Strong Secrecy on a Class of Degraded Broadcast Channels Using Polar Codes

Jaume del Olmo and Javier Rodríguez Fonollosa

Universitat Politècnica de Catalunya (UPC), Barcelona, Spain
Emails: jaume.delolmo@tsc.upc.edu, javier.fonollosa@upc.edu

***Abstract*—Two polar coding schemes are proposed for the degraded broadcast channel under different reliability and secrecy requirements. In these settings, the transmitter wishes to send multiple messages to a set of legitimate receivers keeping them masked from a set of eavesdroppers, and individual channels are assumed to gradually degrade in such a way that each legitimate receiver has a better channel than any eavesdropper. The layered decoding structure requires receivers with better channel quality to reliably decode more messages, while the layered secrecy structure requires eavesdroppers with worse channel quality to be kept ignorant of more messages.**

I. Introduction

Information theoretic security over noisy channels was introduced by Wyner in [1], which characterized the secrecy-capacity of the degraded wiretap channel. Csiszár and Körner in [2] generalized Wyner's results to the general *wiretap* channel. In the last decade, information theoretic security has been extended to a large variety of contexts, and this paper focuses on two classes of discrete memoryless Degraded Broadcast Channels (DBC) introduced in [3] [1]:*a)* with Layered Decoding and Non-Layered Secrecy (DBC-LD-NLS), *b)* with Non-Layered Decoding and Layered Secrecy (DBC-NLD-LS).

The secrecy-capacity region of these models was first characterized in [3], [5], [6]. However, the achievable schemes used by these works rely on random coding arguments that are nonconstructive in practice. In that sense, the purpose of this paper is to provide coding schemes based on *polar codes*, which were originally proposed by Arikan [7]. Polar codes for the symmetric degraded wiretap channel were introduced in [8] and [9], and recently have been extended to the general wiretap channel in [10]–[13]. Furthermore, [12] and [13] generalize their results providing polar codes for the broadcast channel with confidential messages and [11] also proposes polar coding strategies to achieve the best-known inner bounds on the secrecy-capacity region of some multi-user settings.

Although recent literature has explored different polar coding schemes for multi-user scenarios, practical polar codes for the two models considered in this paper are, as far as we know, not analyzed yet. As mentioned in [3], these settings captures practical scenarios in wireless systems, in which channels can be ordered based on the quality of the received signals (for example, in the context of Gaussian fading channels). Our proposed polar coding schemes are based mainly on that introduced by [13] for the broadcast channel with confidential messages and the polar coding strategies given in [14] for secret-key generation. As in [13], a superposition-based polar coding scheme [15, Sec. VI] is used for the models with an imposed layered decoding structure. However, the secrecy constraints require to protect a set of messages from more than one eavesdropper, which is possible because of the degraded nature of the channels. Although [13] highlights the connection between polar code constructions and random binning proofs that allows polar codes to be applied to different problems in network information theory, the particularization to polar code constructions for the two models proposed in this paper is not straightforward. Indeed, while one of the goals of the scheme proposed in [13] is to minimize the use of the total randomness by the system, our aim is to avoid the use of the chaining construction in order to reduce the complexity of the encoding and decoding algorithms, which would be crucial when the number of legitimate receivers and eavesdroppers is very large. However, as in [13], the transmitter and legitimate receivers needs to share a secret seed of negligible size (in terms of rate penalty) to deal with the non-uniform input distribution and to provide explicit coding schemes which do not rely on the existence of certain deterministic mappings.

Notation: Through this paper, let $[n] = \{1, \dots, n\}$ for $n \in \mathbb{Z}^+$, a^n denotes a row vector $(a(1), \dots, a(n))$. We write $a^{1:j}$ for $j \in [n]$ to denote the subvector $(a(1), \dots, a(j))$. Finally, let $\mathcal{A} \subset [n]$, then we write $a[\mathcal{A}]$ to denote the sequence $\{a(j)\}_{j\in\mathcal{A}}$ and we use $\mathcal{A}^{\mathrm{C}}$ to denote the set complement with respect to the universal set $[n]$.

II. System Model and Secrecy-Capacity Region

A. DBC-LD-NLS

In this model, the transmitter wishes to send K messages, $\{W_k\}_{k=1}^K$, to K legitimate receivers with the presence of M eavesdroppers. The broadcast channel is assumed to gradually degrade in such a way that each legitimate receiver has better channel than any eavesdropper, that is,

$$X - Y_K - \cdots - Y_1 - Z_M - \cdots - Z_1 \tag{1}$$

forms a Markov chain. The layered decoding structure requires the k-th receiver to reliably decode the messages $\{W_i\}_{i=1}^k$, and the non-layered secrecy requires all eavesdroppers to be kept ignorant of all K messages. Consider a

This work is supported by the Ministerio de Economa y Competitividad of the Spanish Government and ERDF funds (TEC2013-41315-R, TEC2015-69648-REDC and TEC2016-75067-C4-2-R) and the Catalan Government (2014 SGR 60 AGAUR).

