Polar Codes for Covert Communications over Asynchronous Discrete Memoryless Channels

Guillaume Frèche, Matthieu Bloch, Michel Barret

entropy

MDPI

Article

Polar Codes for Covert Communications over Asynchronous Discrete Memoryless Channels

Guillaume Frèche [1,2,3], Matthieu R. Bloch [1,2,*] and Michel Barret [1,3]

1 UMI 2958 Georgia Tech-CNRS, 57070 Metz, France; grfreche@gmail.com (G.F.); Michel.Barret@centralesupelec.fr (M.B.)
2 School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA
3 CentraleSupélec, 57070 Metz, France
* Correspondence: matthieu.bloch@ece.gatech.edu; Tel.: +1-404-485-3825

Received: 7 August 2017; Accepted: 14 November 2017; Published: 22 December 2017

Abstract: This paper introduces an explicit covert communication code for binary-input asynchronous discrete memoryless channels based on binary polar codes, in which legitimate parties exploit uncertainty created by both the channel noise and the time of transmission to avoid detection by an adversary. The proposed code jointly ensures reliable communication for a legitimate receiver and low probability of detection with respect to the adversary, both observing noisy versions of the codewords. Binary polar codes are used to shape the weight distribution of codewords and ensure that the average weight decays as the block length grows. The performance of the proposed code is severely limited by the speed of polarization, which in turn controls the decay of the average codeword weight with the block length. Although the proposed construction falls largely short of achieving the performance of random codes, it inherits the low-complexity properties of polar codes.

Keywords: physical-layer security; covert communication; polar codes

1. Introduction

Following the proof of existence of a "square root law" [1] for covert communication, several works have revisited the problem of communicating while ensuring a low probability of detection by an adversary. The square root law essentially states that, under mild conditions about the channel, covert communication is possible if and only if the number of message bits scales as the square root of the block length. The exact information-theoretic limits of covert communication over point-to-point Discrete Memoryless Channels (DMCs) and Gaussian channels are now known [2–4], and for models relaxing assumptions regarding channel knowledge and synchronicity, the square root law can be circumvented [5,6]. Despite recent results showing, through a random coding argument, the existence of low-complexity covert codes using a concatenated scheme [7], i.e., codes ensuring covert communication with an encoding and decoding complexity that only scale *linearly* with the block length, no explicit low-complexity constructions are known to date.

As highlighted in [3], the coding mechanism behind covert communication may be linked to the concept of *channel output approximation* [8], which allows us to leverage recent error control coding approaches to secrecy exploiting similar ideas [9]. However, the main challenge faced when designing explicit instantiations of covert codes is the control of the codeword weight distribution, whose average weight should scale *sub-linearly* with the block-length [2–4].

In this paper, we develop a polar-code based covert code for the asynchronous covert communication model of [6]. The choice of polar codes is motivated by their low-complexity and capacity-achieving properties [10], which have already proved useful in the context of channel resolvability [11]. Existing results, however, do not directly apply to covert communications since the

average codeword weight must decay with the block length. We address this issue by first adapting the finite-length analysis of channel polarization [12,13] to source polarization and then analyzing the tension between the speed of polarization and the decay of the average codeword weight.

The remainder of the paper is organized as follows. Section 2 formally introduces the model of covert communication and presents our main contributions. Section 3 establishes several preliminary technical lemmas concerning the polarization of sources with vanishing entropy. Section 4 describes the proposed polar-coding scheme for covert communications and analyzes its performance. Section 5 concludes the paper with a discussion of extensions and possible improvements.

2. Asynchronous Covert Communication Model and Results

2.1. Notation

Before describing the asynchronous covert communication model, we briefly introduce the notation used throughout the paper. Random variables are denoted by upper case letters, e.g., X, and their realizations by lower case letters, e.g., x. Sets are denoted with calligraphic fonts, e.g., $\mathcal{X}$. Vectors of length n are denoted as $X^{1:n} = (X_1, \cdots, X_n)$ and $x^{1:n} = (x_1, \cdots, x_n)$ when the length needs to be explicit, and by boldface fonts, e.g., $\mathbf{X}$ and $\mathbf{x}$, when the length can be inferred from the context without ambiguity. When multiple blocks of length n are used, we denote the block index as a subscript, e.g, $X_{1:b}^{1:n}$ denotes a sequence of b blocks of length n. The function log is understood in the base 2, while ln denotes the logarithm to the base e. For two distributions P, Q on some countable set $\mathcal{X}$, we write the Kullback–Leibler divergence and the total variation distance as

$$\mathbb{D}(P\|Q) \triangleq \sum_{x\in\mathcal{X}} P(x) \log \frac{P(x)}{Q(x)} \quad \text{and} \quad \mathbb{V}(P,Q) \triangleq \frac{1}{2} \sum_{x\in\mathcal{X}} |P(x) - Q(x)|,$$

respectively. We also denote $P^{\otimes n}(\mathbf{x})$ as the product distribution $\prod_{i=1}^{n} P(x_i)$ for $\mathbf{x} \in \mathcal{X}^n$.

