Strong Secrecy for Relay Wiretap Channels with Polar Codes and Double-Chaining

Manos Athanasakos, *Student, IEEE*
Department of Informatics and Telecommunications
National University of Athens
Athens, Greece
emathan@di.uoa.gr

George Karagiannidis, *Fellow, IEEE*
Department of Electrical and Computer Engineering
Aristotle University of Thessaloniki
Thessaloniki, Greece
geokarag@auth.gr

GLOBECOM 2020 - 2020 IEEE Global Communications Conference | 978-1-7281-8298-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/GLOBECOM42002.2020.9347956

***Abstract*—Secure communication for the primitive relay wiretap channel under the decode-and-forward protocol, is considered. A polar coding-based technique is proposed and we show that is suitable to provide reliability and a level of information-theoretic security. We focus on the strong secrecy criterion where in order to satisfy it we implement a double-chaining construction to overcome the obstacle of misaligned bits.**

I. Introduction

The wiretap channel, introduced by A. Wyner in his seminal work [1], paved the way for the exploitation of the channel medium characteristics in terms of information-theoretic security. This approach has as a major advantage that security does not rely on any shared secret key, i.e. keyless security. In view of the emergence of wireless communication and massive connectivity, this benefit has led to a rich literature, which investigates several channel models towards the design of low-complexity coding schemes for both reliability and secrecy.

After van der Meulen's introduction of the relay channel in [2] and the extension of the work of Cover and El Gamal in [3], cooperative diversity is considered as an important advancement in wireless networks, since it can achieve higher rates in comparison to direct transmission. In practice, a network may be comprised with illegitimate users; cooperation between trusted users have been exploited as a way to establish secure communication. The rate-equivocation region was characterized in [4] and [5] for a four-terminal relay channel and an eavesdropper, under several cooperation protocols. Half-duplex relay channel models considered in [6], where the authors studied coding techniques for the relay channel with orthogonal components (primitive relay channel). The secrecy capacity for this class of channels investigated in [7] for the binary-input discrete memoryless channel (B-DMC) and the Gaussian case. Although the importance of cooperation for reliability and security in large networks is well established, the aforementioned works presented bounds on the secrecy capacity, while relying on random coding arguments. Undoubtedly, designing codes for these type of channels is of great importance as the evolution of networks require security solutions with low consumption and complexity.

Since the pioneering work of Arikan on the polar codes [8], which are capacity-achieving for the symmetric B-DMC, several polar coding schemes have been proposed to fulfill the secrecy requirement. These codes are constructed based on the phenomenon of channel polarization, that is the channel is splitted into N "bit-channels" and tend to be either error-free or fully noisy channels, as N grows. This result is the basic tool in designing a polar coding scheme, which satisfies both reliability and secrecy conditions. In [9], a scheme for the degraded wiretap channel, which meets the requirement for weak secrecy was proposed, while in [10] the authors using a different partition of the index set developed a scheme for strong secrecy. Under this framework, several coding schemes for multi-user channels have been investigated in [11], [12] and [13]. However, although in the open literature there are some applications of polar codes without security constraints for the relay channel [14], [15], [16], [17] and [18], the investigation whether polar codes are suitable for the relay wiretap scenario has drawn little attention. Finally, the authors in [19] proposed a coding scheme capable to achieve weak secrecy for the relay-eavesdropper channel. Note that, the natural nested structure of polar codes and their low encoding/decoding complexity identifies them as a promising choice for practical implementation of merging coding and security in one scheme.

Motivated by the above, in this paper, we consider a primitive relay wiretap channel when decode-and-forward (DF) protocol is used and propose a polar coding scheme, which satisfies the strong secrecy condition along with the reliability constraint. In particular, the proposed scheme exploits the nested structure of polar codes for the stochastically degraded relay wiretap channel and the new encoding algorithm achieves strong secrecy through a double-chaining construction.

The rest of the paper is organized as follows. In Section II, we introduce the system model and the constraints in designing the coding scheme. In Section III, we briefly describe the weak secrecy scheme, followed by the main results of this paper; the encoding scheme for strong secrecy and the analysis on reliability and security. Finally, Section IV concludes the paper.