[1] In the long version of this paper [4], another class is investigated.

$(\lceil 2^{nR_1}\rceil,\ldots,\lceil 2^{nR_K}\rceil,n)$ code for the DBC-LD-NLS, where $W_k \in [\lceil 2^{nR_k}\rceil]$ for $k=1,\ldots,K$. The reliability condition of this code is measured in terms of the average probability of error at each receiver and is given by

$$\lim_{n\to\infty}\Pr\Big[(\hat{W}_k,\ldots,\hat{W}_1)\neq(W_k,\ldots,W_1)\Big|\,Y_k^n\Big]=0, \quad (2)$$

for $k=1,\ldots,K$. The *strong* secrecy condition is measured in terms of the information leakage to each eavesdropper,

$$\lim_{n\to\infty} I(W_1,\ldots,W_K;Z_m^n)=0, \quad \text{for } m=1,\ldots,M. \quad (3)$$

Proposition 1 (Adapted from [3] and [5])**.** *The secrecy-capacity region of the DBC-LD-NLS contains all K-tuples of rates $(R_1,\ldots,R_K)\in\mathbb{R}_+^K$ satisfying*

$$\sum_{i=1}^{k}R_i\le\sum_{i=1}^{k}I(V_i;Y_i|V_{i-1})-I(V_k;Z_M), \quad k=1,\ldots,K,$$

where $V_0\triangleq\phi$ and $V_K\triangleq X$, for some distribution $p_{V_1\ldots V_K}$ such that $V_1-V_2-\cdots-V_K$ forms a Markov chain.

Corollary 1. *The sub-region of the secrecy-capacity given in Prop. 1 without considering rate-sharing is the closure of all K-tuples of rates $(R_1,\ldots,R_K)\in\mathbb{R}_+^K$ satisfying*

$$R_k\le I(V_k;Y_k|V_{k-1})-I(V_k;Z_M|V_{k-1}), \quad k=1,\ldots,K,$$

where $V_0\triangleq\phi$ and $V_K\triangleq X$, for some distribution $p_{V_1\ldots V_K}$ such that $V_1-V_2-\cdots-V_K$ forms a Markov chain.

B. DBC-NLD-LS

In this setting, the transmitter wishes to send M messages, $\{W_m\}_{m=1}^M$, to K legitimate receivers with the presence of M eavesdroppers. The broadcast channel is assumed to gradually degrade in the same way as described in Eq. (1). The non-layered decoding structure requires each receiver to reliably decode all M messages and the layered secrecy structure requires the m-th eavesdropper to be kept ignorant of messages $\{W_i\}_{i=m}^M$. Consider a $(\lceil 2^{nR_1}\rceil,\ldots,\lceil 2^{nR_M}\rceil,n)$ code for the DBC-NLD-LS, where $W_m\in[\lceil 2^{nR_m}\rceil]$ for $m=1,\ldots,M$, the reliability condition for this code is given by

$$\lim_{n\to\infty}\Pr\Big[(\hat{W}_1,\ldots,\hat{W}_M)\neq(W_1,\ldots,W_M)\Big|\,Y_k^n\Big]=0, \quad (4)$$

for $k=1,\ldots,K$; and the *strong* secrecy condition by

$$\lim_{n\to\infty} I(W_m,\ldots,W_M;Z_m^n)=0 \quad \text{for } m=1,\ldots,M. \quad (5)$$

Proposition 2 (Adapted from [3] and [6])**.** *The secrecy-capacity region of the DBC-NLD-LS contains all M-tuples of rates $(R_1,\ldots,R_M)\in\mathbb{R}_+^M$ satisfying*

$$\sum_{i=m}^{M}R_i\le I(X;Y_1)-I(X;Z_m), \qquad m=1,\ldots,M,$$

for some distribution p_X.

Corollary 2. *The sub-region of the secrecy-capacity given in Prop. 2 without considering rate-sharing is the closure of all K-tuples of rates $(R_1,\ldots,R_M)\in\mathbb{R}_+^M$ satisfying*

$$R_m\le I(X;Z_{m+1})-I(X;Z_m), \qquad m=1,\ldots,M-1,$$
$$R_M\le I(X;Y_1)-I(X;Z_M),$$

for some distribution p_X.