We make repeated use of the Landau notation. In particular, for two real-valued functions $f(n)$ and $g(n)$ of $n \in \mathbb{N}$, we write $f(n) = o\left(g(n)\right)$ if $\forall \alpha > 0\ \exists n_0 \in \mathbb{N}^*$ such that $\forall n \geq n_0\ |f(n)| \leq \alpha\, |g(n)|$; $f(n) = O\left(g(n)\right)$ if $\exists \alpha > 0\ \exists n_0 \in \mathbb{N}^*$ such that $\forall n \geq n_0\ |f(n)| \leq \alpha\, |g(n)|$; $f(n) = \omega\left(g(n)\right)$ if $\forall \alpha > 0$ $\exists n_0 \in \mathbb{N}^*$ such that $\forall n \geq n_0\ |f(n)| \geq \alpha\, |g(n)|$.

The polarization kernel matrix $G_2 = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ will be merely denoted G. We denote $G^{\otimes \nu}$ the matrix representing the recursive transformation over ν levels of polarization. Thus, the corresponding polar code is of length $n = 2^\nu$. Since the length of binary polar codes is a power of two, we restrict our attention to block lengths $n \in \mathbb{D} \triangleq \{2^\nu : \nu \in \mathbb{N}^*\}$.

2.2. Channel Model

The channel model for covert communication is illustrated in Figures 1 and 2. A legitimate transmitter (Alice) attempts to reliably communicate to a legitimate receiver (Bob) over a DMC $(\mathcal{X}, W_{Y|X}, \mathcal{Y})$, while avoiding detection from an adversary (Willie) who observes signals through another DMC $(\mathcal{X}, W_{Z|X}, \mathcal{Z})$. In the remainder of the paper, we restrict our attention to a binary input alphabet $\mathcal{X} = \{0, 1\}$, with 0 representing the innocent input symbol in the absence of communication. We denote $P_0 \triangleq W_{Y|X=0}$ and $Q_0 \triangleq W_{Z|X=0}$ as the output distributions induced by the innocent symbol 0. Similarly, we denote $P_1 \triangleq W_{Y|X=1}$ and $Q_1 \triangleq W_{Z|X=1}$ as the output distributions induced by symbol 1. We assume that both P_1 and Q_1 are absolutely continuous with respect to (w.r.t.) P_0 and Q_0, respectively, to avoid the special situations discussed in Appendix V of [3].

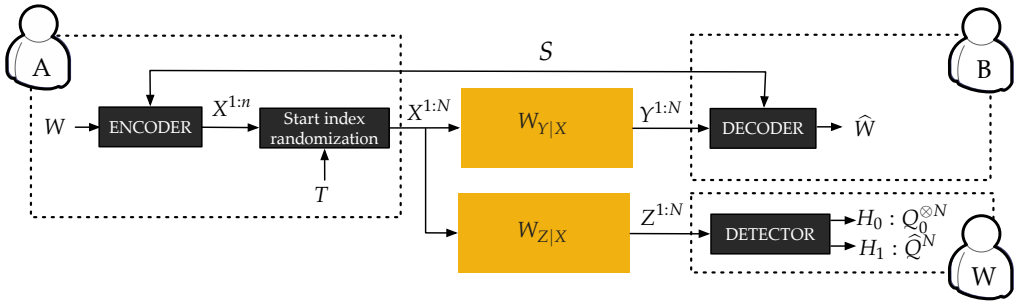

Figure 1. Model of covert communication.

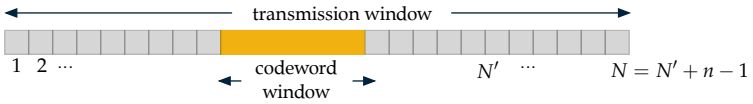

Figure 2. Asynchronous covert communication.