II. System model and requirements

The relay wiretap channel models a multi-hop transmission scheme where a relay cooperates with the source to communicate with the destination in the presence of an eavesdropper.

We consider a four-terminal B-DMC with orthogonal receiver components, with transition probability mass function

$$p(y, y_{sr}, z|x_s, x_r) = p(y_{sd}, y_{sr}, z_{se}|x_s)p(y_{rd}, z_{re}|x_r). \quad (1)$$

In this model, $\mathcal{X}_S$ and $\mathcal{X}_R$ are the the channel inputs from

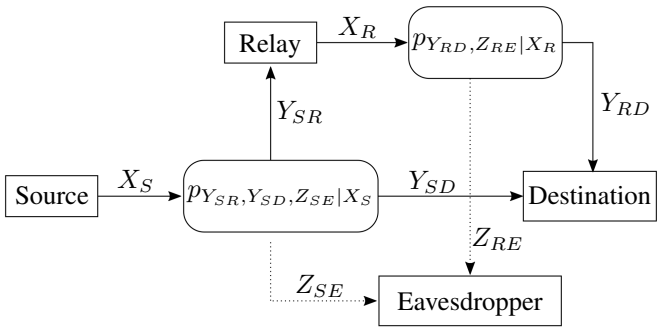

Fig. 1. The relay wiretap channel model with orthogonal components.

source and relay respectively, while $\mathcal{Y}$, $\mathcal{Y}_{SR}$ and $\mathcal{Z}$ are the channel outputs at the destination, relay and eavesdropper respectively. The observation vectors at the destination's and eavesdropper's output are $\mathbf{Y} = (Y_{SD}, Y_{RD})$ and $\mathbf{Z} = (Z_{SE}, Z_{RE})$ respectively. Fig. 1 illustrates the channel, which consists of a source, a relay, the legitimate receiver and the eavesdropper. The source wishes to communicate reliably a message $\mathbf{M}$ with the legitimate receiver under the assistance of a trusted relay while keeping it safe from the eavesdropper.

We aim to design a coding scheme which satisfies both reliability and secrecy requirements. Probability of error is used to quantify the *reliability* of the scheme, where the goal is to satisfy

$$\lim_{N\to\infty} Pr\{\mathbf{M} \neq \hat{\mathbf{M}}\} = 0. \quad (2)$$

To measure the statistical independence between the message transmitted and eavesdropper observation we use the following metrics:

$$\lim_{N\to\infty} \frac{I(\mathbf{M};\mathbf{Z})}{N} = 0, \quad (3)$$

$$\lim_{N\to\infty} I(\mathbf{M};\mathbf{Z}) = 0. \quad (4)$$

In (3) *security* is measured in terms of the normalized mutual information between transmitted message $\mathbf{M}$ and received vector by the eavesdropper $\mathbf{Z}$. The encoding scheme designed to satisfy this requirement in order to operate with *weak secrecy*. However, as shown by Maurer in [20], is too weak for cryptographic applications as it is possible for the eavesdropper to retrieve a considerable amount of information even if (3) is satisfied. Consequently, our focus here is to design a coding scheme which satisfies a stronger secrecy criterion, as in (4).

III. Polar Coding for strong secrecy

A. Weak Secrecy Scheme

Before presenting the main result of this paper, we briefly explain the difficulty on designing a polar coding scheme which satisfies strong secrecy and simultaneously guarantees low probability of error at the legitimate receiver. We first consider a coordinate partition similar to the one proposed in [9] which help us identify the main obstacle in achieving strong secrecy.

