks (grey pentagons). Nevertheless, now only those that correspond to the *bad* indices for both receivers replicate this sequence, and the remaining elements of good indices for Receiver 2, namely $\Pi^{(V)}_{(1),i}$, store additional confidential information (dark green shaded region in all blocks).

As in [12], we construct the remaining entries of $\tilde{A}^n_{1:L}$ by means of Successive Cancellation (SC) encoding: one part will be draw deterministically while the other randomly [16]. Also, part of these elements will be secretly send to both receivers by incurring a negligible rate penalty, jointly with part of $\tilde{A}^n_1$ and $\tilde{A}^n_L$ required to initialize the decoding algorithms.

B. Encoding of outer-layer associated to Receiver 2

Besides the previous sets associated to $U_{(2)}$, we define

$$\mathcal{F}^{(n)}_0 \triangleq \mathcal{H}^{(n)}_{U_{(2)}|VZ} \cap \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}, \tag{15}$$

$$\mathcal{F}^{(n)}_2 \triangleq \mathcal{H}^{(n)}_{U_{(2)}|VZ} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}, \tag{16}$$

$$\mathcal{J}^{(n)}_0 \triangleq \mathcal{H}^{(n)}_{U_{(2)}|V} \cap \big(\mathcal{H}^{(n)}_{U_{(2)}|VZ}\big)^{\mathrm{C}} \cap \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}, \tag{17}$$

$$\mathcal{J}^{(n)}_2 \triangleq \mathcal{H}^{(n)}_{U_{(2)}|V} \cap \big(\mathcal{H}^{(n)}_{U_{(2)}|VZ}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2}}. \tag{18}$$

For $i \in [1, L]$, $\tilde{T}_{(2),i}\big[\mathcal{H}^{(n)}_{U_{(2)}|V}\big]$ will be suitable for storing uniform sequences that are independent of $\tilde{V}^n_i$, and $\tilde{T}_{(2),i}\big[\mathcal{F}^{(n)}_0 \cup \mathcal{F}^{(n)}_2\big]$ is suitable for storing information to be secured from the eavesdropper. Moreover, $\tilde{T}_{(2),i}\big[\mathcal{F}^{(n)}_2 \cup \mathcal{J}^{(n)}_2\big]$ is the uniformly distributed part independent of $\tilde{V}^n_i$ needed by Receiver 2 to reliably reconstruct $\tilde{T}^n_{(2),i}$ from $\tilde{Y}^n_{(2),i}$ and $\tilde{V}^n_2$.

We assume $I(U_{(k)}; Y_{(k)}|V) \geq I(U_{(k)}; Z|V)$ (see Remark 2). Thus, besides the partition defined in (15)–(18), we define

$$\mathcal{D}^{(n)}_2 \triangleq \text{ any subset of } \mathcal{F}^{(n)}_0 \text{ with size } \big|\mathcal{J}^{(n)}_2\big|. \tag{19}$$

The encoding is as follows. At block $i \in [1, L]$, the encoder stores the remaining part of the private message intended for Receiver 2 in $\tilde{T}_{(2),i}\big[\mathcal{J}^{(n)}_0 \cup \mathcal{J}^{(n)}_2\big]$. The elements $\tilde{T}_{(2),i}\big[\mathcal{J}^{(n)}_2\big]$ correspond to *bad* indices for Receiver 2, and they are repeated at the next block in $\tilde{T}_{(2),i+1}\big[\mathcal{D}^{(n)}_2\big] \subseteq \tilde{T}_{(2),i+1}\big[\mathcal{F}^{(n)}_0\big]$. Indeed, they are not repeated directly but they are previously encrypted by using a secret-key that is reused in all blocks. At Block 1, the confidential message intended for Receiver 2 is stored into $\tilde{T}_{(2),1}\big[\mathcal{F}^{(n)}_0 \cup \mathcal{F}^{(n)}_2\big]$. Otherwise, at Block $[2, L]$, it is stored into $\tilde{T}_{(2),i}\big[\mathcal{F}^{(n)}_0 \setminus \mathcal{D}_2\big]$, and $\tilde{T}_{(2),i}\big[\mathcal{F}^{(n)}_2\big]$ replicates $\tilde{F}_{(2),1}\big[\mathcal{F}^{(n)}_2\big]$.