Formally, a message $W \in [\![1, M_n]\!]$ with uniform distribution is encoded into a codeword of length n, possibly with the help of secret key $S \in [\![1, K_n]\!]$ only known to Alice and Bob but using a public codebook known to all parties; the codeword is hidden within a larger *transmission window* of size $N > n$, with N a function of n, by choosing the starting index T of the codeword uniformly at random between 1 and $N' \triangleq N - n + 1$. The set of indices corresponding to the codeword forms the *codeword window*. The sequence transmitted during the transmission window is denoted $X^{1:N}$, and the corresponding observations of Bob and Willie are denoted $Y^{1:N}$ and $Z^{1:N}$, respectively. It is convenient to introduce the following distributions. The distribution induced at the output of the adversary's channel in a codeword window is denoted $\widehat{Q}^n$. When the codeword is embedded in a transmission window starting at a known index t, the distribution induced at the output of the adversary's channel in the transmission window is

$$\widehat{Q}_t^N(\mathbf{z}) = \prod_{k=1}^{t-1} Q_0(z_k) \prod_{k=t}^{t+n-1} \widehat{Q}^n(z_k) \prod_{k=t+n}^{N} Q_0(z_k). \tag{1}$$

Finally, the distribution induced at the output of the adversary's channel in the transmission window when *randomizing* the start index T is $\widehat{Q}^N \triangleq \mathbb{E}_T\left(\widehat{Q}_T^N\right)$.

Given the secret key S and the observation $Y^{1:N}$, Bob forms an estimate $\widehat{W}$ of the original message W, whose performance is measured by the probability of error $P_e^{(n)} \triangleq \mathbb{E}_S\left(\mathbb{P}\left(\widehat{W} \neq W|S\right)\right)$. Given the observation $Z^{1:N}$ and the knowledge of Alice's codebook, Willie performs a hypothesis test to determine if communication took place. Hypothesis H_0 corresponds to the absence of communication, in which case the distribution of $Z^{1:N}$ is $Q_0^{\otimes N}$; Hypothesis H_1 corresponds to communication, in which case the distribution induced by the code is $\widehat{Q}^N$ over the transmission window. Note that $\widehat{Q}^N$ can be computed using knowledge of the codebook and the distribution of T. The covertness of the transmission is measured by the total variation $V^{(n)} \triangleq \mathbb{V}\left(\widehat{Q}^N, Q_0^{\otimes N}\right)$. A small value of $V^{(n)}$ ensures that the best binary hypothesis test is not significantly better than a "blind" test that would ignore the observation $Z^{1:N}$ [3].

Our objective is to construct sequences of codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$ and $\lim_{n\to\infty} V^{(n)} = 0$.

2.3. Main Results

We start by recalling a known result established with a random coding argument, which serves as a benchmark for our code construction.

Proposition 1 (adapted from [6]). *Consider sequences of positive numbers* $\{\alpha_n\}_{n\in\mathbb{N}^*}$, $\{\beta_n\}_{n\in\mathbb{N}^*}$ *such that* $\alpha_n \in \omega\left(\frac{1}{\sqrt{n}}\right) \cap o(1)$, $\beta_n = \omega\left(2^{-\frac{n\alpha_n}{\log n}}\right) \cap o(1)$ *as* n *goes to infinity. Let* $N = \frac{2^{n\alpha_n^2}}{\beta_n \alpha_n^2}$. *There exist codes of increasing block length* n *hidden in transmission windows of size* N *such that*

$$\begin{aligned}
\lim_{n\to\infty} \frac{\log M_n}{n\alpha_n} &\geq \mathbb{D}(P_1\|P_0) \\
\lim_{n\to\infty} \frac{\log K_n}{n\alpha_n} &\leq [\mathbb{D}(Q_1\|Q_0) - \mathbb{D}(P_1\|P_0)]^+ \\
\lim_{n\to\infty} P_e^{(n)} &= 0 \\
\lim_{n\to\infty} V^{(n)} &= 0.
\end{aligned}$$

Proposition 1 states that the number of bits $\log M_n$ scales as $n\alpha_n$ with a constant pre-factor at least equal to $\mathbb{D}(P_1\|P_0)$ for all admissible choices of α_n. As α_n increases, so does the scaling of $\log M_n$, but at the expense of increasingly larger monitoring windows. Proposition 1 captures the correct scaling for the transmission window size, the number of message bits, and the number of key bits with the block length n, as shown by the converse proof in [5]. While this result has been obtained with a random coding argument, in which codewords are sampled independently according to product distributions, the main contribution of the present paper is to establish a similar result using polar codes in place of random codes.

In the following, we allow ourself a slight modification of the coding scheme defined in Section 2.2 to consider b_n consecutive transmission windows of size N, where b_n will be specified later. The messages and keys used in the transmission windows might be dependent, but the codeword in each of them is otherwise created as defined earlier. The probability of error $P_e^{(n)}$ is appropriately modified to consider the set of messages $\{W_i\}_{i=1}^{b_n}$ as

$$P_e^{(n)} = \mathbb{P}\left(\{\widehat{W}_i\}_{i=1}^{b_n} \neq \{W_i\}_{i=1}^{b_n}\right), \tag{2}$$

and $V^{(n)}$ considers the distribution induced over the b_n consecutive transmission windows

$$V^{(n)} = \mathbb{V}\left(\widehat{Q}^{b_n N}, Q_0^{\otimes b_n N}\right). \tag{3}$$

Our results also depend on a constant κ, whose value results from the analysis of finite length polarization and is further discussed in Section 3.