III. Polar Codes for DBCs

For compactness of the notation, let L denote the number of *input* random variables, i.e., the channel input X and the auxiliary random variables involved in the characterization of the secrecy-capacity for the two models: $L\triangleq K$ for the DBC-LD-NLS, and $L\triangleq 1$ for the DBC-NLD-LS. Thus, consider the Discrete Memoryless Source (DMS) that represents the input and output random variables of the DBC of Sec. II,

$$(\mathcal{V}_1\times\cdots\times\mathcal{V}_L\times\mathcal{Y}_K\times\cdots\times\mathcal{Y}_1 \times\mathcal{Z}_M\times\cdots\times\mathcal{Z}_1,p_{V_1\ldots V_LY_K\ldots Y_1Z_M\ldots Z_1}), \quad (6)$$

such that $V_1-\cdots-V_L-Y_K-\cdots-Y_1-Z_M-\cdots-Z_1$ forms a Markov chain and where $V_L\triangleq X$. Without loss of generality, $\{V_\ell\}_{\ell=1}^L$ are assumed to have binary alphabet and an extension to q-ary alphabets is entirely possible [16].

Consider an i.i.d. n-sequence of the DMS, being n any power of 2. The following polar transforms are defined for the n-sequence of input random variables $(V_1^n,\ldots,V_L^n)$:

$$U_\ell^n\triangleq V_\ell^nG_n, \quad \text{for } \ell=1,\ldots,L, \quad (7)$$

being G_n the polar generation matrix defined in [7]. Since $G_n=G_n^{-1}$ then $U_1^n-U_2^n-\cdots-U_L^n$ also forms a Markov chain and, for polar coding purposes, the joint distribution of $(U_1^n,\ldots,U_L^n)$ can be expressed as

$$p_{U_1^n\ldots U_L^n}(u_1^n,\ldots,u_L^n) \triangleq\prod_{\ell=1}^{L}\prod_{j=1}^{n}p_{U_\ell(j)|U_\ell^{1:j-1}V_{\ell-1}^n}\big(u_\ell(j)\big|u_\ell^{1:j-1},u_{\ell-1}^nG_n\big). \quad (8)$$

Consider the polar transform $U_\ell^n=V_\ell^nG_n$, reference [17] shows that this polarization transform extracts the randomness of V_ℓ^n in the sense that, as $n\to\infty$, the set of indices $j\in[n]$ can be divided practically into two disjoint sets (*polarized sets*), namely $\mathcal{H}_{V_\ell}^{(n)}$ and $\mathcal{L}_{V_\ell}^{(n)}$, such that $U_\ell(j)$ for $j\in\mathcal{H}_{V_\ell}^{(n)}$ is practically independent of $U_\ell^{1:j-1}$ and uniformly distributed, i.e., $H\big(U_\ell(j)|U_\ell^{1:j-1}\big)\to 1$, and $U_\ell(j)$ for $j\in\mathcal{L}_{V_\ell}^{(n)}$ is almost determined by $U_\ell^{1:j-1}$, i.e., $H\big(U_\ell(j)|U_\ell^{1:j-1}\big)\to 0$.

Different polarized sets can be defined for the input random sequence V_ℓ^n by considering $V_{\ell-1}^n$, and Y_k^n (for some $k=1,\ldots,K$) or Z_m^n (for some $m=1,\ldots,M$) as side information [17]. Typically, these sets are specified based on the Bhattacharyya parameter, defined as

$$Z(U_\ell|W)\triangleq 2\sum_{w\in\mathcal{W}}p_W(w)\sqrt{p_{U_\ell|W}(0|w)p_{U_\ell|W}(1|w)},$$

for some $U_\ell\in\{0,1\}$ and $W\in\mathcal{W}$. Although the polarized sets are defined based on the Bhattacharyya parameter, [15,

Lemma 16] proves that $Z(U_\ell|W) \to 1$ implies $H(U_\ell|W) \to 1$, and $Z(U_\ell|W) \to 0$ implies $H(U_\ell|W) \to 0$.

Definition 1 (Polarized sets)**.** *For compactness of the notation, let $\{O_{k'}\}_{k'=1}^{K'}$ denote all output variables, where $K' = K+M$, and define $O_0 \triangleq \phi$. Let $\delta_n = 2^{-n^\beta}$ for some $\beta \in \left(0, \frac{1}{2}\right)$. The following $K'+1$ partitions of the universal set $[n]$ are defined for the polar transform $U_\ell^n = V_\ell^n G_n$ by considering $V_{\ell-1}^n$, and a given $O_{k'}^n$ as side information:*

$$\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}O_{k'}} \triangleq \left\{j\in[n]: Z\left(U_\ell(j)\middle|U_\ell^{1:j-1}, V_{\ell-1}^n, O_{k'}^n\right) \geq 1-\delta_n\right\},$$

$$\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}O_{k'}} \triangleq \left\{j\in[n]: Z\left(U_\ell(j)\middle|U_\ell^{1:j-1}, V_{\ell-1}^n, O_{k'}^n\right) \leq \delta_n\right\},$$

$$\mathcal{B}^{(n)}_{V_\ell|V_{\ell-1}O_{k'}} \triangleq \left(\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}O_{k'}}\right)^{\mathrm{C}} \cap \left(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}O_{k'}}\right)^{\mathrm{C}},$$

for $k' = 0, \ldots, K'$.