Let us first define the following "good" and "bad" subset of indices:

$$\begin{aligned} \mathcal{G}_N(W_{kl}) &= \{i \in [N] : Z(W_N^{(i)}) < \delta_N\} \\ \mathcal{B}_N(W_{kl}) &= \{i \in [N] : Z(W_N^{(i)}) \geq \delta_N\}, \end{aligned} \quad (5)$$

where W_{kl} is the channel from $k \in \{S, R\}$ to $l \in \{R, D, E\}$, for $k \neq l$ and $[N] = \{1, 2, \ldots, N\}$. $Z(W_N^{(i)})$ is the Bhattacharyya parameter of bit-channel $W_N^{(i)}$ and $\delta_N = 2^{-N^\beta}$ with $0 < \beta < 1/2$. Next we partition the set $[N]$ based on [9] for the source's transmission, as follows:

$$\begin{aligned} \mathcal{I}_1 &= \mathcal{G}_N(W_{SR}) \cap \mathcal{B}_N(W_{SE}) \\ \mathcal{F}_1 &= \mathcal{B}_N(W_{SR}) \\ \mathcal{R}_1 &= \mathcal{G}_N(W_{SE}) \end{aligned} \quad (6)$$

and similarly for the relay's transmission:

$$\begin{aligned} \mathcal{I}_2 &= \mathcal{G}_N(W_{RD}) \cap \mathcal{B}_N(W_{RE}) \\ \mathcal{F}_2 &= \mathcal{B}_N(W_{RD}) \\ \mathcal{R}_2 &= \mathcal{G}_N(W_{RE}), \end{aligned} \quad (7)$$

where $\mathcal{I}_i, \mathcal{F}_i, \mathcal{R}_i$ are the subsets containing the information bits, the frozen bits and the random bits, respectively, for source's ($i = 1$) and relay's ($i = 2$) transmission. However, the above scheme can only achieve weak secrecy, measured as in (3), due to the assumptions that $\mathcal{B}_N^c(W_{SE}) \subset \mathcal{G}_N(W_{SR})$ and $\mathcal{B}_N^c(W_{RE}) \subset \mathcal{G}_N(W_{RD})$, while in general this is not true. Although the number of coordinates in $\mathcal{G}_N^c(W_{SR}) \cap \mathcal{B}_N^c(W_{SE})$ and $\mathcal{G}_N^c(W_{RD}) \cap \mathcal{B}_N^c(W_{RE})$ is very small, this constitutes the difficulty in obtaining reliability and strong secrecy simultaneously. The authors in [10], proposed a different partition of the coordinates which resolves the above problem.

B. Dealing with the Misaligned bits

The transmission takes place over $k+1$ blocks of N bits. Prior the communication, trusted parties share a secret seed of random bits $\mathcal{D}$ which is used as a "chain" between transmitted blocks. In particular, encoding is performed so the bits of $\mathcal{D}$ passed on the legitimate receiver (relay or destination) using their reliable and secure indices. The chaining is implemented by sending the bits in $\mathcal{D}(j)$ of block j as part of the message block $j-1$ for all $j \in [1, \ldots, k]$. This construction allows the legitimate receiver to employ successive cancellation (SC) for block j and recover these bits reliably, while security is guaranteed.

Let apply the aforementioned construction to the relay wiretap channel under investigation. We consider the following partition of the index set

$$\begin{aligned} \mathcal{I}_1 &= \mathcal{G}_N(W_{SR}) \cap \mathcal{B}_N(W_{SE}) \\ \mathcal{F}_1 &= \mathcal{G}_N^c(W_{SR}) \cap \mathcal{B}_N(W_{SE}) \\ \mathcal{R}_1 &= \mathcal{G}_N(W_{SR}) \cap \mathcal{B}_N^c(W_{SE}) \\ \mathcal{D}_1 &= \mathcal{G}_N^c(W_{SR}) \cap \mathcal{B}_N^c(W_{SE}), \end{aligned} \quad (8)$$

where in the set $\mathcal{I}_1$ information bits are stored, set $\mathcal{F}_1$ is the set of frozen bits, $\mathcal{R}_1$ are the randomly chosen bits and $\mathcal{D}_1$ are the misaligned bits. We note that, as in the weak secrecy case in Section III.A, the information bits in $\mathcal{I}_1$ are distributed in $\mathcal{I}_1^{SD}$ which is decodable by the destination and $\mathcal{I}_1^{RD}$ which is the message that the relay forwards through the W_{RD}. Thus, for this transmission the relay uses the following partition

$$\begin{aligned}\mathcal{I}_2 &= \mathcal{G}_N(W_{RD}) \cap \mathcal{B}_N(W_{RE}) \\ \mathcal{F}_2 &= \mathcal{G}_N^c(W_{RD}) \cap \mathcal{B}_N(W_{RE}) \\ \mathcal{R}_2 &= \mathcal{G}_N(W_{RD}) \cap \mathcal{B}_N^c(W_{RE}) \\ \mathcal{D}_2 &= \mathcal{G}_N^c(W_{RD}) \cap \mathcal{B}_N^c(W_{RE}).\end{aligned} \tag{9}$$