Proposition 2. *There exists a constant* $\kappa \in]0, \frac{1}{2}[$, *such that for all sequences of positive numbers* $\{\alpha_n\}_{n\in\mathbb{D}} \in \omega\left(\frac{1}{n^\kappa}\right) \cap o(1)$, $\{\beta_n\}_{n\in\mathbb{D}} \in \omega\left(2^{-\frac{n\alpha_n}{\log n}}\right) \cap o\left(\frac{1}{\log n}\right)$, *and sequence of integers* $\{b_n\}_{n\in\mathbb{D}} \in \omega(\log n) \cap o\left(\frac{1}{\beta_n}\right) \cap o(n)$ *as* n *goes to infinity, there exist low-complexity polar-code based schemes operating over* b_n *transmission windows of size* $N = \frac{2^{n\alpha_n^2}}{\beta_n\alpha_n^2}$, *each embedding a codeword window of length* n, *with*

$$\begin{aligned}
\lim_{n\in\mathbb{D}\to\infty} \frac{\log M_n}{n b_n \alpha_n} &\geq \mathbb{D}(P_1\|P_0), \\
\lim_{n\in\mathbb{D}\to\infty} \frac{\log K_n}{n b_n \alpha_n} &\leq [\mathbb{D}(Q_1\|Q_0) - \mathbb{D}(P_1\|P_0)]^+, \\
\lim_{n\in\mathbb{D}\to\infty} P_e^{(n)} &= 0, \\
\lim_{n\in\mathbb{D}\to\infty} V^{(n)} &= 0.
\end{aligned}$$

Proof. See Section 4. □

The constant κ in the statement of Proposition 2 is more precisely identified in Proposition 3. The precise code construction behind the statement is provided in Section 4, and the exact encoding and decoding algorithms are given in Algorithms 1 and 2 in Section 4.2. The complexity of both algorithms scales linearly with the number of transmission windows b_n and as $n \log n$ with the codeword length n. Note that Proposition 2 differs from Proposition 1 on two accounts. First, the polar-code based scheme only holds for a limited range of scalings for α_n. A numerical investigation suggests that κ is on the order of 10^{-3}, which completely precludes our codes from operating in the square-root law regime and requires absurdly large code length; however, if one backs away from the optimal scalings identified above, our approach does provide a low-complexity construction with provable guarantees. As further discussed in Section 3, this results from our inability to establish a faster polarization speed. In particular, as will be clear from our analysis, we rely on a fine polarization result from [12] to show that covertness holds, and the value of κ is therefore much more constrained than what would be expected by only looking at the inverse scaling exponent [14,15]. Our results might be improved by considering a "moderate deviation regime" in the same spirit as [14], but this would require a non-trivial extension of existing results, which we defer to future work. Second, the proposed scheme requires a chaining over b_n transmission windows; we shall see in Section 4 that the chaining allows us to "realign" polarization sets. Although this chaining does not fall into the exact situation of Section 2.2 in which a single block is considered, covertness is guaranteed over the *entire* chain of blocks; in addition, a mild scaling such as $b_n = \omega(\log n)$ is valid so that the number of blocks may be much smaller than the block-length. Finally, the proposed code construction is non-trivial, but its performance is still far from that of the random codes in Proposition 1. Section 5 discusses several ongoing efforts to improve performance.

Algorithm 1 Alice's encoder

Require:
Vector C of $|\mathcal{V}_C|$ uniformly distributed key bits;
b_n vectors $\{W_i\}_{i=1,b_n}$ of $|\mathcal{V}_W|$ uniformly distributed message bits;
b_n vectors $\{W'_i\}_{i=1,b_n}$ of $|\mathcal{V}_{W'}|$ uniformly distributed message bits;
Vector S_1 of $|\mathcal{V}_S| + |\mathcal{V}_{S'}|$ uniformly distributed key bits;
$b_n - 1$ vectors $\{S_i\}_{i=2,b_n}$ of $|\mathcal{V}_S|$ uniformly distributed key bits;
b_n vectors $\{S'_i\}_{i=1,b_n}$ of $|\mathcal{V}_{C'}|$ uniformly distributed key bits;
b_n vectors $\{S''_i\}_{i=1,b_n}$ of $\log N$ uniformly distributed key bits;