The remaining entries of $\tilde{T}^n_{(2),1:L}$ are drawn by SC encoding. Part of them together with others from Block 1 and L will be secretly send to receivers by incurring a negligible rate penalty.

Remark 2: If $I(U_{(2)}; Y_{(2)}|V) < I(U_{(2)}; Z|V)$, notice that $\big|\mathcal{F}^{(n)}_0\big| - \big|\mathcal{J}^{(n)}_2\big| < 0$. Consequently, for $i \in [1, L-1]$ the encoder cannot repeat $\tilde{T}_{(2),i}\big[\mathcal{J}^{(n)}_2\big]$ at Block $i+1$. Therefore, under this assumption, part of this sequence that cannot be repeated in the outer-layer will be repeated in some elements of the inner-layer. This will be possible because we assume input distributions such that $R^{\star 2}_{S_{(2)}}$ in (3) is strictly positive.

C. Encoding of outer-layer associated to Receiver 1

Besides the previous sets associated to $U_{(1)}$, we define

$$\mathcal{Q}^{(n)}_0 \triangleq \mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}Z} \cap \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}, \tag{20}$$

$$\mathcal{Q}^{(n)}_1 \triangleq \mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}Z} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}, \tag{21}$$

$$\mathcal{B}^{(n)}_0 \triangleq \mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}} \cap \big(\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}Z}\big)^{\mathrm{C}} \cap \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}, \tag{22}$$

$$\mathcal{B}^{(n)}_1 \triangleq \mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}} \cap \big(\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}Z}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}. \tag{23}$$

For $i \in [1, L]$, $\tilde{T}_{(1),i}\big[\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}}\big]$ will be suitable for storing uniformly distributed random sequences that are independent of $(\tilde{V}^n_i, \tilde{U}^n_{(2),i})$, and $\tilde{T}_{(1),i}\big[\mathcal{Q}^{(n)}_0 \cup \mathcal{Q}^{(n)}_1\big]$ will be suitable for storing information to be secured from the eavesdropper. Moreover, the elements of $\tilde{T}_{(1),i}\big[\mathcal{B}^{(n)}_1 \cup \mathcal{Q}^{(n)}_1\big]$ are required by Receiver 1 to reliably construct the entire sequence $\tilde{T}^n_{(1),i}$ from $(\tilde{V}^n_i, \tilde{Y}^n_{(1),i})$. Additionally, we define

$$\begin{aligned}
\mathcal{O}^{(n)}_1 \triangleq\ & \text{any subset of } \mathcal{Q}^{(n)}_0 \\
& \text{with size } \Big|\big(\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}}\big)^{\mathrm{C}} \cap \mathcal{H}^{(n)}_{U_{(1)}|V} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\Big|, \\
\mathcal{N}^{(n)}_1 \triangleq\ & \text{any subset of } \mathcal{Q}^{(n)}_0 \setminus \mathcal{O}^{(n)}_1 \text{ with size } \big|\mathcal{B}^{(n)}_1\big|, \\
\mathcal{M}^{(n)}_1 \triangleq\ & \text{any subset of } \mathcal{Q}^{(n)}_0 \setminus (\mathcal{O}^{(n)}_1 \cup \mathcal{N}^{(n)}_1) \\
& \text{with size} \big|\mathcal{G}^{(n)}_1\big| + \big|\mathcal{C}^{(n)}_1\big| - \big|\mathcal{G}^{(n)}_2\big| - \big|\mathcal{C}^{(n)}_2\big|.
\end{aligned}$$