Before describing the encoding procedure, we define the following set $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$ which is used as the secret seed and is shared among the source, relay and destination. Also, fix two arbitrary sets $\mathcal{E}_1 \subset \mathcal{I}_1$ and $\mathcal{E}_2 \subset \mathcal{I}_2$ with $|\mathcal{E}_1| = |\mathcal{D}_1|$ and $|\mathcal{E}_2| = |\mathcal{D}_2|$ and $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2$ with $|\mathcal{E}| = |\mathcal{D}|$. Consequently, the messages of the two-hop transmission are indexed by the bits in $\tilde{\mathcal{I}}_1 = \mathcal{I}_1 \setminus \mathcal{E}$ and $\tilde{\mathcal{I}}_2 = \mathcal{I}_2 \setminus \mathcal{E}$, respectively.

Overall, the transmission is performed in two stages where in order to satisfy the strong secrecy requirement while the probability of error vanishes, we manipulate the misaligned bits in both transmissions by creating a double-chaining structure, i.e. the bits in $\mathcal{D}$ and their links $\mathcal{E}$ of the previous block create a chain for each transmission, as in Fig. 2.

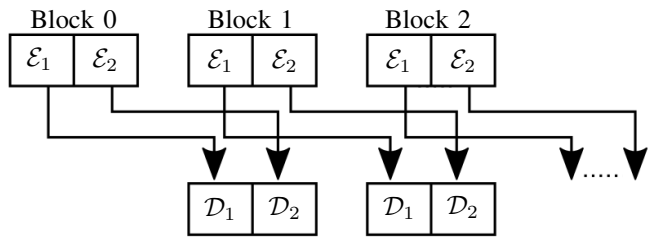

Fig. 2. The double-chaining construction.

Let us describe this double-chaining construction, assuming that the legitimate parties have knowledge of the seed $\mathcal{D}(1)$, by transmitting $\mathcal{E}(0)$ with a separate code, the first chain is formed by $\mathcal{D}_1(j) = \mathcal{E}_1(j-1)$ during the source transmission towards the relay and the destination and the second chain is formed by $\mathcal{D}_2(j) = \mathcal{E}_2(j-1)$ when the relay sends the missing bits to the legitimate receiver. After each source block transmission, the first $|\mathcal{D}_1|$ bits of $\mathcal{D}$ are used to create the chain and are being replaced block by block. Similarly, the second-hop chain is created after each block is transmitted by the relay by using the rest $|\mathcal{D}_2|$ bits of $\mathcal{D}$.

Source encoding: Choose a rate $R < I(W_{SR})$ and use a capacity achieving sequence of polar codes for the channel W_{SR}. For block $j = 1, \ldots, k$, set $\tilde{\mathcal{I}}_1$ carries the message bits, set $\mathcal{R}_1$ is filled up with uniformly distributed random bits, while the first $|\mathcal{D}_1|$ bits of the set $\mathcal{D}$ are chained with the bits of $\mathcal{E}_1$, i.e. $\mathcal{D}_1(j) = \mathcal{E}_1(j-1)$ and the bits in $\mathcal{F}_1$ are fixed and known. Moreover, due to degradation, the bits in $\mathcal{G}(W_{SR}) \cap \mathcal{B}(W_{SD})$ need to be delivered to the destination by the relay during the second-hop transmission. That is, the message bits of $\tilde{\mathcal{I}}_1$ are loaded in $\tilde{\mathcal{I}}_1^{SD} = \mathcal{G}(W_{SD}) \cap \mathcal{B}(W_{SE})$ and $\tilde{\mathcal{I}}_1^{RD} = \mathcal{G}(W_{SR}) \cap \mathcal{B}(W_{SD})$. Fig. 3 shows the coding scheme, the lines on $\mathcal{D}_2$ and $\mathcal{E}_2$ imply the first chain construction.