for block $i = 1$ to b_n **do**
  $\widetilde{U}_i^{1:n}[\mathcal{V}_C] \leftarrow C$
  $\widetilde{U}_i^{1:n}[\mathcal{V}_W] \leftarrow W_i$
  $\widetilde{U}_i^{1:n}[\mathcal{V}_{W'}] \leftarrow W'_i$
  if $i = 1$ **then**
    $\widetilde{U}_i^{1:n}[\mathcal{V}_S] \leftarrow S_1$
  else
    $\widetilde{U}_i^{1:n}[\mathcal{V}_{S'}] \leftarrow W'_{i-1}$
    $\widetilde{U}_i^{1:n}[\mathcal{V}_S] \leftarrow S_i$
  end if
  Successively draw the components of $\widetilde{U}_i^{1:n}$ in $\mathcal{V}_X^c$ according to

$$\forall j \in \mathcal{V}_X^c \qquad \tilde{p}_{U_i^j|U_i^{1:j-1}}\left(u_i^j|\widetilde{U}_i^{1:j-1}\right) \triangleq q_{U^j|U^{1:j-1}}\left(u_i^j|\widetilde{U}_i^{1:j-1}\right) \tag{4}$$

  Transmit $\widetilde{X}_i^{1:n} \triangleq \widetilde{U}_i^{1:n} G^{\otimes \nu}$ over the channel $W_{Y|X}$, which gives the output $\widetilde{Y}_i^{1:n}$, and over the channel $W_{Z|X}$, which gives the output $\widetilde{Z}_i^{1:n}$. Assume that $C'_i \oplus S'_i \triangleq \widetilde{U}_i^{1:n}[\mathcal{V}_{C'}]$ is made available at the decoder. Randomize the position of the codeword window using S''_i
end for

Algorithm 2 Bob's decoder

Require:
Vector C of $|\mathcal{V}_C|$ uniformly distributed key bits;
Vector S_1 of $|\mathcal{V}_S| + |\mathcal{V}_{S'}|$ uniformly distributed key bits;
$b_n - 1$ vectors $\{S_i\}_{i=2,b_n}$ of $|\mathcal{V}_S|$ uniformly distributed key bits;
b_n vectors $\{S'_i\}_{i=1,b_n}$ of $|\mathcal{V}_{C'}|$ uniformly distributed key bits;
b_n vectors $\{S''_i\}_{i=1,b_n}$ of $\log N$ uniformly distributed key bits;
b_n vectors $\{C'_i \oplus S'_i\}_{i=1,b_n}$ of $|\mathcal{V}_{C'}|$ made available;
Form an estimate $\widehat{X}_1^{1:n}$ of $\widetilde{X}_1^{1:n}$ from $(C, S_1, C'_1, \widetilde{Y}_1^{1:n})$
Form the estimate $\widehat{U}_1^{1:n} = \widehat{X}_1^{1:n} G^{\otimes \nu}$
$\widehat{W}_1 \leftarrow \widehat{U}_1^{1:n}[\mathcal{V}_W]$
$\widehat{W}'_1 \leftarrow \widehat{U}_1^{1:n}[\mathcal{V}_{W'}]$
for block $i = 2$ to b_n **do**
    Form an estimate $\widehat{X}_i^{1:n}$ of $\widetilde{X}_i^{1:n}$ from $(C, \widehat{W}'_{i-1}, S_i, C'_i, \widetilde{Y}_i^{1:n})$
    Form the estimate $\widehat{U}_i^{1:n} = \widehat{X}_i^{1:n} G^{\otimes \nu}$
    $\widehat{W}_i \leftarrow \widehat{U}_i^{1:n}[\mathcal{V}_W]$
    $\widehat{W}'_i \leftarrow \widehat{U}_i^{1:n}[\mathcal{V}_{W'}]$
end for

3. Preliminaries: Polarization of Sources with Vanishing Entropy Rate

Our code construction exploits recent results on polar codes that suggest how information-theoretic proofs exploiting source coding with side information and privacy amplification as primitives [16,17] may be converted into polar coding schemes by a suitable identification of polarization sets [11,18]. Specifically, the approach consists in recognizing that both primitives have counterparts based on polar codes, see Lemma 3 and Lemma 4 of [11], as well as [19,20]. Before we pursue a similar approach here, we must first extend Lemmas 3 and 4 of [11] to the case relevant for covert communications.