Notice that, in fact, the sets $\mathcal{B}^{(n)}_{V_\ell|V_{\ell-1}O_{k'}}$ contain those indices that have not been polarized.

The following lemma provides a useful property of the polarized sets under the assumption of channels being degraded.

Lemma 1 (Adapted from [15, Lemma 4])**.** *Consider the polar transform $U_\ell^n = V_\ell^n G_n$. If $V_{\ell-1} - V_\ell - O_{K'} - \cdots - O_1$ forms a Markov chain, then*

$$\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}} \subseteq \mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}O_1} \subseteq \cdots \subseteq \mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}O_{K'}}, \quad \textit{and,}$$
$$\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}O_{K'}} \subseteq \cdots \subseteq \mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}O_1} \subseteq \mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}}.$$

Remark 1. *Although we have considered physically degradedness, Lemma 1 is also valid for stochastically degraded channels and, therefore, the following polar coding schemes and their performance analysis are suitable for both cases.*

IV. Polar Coding Scheme for the DBC-LD-NLS

The polar coding scheme provided in this section is designed to achieve the corner point of the secrecy-capacity subregion given in Cor. 1. Consider an i.i.d. n-sequence of the DMS, $(V_1^n, \ldots, V_K^n, Y_K^n, \ldots, Y_1^n, Z_M^n, \ldots, Z_1^n)$, and define the K polar transforms $(U_1^n, \ldots, U_K^n)$ for the input random variables $(V_1^n, \ldots, V_K^n)$.

A. Polar Encoding

The polarization-based encoder consist of K encoding blocks operating sequentially at each superposition layer.

Polar code construction at layer k. Based on the polarized sets given in Def. 1, the following partition of the universal set $[n]$ is defined for each polar transform $U_k^n = V_k^n G_n$:

$$\mathcal{I}_k^{(n)} \triangleq \mathcal{H}^{(n)}_{V_k|V_{k-1}} \cap \mathcal{L}^{(n)}_{V_k|V_{k-1}Y_k} \cap \mathcal{H}^{(n)}_{V_k|V_{k-1}Z_M}, \tag{9}$$

$$\mathcal{C}_k^{(n)} \triangleq \mathcal{H}^{(n)}_{V_k|V_{k-1}} \cap \mathcal{L}^{(n)}_{V_k|V_{k-1}Y_k} \cap \left(\mathcal{H}^{(n)}_{V_k|V_{k-1}Z_M}\right)^{\mathrm{C}}, \tag{10}$$

$$\mathcal{F}_k^{(n)} \triangleq \mathcal{H}^{(n)}_{V_k|V_{k-1}} \cap \mathcal{H}^{(n)}_{V_k|V_{k-1}Y_k}, \tag{11}$$

$$\mathcal{D}_k^{(n)} \triangleq \mathcal{H}^{(n)}_{V_k|V_{k-1}} \cap \mathcal{B}^{(n)}_{V_k|V_{k-1}Y_k}, \tag{12}$$

$$\mathcal{J}_k^{(n)} \triangleq \left(\mathcal{H}^{(n)}_{V_k|V_{k-1}}\right)^{\mathrm{C}} \cap \mathcal{B}^{(n)}_{V_k|V_{k-1}Y_k}, \tag{13}$$

$$\mathcal{T}_k^{(n)} \triangleq \left(\mathcal{H}^{(n)}_{V_k|V_{k-1}}\right)^{\mathrm{C}} \cap \left(\mathcal{B}^{(n)}_{V_k|V_{k-1}Y_k}\right)^{\mathrm{C}}. \tag{14}$$

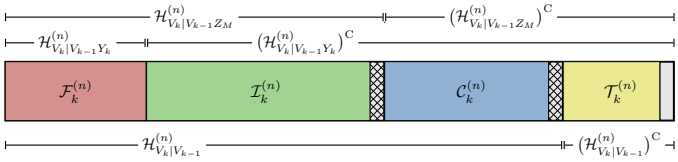

Fig. 1: Polar code construction for the DBC-LD-NLS at layer k. The cross-hatched gray area represents those indices $j \in \mathcal{D}_k^{(n)}$ and the solid gray area represents those indices $j \in \mathcal{J}_k^{(n)}$.