Processing at the relay: Relay decodes message block j, knowing $\mathcal{F}_1$ and the seed $\mathcal{D}_1(j) = \mathcal{E}_1(j-1)$, then extracts the bits in $\tilde{\mathcal{I}}_1^{RD}$ and forwards them to the destination by using a polar code for the channel W_{RD} using partition (9). Specifically, for block $j = 1, \ldots, k$ message bits are loaded in the set $\tilde{\mathcal{I}}_2$, random bits in the set $\mathcal{R}_2$ and the bits in the set $\mathcal{D}_2$ are chained with those of $\mathcal{E}_2$, i.e. $\mathcal{D}_2(j) = \mathcal{E}_2(j-1)$, as shown in Fig. 4. The frozen set for this transmission is $\mathcal{F}_2$, which is known to the destination.

Destination decoding: At the destination, the process starts by decoding the first block message of the relay transmission, knowing $\mathcal{F}_2$ and $\mathcal{D}_2(j) = \mathcal{E}_2(j-1)$. Then uses those bits to decode the corresponding message block received from the source transmission at the first stage, by employing the SC algorithm.

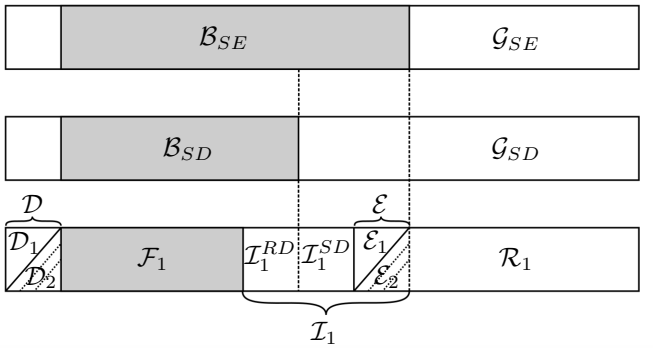

Fig. 3. Index partitioning (8) at the source encoding.

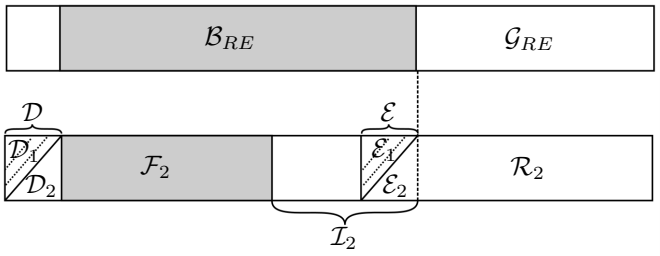

Fig. 4. Index partitioning (9) at the relay.

Let us now introduce the following random variables needed for the reliability and secrecy analysis. For the transmission in blocks $j = 1, \ldots, k$, denote source's message bits in $\tilde{\mathcal{I}}_1$ by $M_{1,k}$ and let $M_{2,k}$ be the message transmitted by the relay with bits in $\tilde{\mathcal{I}}_2$, frozen bits in $\mathcal{F}_1$ and $\mathcal{F}_2$ are denoted by $F_{1,k}$ and let $F_{2,k}$. Also, let $E_{1,k}$ and $E_{2,k}$ correspond to the bits belong to $\mathcal{E}_1(j)$ and $\mathcal{E}_2(j)$, respectively, for $j = 0, \ldots, k$. To make the analysis compact we also denote, $\mathbf{M}_k = (M_{1,k}, M_{2,k})$, $\mathbf{F}_k = (F_{1,k}, F_{2,k})$, $\mathbf{E}_k = (E_{1,k}, E_{2,k})$ and the k-length vectors $\mathbf{M}_1^k = (\mathbf{M}_1, \ldots, \mathbf{M}_k)$, $\mathbf{F}_1^k = (\mathbf{F}_1, \ldots, \mathbf{F}_k)$ and $\mathbf{E}_0^k = (\mathbf{E}_0, \ldots, \mathbf{E}_k)$ and let $\mathbf{Z}_0^k = (\mathbf{Z}_0, \ldots, \mathbf{Z}_k)$ the sequence of eavesdropper's observations $\mathbf{Z} = (Z_{SE}, Z_{RE})$ during the k-th block transmission from source and relay.