Formally, consider the sequences of positive numbers $\{\alpha_n\}_{n\in\mathbb{D}}$ such that $\alpha_n \in \omega\left(\frac{1}{\sqrt{n}}\right) \cap o(1)$. For every $n \in \mathbb{D}$, define the Bernoulli distribution Π_{α_n} over $\{0,1\}$ as $\Pi_{\alpha_n}(1) = 1 - \Pi_{\alpha_n}(0) = \alpha_n$ and its associated product distribution

$$\Pi_{\alpha_n}^{\otimes n}(\mathbf{x}) = \prod_{i=1}^{n} \Pi_{\alpha_n}(x_i). \tag{5}$$

Define the joint distribution of sequences in $\mathcal{X}^n \times \mathcal{Y}^n$

$$q_{X^{1:n}Y^{1:n}}(\mathbf{x}, \mathbf{y}) \triangleq \Pi_{\alpha_n}^{\otimes n}(\mathbf{x}) W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}), \tag{6}$$

with $W_{Y|X}$ defined in Section 2.2. In other words, for a fixed n, the process $X^{1:n}Y^{1:n}$ has a product distribution but the process $\{X^{1:n}Y^{1:n}\}_{n\in\mathbb{D}}$ is not stationary and the entropy rate $\frac{1}{n}H(X^{1:n}|Y^{1:n})$ vanishes. We refer to such a source as a "vanishing entropy rate source". Assume now that the random vector $X^{1:n} \in \mathcal{X}^n$ is transformed into $U^{1:n} = X^{1:n}G^{\otimes\nu}$. For $\delta_n \in]0, \frac{1}{2}[$, the set of high entropy bits is defined as

$$\mathcal{H}_{X|Y}(\delta_n) \triangleq \left\{ i \in [\![1,n]\!] : H\left(U_i | U^{1:i-1} Y^{1:n}\right) > \delta_n \right\}, \tag{7}$$

and the set of very high entropy bits is defined as

$$\mathcal{V}_{X|Y}(\delta_n) \triangleq \left\{ i \in [\![1,n]\!] : H\left(U_i | U^{1:i-1} Y^{1:n}\right) > 1 - \delta_n \right\} \tag{8}$$

The following proposition shows that the sets $\mathcal{H}_{X|Y}$ and $\mathcal{V}_{X|Y}$ can still polarize for vanishing entropy rate sources.

Proposition 3 (Fine polarization of vanishing entropy sources). *For any $\delta \in \left[0\,,\,\frac{1}{2}\right]$, set $\delta_n = 2^{-n^\delta}$. For any $\varepsilon \in [0\,,\,1-2\delta]$, there exists $\kappa_{\delta,\varepsilon} > 0$, $A_{\delta,\varepsilon} > 0$ and $C_{\delta,\varepsilon}$ such that for any vanishing entropy rate source $q_{X^{1:n}Y^{1:n}}(\mathbf{x},\mathbf{y})$ as in (6) and for any integer $n \in \mathbb{D}$ with $n > 2^{C_{\delta,\varepsilon}}$, we have*

$$0 \;\leq\; \frac{\left|\mathcal{H}_{X|Y}(\delta_n) \cap \mathcal{V}_{X|Y}(\delta_n)^c\right|}{n} \leq \frac{A_{\delta,\varepsilon}}{n^{\kappa_{\delta,\varepsilon}\varepsilon}} \tag{9}$$

$$\frac{1}{n}H\left(X^{1:n}|Y^{1:n}\right) - \delta_n \;\leq\; \frac{\left|\mathcal{H}_{X|Y}(\delta_n)\right|}{n} \leq \frac{1}{n}H\left(X^{1:n}|Y^{1:n}\right) + \frac{A_{\delta,\varepsilon}}{n^{\kappa_{\delta,\varepsilon}\varepsilon}} \tag{10}$$

$$\frac{1}{n}H\left(X^{1:n}|Y^{1:n}\right) - \frac{A_{\delta,\varepsilon}}{n^{\kappa_{\delta,\varepsilon}\varepsilon}} \;\leq\; \frac{\left|\mathcal{V}_{X|Y}(\delta_n)\right|}{n} \leq \frac{1}{n}H\left(X^{1:n}|Y^{1:n}\right) + \delta_n. \tag{11}$$

Proof. The proof adapts the approach developed for finite length channel polarization [12] to source polarization. The idea is to first analyze a "rough" polarization to obtain a bound on the cardinality of the set of unpolarized sources, followed by a "fine" polarization to boost the polarization. Details require a careful adaptation but are otherwise similar to [12], and are therefore provided as supplementary material. □

