entropy

MDPI

Article

Secure Polar Coding for the Primitive Relay Wiretap Channel

Manos Athanasakos [1,*] and George Karagiannidis [2]

[1] Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, 157 72 Athens, Greece
[2] Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 541 24 Thessaloniki, Greece; geokarag@auth.gr
* Correspondence: emathan@di.uoa.gr

Abstract: With the emergence of wireless networks, cooperation for secrecy is recognized as an attractive way to establish secure communications. Departing from cryptographic techniques, secrecy can be provided by exploiting the wireless channel characteristics; that is, some error-correcting codes besides reliability have been shown to achieve information-theoretic security. In this paper, we propose a polar-coding-based technique for the primitive relay wiretap channel and show that this technique is suitable to provide information-theoretic security. Specifically, we integrate at the relay an additional functionality, which allows it to smartly decide whether it will cooperate or not based on the decoding detector result. In the case of cooperation, the relay operates in a decode-and-forward mode and assists the communication by transmitting a complementary message to the destination in order to correctly decode the initial source's message. Otherwise, the communication is completed with direct transmission from source to the destination. Finally, we first prove that the proposed encoding scheme achieves weak secrecy, then, in order to overcome the obstacle of misaligned bits, we implement a double-chaining construction, which achieves strong secrecy.

Keywords: polar codes; relay channel; information-theoretic security; decode-and-forward; strong secrecy

Citation: Athanasakos, M.; Karagiannidis, G. Secure Polar Coding for the Primitive Relay Wiretap Channel. *Entropy* **2021**, *23*, 442. https://doi.org/10.3390/e23040442

Academic Editor: Eirik Rosnes

Received: 2 February 2021
Accepted: 6 April 2021
Published: 9 April 2021

1. 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 the 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 has been exploited as a way to establish secure communication. The rate-equivocation region was characterized in [4,5] for a four-terminal relay channel and an eavesdropper under several cooperation protocols. Half-duplex relay channel models are 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 was 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 split into N "bit-channels", which 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 that meets the requirement for weak secrecy was proposed; in [10], the authors used a different partition of the index set to develop a scheme for strong secrecy. Under this framework, several coding schemes for multiuser channels have been investigated in [11–13]. However, although in the open literature there are some applications of polar codes without security constraints for the relay channel [14–18], the investigation of whether polar codes are suitable for the relay wiretap scenario has drawn little attention. Finally, the authors in [19] proposed a coding scheme capable of achieving weak secrecy for the relay-eavesdropper channel, whereas in [20], the proposed polar coding scheme guarantees strong secrecy for the case of symmetric channels and under the assumption that the eavesdropper's channel is degraded. Note that the natural nested structure of polar codes and their low encoding/decoding complexity identify them as a promising choice for the practical implementation of merging coding and security into one scheme.

1.1. Related Work and Contributions

Since the introduction of the chaining technique [21] for polar codes, several explicit and efficient coding schemes for different information-theoretic models have been proposed. The work of [10] introduced the polar coding chaining construction in order to provide strong secrecy for the symmetric and degraded point-to-point wiretap channel. Later on, a polar code technique for asymmetric models was proposed in [22] and, along with the chaining construction, were the basic tools used to prove the secrecy capacity achievability of general wiretap channels. Specifically, in [12], the authors considered the chaining technique to deal with the nondegraded wiretap channel by artificially constructing the subset property and polar coding for asymmetric models to prove that polar codes achieve secrecy capacity in general. However, they considered only the weak secrecy case. Concurrently, refs. [11,13] developed a polar coding scheme for the general broadcast wiretap channel relying on different approaches. While both works considered the strong secrecy criterion, the first drew parallels between the achievability proof through output statistic of random binning and their proposed encoding scheme and avoided using randomized decisions during the encoding and decoding procedures ([23], Theorem 3), while the latter relied on shared random mappings ([22], Theorem 3) that may require exponential storage complexity. Recently, the authors of [24] extended the scheme of [13] by considering a more general model, in which the transmitter sends common and confidential messages over a broadcast wiretap channel. In their scheme, a new chaining construction is proposed to deal with the common information transmission.

Motivated by the above, in this paper, we consider the primitive relay wiretap channel and propose polar coding schemes based on different coordinate partitions. We prove that these schemes satisfy weak and strong secrecy requirements, while simultaneously guarantee a low probability of error at the legitimate receiver. Specifically, by careful partitioning of the coordinates, we first improve the analysis of [19] for the case of weak secrecy in a single transmission block. Then, we propose a new encoding algorithm under the strong secrecy criterion. In particular, we consider the general primitive relay wiretap channel, without assuming degradedness or symmetric channels as in [20]. The scheme utilizes previous polar coding techniques using the minimum rate of shared randomness and relies on both choosing the coordinate partitions properly and a transmission protocol that divides the communication into multiple blocks. Due to the nature of the channel under consideration, a new double-chaining construction is designed in order to satisfy the stronger secrecy requirement. Finally, an additional functionality is considered at the relay node; using the results from [15], the relay possesses a detector deciding if the result

is erroneous or not and, based on that, discards it or cooperates in decode-and-forward (DF) mode.

1.2. Structure

The rest of the paper is organized as follows. In Section 2, some preliminaries on polar codes and the basic concept of the proposed scheme are introduced. The system model and the constraints in designing the coding scheme are presented in Section 3, followed by the main results of this paper; the encoding schemes for weak and strong secrecy and the analysis of reliability and security are presented in Section 4. Finally, Section 5 concludes the paper.

2. Polar Codes and the Relay Channel

2.1. Some Fundamentals on Polar Coding

We consider a binary-input channel with input alphabet $\mathcal{X}$, output alphabet $\mathcal{Y}$, and the conditional probability distribution $W_{X|Y}(\cdot|\cdot)$, with capacity $C(W) = \max_{P_X} I(X;Y)$. The symmetric capacity $I(W)$ is the value of mutual information $I(X;Y)$ when X is uniformly distributed. Moreover, if W is symmetric, then $I(W) = C(W)$.

The Bhattacharyya parameter of the channel W is defined as

$$Z(W) = \sum_{y\in\mathcal{Y}} \sqrt{W_{X|Y}(0|y)W_{Y|X}(y|1)}. \tag{1}$$

For length $N = 2^n$ with $n \in \mathbb{N}$, let $G_N = B_N F^{\otimes n}$ be the polarizing matrix, where B_N is the bit-reversal mapping, $F = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ and $F^{\otimes n}$ denote the nth Kronecker power of F. By applying transformation G_N to N bits u_1^N and sending it through N independent uses of a B-DMC $W : X \to Y$, thus, an N-dimensional channel is created, defined by

$$W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) = \frac{1}{2^{N-1}} \sum_{u_{i+1}^N \in \{0,1\}^{N-i}} W_N(y_1^N|u_1^N), \tag{2}$$

where $W_N^{(i)}$ denotes the i-th bit-channel created by synthesizing N uses of the channel W. As N grows, $W_N^{(i)}$ approaches either an error-free or a completely noisy channel. The idea is to transmit information only over the "good" channels while keeping the inputs of "bad" channels fixed and known to all parties. Thus, the N bit-channels are partitioned into "good" channels $\mathcal{G}_N(W)$ and "bad" channels $\mathcal{B}_N(W)$ based on the value of their Bhattacharyya parameter.

$$\begin{aligned} \mathcal{G}_N(W) &= \{i \in [N] : Z(W_N^{(i)}) \le \delta_N\} \\ \mathcal{B}_N(W) &= \{i \in [N] : Z(W_N^{(i)}) \ge 1 - \delta_N\}, \end{aligned} \tag{3}$$

where $[N] = \{1, 2, \ldots, N\}$, $\delta_N = 2^{-N^\beta}$ with $0 < \beta < 1/2$ and $Z(W_N^{(i)})$ is the Bhattacharyya parameter of channel $W_N^{(i)}$. It has been shown [25,26] that for any symmetric binary-input channel W and for any $\beta < 1/2$,

$$\begin{aligned} \lim_{N\to\infty} &= \frac{\mathcal{G}_N(W)}{N} = C(W) \\ \lim_{N\to\infty} &= \frac{\mathcal{B}_N(W)}{N} = 1 - C(W). \end{aligned} \tag{4}$$

Based on the above, we can transmit a message of $k = |\mathcal{G}_N(W)|$ bits, which is written in the bits u_i, $i \in \mathcal{G}_N(W)$ and the rest $N - k$ bits of u_1^N are frozen and set to 0. Thus, a code word $x_1^N = u_1^N G_N$ is sent over the channel. On the other side, the received sequence y_1^N

can be decoded by finding an estimate of u_1^N by computing the values $\hat{u}_i$, $i \in [N]$ based on the following successive cancellation (SC) rule:

$$\hat{u}_i = \begin{cases} 0, & \text{if } \frac{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|0)}{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|1)} \geq 1 \text{ and } i \in \mathcal{G}_N(W) \\ 0, & \text{if } i \in \mathcal{B}_N(W) \\ 1, & \text{otherwise.} \end{cases} \tag{5}$$

Using this decoding rule [8,25], we can upper bound the error probability

$$P_e \leq \sum_{i \in \mathcal{G}_N(W)} Z(W_N^{(i)}) \leq \delta_N, \tag{6}$$

where $\beta \in (0, 1/2)$.