C. Reliability Analysis

To examine the reliability of this scheme, we focus to the error probability for the legitimate parties. First, for the relay, since the rate of the transmission uses a polar coding sequence with $R < I(W_{SR})$ and assuming that $Pr\{\hat{\mathbf{E}}_0 \neq \mathbf{E}_0\} \to 0$, i.e. there is a code with $\epsilon_N \to 0$ and used to convey the seed to the legitimate users, the probability of erroneous decoding at the relay in the $k+1$ blocks is

$$P_e^{SR} \leq \epsilon_N + k\mathcal{O}(2^{-N^\beta}), \tag{10}$$

for all $\beta < 1/2$.

Similarly, the destination will recover relay's message $\mathbf{M}_2$, with the error probability bounded by

$$P_e^{RD} \leq k\mathcal{O}(2^{-N^\beta}), \tag{11}$$

since $\tilde{\mathcal{I}}_2 \cup \mathcal{R}_2 \subset \mathcal{G}(W_{RD})$, and knowing $\mathcal{F}_2$ and $\mathcal{D}_2(j)$. Then, using those bits can decode source's message $\mathbf{M}_1$, using SC algorithm. Overall, the probability of error at the destination after the second transmission is then bounded as,

$$P_e \leq \epsilon_N + k\mathcal{O}(2^{-N^\beta}), \tag{12}$$

where ϵ_N is the vanishing error of the code transmitting the seed prior the communication.

D. Secrecy Analysis

We will show that the strong secrecy requirement is satisfied by utilizing the double-chaining construction described above. For the proposed encoding scheme the information leakage to the eavesdropper can be analysed as follows

$$\begin{aligned} I(\mathbf{M}_1^k; \mathbf{Z}_0^k) &\leq I(\mathbf{M}_1^k \mathbf{E}_k; \mathbf{Z}_0^k) \\ &= I(\mathbf{M}_1^k \mathbf{E}_k; \mathbf{Z}_k) + I(\mathbf{M}_1^k \mathbf{E}_k; \mathbf{Z}_0^{k-1} | \mathbf{Z}_k) \\ &= I(\mathbf{M}_k \mathbf{E}_k; \mathbf{Z}_k) + I(\mathbf{M}_1^k \mathbf{E}_k; \mathbf{Z}_0^{k-1} | \mathbf{Z}_k) \quad (13) \\ &\leq I(\mathbf{M}_k \mathbf{E}_k; \mathbf{Z}_k) + I(\mathbf{M}_1^k \mathbf{E}_k \mathbf{Z}_k; \mathbf{Z}_0^{k-1}) \\ &\leq I(\mathbf{M}_k \mathbf{E}_k; \mathbf{Z}_k) + I(\mathbf{M}_1^k \mathbf{E}_{k-1}^k \mathbf{Z}_k; \mathbf{Z}_0^{k-1}) \\ &= I(\mathbf{M}_k \mathbf{E}_k; \mathbf{Z}_k) + I(\mathbf{M}_1^{k-1} \mathbf{E}_{k-1} \mathbf{Z}_k; \mathbf{Z}_0^{k-1}), \quad (14) \end{aligned}$$

where (13) and (14) is due to the Markov chains $\mathbf{M}_1^{k-1} \to \mathbf{M}_k \mathbf{E}_k \to \mathbf{Z}_k$ and $\mathbf{M}_k \mathbf{E}_k \mathbf{Z}_k \to \mathbf{M}_1^{k-1} \mathbf{E}_{k-1} \to \mathbf{Z}_0^{k-1}$, respectively. Now if we summate over all k blocks we get