The construction of $\tilde{T}^n_{(1),1:L}$ associated to Receiver 1 is as follows. At Block $i \in [1, L]$, the encoder stores the private message intended for Receiver 1 in $\tilde{T}_{(1),i}\big[\mathcal{B}^{(n)}_0 \cup \mathcal{B}^{(n)}_1\big]$. The entries $\Theta^{(U)}_{(1),i} \triangleq \tilde{T}_{(1),i}\big[\mathcal{B}^{(n)}_1\big]$ correspond to *bad* indices for Receiver 1 and are repeated in $\tilde{T}_{(1),i-1}\big[\mathcal{N}^{(n)}_1\big] \subseteq \tilde{T}_{(1),i-1}\big[\mathcal{Q}^{(n)}_0\big]$ from the previous block. At Block 1, into the elements $\tilde{T}_{(1),1}\big[\big(\mathcal{Q}^{(n)}_0 \cup \mathcal{Q}^{(n)}_1\big) \setminus \big(\mathcal{O}^{(n)}_1 \cup \mathcal{N}^{(n)}_1 \cup \mathcal{M}^{(n)}_1\big)\big]$, the encoder stores the confidential message intended for Receiver 1; at Block $i \in [2, L-1]$, $\tilde{T}_{(1),i}\big[\mathcal{Q}^{(n)}_0 \setminus \big(\mathcal{O}^{(n)}_1 \cup \mathcal{N}^{(n)}_1 \cup \mathcal{M}^{(n)}_1\big)\big]$ contains this message; and at Block L, this message is stored into $\tilde{T}_{(1),L}\big[\mathcal{Q}^{(n)}_0\big]$. Indeed, for $i \in [2, L]$, $\tilde{T}_{(1),i}\big[\mathcal{Q}^{(n)}_1\big]$ replicates $\tilde{T}_{(1),1}\big[\mathcal{Q}^{(n)}_1\big]$. Furthermore, for $i \in [2, L]$, the encoder repeats $\Pi^{(V)}_{(1),i}$ in $\tilde{T}_{(1),i-1}\big[\mathcal{M}^{(n)}_1\big]$, which contains part of the confidential message intended for Receiver 2 stored in $\tilde{A}^n_i$. Finally, for $i \in [2, L]$, $\tilde{T}_{(1),i-1}[\mathcal{O}^{(n)}_1]$ repeats a sequence from $\tilde{T}^n_{(1),i}$ that is problematic. Indeed, for $i \in [1, L]$, $\tilde{T}_{(1),i}\big[\big(\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}Z}\big)^{\mathrm{C}}\big]$ is drawn by means of SC encoding. The problematic sequence is $O^{(U)}_{(1),i} \triangleq \tilde{T}_{(1),i}\big[\big(\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}}\big)^{\mathrm{C}} \cap \mathcal{H}^{(n)}_{U_{(1)}|V} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big]$ because it is non-negligible with respect to the blocklength n, corresponds to bad indices of Receiver 1, and is not uniformly-distributed. Consequently, it cannot be repeated directly and is previously encrypted by using a secret-key that is reused in all blocks. The secret-key ensures that the repeated sequence is uniform and, consequently, it can be stored in $\tilde{T}_{(1),i-1}\big[\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}Z}\big]$ without introducing distortion.

Finally, the encoder obtains $\tilde{X}^n_i \triangleq f\big(\tilde{V}^n_i, \tilde{U}^n_{(1),i}, \tilde{U}^n_{(2),i}\big)$. The transmitter sends $\tilde{X}^n_i$ over the WTBC, which induces the channel outputs $(\tilde{Y}^n_{(1),i}, \tilde{Y}^n_{(2),i}, \tilde{Z}^n_i)$. Additionally, part of

$\tilde{T}^n_{(1),i-1}$ needed to initialize the decoding algorithms will be secretly send to receivers by incurring a negligible rate penalty.