2.2. Bounds and Nested Structure

In this paper, one of the main characteristics of the proposed coding scheme is the nested structure of the polar codes. Next, we briefly explain this structure and its usage for binning in multiterminal communication scenarios. In particular, the authors in [14] designed a coding scheme for the three-terminal stochastically degraded relay channel with orthogonal receivers. First however, let us review the capacity bounds of the relay channel.

It is well-known that a bound for the capacity of the general relay channel is given by the cut-set upper bound [3]

$$C \leq \max_{P_X, P_{X_R}} \min\{I(X; Y_{SR} Y_{SD}), I(X; Y_{SD}) + I(X_R; Y_{RD})\}, \tag{7}$$

and for the primitive relay channel, the DF lower bound reduces to [6]

$$R^{DF} = \max_{P_X} \min\{I(X; Y_{SR}), I(X; Y_{SD}) + I(X_R; Y_{RD})\}. \tag{8}$$

Next, we briefly describe the nested structure of polar codes proposed in [14] for DF relaying, which, for any rate $R < R^{DF}$, there exists a sequence of polar codes with a vanishing probability of error at the destination. The following Lemma from [27] is used to exploit the nested nature of polar codes.

Lemma 1. *Let Q and V be BSM channels such that Q is degraded with respect to V. Further, let $Q_1, \ldots Q_i$ and $V_1, \ldots V_i$ denote the N corresponding bit-channels. Then, Q_i is degraded with respect to V_i, that is, $I(Q_i) \leq I(V_i)$ and $Z(Q_i) \geq Z(V_i)$.*

From the above lemma, it follows directly that if the channel Q is degraded with respect to V, the set of good channels for Q is a subset of the set of good channels of V, i.e., for all constants β, we have $\mathcal{G}_N(Q) \subseteq \mathcal{G}_N(V)$. Degradation implies that a channel is better than another one. The primitive relay channel is said to be degraded when the source-destination link is worse than that between source and relay. The encoding process starts at the source when a rate $R < I(W_{SR})$ is chosen and a capacity-achieving polar code for the channel W_{SR} is used. We define $\mathcal{G}_{SR}$ and $\mathcal{B}_{SR}$ as in (3) for channel W_{SR} as the information and frozen set, respectively. Let $\mathbf{M}$ contain the information and the frozen bits transmitted by the source. Moreover, the bits m_i, $i \in \mathcal{G}_{SR}$ carry the message and m_i, $i \in \mathcal{B}_{SR}$ are the frozen bits, which are known to the relay and the destination prior to transmission. As shown in Figure 1, the destination cannot decode this sequence in its entirety due to its degraded channel. So, we also select a set of indices for direct communication over W_{SD} and define $\mathcal{G}_{SD}$ and $\mathcal{B}_{SD}$ similarly. From Lemma 1, it holds that $\mathcal{G}_{SD} \subseteq \mathcal{G}_{SR}$, as W_{SD} is degraded compared to W_{SR}, i.e., the decoder at the destination knows the values of the

symbols m_i, $i \in \mathcal{G}_{SD} \cup \mathcal{G}_{SR}$ and in order to employ SC decoding, the relay must forward the information m_i, $i \in \mathcal{G}_{SR} \cup \mathcal{B}_{SD}$.

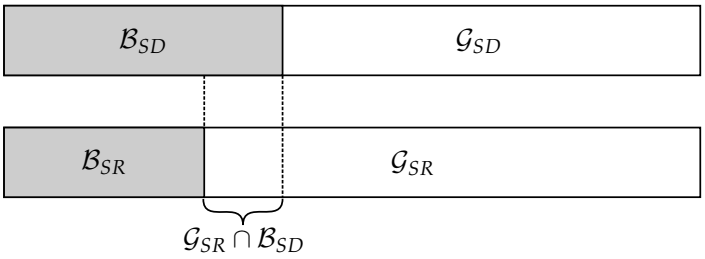

Figure 1. Nested structure of polar codes for the relay channel.

2.3. Smart Relaying

It has been shown in [15] that by providing the relay with a simple error detector, we can significantly improve the error performance by letting the decoder at the relay select whether it will cooperate or not. We consider a DF cooperative transmission, where the message is encoded by using the nested polar coding scheme of Section 2.2. The relay carries a detector for erroneous decoding, i.e., if the likelihood ratio is less than a threshold, then the relay discards the decoded result and does not transmit to the destination, otherwise, the communication takes place under the assistance of the relay node.

We consider a threshold s for the relay decoder and the log-likelihood ratio (LLR) as defined for the successive decoding process [8]:

$$L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) = \log \frac{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|0)}{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|1)}, \tag{9}$$

where the decoder decides based on the rule in (5). A flag F is used to determine if the decoding result will be discarded or not according to

$$F = \begin{cases} 0, & \text{if } -s \leq L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) \leq s \\ 1, & \text{otherwise.} \end{cases} \tag{10}$$

The above procedure does not introduce any additional complexity during the relay's decoding, thus, this functionality improves the error probability of the overall communication for free. In the next section, we bind together the smart relaying and the exploitation of the nested structure of polar codes to design a scheme that satisfies secrecy and reliability requirements for the primitive relay channel in the presence of an eavesdropper.

3. System Model and Requirements

In this section, we describe the primitive relay wiretap channel and set the goals of our encoding scheme; reliability and secrecy. Then, we present the architecture of the proposed communication model with the smart error detector at the relay.

3.1. The Relay Wiretap Channel

The relay wiretap channel models a multihop 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 the transition probability mass function

$$p(y, y_{sr}, z|x_s, x_r) = p(y_{sd}, y_{sr}, z_{se}|x_s)p(y_{rd}, z_{re}|x_r). \tag{11}$$

In this model, $\mathcal{X}_S$ and $\mathcal{X}_R$ are the channel inputs from the 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. Figure 2 illustrates the channel, which consists of a source, a relay, the legitimate receiver, and the eavesdropper. The source wishes to reliably communicate a message $\mathbf{M}$ with the legitimate receiver under the assistance of a trusted relay while keeping it safe from the eavesdropper. The transmission takes place in two stages as follows:

- In the first stage, the Source encodes a message $\mathbf{M}$ into a code word $\mathbf{X}_S$ and broadcasts it to the destination and relay.
- In the second stage, the Relay first decodes the Y_{SR} and obtains $\hat{\mathbf{M}}_R$, then re-encodes it and transmits $\mathbf{X}_R$ to the destination.
- The Destination combines the two observations to produce an estimate $\hat{\mathbf{M}}$ of the original message.
- The Eavesdropper observes $\mathbf{Z} = (Z_{SE}, Z_{RE})$ during both transmissions.

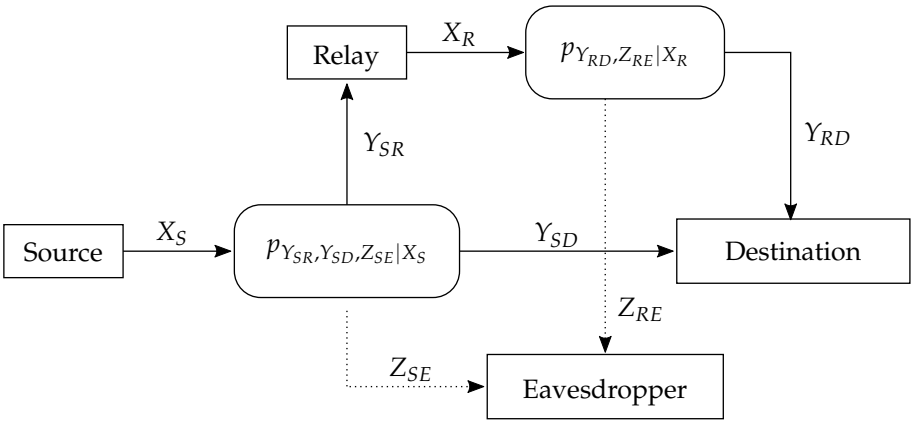

Figure 2. The relay wiretap channel model with orthogonal components.

3.2. Coding Requirements

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

$$\lim_{N\to\infty} Pr\{\mathbf{M} \neq \hat{\mathbf{M}}\} = 0. \tag{12}$$

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

$$\lim_{N\to\infty} \frac{I(\mathbf{M};\mathbf{Z})}{N} = 0, \tag{13}$$

$$\lim_{N\to\infty} I(\mathbf{M};\mathbf{Z}) = 0. \tag{14}$$

In (13), security is measured in terms of the normalized mutual information between the transmitted message $\mathbf{M}$ and received vector by the eavesdropper $\mathbf{Z}$. The encoding scheme is designed to satisfy this requirement in order to operate with *weak secrecy*. However, as shown by Maurer in [28], it is too weak for cryptographic applications as it is possible for the eavesdropper to retrieve a considerable amount of information even if (13) is satisfied. As a solution, we can use a stronger metric, that is, the encoding scheme operates with *strong secrecy* if (14) is satisfied.