$$I(\mathbf{M}_1^k \mathbf{E}_k; \mathbf{Z}_0^k) \leq \sum_{j=1}^{k} I(\mathbf{M}_j \mathbf{E}_j; \mathbf{Z}_j) + \underbrace{I(\mathbf{E}_0; \mathbf{Z}_0)}_{\epsilon_N}, \tag{15}$$

where the last term is the secret seed shared between the legitimate parties prior the communication and we assumed that there exists a secure coding scheme with $\epsilon_N \to 0$. Noting that $I(\mathbf{M}_j \mathbf{E}_j; \mathbf{Z}_j) = I(\mathbf{M}_j \mathbf{E}_j \mathbf{F}_j; \mathbf{Z}_j)$, due to $\mathbf{F}_j = 0$, we can rewrite (15) as

$$I(\mathbf{M}_1^k \mathbf{E}_k; \mathbf{Z}_0^k) \leq \sum_{j=1}^{k} I(\mathbf{M}_j \mathbf{E}_j \mathbf{F}_j; \mathbf{Z}_j) + \epsilon_N, \tag{16}$$

where in order to complete the proof of strong secrecy it remains to show that the first term of the RHS in (16) vanishes as well. Therefore, we need to bound the capacity of eavesdropper's channel induced by our encoding, which for the symmetric case is given by the mutual information between its input and output under uniform input distribution. For this purpose we prove the following lemma.

Lemma 1. *For any $j = 1, \ldots, k$ we have*

$$I(\mathbf{M}_j \mathbf{E}_j \mathbf{F}_j; \mathbf{Z}_j) \leq \mathcal{O}(2^{-N^\beta}).$$

Proof. Let $\tilde{\mathbf{M}}_j$, $\tilde{\mathbf{E}}_j$ and $\tilde{\mathbf{F}}_j$ be independent and uniformly distributed versions of $\mathbf{M}_j$, $\mathbf{E}_j$ and $\mathbf{F}_j$, respectively, and let $\tilde{\mathbf{Z}}_j$ denote the corresponding channel output. Since symmetry holds for both channels W_{SE} and W_{RE}, as proven in [9], the mutual information is maximized with uniform input distribution and we have that

$$\begin{aligned} I(\mathbf{M}_j \mathbf{E}_j \mathbf{F}_j; \mathbf{Z}_j) &\leq I(\tilde{\mathbf{M}}_j \tilde{\mathbf{E}}_j \tilde{\mathbf{F}}_j; \tilde{\mathbf{Z}}_j) \\ &\leq \sum_{m=1}^{|\mathcal{A}|} I(W_{SE}^{(i_m)}) + \sum_{m=1}^{|\mathcal{B}|} I(W_{RE}^{(i_m)}) \quad (17) \\ &\leq \mathcal{O}(2^{-N^\beta}), \quad (18) \end{aligned}$$

where $\mathcal{A} = \mathcal{I}_1 \cup \mathcal{E}_1 \cup \mathcal{F}_1$ and $\mathcal{B} = \mathcal{I}_2 \cup \mathcal{E}_2 \cup \mathcal{F}_2$, also we let $i_1 < \ldots < i_{|\mathcal{A}|}$ and $i_1 < \ldots < i_{|\mathcal{B}|}$ be the elements of $\mathcal{A}$ and $\mathcal{B}$, respectively. Inequality (17) follows from [9, Lemma 15] and (18) is consequent of the definitions in (8) and (9). ■

Finally, combining Lemma 4 and (16) we get the desired result

$$I(\mathbf{M}_1^k; \mathbf{Z}_0^k) \leq I(\mathbf{M}_1^k \mathbf{E}_k; \mathbf{Z}_0^k) \leq \epsilon_N + k\mathcal{O}(2^{-N^\beta}), \tag{19}$$

which for k fixed and $N \to \infty$ we observe that $I(\mathbf{M}_1^k; \mathbf{Z}_0^k)$ vanishes, as we have assumed that $\epsilon_N \to 0$ and that completes the secrecy analysis.