IV. Joint decoding vs. successive decoding

In this section we discuss the importance of joint decoding to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}$ defined in (3)–(6) when $I(V;Y_{(1)}) \leq I(V;Y_{(1)}) \leq I(V;Z)$. Since the polar coding scheme is based on Marton's coding, Receiver $k \in [1,2]$ needs to reliably decode the inner-layer before being able to decode its associated outer-layer. From the additional transmission needed to initialize the decoding algorithm, Receiver k knows, for $i \in [1,L]$, $\Phi_{(k),i} \triangleq \tilde{A}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{V|Y_{(k)}}\big]$. Also, $\Upsilon_{(1)} \triangleq \tilde{A}_1\big[\mathcal{H}_V^{(n)} \setminus \mathcal{L}^{(n)}_{V|Y_{(1)}}\big]$ is known by Receiver 1 (entries into the red curve at Block 1 in Fig. 3), and Receiver 2 knows $\Upsilon_{(2)} \triangleq \tilde{A}_L\big[\mathcal{H}_V^{(n)} \setminus \mathcal{L}^{(n)}_{V|Y_{(2)}}\big]$ (ones in the blue curve at Block L).

First, consider that Receiver $k \in [1,2]$ uses successive decoding, which means having to decode $\tilde{A}^n_i$, for all $i \in [1,L]$, before moving to decode its associated outer-layer $\tilde{T}^n_{(k),i}$. Receiver 2, which decodes backward, from $(\Upsilon_{(2)}, \Phi_{(2),L})$ obtains $\tilde{A}^n_L$ entirely. In Figure 3, notice that the elements corresponding to its bad indices at Block i (inside the blue curve) are previously decoded at Block $i+1$ and, consequently, Receiver 2 is able to reconstruct $\tilde{A}^n_i$ for all $i \in [1,L]$. Receiver 1, which decodes forward, is able to obtain $\tilde{A}^n_1$ entirely from $(\Upsilon_{(1)}, \Phi_{(1),1})$. In Figure 3, notice that only part of the elements corresponding to its bad indices at Block i (inside the red curve) are previously decoded at Block $i-1$. Indeed, the elements that are problematic are those in the sequence $\Pi^{(V)}_{(1),i}$ (dark green shaded region), which is not repeated in the inner-layer but in the outer-layer $\tilde{T}^n_{(1),i-1}$ associated to Receiver 1. Consequently, this later receiver is not able to reconstruct $\tilde{A}^n_i$, for all $i \in [1,L]$ before moving to decode its associated outer-layer.

On the other hand, consider that Receiver $k \in [1,2]$ uses joint decoding, which means having to decode $\tilde{A}^n_i$ and then $\tilde{T}^n_{(k),i}$ for some $i \in [1,L]$, before decoding $(\tilde{A}^n_m, \tilde{T}^n_{(k),m})$, where $m = i+1$ for Receiver 1, and $m = i-1$ for Receiver 2. In this case, not only Receiver 2 is able to reliably reconstruct both $\tilde{A}^n_i$ and $\tilde{T}^n_{(k),i}$ for all $i \in [1,L]$, but also Receiver 1 does. Now, notice that this later receiver will obtain the problematic sequence $\Pi^{(V)}_{(1),i}$ when decoding $\tilde{T}^n_{(k),i-1}$ and, therefore, it is able to reliably reconstruct $\tilde{A}^n_i$.

In fact, in the full version of the paper we show that, with joint decoding, the inner-layer is able to carry confidential information intended for Receiver 2 at rate $I(V;Y_{(2)}) - I(V;Z)$. Although this rate is greater than the one that Receiver 1 can reliably decode—because $I(V;Y_{(2)}) \geq I(V;Y_{(1)})$—, we have mentioned that it will be achievable because the outer-layer associated to this receiver will sacrifice part of its corresponding rate—specifically, it will sacrifice $I(V;Y_{(2)}) - I(V;Y_{(1)})$. Otherwise, with successive decoding, notice that the problematic sequence $\Pi^{(V)}_{(1),i}$ could not contain *useful* information, but *padding* elements replicated in all blocks so that both receivers are able to reconstruct the inner-layer first (see [12]). In this case, the inner-layer could only convey useful information at rate $I(V;Y_{(1)}) - I(V;Z)$.

Remark 3: In this paper, due to space constraints, we have explained for one case only why joint decoding allows to enlarge the capacity region for a particular input distribution. Nevertheless, in the full version of the paper we have showed that joint decoding is crucial in other situations: input distributions such that $I(V;Z) \leq I(V;Y_{(k)})$, $k \in [1,2]$, can only be considered if the polar coding scheme uses joint decoding. Despite these other situations could seem irrelevant if we consider confidential messages rates only, they are important when the private messages rates are also taken into account.