3.3. Architecture

Our model is very similar to that described in Section 3.1, where in order to enjoy the benefits of smart relaying, we add an error detector at the relay. This allows the relay to select whether it is beneficial to cooperate with the source or not. As illustrated in Figure 3, the relay operates based on the detector result, i.e., if $F = 0$, the relay discards the decoding result and the communication is completed via direct transmission from source to the

destination. In this case, the secure polar coding scheme of [9] or [10] for the classic wiretap channel can be used. On the other hand, if $F = 1$, the communication is assisted by the DF relay and the designing of such a coding scheme for reliability and secrecy is proposed in this paper.

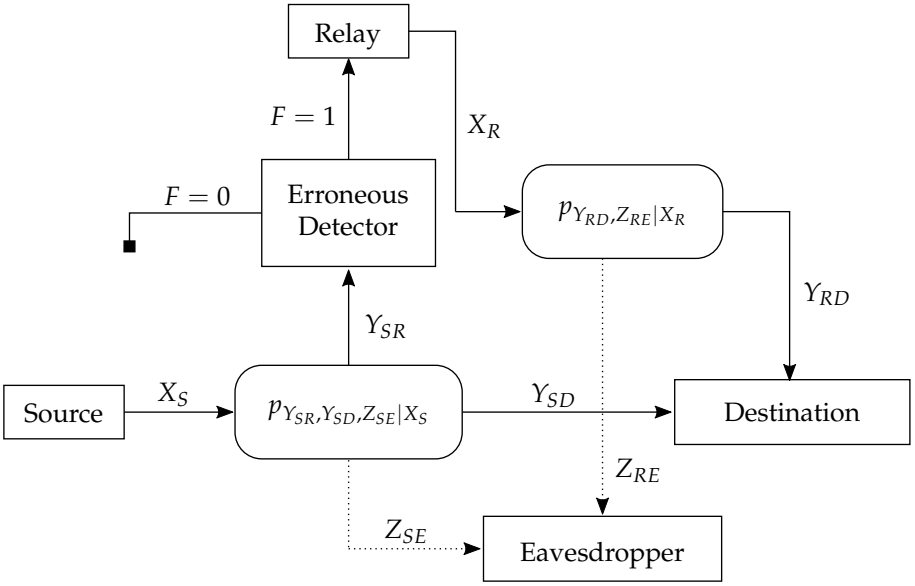

Figure 3. The relay wiretap channel with the erroneous detector.

4. Polar Coding for Secrecy

In this section, we present the encoding scheme, which simultaneously satisfies the reliability and weak secrecy constraints for the model of Section 3.2. Then, we identify the difficulties to achieve strong secrecy and introduce a new construction that satisfies this condition by using a double-chaining technique.

4.1. Weak Secrecy

As already mentioned above, polarization results into noiseless and pure-noisy bit-channels. Having in mind that the system needs to meet only the reliability requirement, one shall fill the good channels with information bits and keep the value of the bad channels fixed. However, when a third unauthorized party eavesdrops the communication, the secrecy constraint must be satisfied. The idea behind coding for secrecy is to confuse the nonlegitimate user with random messages, so their observation is different from the real message. Utilizing polar codes, we can design a secure coding scheme by properly partitioning the bit-channels. First, in order to achieve reliability, we send the message over the good channels (low entropy) for the legitimate users and bad channels (high entropy) for the eavesdropper. To confuse the eavesdropper and secure the transmission, we choose to hide the message by sending random bits over the reliable channels. That is, the goal is to construct an encoding process that makes the communication reliable and secure simultaneously, i.e., satisfying conditions (12) and (13). For the relay wiretap channel and under the DF protocol, these conditions must be satisfied in both transmission stages.

First, as in (3), we define the following subset of indices:

$$\begin{aligned} \mathcal{G}_N(W_{kl}) &= \{i \in [N] : Z(W_N^{(i)}) \leq \delta_N\} \\ \mathcal{B}_N(W_{kl}) &= \{i \in [N] : Z(W_N^{(i)}) \geq 1 - \delta_N\}, \end{aligned} \tag{15}$$

where $k \in \{S, R\}$ and $l \in \{R, D, E\}$, for $k \neq l$. Next, we partition the set $[N]$ based on [9] as follows:

$$\begin{aligned} \mathcal{I}_1 &= \mathcal{G}_N(W_{SR}) \cap \mathcal{B}_N(W_{SE}) \\ \mathcal{F}_1 &= \mathcal{B}_N(W_{SR}) \\ \mathcal{R}_1 &= \mathcal{G}_N(W_{SE}). \end{aligned} \tag{16}$$

Encoding at source: We choose a rate $R < I(W_{SR})$ and use the indices in $\mathcal{G}_N(W_{SR})$ to encode the information and broadcast it to the relay and the destination. All parties know the values of frozen bits $\mathcal{F}_1$. We fill with random bits the indices in $\mathcal{R}_1$ in order to protect the message. The information is stored in the bits of set $\mathcal{I}_1$. However, due to Lemma 1, degradation implies that the destination cannot decode the whole information due to $\mathcal{G}_N(W_{SD}) \subseteq \mathcal{G}_N(W_{SR})$, we distribute the message in $\mathcal{I}_1^{SD} = \mathcal{G}_N(W_{SD}) \cap \mathcal{B}_N(W_{SE})$ and $\mathcal{I}_1^{RD} = \mathcal{G}_N(W_{SR}) \cap \mathcal{B}_N(W_{SD})$, with $\mathcal{I}_1 = \mathcal{I}_1^{SD} \cup \mathcal{I}_1^{RD}$ (Figure 4). The message bits in $\mathcal{I}_1^{RD}$ must be provided by the relay during the second transmission using the following partition.

$$\begin{aligned} \mathcal{I}_2 &= \mathcal{G}_N(W_{RD}) \cap \mathcal{B}_N(W_{RE}) \\ \mathcal{F}_2 &= \mathcal{B}_N(W_{RD}) \\ \mathcal{R}_2 &= \mathcal{G}_N(W_{RE}). \end{aligned} \tag{17}$$

Processing at the relay: The relay using SC and the knowledge of frozen bits decodes the message transmitted by the source, then extracts and encodes the information bits with indices in $\mathcal{I}_1^{RD}$ and forwards them to the destination using a capacity-achieving polar code for W_{RD} and partition (17). To protect this transmission, we again fill with random bits the indices in $\mathcal{R}_2$, the information bits are in the set $\mathcal{I}_2$ and the bits in $\mathcal{F}_2$ are frozen and known (Figure 5).

Decoding at the destination: Having received Y_{RD} and recovered the missing bits from the relay, the destination uses these bits in addition to the first observation Y_{SD} and employs the SC algorithm to recover the source's message.

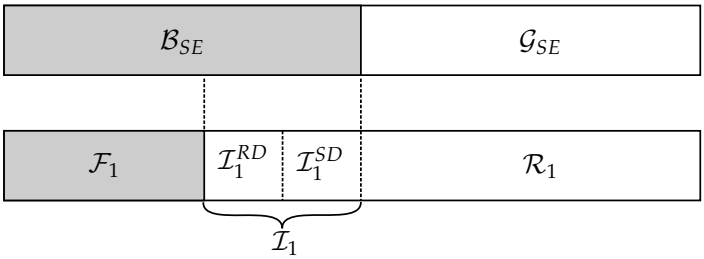

Figure 4. Stage I: Index partitioning (16) at the source.

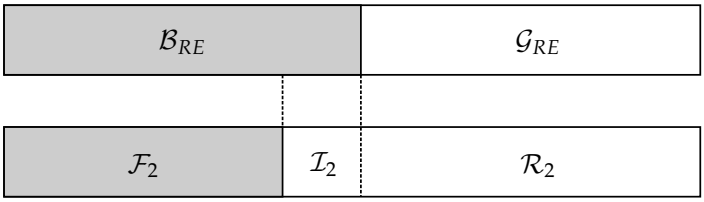

Figure 5. Stage II: Index partitioning (17) at the relay.

Based on the above encoding and decoding process, we prove that the coding scheme satisfies both requirements (12) and (13).