For Proposition 3 to be meaningful, the relative size of the sets $\mathcal{H}_{X|Y}(\delta_n)$ and $\mathcal{V}_{X|Y}(\delta_n)$ in (10) and (11) should be asymptotically equivalent to the entropy rate $\frac{1}{n}H(X^{1:n}|Y^{1:n})$. This is possible if $\frac{1}{n}H(X^{1:n}|Y^{1:n}) = \omega(\frac{1}{n^{\kappa_{\delta,\varepsilon}\varepsilon}})$, i.e., polarization happens "fast enough" and the relative number of unpolarized symbols in (9) decays faster than the entropy rate. Therefore, our result only ensures the polarization of vanishing entropy rate sources for values of α_n that do not decay too rapidly; specifically, we require $\alpha_n = \omega\left(\frac{1}{n^{\kappa_{\delta,\varepsilon}\varepsilon}}\right) \cap o(1)$. Numerical analysis shows, for instance, that for $\delta = 0.1$ and $\varepsilon = 0.59$, $\kappa_{\delta,\varepsilon}\varepsilon \approx 6.53 \times 10^{-3}$. Note that this falls short of $\frac{1}{\sqrt{n}}$, which would be required for the square-root-law of communication. Nevertheless, we are now able to extend Lemma 3 and Lemma 4 of [11] to the finite length regime, which forms the basis of our construction for covert communications.

Lemma 1 (Source coding with side information). *Let $\delta \in [0\,,\,\frac{1}{2}]$, $\varepsilon \in [0\,,\,1-2\delta]$; set $\delta_n = 2^{-n^\delta}$ and let $\kappa_{\delta,\varepsilon} > 0$ be the constant identified by Proposition 3. Consider a vanishing entropy rate source $q_{X^{1:n}Y^{1:n}}$, as per (6) with $\alpha_n = \omega\left(\frac{1}{n^{\kappa_{\delta,\varepsilon}\varepsilon}}\right) \cap o(1)$. For $X^{1:n}$ polarized as $U^{1:n} = X^{1:n}G^{\otimes\nu}$, let $U^{1:n}\left[\mathcal{H}_{X|Y}(\delta_n)\right]$ denote the high entropy bits of $U^{1:n}$. For every $i \in [\![1,n]\!]$, sample $\widetilde{U}^{1:n}$ from the distribution*

$$\tilde{p}_{U_i|U^{1:i-1}}(\tilde{u}_i|\tilde{u}^{1:i-1}) \triangleq \begin{cases} \mathbb{1}\{\tilde{u}_i = u_i\} & \text{if } i \in \mathcal{H}_{X|Y}(\delta_n) \\ q_{U_i|U^{1:i-1}Y^{1:n}}(\tilde{u}_i|\tilde{u}^{1:i-1}\mathbf{y}) & \text{if } i \in \mathcal{H}_{X|Y}(\delta_n)^c \end{cases} \tag{12}$$

and create $\tilde{\mathbf{x}} = \tilde{\mathbf{u}}G^{\otimes\nu}$. Then $\mathbb{P}(\widetilde{X}^{1:n} \neq X^{1:n}) = O(n\delta_n)$.

Proof. See the proof of Lemma 3 in [11], using Proposition 3 instead of the standard polarization result. □

Lemma 2 (Privacy amplification). *Let $\delta \in [0\,,\,\frac{1}{2}]$, $\varepsilon \in [0\,,\,1-2\delta]$; set $\delta_n = 2^{-n^\delta}$ and let $\kappa_{\delta,\varepsilon} > 0$ be the constant identified by Proposition 3. Consider a vanishing entropy rate source $q_{X^{1:n}Y^{1:n}}$, as per (6) with $\alpha_n = \omega\left(\frac{1}{n^{\kappa_{\delta,\varepsilon}\varepsilon}}\right) \cap o(1)$. For $X^{1:n}$ polarized as $U^{1:n} = X^{1:n}G^{\otimes\nu}$, let $U^{1:n}\left[\mathcal{V}_{X|Y}(\delta_n)\right]$ denote the very high entropy bits of $U^{1:n}$. Denote by $q_{U^{1:n}[\mathcal{V}_{X|Y}(\delta_n)]Y^{1:n}}$ the joint distribution between $U^{1:n}\left[\mathcal{V}_{X|Y}(\delta_n)\right]$ and $Y^{1:n}$, and denote by q_U the uniform distribution over $[\![1, 2^{|\mathcal{V}_{X|Y}|}]\!]$. Then, $\mathbb{V}(q_{U^{1:n}[\mathcal{V}_{X|Y}(\delta_n)]Y^{1:n}}, q_U q_{Y^{1:n}}) = O\left(\sqrt{n\delta_n}\right)$.*

Proof. See the proof of Lemma 4 in [11], using Proposition 3 instead of the standard polarization result. □

4. Polar Codes for Covert Communication

In this section, we describe our proposed polar-code based scheme for covert communication. After preliminaries regarding covert processes in Section 4.1, the algorithms used for encoding and decoding are described in Section 4.2, and their performance is analyzed in Sections 4.3–4.5.