V. Conclusion

A strongly secure polar coding scheme has been proposed for the WTBC with two legitimate receivers and one eavesdropper. This polar code achieves the best known inner-bound on the achievable region of the MI-WTBC model, where transmitter wants to send different private and confidential messages to two different receivers. This model generalizes the ones in [12] and [15] and, consequently, the chaining structure of the polar coding scheme is not straightforward from previous results.

Moreover, in this paper we have described one situation where polar-based joint decoding is crucial for the polar coding scheme to achieve a particular rate tuple of this inner-bound. In fact, in the full version of the paper we show that the coding scheme must consider different cases and situations, and polar-based decoding is crucial in most of them.

The polar coding scheme uses different secret keys whose length is negligible in terms of rate, and which are previously shared between transmitter and legitimate receivers. On the one hand, we use a secret-key for repeating some elements from Block i to Block $(i-1)$ or $(i+1)$, which is reused in all blocks and therefore its length is negligible when the number of transmission blocks is large enough. This key is needed for proving that the polar coding scheme satisfies the strong secrecy condition although we conjecture that its use is not necessary. On the other hand, we use a secret-key, which is also negligible, in order to privately send the additional transmission required to initialize the decoding algorithms. Finally, we need an additional secret-key in order to randomize elements from one outer-layer that are drawn by successive cancellation encoding (not uniformly distributed) and must be repeated in some adjacent block.

Acknowledgment

This work has been funded by the AEI of Ministerio de Ciencia, Innovación y Universidades of Spain, TEC2016-75067-C4-2-R, RED2018-102668-T with ESF and PID2019-104958RB-C41 and Dept. d'Empresa i Coneixement de la Generalitat de Catalunya, 2017 SGR 578 AGAUR and 001-P-001644 QuantumCAT with ERDF.

References

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

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[4] H. Mahdavifar and A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes,” *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, Oct 2011.

[5] E. Sasoglu and A. Vardy, “A new polar coding scheme for strong security on wiretap channels,” in *IEEE International Symposium onInformation Theory Proceedings (ISIT)*, July 2013, pp. 1117–1121.

[6] 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*. Springer, 2013, pp. 194–213.

[7] Y. Wei and S. Ulukus, “Polar coding for the general wiretap channel with extensions to multiuser scenarios,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 2, pp. 278–291, Feb 2016.

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

[9] R. A. Chou and M. R. Bloch, “Polar coding for the broadcast channel with confidential messages: A random binning analogy,” *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.

[10] J. del Olmo Alos and J. Rodríguez Fonollosa, “Strong secrecy on a class of degraded broadcast channels using polar codes,” *Entropy*, vol. 20, no. 6:467, 2018. [Online]. Available: http://www.mdpi.com/1099-4300/20/6/467

[11] R. A. Chou and A. Yener, “Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming,” *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 7903–7921, Dec 2018.

[12] J. d. Olmo Alòs and J. R. Fonollosa, “Polar coding for common message only wiretap broadcast channel,” in *2019 IEEE International Symposium on Information Theory (ISIT)*, July 2019, pp. 1762–1766.

[13] M. Benammar and P. Piantanida, “Secrecy capacity region of some classes of wiretap broadcast channels,” *IEEE Transactions on Information Theory*, vol. 61, no. 10, pp. 5564–5582, Oct 2015.

[14] E. Ekrem and S. Ulukus, “Multi-receiver wiretap channel with public and confidential messages,” *IEEE Transactions on Information Theory*, vol. 59, no. 4, pp. 2165–2177, April 2013.

[15] M. Mondelli, S. Hassani, I. Sason, and R. Urbanke, “Achieving Marton’s region for broadcast channels using polar codes,” *IEEE Transactions on Information Theory*, vol. 61, no. 2, pp. 783–800, Feb 2015.

[16] R. A. Chou and M. R. Bloch, “Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes,” in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2015, pp. 1380–1385.