4.1.1. Reliability Analysis

The reliability follows immediately from the design of the coding scheme and the results developed in [8]. Specifically, the low error probability claim must be satisfied for

the relay and destination. First, since $\mathcal{I}_1 \cup \mathcal{R}_1 = \mathcal{G}_N(W_{SR})$, the error probability at the relay is upper bounded as

$$P_e^{SR} \leq \sum_{i \in \mathcal{I}_1 \cup \mathcal{R}_1} Z(W_{SR}^{(i)}) \leq 2^{-N^\beta}. \tag{18}$$

The probability of error for the relay–destination transmission of the second time-slot, since $\mathcal{I}_2 \cup \mathcal{R}_2 = \mathcal{G}_N(W_{RD})$ by design, is upper bounded as

$$P_e^{RD} \leq \sum_{i \in \mathcal{I}_2 \cup \mathcal{R}_2} Z(W_{RD}^{(i)}) \leq 2^{-N^\beta}. \tag{19}$$

The bits from the relay are then decoded by the destination and, together with the source's transmission Y_{SD}, the original message is retrieved using the SC algorithm. Consequently, the overall error probability at the destination is upper bounded by

$$P_e \leq \mathcal{O}(2^{-N^\beta}). \tag{20}$$

Moreover, we obtain the constraints on the transmission rate, i.e., $R < I(W_{SR})$ and $R < I(W_{SD}) + I(W_{RD})$, which yields the symmetric DF rate for relay channels R^{DF}.

4.1.2. Secrecy Analysis

Let us turn to the security analysis. Let $\mathbf{U}$ denote the intermediate vector constructed by the encoding process, with $\mathbf{U}_\mathcal{I} = \mathbf{U}_{\mathcal{I}_1 \cup \mathcal{I}_2}$, $\mathbf{U}_\mathcal{R} = \mathbf{U}_{\mathcal{R}_1 \cup \mathcal{R}_2}$, and $\mathbf{U}_\mathcal{F} = \mathbf{U}_{\mathcal{F}_1 \cup \mathcal{F}_2} = 0$. Moreover, the source's message $\mathbf{M} = (\mathbf{M}_1, \mathbf{M}_2)$ and takes values in $\{0,1\}^{|\mathcal{I}|}$, with $\mathbf{M}_1$ and $\mathbf{M}_2$ denoting messages from the source and relay, respectively. We need to prove that the normalized mutual information, (13), between $\mathbf{M}$ and $\mathbf{Z}$ vanishes asymptotically. We evaluate the statistical independence between the message and eavesdropper's observations using random frozen vector over all possible choices of frozen bits as follows:

$$\begin{aligned}
I(\mathbf{M}; \mathbf{Z}|\mathbf{U}_\mathcal{F}) &= I(\mathbf{U}_\mathcal{I}; \mathbf{Z}|\mathbf{U}_\mathcal{F}) && (21)\\
&= I(\mathbf{U}_\mathcal{I}, \mathbf{U}_\mathcal{R}; \mathbf{Z}|\mathbf{U}_\mathcal{F}) - I(\mathbf{U}_\mathcal{R}; \mathbf{Z}|\mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I}) && (22)\\
&= I(\mathbf{U}; \mathbf{Z}) - I(\mathbf{U}_\mathcal{R}; \mathbf{Z}|\mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I}) && (23)\\
&= I(\mathbf{U}; \mathbf{Z}) - H(\mathbf{U}_\mathcal{R}|\mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I}) + H(\mathbf{U}_\mathcal{R}|\mathbf{Z}, \mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I}) && (24)\\
&= I(\mathbf{U}; \mathbf{Z}) - H(\mathbf{U}_\mathcal{R}) + H(\mathbf{U}_\mathcal{R}|\mathbf{Z}, \mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I}) && (25)\\
&= I(\mathbf{U}; \mathbf{Z}) - |\mathcal{R}| + H(\mathbf{U}_\mathcal{R}|\mathbf{Z}, \mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I}) && (26)\\
&\leq N(I(W_{SE}) + I(W_{RE})) - |\mathcal{R}| + H(\mathbf{U}_\mathcal{R}|\mathbf{Z}, \mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I}), && (27)
\end{aligned}$$

where (22) is derived from the chain rule of mutual information and (23) is due to $I(\mathbf{U}_\mathcal{I}, \mathbf{U}_\mathcal{R}; \mathbf{Z}|\mathbf{U}_\mathcal{F}) = I(\mathbf{U}_\mathcal{I}, \mathbf{U}_\mathcal{R}; \mathbf{Z}|\mathbf{U}_\mathcal{F}) + I(\mathbf{U}_\mathcal{F}; \mathbf{Z}) = I(\mathbf{U}_\mathcal{I}, \mathbf{U}_\mathcal{R}, \mathbf{U}_\mathcal{F}; \mathbf{Z}) = I(\mathbf{U}; \mathbf{Z})$ and that $I(\mathbf{U}_\mathcal{F}; \mathbf{Z}) = 0$. Consequently, (25) follows from the independence of $\mathbf{U}_\mathcal{R}, \mathbf{U}_\mathcal{F}$, and $\mathbf{U}_\mathcal{I}$, while (27) is concluded by the fact that $I(W_{SE})$ and $I(W_{RE})$ are the capacity of W_{SE} and W_{RE}, respectively, and the data processing inequality.

Examining (27), we observe that in order to upper bound the mutual information of (21), we need to find an upper bound for the entropy term $H(\mathbf{U}_\mathcal{R}|\mathbf{Z}, \mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I})$. Hence, we have the following lemma:

Lemma 2. *The conditional entropy is upper bounded as*

$$H(\mathbf{U}_\mathcal{R}|\mathbf{Z}, \mathbf{U}_\mathcal{F}, \mathbf{U}_\mathcal{I}) \leq h_2(2^{-N^\beta}) + |\mathcal{R}|2^{-N^\beta},$$

where $h_2(\cdot)$ is the binary entropy function and $|\mathcal{R}|$ is the size of random vector $\mathbf{U}_\mathcal{R}$.

Proof. Let us assume that the eavesdropper has knowledge of $\mathbf{U}_\mathcal{I}$ in addition to $\mathbf{Z}$ and the frozen bits. Therefore, the eavesdropper can compute an estimate of $\hat{\mathbf{U}}_\mathcal{R}$ (since $\mathcal{R}$ is

transmitted via the good channels $\mathcal{G}_N(W_{SE})$ and $\mathcal{G}_N(W_{RE})$), by using the SC algorithm with

$$P_e^{Eve} = \mathbb{P}[\hat{\mathbf{U}}_{\mathcal{R}} \neq \mathbf{U}_{\mathcal{R}}] \leq \sum_{i \in \mathcal{R}} \left(Z(W_{SE}^{(i)}) + Z(W_{RE}^{(i)}) \right) \leq 2^{-N^{\beta}}. \tag{28}$$

We then introduce a random variable E for the error as follows:

$$E = \begin{cases} 1, & \text{if } \hat{\mathbf{U}}_{\mathcal{R}} \neq \mathbf{U}_{\mathcal{R}} \\ 0, & \text{if } \hat{\mathbf{U}}_{\mathcal{R}} = \mathbf{U}_{\mathcal{R}}, \end{cases} \tag{29}$$

and we derive the following

$$\begin{aligned} H(E, \mathbf{U}_{\mathcal{R}} | \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) &= H(\mathbf{U}_{\mathcal{R}} | \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) + H(E | \mathbf{U}_{\mathcal{R}}, \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) && (30) \\ &= H(\mathbf{U}_{\mathcal{R}} | \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}), && (31) \end{aligned}$$

since the second entropy term in (30) equals zero. Moreover, note that

$$\begin{aligned} H(E, \mathbf{U}_{\mathcal{R}} | \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) &= H(\mathbf{U}_{\mathcal{R}} | E, \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) + H(E | \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) && (32) \\ &\leq H(\mathbf{U}_{\mathcal{R}} | E, \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) + H(E), && (33) \end{aligned}$$

since the second entropy term in (32) can be upper bounded by $H(E) = H(P_e^{Eve})$. Thus, from (31) and (33), we get

$$\begin{aligned} H(\mathbf{U}_{\mathcal{R}} | \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) &\leq H(\mathbf{U}_{\mathcal{R}} | E, \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) + H(\mathbb{E}) && (34) \\ &= \mathbb{P}[E = 0] H(\mathbf{U}_{\mathcal{R}} | E = 0, \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) \\ &\quad + \mathbb{P}[E = 1] H(\mathbf{U}_{\mathcal{R}} | E = 1, \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) + H(P_e^{Eve}) && (35) \\ &\leq P_e^{Eve} |\mathcal{R}| + H(P_e^{Eve}), && (36) \end{aligned}$$

where (36) is because $H(\mathbf{U}_{\mathcal{R}} | E = 0, \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) = 0$ and $H(\mathbf{U}_{\mathcal{R}} | E = 1, \mathbf{Z}, \mathbf{U}_{\mathcal{F}}, \mathbf{U}_{\mathcal{I}}) \leq H(\mathbf{U}_{\mathcal{R}}) = |\mathcal{R}|$. Rearranging (36) and using (28), we get the desired upper bound and the proof is completed. □

Finally, considering Lemma 2 and (27), we get the following upper bound:

$$I(\mathbf{M}; \mathbf{Z} | \mathbf{U}_{\mathcal{F}}) \leq N\epsilon_N + h_2(2^{-N^{\beta}}) + |\mathcal{R}| 2^{-N^{\beta}}, \tag{37}$$

where $\epsilon_N = I(W_{SE}) + I(W_{RE}) - |\mathcal{R}|/N$ and if we divide both sides of (37) by N, all terms tend to zero as $N \to \infty$, since $\lim_{N \to \infty} \epsilon_N = 0$, with $\mathcal{R}_1 \in \mathcal{G}_N(W_{SE})$ and $\mathcal{R}_2 \in \mathcal{G}_N(W_{RE})$.