Fig. 1 depicts the polar code construction at the k-th layer. Note that, in general, if $j \in \mathcal{D}_k^{(n)} \subseteq \mathcal{B}^{(n)}_{V_k|V_{k-1}Y_k}$ then this index can belong to $\mathcal{B}^{(n)}_{V_k|V_{k-1}Z_M} \subseteq (\mathcal{H}^{(n)}_{V_k|V_{k-1}Z_M})^{\mathrm{C}}$ or $\mathcal{H}^{(n)}_{V_k|V_{k-1}Z_M}$. Furthermore, notice that only the eavesdropper's channel corresponding to the channel output random variable Z_M is involved in the polar code construction at each layer. The polar encoding process modifies the joint distribution of the original DMS. In this sense, we introduce $(\tilde{V}_1, \ldots, \tilde{V}_K, \tilde{Y}_K, \ldots, \tilde{Y}_1, \tilde{Z}_M, \ldots, \tilde{Z}_1)$ and define $\tilde{U}_k^n = \tilde{V}_k^n G_n$, for $k = 1, \ldots, K$, to distinguish the random variables of the original DMS and the ones after the encoding procedure.

Encoding at layer k. Let W_k and C_k be uniformly distributed random vectors of size $\left|\mathcal{I}_k^{(n)}\right|$ and $\left|\mathcal{C}_k^{(n)}\right|$ respectively, where W_k represents the message intended to receivers k to K, and C_k the local randomness required at the k-th layer to confuse the eavesdroppers about this message. In addition, let F_k be a given uniformly distributed binary random $\left|\mathcal{F}_k^{(n)}\right|$-sequence, which represents a source of common randomness that is available to all parties. The encoder constructs the sequence $\tilde{U}_k^n$ as follows. First, the encoder stores W_k, C_k and F_k into $\tilde{U}_k\left[\mathcal{I}_k^{(n)}\right]$, $\tilde{U}_k\left[\mathcal{C}_k^{(n)}\right]$ and $\tilde{U}_k\left[\mathcal{F}_k^{(n)}\right]$, respectively. Then, given $\tilde{U}_k\left[\mathcal{I}_k^{(n)} \cup \mathcal{C}_k^{(n)} \cup \mathcal{F}_k^{(n)}\right]$ and the sequence $\tilde{V}_{k-1}^n = \tilde{U}_{k-1}^n G_n$ provided by the previous encoding block that operates at the $(k-1)$-th layer (recall that $\tilde{U}_0^n = \tilde{V}_0^n = \phi$), the encoder samples the remaining entries $\tilde{U}_k(j)$ from the distribution

$$q_{U_k(j)|U_k^{1:j-1}V_{k-1}^n}\left(\tilde{u}_k(j)|\tilde{u}_k^{1:j-1}, \tilde{v}_{k-1}^n\right)$$
$$\triangleq \begin{cases} \frac{1}{2} & \text{if } j \in \mathcal{D}_k^{(n)}, \\ p_{U_k(j)|U_k^{1:j-1}V_{k-1}^n}\left(\tilde{u}_k(j)|\tilde{u}_k^{1:j-1}, \tilde{v}_{k-1}^n\right) & \text{if } j \in \mathcal{J}_k^{(n)} \cup \mathcal{T}_k^{(n)}, \end{cases}$$

where $p_{U_k(j)|U_k^{1:j-1}V_{k-1}^n}$ is the distribution induced by the original DMS (see Eq. (8)). Finally, the k-th encoder block computes $\tilde{V}_k^n = \tilde{U}_k^n G_n$ and delivers it to the next encoding block, which is responsible of the encoding at the $(k+1)$-th superposition layer. If $k = K$, then $\tilde{V}_K^n \triangleq \tilde{X}^n$ and the K-th encoding block transmits $\tilde{X}^n$ over the broadcast channel.

Secret messages. In addition of the sequence $\tilde{X}^n$, the encoder outputs the following messages from each layer

$$S_k \triangleq \tilde{U}_k\left[\mathcal{D}_k^{(n)} \cup \mathcal{J}_k^{(n)}\right], \quad k = 1, \ldots, K, \tag{15}$$

which must be transmitted secretly to the legitimate receivers k to K to help them reconstruct the message W_k. Nevertheless, transmitting these messages can be accomplished with negligible rate penalty.

B. Polar Decoding

The random sequences $\{F_k\}_{k=1}^K$ are assumed to be known by all parties. Moreover, each secret message S_k, for $k = 1,\dots,K$, is assumed to be received by the corresponding legitimate receivers previously to the decoding procedure.