Moreover, the achievable rate under this encoding scheme is given by

$$R_s^{strong} = \frac{k}{k+1}[R^{DF} - (I(W_{SE}) + I(W_{RE})) - 2\Delta], \tag{20}$$

as N grows large and by choosing k to be large enough, where 2Δ is a small rate penalty induced by the double-chaining structure and R^{DF} is the lower bound for the primitive relay channel under DF protocol [6].

Remark 1. The rate penalty Δ is negligible since it depends on the cardinality of subset $\mathcal{D}$ which is fixed prior the transmission and is considered to be small. Thus, the achievable rate of (20) can be close to the results of [4], for sufficiently large k and N.

IV. Conclusion

In this work we have proposed an efficient coding scheme, based on polar codes, for the primitive relay wiretap channel which guarantees information-theoretic security. In our setup we exploited the nested structure of polar codes for cooperative relaying in a DF strategy. We presented an encoding scheme which achieves reliability and weak secrecy, but fails to provide strong secrecy. To solve the problem of misaligned bits we used a different partition of the coordinates and a chaining construction we were able to prove that reliability and strong secrecy can be obtained simultaneously for the channel model into consideration.

REFERENCES

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

[2] E. C. van der Meulen, "Three-terminal communication channels," *Advances in Applied Probability*, no. 3, pp. 120 – 154, 1971.

[3] T. Cover and A. A. El Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, pp. 572 – 584, Sep. 1979.

[4] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005-4019, Sept. 2008.

[5] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proc. 2007 41st Annual Conference on Information Sciences and Systems*, Baltimore, MD, 2007, pp. 13-18.

[6] Y. H. Kim, "Coding techniques for primitive relay channels," in *Proc. 2007 Allerton Conf. Commun., Control, Computing* , pp. 129–135.

[7] V. Aggarwal, L. Sankar, A. R.Calderbank, and H. .V.Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," in *Proc. 2009 Information Theory and Applications Workshop*, San Diego, CA, 2009, pp. 295-300.

[8] 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.

[9] 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, 2011.

[10] E. Sasoglou and A. Vardy, "A New Polar Coding Scheme for Strong Security on Wiretap Channels," in *Proc. 2013 IEEE International Symposium on Information Theory*, Istanbul, 2013, pp. 1117-1121.

[11] T. Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," *IEEE Transactions on Information Theory*, vol. 63, no. 2, pp. 1311-1324, 2017.

[12] Y. P. 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, 2016.

[13] R. .A. Chou and M. 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, 2016.

[14] R. Blasco-Serrano, R. Thobanen, M. Andersson, V. Rathi, M. Skoglund, "Polar codes for cooperative relaying," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3263-3273, November 2012.

[15] D. S. Karas, K. N. Pappi and G. Karagiannidis, "Smart Decode-and-Forward Relaying with Polar Codes," *IEEE Wireless Communications Letters*, vol. 3, no. 1, pp. 62-65, February 2014.

[16] L. Wang, "Polar Coding for the Relay Channels," in *Proc. 2015 IEEE International Symposium on Information Theory*, Hong Kong, 2015, pp. 1532-1536.

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

[18] M. Mondelli, S. H.Hassani, and R. Urbanke, "A new Coding Paradigm for the Primitive Relay Channel," in *Proc. 2018 IEEE International Symposium on Information Theory*, Vail, CO, 2018, pp. 351-355.

[19] B. Duo, P. Wang, Y. Li, and B. Vucetic, "Secure Transmission for Relay-Eavesdropper Channels Using Polar Coding," *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, 2014, pp. 2197-2202.

[20] U. M. Mauerer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology - Eurocrypt 2000*, Lecture Notes in Computer Science. B. Preneel, 2000, pp. 351-368.

[21] E. Arikan and E. Telatar, "On the rate of Channel Polarization," in *Proc. 2009 IEEE International Symposium on Information Theory*, pp. 1493–1495.

[22] S. B. Korada and R. L. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1751-1768, 2010.

[23] S. B. Korada, *"Polar codes for channel and source coding,"* Ph.D. dissertation, École Polytechnique Fédérale de Lausanne, Switzerland, 2009.