Thus, the proposed polar coding scheme satisfies the weak secrecy requirement for all possible choices of frozen vector,

$$\lim_{N \to \infty} \frac{I(\mathbf{M}; \mathbf{Z})}{N} = 0 \tag{38}$$

and the achievable rate under this encoding procedure is given by

$$R_s^{weak} = R^{DF} - (I(W_{SE}) + I(W_{RE})), \tag{39}$$

for large enough N.

4.2. Strong Secrecy

The above scheme can only achieve the weak secrecy requirement, 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. For the case of the symmetric relay wiretap channel and degraded eavesdropper link, the strong secrecy claim was proved in [20]. In the following, we provide a solution for a more general case, where we do not make any assumption on eavesdropper's channel quality and consider a nonsymmetric channel model.

4.2.1. Asymmetric Channel Coding

In [22], the authors presented a polar coding scheme, which achieves the capacity of a B-DMC, to cover the general case of arbitrary input distributions. Let $U^N = X^N G_N$ and define the following sets:

$$\begin{aligned} \mathcal{H}_X &= \{i \in [N] : Z(U_i|U^{i-1}) \geq 1 - \delta_N\} \\ \mathcal{L}_X &= \{i \in [N] : Z(U_i|U^{i-1}) \leq \delta_N\} \\ \mathcal{H}_{X|Y} &= \{i \in [N] : Z(U_i|U^{i-1}, Y^N) \geq 1 - \delta_N\} \\ \mathcal{L}_{X|Y} &= \{i \in [N] : Z(U_i|U^{i-1}, Y^N) \leq \delta_N\}, \end{aligned} \tag{40}$$

where $Z(X|Y)$ is the Bhattacharyya parameter of a random variable pair (X, Y), defined as

$$Z(X|Y) = 2 \sum_{y \in \mathcal{Y}} P_Y(y) \sqrt{P_{X|Y}(0|y) P_{X|Y}(1|y)}. \tag{41}$$

From [29], we have

$$\lim_{N \to \infty} \frac{\mathcal{H}_X}{N} = H(X), \tag{42}$$

$$\lim_{N \to \infty} \frac{\mathcal{H}_{X|Y}}{N} = H(X|Y). \tag{43}$$

For a nonsymmetric B-DMC channel $W : X \to Y$, it is not possible to use all the good bit-channels to transmit information. Hence, in [22], a different partition of the set $[N]$ was proposed:

$$\begin{aligned} \mathcal{I} &= \mathcal{H}_X \cap \mathcal{L}_{X|Y} \\ \mathcal{F}_r &= \mathcal{H}_X \cap \mathcal{L}^c_{X|Y} \\ \mathcal{F}_d &= \mathcal{H}^c_X. \end{aligned} \tag{44}$$

For $i \in \mathcal{H}_X$, U_i is almost uniformly distributed and independent of the past U^{i-1}, therefore, it can carry information. For $i \in \mathcal{L}_{X|Y}$, U_i is almost determined by U^{i-1} and Y^N, implying that it can be decoded in a successive manner, and from (42) and (43), we have

$$\lim_{N \to \infty} \frac{|\mathcal{I}|}{N} = I(X;Y). \tag{45}$$

The remaining indices are frozen; for $i \in \mathcal{F}_r$, U_i is almost uniformly distributed and independent of the past U^{i-1} but cannot be reliably decoded given Y^N; for $i \in \mathcal{F}_d$, U_i is almost determined by U^{i-1}. As suggested in [22], the values of bits in $\{i \in \mathcal{F}_r \cup \mathcal{F}_d\}$ are assigned by random mappings $\lambda_i : \{0,1\}^{i-1} \to \{0,1\}$ according to the following probability rule:

$$\lambda_i(u^{i-1}) = u, \text{ w.p. } P_{U_i|U^{i-1}}, \tag{46}$$

which are shared between the encoder and the decoder. However, this operation requires sharing a large amount of randomness which is often undesirable. As a remedy to this, simplified schemes that require a vanishing rate of shared randomness were proposed in [23,30].

Let the bits in $\{i \in \mathcal{I}\}$ be used to store information as mentioned above, and let bits in $\{i \in \mathcal{F}_r\}$ be uniformly distributed random bits shared between the encoder and the decoder. This sequence can be reused over several blocks, making the rate loss negligible. The values of $\{i \in \mathcal{F}_d\}$ are sampled from the distribution $P_{U_i|U^{i-1}}$, and the bits in $\{i \in \mathcal{H}_X^c \cap \mathcal{L}_{X|Y}^c\}$ are transmitted to the receiver separately with some reliable code, with negligible rate loss (since $|\mathcal{L}_{X|Y}^c \setminus \mathcal{H}_{X|Y}| = o(n)$ and $\mathcal{H}_{X|Y} \subseteq \mathcal{H}_X$, we have that $|\mathcal{H}_X^c \cap \mathcal{L}_{X|Y}^c| = o(n)$).

After the transmission of $x^N = u^N G_N$, the receiver knows the sequences $\{i \in \mathcal{F}_r\}$ and $\{i \in \mathcal{H}_X^c \cap \mathcal{L}_{X|Y}^c\}$ and successively constructs the estimate $\hat{u}$ using the following rule for each bit-channel:

$$\hat{u}_i = \begin{cases} \arg\max_{u \in [0,1]} P_{U_i|U^{i-1},Y^N}(u|\hat{u}^{i-1}, y^N), & \text{if } i \in \mathcal{L}_{X|Y} \\ u_i, & \text{if } i \in \mathcal{L}_{X|Y}^c. \end{cases} \tag{47}$$

This scheme's rate approaches $I(X;Y)$ and the error probability can be upper bounded by $P_e \leq \sum_{i \in \mathcal{L}_{X|Y}} Z(U_i|U^{i-1}, Y^N) = \mathcal{O}(\delta_N)$.

4.2.2. Encoding Scheme

In the following, we develop the main contribution of this work, the encoding scheme for the primitive relay wiretap channel, and remove the assumptions on degradedness and symmetry. The transmission takes place over $k+1$ blocks of N bits. Prior to 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 that the bits of $\mathcal{D}$ are 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 SC for block j and recover these bits reliably, while security is guaranteed.

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

$$\begin{aligned} \mathcal{I}_1 &= \mathcal{H}_{X_S} \cap \mathcal{G}_N(W_{SR}) \cap \mathcal{B}_N(W_{SE}) \\ \mathcal{F}_1 &= \mathcal{H}_{X_S} \cap \mathcal{G}_N^c(W_{SR}) \cap \mathcal{B}_N(W_{SE}) \\ \mathcal{R}_1 &= \mathcal{H}_{X_S} \cap \mathcal{G}_N(W_{SR}) \cap \mathcal{B}_N^c(W_{SE}) \\ \mathcal{D}_1 &= \mathcal{H}_{X_S} \cap \mathcal{G}_N^c(W_{SR}) \cap \mathcal{B}_N^c(W_{SE}) \\ \mathcal{B}_1 &= \mathcal{H}_{X_S}^c, \end{aligned} \tag{48}$$

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; $\mathcal{D}_1$ are the misaligned bits; and $\mathcal{B}_1$ are the almost deterministic bits. We note that, as in the weak secrecy case in Section 4.1, the information bits in $\mathcal{I}_1$ are distributed in both $\mathcal{I}_1^{SD}$, which can be decoded 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:

$$\begin{aligned} \mathcal{I}_2 &= \mathcal{H}_{X_R} \cap \mathcal{G}_N(W_{RD}) \cap \mathcal{B}_N(W_{RE}) \\ \mathcal{F}_2 &= \mathcal{H}_{X_R} \cap \mathcal{G}_N^c(W_{RD}) \cap \mathcal{B}_N(W_{RE}) \\ \mathcal{R}_2 &= \mathcal{H}_{X_R} \cap \mathcal{G}_N(W_{RD}) \cap \mathcal{B}_N^c(W_{RE}) \\ \mathcal{D}_2 &= \mathcal{H}_{X_R} \cap \mathcal{G}_N^c(W_{RD}) \cap \mathcal{B}_N^c(W_{RE}) \\ \mathcal{B}_2 &= \mathcal{H}_{X_R}^c. \end{aligned} \tag{49}$$

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. Additionally, we 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. As a consequence of removing the eavesdropper's degraded channel assumption, the cardinality of $\mathcal{D}_1$ and $\mathcal{D}_2$ is not $o(N)$ anymore and we must ensure that by removing the bits $\mathcal{E}_1$ and $\mathcal{E}_2$ from $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively, there is no loss in the rate. However, the preshared rate can be made very small by choosing a large enough k, i.e., $|\mathcal{D}|/kN$.