Decoding at the k-th legitimate receiver. The k-th receiver must form an estimate of the sequences $\{\tilde{U}_i^n\}_{i=1}^k$ in a successive manner from $\tilde{U}_1^n$ to $\tilde{U}_k^n$, and the procedure to estimate $\tilde{U}_i^n$, for some $i \leq k$, is as follows. First, given that S_i and F_i are available to the k-th receiver, notice that the receiver knows $\tilde{U}_i\big[\big(\mathcal{L}^{(n)}_{V_i|V_{i-1}Y_i}\big)^{\mathrm{C}}\big]$. By Lemma 1, we have $\big(\mathcal{L}^{(n)}_{V_i|V_{i-1}Y_k}\big)^{\mathrm{C}} \subseteq \big(\mathcal{L}^{(n)}_{V_k|V_{k-1}Y_i}\big)^{\mathrm{C}}$ for any $i \leq k$. Thus, the k-th legitimate receiver uses SC decoding for source coding with side information [17] to estimate $\tilde{U}_i\big[\mathcal{L}^{(n)}_{V_i|V_{i-1}Y_k}\big]$ from $\tilde{U}_i\big[\big(\mathcal{L}^{(n)}_{V_i|V_{i-1}Y_k}\big)^{\mathrm{C}}\big]$, its observations $\tilde{Y}_k$ and the sequence $\hat{V}_{i-1}^n = \hat{U}_{i-1}^n G_n$ estimated previously. Finally, the decoder outputs $\hat{W}_i = \hat{U}_i\big[\mathcal{I}_i^{(n)}\big]$ for $i = 1,\dots,k$.

C. Performance of the polar coding scheme

Theorem 1. *Consider the DBC-LD-NLS defined in Sec. II-A. The coding scheme defined in Secs. IV-A and IV-B achieves any rate tuple of the secrecy-capacity subregion defined in Cor. 1 satisfying the reliability and the strong secrecy conditions.*

Sketch of the proof[2]. The proof follows in four steps,

1) By applying the polarization theorem [17] and by the definition of the sets $\mathcal{I}_k^{(n)}$ for $k = 1,\dots,K$, we prove that the corner point of the secrecy-capacity subregion given in Cor. 1 is achieved and, moreover, the overall additional rate required to transmit the secret messages defined in Eq. (15) is negligible in terms of rate penalty.
2) We show that the total variation distance between the joint distribution of the original DMS and the one after the encoding is bounded to some $\delta^{(n)}_{\text{ld-nls}}$ such that $\delta^{(n)}_{\text{ld-nls}} \xrightarrow{n\to\infty} 0$, which is crucial for the reliability and secrecy analysis.
3) We show that the reliability condition of Eq. (2) is satisfied by upperbounding the average probability of error at the k-th receiver as the sum of to terms: one which depends on the total variation distance mentioned above, and another which is the average probability of error of SC decoding for source coding with side information [17]. Since the k-th receiver knows $\big(\mathcal{L}^{(n)}_{V_i|V_{i-1}Y_k}\big)^{\mathrm{C}}$ for any $i \leq k$, the second probability term also tends to zero as n grows to infinity.
4) Besides the channel output observations $\tilde{Z}_m^n$, the m-th eavesdropper has access to the common randomness $\{F_k\}_{k=1}^K$. Thus, we provide the following upperbound,

$$H\big(W_1,\dots,W_K,F_1,\dots,F_K\big|\tilde{Z}_m^n\big) \geq H\big(U_1\big[\mathcal{I}_1^{(n)}\cup\mathcal{F}_1^{(n)}\big],\dots,U_K\big[\mathcal{I}_K^{(n)}\cup\mathcal{F}_K^{(n)}\big]\big|Z_m^n\big)-\epsilon_n,$$

where $\epsilon_n \triangleq f(\delta^{(n)}_{\text{ld-nls}}) \xrightarrow{n\to\infty} 0$ because $f(\cdot)$ is a monotonically decreasing function of the total variation distance mentioned previously when n grows to infinity. Finally, we show that the secrecy condition of Eq. (3) is satisfied by proving that the first term of the previous bound tends to $\sum_{k=1}^K \big|\mathcal{I}_k^{(n)}\cup\mathcal{F}_k^{(n)}\big|$ for n sufficiently large, and therefore, $I(W_1,\dots,W_K;F_1,\dots,F_K,\tilde{Z}_m^n) \xrightarrow{n\to\infty} 0$, which follows from the chain rule for entropy, the definition of the sets given in Eqs. (9)-(14) and, therefore, on the properties of the polarized sets given in Def. 1. Intuitively, eavesdroppers cannot leak enough information about messages because $\mathcal{I}_k^{(n)} \subseteq \mathcal{H}^{(n)}_{V_k|V_kZ_m}$ for any $k = 1,\dots,K$ and $m = 1,\dots,M$. Moreover, since $\mathcal{F}_k^{(n)} \subseteq \mathcal{H}^{(n)}_{V_k|V_kZ_m}$, the source of common randomness do not compromise the secrecy.

Indeed, by a slight modification of the polar coding scheme, any border point of the secrecy-capacity region of Def. 1 can be achieved (see [4] for details).

[2]The full proof is omitted for lack of space and is given in [4].

V. Polar Coding Scheme For the DBC-NLD-LS

The polar coding scheme for the DBC-NLD-LS provided in this section is designed to achieve the corner point of the secrecy-capacity subregion given in Cor. 2. Consider an i.i.d. n-sequence of the DMS, $(X^n, Y_K^n,\dots,Y_1^n,Z_M^n,\dots,Z_1^n)$, and define the polar transform $U^n \triangleq X^nG_n$.

A. Polar Encoding

Polar code construction. Based on the polarized sets given in Def. 1, the following partition of the universal set $[n]$ is defined for the polar transform $U^n = X^nG_n$:

$$\mathcal{I}_m^{(n)} \triangleq \mathcal{H}_X^{(n)} \cap \mathcal{L}^{(n)}_{X|Z_{m+1}} \cap \mathcal{H}^{(n)}_{X|Z_m} \ (m=1,\dots,M-1), \quad (16)$$

$$\mathcal{I}_M^{(n)} \triangleq \mathcal{H}_X^{(n)} \cap \mathcal{L}^{(n)}_{X|Y_1} \cap \mathcal{H}^{(n)}_{X|Z_M}, \quad (17)$$

$$\mathcal{C}^{(n)} \triangleq \mathcal{H}_X^{(n)} \cap \mathcal{L}^{(n)}_{X|Y_1} \cap \Big(\mathcal{H}^{(n)}_{X|Z_1}\Big)^{\mathrm{C}}, \quad (18)$$

$$\mathcal{F}^{(n)} \triangleq \mathcal{H}_X^{(n)} \cap \mathcal{H}^{(n)}_{X|Y_1}, \quad (19)$$

$$\mathcal{D}^{(n)} \triangleq \mathcal{H}_X^{(n)} \cap \mathcal{B}^{(n)}_{X|Y_1}, \quad (20)$$

$$\mathcal{J}^{(n)} \triangleq \Big(\mathcal{H}_X^{(n)}\Big)^{\mathrm{C}} \cap \mathcal{B}^{(n)}_{X|Y_1}, \quad (21)$$

$$\mathcal{T}^{(n)} \triangleq \Big(\mathcal{H}_X^{(n)}\Big)^{\mathrm{C}} \cap \Big(\mathcal{B}^{(n)}_{X|Y_1}\Big)^{\mathrm{C}}. \quad (22)$$

Fig. 2 shows graphically this partition of the universal set $[n]$. Notice that, in general, if $j \in \mathcal{D}^{(n)} \subseteq \mathcal{B}^{(n)}_{X|Y_1}$ then this index can belong to the set $\mathcal{B}^{(n)}_{X|Z_m} \subseteq (\mathcal{H}^{(n)}_{X|Z_m})^{\mathrm{C}}$ or to the set $\mathcal{H}^{(n)}_{X|Z_m}$ (for any $m = 1,\dots,M$). Also, note that only the legitimate receiver's channel corresponding to the channel output random variable Y_1 is involved in the polar code construction.

Again, since the polar encoding process modifies the joint distribution of the original DMS, we introduce $(\tilde{X},\tilde{Y}_K,\dots,\tilde{Y}_1,\tilde{Z}_M,\dots,\tilde{Z}_1)$ and define $\tilde{U}^n = \tilde{X}^nG_n$ to distinguish the random variables of the original DMS and the ones after the encoding procedure.

Encoding. Let $\{W_m\}_{m=1}^M$ and C be uniformly distributed random vectors of size $\{\big|\mathcal{I}_m^{(n)}\big|\}_{m=1}^M$ and $\big|\mathcal{C}^{(n)}\big|$ respectively, where $\{W_m\}_{m=1}^M$ represent the messages intended to all legitimate receivers, and C the additional local randomness

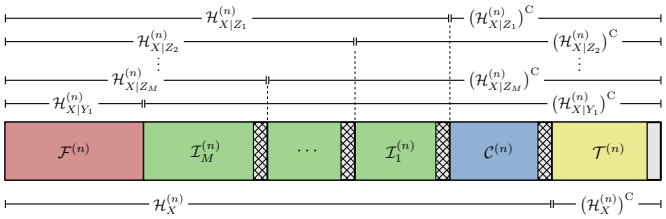

Fig. 2: Polar code construction for the DBC-NLD-LS. The cross-hatched gray area represents those indices $j \in \mathcal{D}^{(n)}$ and the solid gray area represents those indices $j \in \mathcal{J}^{(n)}$.