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 Figure 6.

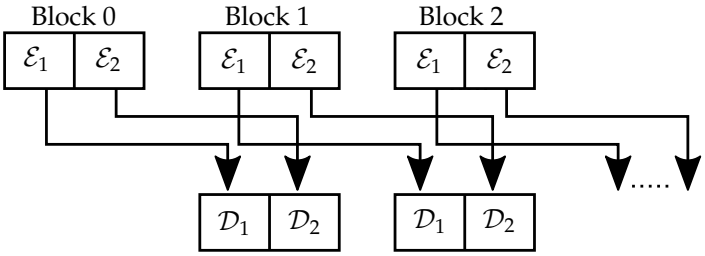

Figure 6. The double-chaining construction.

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 remaining $|\mathcal{D}_2|$ bits of $\mathcal{D}$.

Source encoding: For block $j = 1, \ldots, k$, set $\tilde{\mathcal{I}}_1$ carries the message bits; set $\mathcal{R}_1$ is filled with uniformly distributed random bits; the first $|\mathcal{D}_1|$ bits of the set $\mathcal{D}$ are chained with the bits of $\mathcal{E}_1$, i.e., $\mathcal{D}_1(j) = \mathcal{E}_1(j-1)$; the bits in $\mathcal{F}_1$ are fixed, known, and can be reused over blocks; and the bits of $\mathcal{B}_1$ are sampled from $P_{U_{i,S}|U_S^{i-1}}$. Moreover, since the source–destination link is weaker, 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 $\tilde{\mathcal{I}}_1^{RD} = \mathcal{G}(W_{SR}) \cap \mathcal{B}(W_{SD})$. Finally, as described in Section 4.2.1, let Φ_1 be the vector storing the not completely polarized bit-channels $\{i \in \mathcal{H}_{X_S}^c \cap \mathcal{G}_N^c(W_{SR})\}$, which is shared secretly between the legitimate users with some reliable error-correcting code. Figure 7 shows the coding scheme, the lines on $\mathcal{D}_2$ and $\mathcal{E}_2$ imply the first chain construction.

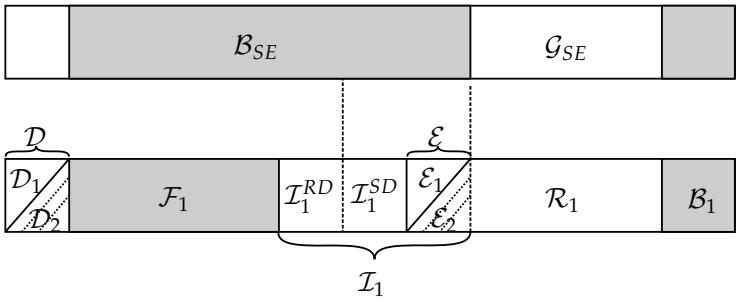

Figure 7. Index partitioning (48) at the source.

Processing at the relay: The relay decodes message block j, knowing $\mathcal{F}_1$, the seed $\mathcal{D}_1(j) = \mathcal{E}_1(j-1)$, and the bits of Φ_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 (49). Specifically,

for block $j = 1, \ldots, k$ message bits are loaded in the set $\tilde{\mathcal{I}}_2$; random bits in the set $\mathcal{R}_2$; 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 Figure 8; and the bits of $\mathcal{B}_2$ are sampled from $P_{U_{i,R}|U_R^{i-1}}$. Furthermore, let Φ_2 be the vector storing the not completely polarized bit-channels $\{i \in \mathcal{H}^c_{X_R} \cap \mathcal{G}^c_N(W_{RD})\}$, which is shared secretly with the destination using some reliable error-correcting code. The frozen set for this transmission is $\mathcal{F}_2$, which is known to the destination.

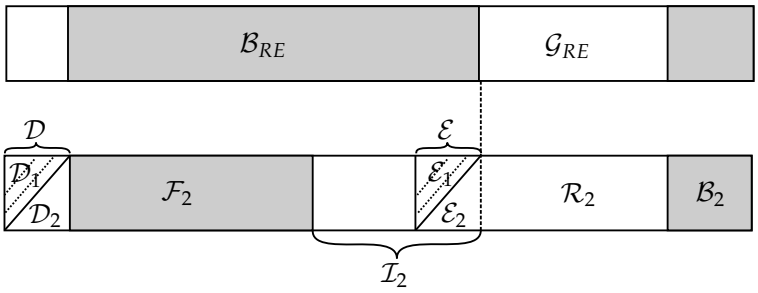

Figure 8. Index partitioning (49) at the relay.

Destination decoding: At the destination, the process starts by decoding the first block message of the relay transmission, knowing $\mathcal{F}_2$ and $\mathcal{D}_2(j) = \mathcal{E}_2(j-1)$ and the bits of Φ_2. Then, it uses those bits and the knowledge of $\mathcal{F}_1$, $\mathcal{D}_1$, and Φ_1 to decode the corresponding message block received from the source transmission at the first stage by employing the SC algorithm.

Remark 1. *The encoding scheme above requires a certain amount of shared randomness between the legitimate users. Specifically, $\mathcal{F}_1$, $\mathcal{F}_2$ are available to all users (including the eavesdropper), while $\mathcal{D}_1$, $\mathcal{D}_2$, and Φ_1, Φ_2 are known only to the legitimate users. Note that $\mathcal{F}_i$, for $i = 1, 2$, can be reused over blocks and since $|\mathcal{F}_1| + |\mathcal{F}_2| = \mathcal{O}(N)$, the rate needed can become arbitrarily small by choosing a large k. The rate of secret seed $\mathcal{D}_i$, and the rate of the not completely polarized bit-channels Φ_i, for $i = 1, 2$, can also become negligible by choosing a sufficiently large k. In general, the rate loss caused by the shared randomness is minor compared to the overall message rate.*

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 the 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 $F_{2,k}$. Further, let $E_{1,k}$ and $E_{2,k}$ correspond to the bits belonging to $\mathcal{E}_1(j)$ and $\mathcal{E}_2(j)$, respectively, for $j = 0, \ldots, k$. To make the analysis compact, we also denote $\mathbf{M}_k = (M_{1,k}, M_{2,k})$, $\mathbf{F}_k = (F_{1,k}, F_{2,k})$, $\mathbf{E}_k = (E_{1,k}, E_{2,k})$; the k-length vectors $\mathbf{M}_1^k = (\mathbf{M}_1, \ldots, \mathbf{M}_k)$, $\mathbf{F}_1^k = (\mathbf{F}_1, \ldots, \mathbf{F}_k)$, $\mathbf{E}_0^k = (\mathbf{E}_0, \ldots, \mathbf{E}_k)$; and let $\mathbf{Z}_0^k = (\mathbf{Z}_0, \ldots, \mathbf{Z}_k)$ be the sequence of eavesdropper's observations $\mathbf{Z} = (Z_{SE}, Z_{RE})$ during the k-th block transmission from source and relay.

4.2.3. Total Variation Distance and Reliability Analysis

We now analyze the proposed scheme by first examining the closeness in terms of total variation distance of the distribution induced by the encoding process and the target distribution. We would like to find an upper bound on the variation distance between these two distributions. Let $\mathbb{V}(P, Q)$ be the total variation distance and $\mathbb{D}(P||Q)$ be the

Kullback–Leibler divergence between distributions P and Q. Following the analysis of [13], we have that

$$\begin{aligned}
\mathbb{D}(P_{X_S}||Q_{X_S}) &= \mathbb{D}(P_{U_S}||Q_{U_S}) && (50)\\
&= \sum_{i=1}^{N} \mathbb{D}(P_{U_{i,S}||U_S^{i-1}}|Q_{U_{i,S}|U_S^{i-1}}) && (51)\\
&= \sum_{i\in\mathcal{H}_{X_S}} (1 - H(U_{i,S}|U_S^{i-1})) && (52)\\
&\leq \sum_{i\in\mathcal{H}_{X_S}} (1 - Z^2(U_{i,S}|U_S^{i-1})) && (53)\\
&\leq 2|\mathcal{H}_{X_S}|\delta_N \leq 2N\delta_N, && (54)
\end{aligned}$$

where (50) is due to the polar transform $X_S = U_S G_N$, (51) holds by the chain rule of KL divergence, (52) holds since the values of $\mathcal{H}_{X_S}$ are chosen uniformly, (53) follows from the inequality $Z(X|Y)^2 \leq H(X|Y)$ ([29], Proposition 2), and (54) follows by the design of $\mathcal{H}_{X_S}$. Similarly, we have

$$\mathbb{D}(P_{X_R}||Q_{X_R}) \leq 2N\delta_N. \quad (55)$$

To obtain the desired bound in terms of total variation distance between the two joint distributions, we note that

$$\begin{aligned}
\mathbb{V}(P_{X_S,X_R,Y_{SR},Y_{SD},Y_{SE},Y_{RD},Y_{RE}}, Q_{X_S,X_R,Y_{SR},Y_{SD},Y_{SE},Y_{RD},Y_{RE}}) &= \mathbb{V}(P_{X_S,X_R}, Q_{X_S,X_R}) && (56)\\
&\leq 4\sqrt{\ln 2}\sqrt{N\delta_N} \stackrel{\Delta}{=} \delta_N^{(1)}, && (57)
\end{aligned}$$

where (56) and (57) follow from [31] (Lemma 17) and Pinsker's inequality, using (54) and (55), respectively. This result indicates that the induced joint distribution is asymptotically indistinguishable from the target one.

We next examine the reliability of this scheme by estimating 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 $\epsilon_N \to 0$ used to convey the seed to the legitimate users—the probability of erroneous decoding at the relay in the $k+1$ blocks is

$$P_e^{SR} \leq \epsilon_N + k\mathcal{O}(2^{-N^\beta}), \quad (58)$$

for all $\beta < 1/2$.

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

$$P_e^{RD} \leq k\mathcal{O}(2^{-N^\beta}), \quad (59)$$

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, it can decode the source's message $\mathbf{M}_1$ using the SC algorithm. Overall, the probability of error at the destination after the second transmission is then bounded as

$$P_e \leq \epsilon_N + k\mathcal{O}(2^{-N^\beta}), \quad (60)$$

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

4.2.4. 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 analyzed as follows:

$$\begin{aligned} I(\mathbf{M}_1^k; \mathbf{Z}_0^k | \mathbf{F}_1^k) &\leq I(\mathbf{M}_1^k, \mathbf{E}_k; \mathbf{Z}_0^k | \mathbf{F}_1^k) && (61)\\ &= I(\mathbf{M}_1^k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_1^k) + I(\mathbf{M}_1^k, \mathbf{E}_k; \mathbf{Z}_0^{k-1} | \mathbf{Z}_k, \mathbf{F}_1^k) \\ &= I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_1^k) + I(\mathbf{M}_1^k, \mathbf{E}_k; \mathbf{Z}_0^{k-1} | \mathbf{Z}_k, \mathbf{F}_1^k) && (62)\\ &\leq I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_1^k) + I(\mathbf{M}_1^k, \mathbf{E}_k \mathbf{Z}_k; \mathbf{Z}_0^{k-1} | \mathbf{F}_1^k) \\ &\leq I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_1^k) + I(\mathbf{M}_1^k, \mathbf{E}_{k-1}, \mathbf{E}_k, \mathbf{Z}_k; \mathbf{Z}_0^{k-1} | \mathbf{F}_1^k) \\ &= I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_1^k) + I(\mathbf{M}_1^{k-1}, \mathbf{E}_{k-1}; \mathbf{Z}_0^{k-1} | \mathbf{F}_1^k) && (63)\\ &= I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_k) + I(\mathbf{M}_1^{k-1}, \mathbf{E}_{k-1}; \mathbf{Z}_0^{k-1} | \mathbf{F}_1^{k-1}), && (64) \end{aligned}$$

where (62) and (63) are 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. (64) is obtained by noticing that using the chain rule for mutual information, we get

$$\begin{aligned} I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_1^k) &= I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_k) + I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{F}_1^{k-1} | \mathbf{Z}_k, \mathbf{F}_k) - I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{F}_1^{k-1} | \mathbf{F}_k) && (65)\\ &= I(\mathbf{M}_k, \mathbf{E}_k; \mathbf{Z}_k | \mathbf{F}_k), && (66) \end{aligned}$$

where the last two terms equal zero, similar to the second term of (64). Next, from (61), we have the following:

$$I(\mathbf{M}_1^k; \mathbf{Z}_0^k | \mathbf{F}_1^k) \leq \sum_{j=1}^{k} I(\mathbf{M}_j \mathbf{E}_j; \mathbf{Z}_j | \mathbf{F}_1^k) + \underbrace{I(\mathbf{E}_0; \mathbf{Z}_0)}_{\epsilon_N}, \quad (67)$$

where the last term is the secret seed shared between the legitimate parties prior to the communication and we assume that there exists a secure coding scheme with $\epsilon_N \to 0$. In order to complete the proof of strong secrecy, it remains to be shown that the first term of the RHS in (67) vanishes as well. Therefore, we need to bound the capacity of the eavesdropper's channel induced by our encoding. For this purpose, we prove the following lemma.

Lemma 3. *For any $j = 1, \ldots, k$, we have*

$$I(\mathbf{M}_j, \mathbf{E}_j; \mathbf{Z}_j | \mathbf{F}_j) \leq \delta_N^{(3)},$$

where $\delta_N^{(3)} \triangleq 2N\delta_N + \delta_N^{(1)}(N - \log \delta_N^{(1)})$.

Proof. Let $\mathcal{I} = |\mathcal{I}_1| + |\mathcal{I}_2|$ with indices labeled as $\{a_1, \ldots, a_{\mathcal{I}}\}$ with $a_1 < \ldots < a_{\mathcal{I}}$; similarly, let $\mathcal{F} = |\mathcal{F}_1| + |\mathcal{F}_2|$ and label the indices as $\{b_1, \ldots, b_{\mathcal{F}}\}$ with $b_1 < \ldots < b_{\mathcal{F}}$. Moreover, let $\mathcal{S} = \mathcal{I} + \mathcal{F}$ with labels $\{c_1, \ldots, c_{\mathcal{S}}\}$ and assume that $c_1 < \ldots < c_{\mathcal{S}}$.

$$\begin{aligned} I(\mathbf{M}_j, \mathbf{E}_j; \mathbf{Z}_j | \mathbf{F}_j) &= H(\mathbf{M}_j, \mathbf{E}_j | \mathbf{F}_j) - H(\mathbf{M}_j, \mathbf{E}_j | \mathbf{Z}_j, \mathbf{F}_j) \\ &= H(\mathbf{M}_j, \mathbf{E}_j) - H(\mathbf{M}_j, \mathbf{E}_j, \mathbf{F}_j | \mathbf{Z}_j) + H(\mathbf{F}_j | \mathbf{Z}_j) \\ &= \sum_{i=1}^{\mathcal{I}} H(T_{a_i} | T^{a_1}, \ldots, T_{a_{i-1}}) - \sum_{i=1}^{\mathcal{S}} H(T_{c_i} | \mathbf{Z}_j, T_{c_1}, \ldots, T_{c_{i-1}}) + \sum_{i=1}^{\mathcal{F}} H(T_{b_i} | \mathbf{Z}_j, T_{b_1}, \ldots, T_{b_{i-1}}) \\ &\leq \sum_{i=1}^{\mathcal{S}} (1 - H(T_{c_i} | \mathbf{Z}_j, T^{c_{i-1}})), && (68) \end{aligned}$$

where (68) is due to the fact that conditioning reduces entropy. Considering the entropy term in (68) and noticing that it is derived under the induced distribution of the coding scheme, we would like to find the distance between the induced entropy and the entropy under the target distribution $\tilde{H}(T_{c_i}|\mathbf{Z}_j, T^{c_{i-1}})$, where $\tilde{H}$ denotes the entropy under the target distribution P_{X^N,Z^N}. First, using the inequality $Z(X|Y)^2 \leq H(X|Y)$ ([29], Proposition 2), we get that

$$\begin{aligned}\tilde{H}(T_{c_i}|\mathbf{Z}_j, T^{c_{i-1}}) &\geq Z(T_{c_i}|\mathbf{Z}_j, T^{c_{i-1}})^2 \\ &\geq 1 - 2\delta_N. \end{aligned} \tag{69}$$

To estimate the distance, we rely on Th. 17.3.3 [32], and we have

$$|H(T_{c_i}|\mathbf{Z}_j, T^{c_{i-1}}) - \tilde{H}(T_{c_i}|\mathbf{Z}_j, T^{c_{i-1}})| \leq \mathbb{V}(P_{X^N,Z^N}, Q_{X^N,Z^N}) \times \log \frac{2^N}{\mathbb{V}(P_{X^N,Z^N}, Q_{X^N,Z^N})} \tag{70}$$

$$\leq \delta_N^{(1)}(N - \log \delta_N^{(1)}) \stackrel{\Delta}{=} \delta_N^{(2)}, \tag{71}$$

where (71) follows from (57) and the fact that $f(x) = x(N - \log x)$ is increasing for $0 < x < 1$.