required to confuse the eavesdroppers. In addition, let F be a given uniformly distributed binary random $\left|\mathcal{F}^{(n)}\right|$-sequence, which represents a source of common randomness that is available to all parties. The encoder constructs the sequence $\tilde{U}^n$ as follows. First, the encoder stores the messages W_m into $\tilde{U}\left[\mathcal{I}^{(n)}_m\right]$, for $m = 1, \ldots, M$, and stores C and F into $\tilde{U}\left[\mathcal{C}^{(n)}\right]$ and $\tilde{U}\left[\mathcal{F}^{(n)}\right]$, respectively. Then, given $\tilde{U}\left[\left(\cup_{m=1}^{M} \mathcal{I}^{(n)}_m\right) \cup \mathcal{C}^{(n)} \cup \mathcal{F}^{(n)}\right]$, the encoder samples the remaining entries $\tilde{U}(j)$ from the distribution

$$q_{U(j)|U^{1:j-1}}\left(\tilde{u}(j)|\tilde{u}^{1:j-1}\right) \triangleq \begin{cases} \frac{1}{2} & \text{if } j \in \mathcal{D}^{(n)}, \\ p_{U(j)|U^{1:j-1}}\left(\tilde{u}(j)|\tilde{u}^{1:j-1}\right) & \text{if } j \in \mathcal{J}^{(n)} \cup \mathcal{T}^{(n)}, \end{cases}$$

where $p_{U(j)|U^{1:j-1}}$ is the distribution induced by the original DMS (see Eq. (8)). Finally, the encoder computes the sequence $\tilde{X}^n = \tilde{U}^n G_n$ and transmits it over the DBC.

Secret message. In addition of the sequence $\tilde{X}^n$, the encoder outputs the following message

$$S \triangleq \tilde{U}\left[\mathcal{D}^{(n)} \cup \mathcal{J}^{(n)}\right], \tag{23}$$

which must be transmitted secretly to all legitimate receivers. Nevertheless, transmitting these messages can be accomplished with negligible rate penalty.

B. Polar Decoding

The sequence F is assumed to be known by all parties. Moreover, the secret message S is assumed to be received by all legitimate receivers previously to the decoding procedure.

Decoding at the k-th receiver. The k-th legitimate forms an estimate of the sequence $\tilde{U}^n$ as follows. First, given that S and F are available to the receiver k, notice that the receiver knows $\tilde{U}\left[\left(\mathcal{L}^{(n)}_{X|Y_1}\right)^{\mathrm{C}}\right]$. Since, by Lemma 1, $\left(\mathcal{L}^{(n)}_{X|Y_k}\right)^{\mathrm{C}} \subseteq \left(\mathcal{L}^{(n)}_{X|Y_1}\right)^{\mathrm{C}}$ for any $k > 1$, the k-th legitimate receiver uses SC decoding for source coding with side information to estimate $\tilde{U}\left[\mathcal{L}^{(n)}_{X|Y_k}\right]$ from $\tilde{U}\left[\left(\mathcal{L}^{(n)}_{X|Y_k}\right)^{\mathrm{C}}\right]$ and its channel output observations $\tilde{Y}_k$. Finally, the decoder of the k-th receiver outputs $\hat{W}_m = \hat{U}\left[\mathcal{I}^{(n)}_m\right]$ for $m = 1, \ldots, M$.

C. Performance of the polar coding scheme

Theorem 2. *Consider the DBC-NLD-LS defined in Sec. II-B. The coding scheme described in Secs. V-A and V-B achieves any rate tuple of the secrecy-capacity subregion given in Cor. 2 satisfying the reliability and the strong secrecy conditions.*

Proof. The proof follows similar reasoning to that of Th. 1 and is omitted due to lack of space. See [4].

VI. Conclusions

We have proposed two strongly secure polar coding schemes for the DBC with an arbitrary number of legitimate receivers and eavesdroppers. Each polar coding scheme achieves any rate tuple inside the secrecy-capacity region of the two models for the DBC introduced in Sec. II, which are given by different reliability and secrecy constraints, and which capture practical scenarios in wireless systems. The polar coding schemes do not require any chaining construction because of the degradedness condition of the channels and the assumption of a given source of common randomness available to all parties. However, the transmitter and legitimate receivers must share a secret seed of negligible size (in terms of rate penalty).

References

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

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

[3] S. Zou, Y. Liang, L. Lai, H. Poor, and S. Shamai, "Broadcast networks with layered decoding and layered secrecy: Theory and applications," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1841–1856, Oct 2015.

[4] J. del Olmo and J. R. Fonollosa, "Strong secrecy on a class of degraded broadcast channels using polar codes," *arXiv preprint arXiv:1607.07815*, 2016.

[5] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wirel. Commun. Netw.*, pp. 1:1–1:29, Mar. 2009.

[6] Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "A broadcast approach for fading wiretap channels," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 842–858, Feb 2014.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] T. Cihad Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," *arXiv preprint arXiv:1410.3422*, 2014.

[13] 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.

[14] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6213–6237, Nov 2015.

[15] N. Goela, E. Abbe, and M. Gastpar, "Polar codes for broadcast channels," *IEEE Transactions on Information Theory*, vol. 61, no. 2, pp. 758–782, Feb 2015.

[16] E. Şasoğlu, E. Telatar, and E. Arikan, "Polarization for arbitrary discrete memoryless channels," in *IEEE Information Theory Workshop.*, 2009, pp. 144–148.

[17] E. Arıkan, "Source polarization," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2010, pp. 899–903.