Thus, from (68), (69), and (71), we conclude that

$$I(\mathbf{M}_j, \mathbf{E}_j; \mathbf{Z}_j|\mathbf{F}_j) \leq 2N\delta_N + \delta_N^{(2)} \stackrel{\Delta}{=} \delta_N^{(3)}. \tag{72}$$

□

Finally, combining Lemma 3 and (67), we get the desired result:

$$I(\mathbf{M}_1^k; \mathbf{Z}_0^k|\mathbf{F}_1^k) \leq I(\mathbf{M}_1^k\mathbf{E}_k; \mathbf{Z}_0^k|\mathbf{F}_1^k) \leq \epsilon_N + k\delta_N^{(3)}, \tag{73}$$

where, for k fixed and $N \to \infty$, we observe that $I(\mathbf{M}_1^k; \mathbf{Z}_0^k|\mathbf{F}_1^k)$ 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

$$R_s^{strong} = \frac{k}{k+1}[R^{DF} - (I(W_{SE}) + I(W_{RE})) - 2\Delta], \tag{74}$$

as N grows large and by choosing k to be large enough, where 2Δ is a vanishing small rate penalty induced by the double-chaining structure and the shared seed. Undoubtedly, designing a coding scheme that takes into account reliability and secrecy as requirements, a trade-off between achievable rate and secrecy is introduced. In our scheme (Although we are discussing the strong secrecy encoding scheme, the same applies for the scheme of Section 4.1, where the rate loss is lower due to the absence of the double-chaining construction). the random bits and the bits allocated to convey the misaligned indices are the factors that mean the achievable secret rate is lower than the R^{DF}, which is the lower bound without secrecy constraints. To reduce this loss and attain a higher achievable rate, a line of work exists that proposes a cross-layer security scheme, which combines information-theoretic security with classical encryption mechanisms [33,34].

5. Conclusions

The construction of practical coding schemes for information-theoretic security is of great significance. In this work, we have proposed an efficient coding scheme based on polar codes for the primitive relay wiretap channel, which guarantees a level of 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 that achieves reliability and weak secrecy, but fails to provide strong secrecy. Through 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, without any assumption regarding symmetry and the eavesdropper's channel condition. Moreover, in our strong secrecy scheme, we considered a simplified mechanism that only requires a vanishing rate of shared randomness, instead of sharing random mappings that may heavily increase the storage complexity. Finally, as en extra functionality, a "smart" relay is added, where an erroneous detector at the relay's decoder operates to reduce the error probability while the complexity remains the same.

Author Contributions: Writing—original draft preparation, formal analysis, conceptualization, methodology, M.A.; supervision, writing—review and editing, G.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by Greece and the European Union (European Social Fund- ESF) through the Operational Programme "Human Resources Development, Education and Lifelong Learning" in the context of the project "Strengthening Human Resources Research Potential via Doctorate Research" (MIS-5000432), implemented by the State Scholarships Foundation (IKY).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
2. Van der Meulen, E.C. Three-terminal communication channels. *Adv. Appl. Probab.* **1971**, *3*, 120–154. [CrossRef]
3. Cover, T.; Gamal, A.A.E. Capacity theorems for the relay channel. *IEEE Trans. Inf. Theory* **1979**, *25*, 572–584. [CrossRef]
4. Lai, L.; Gamal, H.E. The Relay-Eavesdropper Channel: Cooperation for Secrecy. *IEEE Trans. Inf. Theory* **2008**, *54*, 4005–4019. [CrossRef]
5. Yuksel, M.; Erkip, E. The relay channel with a wire-tapper. In Proceedings of the 2007 41st Annual Conference on Information Sciences and Systems, Baltimore, MD, USA, 14–16 March 2007; pp. 13–18.
6. Kim, Y.H. Coding techniques for primitive relay channels. In Proceedings of the 2007 Allerton Conference on Communication, Control, Computing, Monticello, IL, USA, 26–28 September 2007; pp. 129–135.
7. Aggarwal, V.; Sankar, L.; Calderbank, A.R.; Poor, H.V. Secrecy capacity of a class of orthogonal relay eavesdropper channels. In Proceedings of the 2009 Information Theory and Applications Workshop, San Diego, CA, USA, 8–14 February 2009; pp. 295–300.
8. Arikan, E. Channel Polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 3051–3073. [CrossRef]
9. Mahdavifar, H.; Vardy, A. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Trans. Inf. Theory* **2011**, *57*, 6428–6443. [CrossRef]
10. Sasoglou, E.; Vardy, A. A New Polar Coding Scheme for Strong Security on Wiretap Channels. In Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013; pp. 1117–1121.
11. Gulcu, T.; Barg, A. Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component. *IEEE Trans. Inf. Theory* **2017**, *63*, 1311–1324. [CrossRef]
12. Wei, Y.P.; Ulukus, S. Polar Coding for the General Wiretap Channel With Extensions to Multiuser Scenarios. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 278–291.
13. Chou, R.A.; Bloch, M. Polar Coding for the Broadcast Channel With Confidential Messages: A Random Binning Analogy. *IEEE Trans. Inf. Theory* **2016**, *62*, 2410–2429. [CrossRef]
14. Blasco-Serrano, R.; Thobanen, R.; Andersson, M.; Rathi, V.; Skoglund, M. Polar codes for cooperative relaying. *IEEE Trans. Commun.* **2012**, *60*, 3263–3273. [CrossRef]
15. Karas, D.S.; Pappi, K.N.; Karagiannidis, G. Smart Decode-and-Forward Relaying with Polar Codes. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 62–65. [CrossRef]
16. Wang, L. Polar Coding for the Relay Channels. In Proceedings of the 2015 IEEE International Symposium on Information Theory, Hong Kong, China, 14–19 June 2015; pp. 1532–1536.
17. Andersson, M.; Rathi, V.; Thobaben, R.; Kliewer, J.; Skoglund, M. Nested polar codes for wiretap and relay channels. *IEEE Wirel. Commun. Lett.* **2010**, *14*, 752–754. [CrossRef]
18. Mondelli, M.; Hassani, S.H.; Urbanke, R. A new Coding Paradigm for the Primitive Relay Channel. In Proceedings of the 2018 IEEE International Symposium on Information Theory, Vail, CO, USA, 17–22 June 2018; pp. 351–355.
19. Duo, B.; Wang, P.; Li, Y.; Vucetic, B. Secure Transmission for Relay-Eavesdropper Channels Using Polar Coding. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 2197–2202.

20. Athanasakos, M.; Karagiannidis, G. Strong Secrecy for Relay Wiretap Channels with Polar Codes and Double-Chaining. In Proceedings of the 2020 IEEE Global Communications Conference—GLOBECOM, Taipei, Taiwan, 7–11 December 2020.
21. Hassani, S.H.; Urbanke, R. Universal polar codes. In Proceedings of the IEEE International Symposium on Information Theory, Honolulu, HI, USA, 29 June–4 July 2014; pp. 1451–1455.
22. Honda, J.; Yamamoto, H. Polar coding without alphabet extension for assymetric models. *IEEE Trans. Inf. Theory* **2013**, *59*, 7829–7838. [CrossRef]
23. Chou, R.; Bloch, M. Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes. In Proceedings of the Annual Allerton Conference on Communication Control and Computing, Monticello, IL, USA, 29 September–2 October 2015.
24. del Olmo Alòs, J.; Fonollosa, J.R. Polar Coding for Confidential Broadcasting. *Entropy* **2020**, *22*, 149. [CrossRef] [PubMed]
25. Arikan, E.; Telatar, E. On the rate of Channel Polarization. In Proceedings of the 2009 IEEE International Symposium on Information Theory, Seoul, Korea, 28 June–3 July 2009; pp. 1493–1495.
26. Korada, S.B.; Urbanke, R.L. Polar codes are optimal for lossy source coding. *IEEE Trans. Inf. Theory* **2010**, *56*, 1751–1768. [CrossRef]
27. Korada, S.B. Polar Codes for Channel and Source Coding. Ph.D. Thesis, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2009.
28. Mauerer, U.M.; Wolf, S. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology—Eurocrypt 2000*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2000; pp. 351–368.
29. Arikan, E. Source polarization. In Proceedings of the IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 899–903.
30. Gad, E.E.; Li, Y.; Kliewer, J.; Langberg, M.; Jiang, A.A.; Bruck, J. Asymmetric error correction and flash-memory rewriting using polar codes. *IEEE Trans. Inf. Theory* **2016**, *62*, 4024–4038. [CrossRef]
31. Cuff, P.W. Communication in Networks for Coordinating Behavior. Ph.D. Thesis, Stanford University, Stanford, CA, USA, 2009.
32. Cover, T.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; Wiley: Hoboken, NJ, USA, 2006.
33. Wu, F.; Xing, C.; Zhao, S.; Gao, F. Encrypted polar codes for wiretap channel. In Proceedings of the 2012 2nd International Conference on Computer Science and Network Technology, Changchun, China, 29–31 December 2012; Volume 1, pp. 579–583.
34. Zhao, Y.; Zou, X.; Lu, Z.; Liu, Z. Chaotic Encrypted Polar Coding Scheme for General Wiretap Channel. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2017**, *25*, 3331–3340. [CrossRef]