4.1. Covert Process

Our code construction follows the idea put forward in [3,6], which suggests to have the code induce a "covert process" at the output of the adversary's channel by leveraging the notion of channel resolvability [8], and to show that the covert process is itself indistinguishable from the product distribution Q_0.

Formally, consider any sequence of positive numbers $\{\alpha_n\}_{n\in\mathbb{D}}$ such that $\alpha_n \in \omega\left(\frac{1}{\sqrt{n}}\right) \cap o(1)$. For every $n \in \mathbb{D}$, recall the definition of the Bernoulli distribution Π_{α_n} over $\{0,1\}$ as $\Pi_{\alpha_n}(1) = 1 - \Pi_{\alpha_n}(0) = \alpha_n$, and its associated product distribution $\Pi_{\alpha_n}^{\otimes n}$; this distribution induces the mixture $Q_{\alpha_n} = \alpha_n Q_1 + (1-\alpha_n)Q_0$ at the output of the channel $(\mathcal{X}, W_{Z|X}, \mathcal{Z})$, for which we also define the product distribution

$$Q_{\alpha_n}^{\otimes n}(\mathbf{z}) = \prod_{i=1}^{n} Q_{\alpha_n}(z_i). \tag{13}$$

The "covert process" is the distribution $Q_{\alpha_n}^N(\mathbf{z}) = \mathbb{E}_T\left(Q_{\alpha_n,T}^N(\mathbf{z})\right)$ where

$$Q_{\alpha_n,t}^N(\mathbf{z}) = \prod_{k=1}^{t-1} Q_0(z_k) \prod_{k=t}^{t+n-1} Q_{\alpha_n}(z_k) \prod_{k=t+n}^{N} Q_0(z_k) \tag{14}$$

In other words, $Q_{\alpha_n}^N$ is the distribution at the output of the channel $(\mathcal{X}, W_{Z|X}, \mathcal{Z})$ obtained when randomizing the start index $T \in [\![1, N']\!]$ of a block of n consecutive bits sampled according to Π_{α_n}. The name "covert process" is justified by the following lemma, which provides the scaling of the parameters α_n and N such that the distribution $Q_{\alpha_n}^N$ becomes asymptotically indistinguishable from the distribution $Q_0^{\otimes N}$.

Lemma 3 (adapted from Lemma 1 and Equation (25) in [6])**.** *Consider sequences of positive numbers* $\{\alpha_n\}_{n\in\mathbb{N}^*}$, $\{\beta_n\}_{n\in\mathbb{N}^*}$ *such that* $\alpha_n \in \omega\left(\frac{1}{\sqrt{n}}\right) \cap o(1)$, $\beta_n = o(1)$ *as n goes to infinity. Let* $N = \frac{2^{n\alpha_n^2}}{\beta_n \alpha_n^2}$. *Then,*

$$\mathbb{D}\left(Q_{\alpha_n}^N \| Q_0^{\otimes N}\right) \leq O(\beta_n). \tag{15}$$

4.2. Encoding and Decoding Algorithms

Let $n \in \mathbb{D}$ be the length of the codeword window. We propose a scheme that operates over b_n transmission windows of length N, where b_n will be specified later. In every transmission window $i \in [\![1, b_n]\!]$:

1. Transmitter and receiver use a secret key S_i'' of $\log N$ bits to determine the position of the codeword window within the transmission window. Note that this secret key is not required in the random coding proof of [6], but is required here to maintain a low complexity at the decoder; fortunately, this change has negligible effect on the scaling of the key.
2. The content of each codeword window is obtained through a polar-code based scheme that ensures reliable decoding to the receiver and approximates the process $Q_{\alpha_n}^{\otimes n}$ at the adversary's output, which we describe next.

In the remainder of this section we fix $\delta \in \left]0, \frac{1}{2}\right[$, $\varepsilon \in]0, 1-2\delta[$, $\delta_n \triangleq 2^{-n^\delta}$. We let $\kappa \triangleq \kappa_{\delta,\varepsilon}\varepsilon$ and $A \triangleq A_{\delta,\varepsilon}$, where $\kappa_{\delta,\varepsilon}$ and $A_{\delta,\varepsilon}$ are the constants identified by Proposition 3. We consider sequences of positive numbers $\{\alpha_n\}_{n\in\mathbb{D}} \in \omega\left(\frac{1}{n^\kappa}\right) \cap o(1)$, $\{\beta_n\}_{n\in\mathbb{D}} \in \omega\left(2^{-\frac{n\alpha_n}{\log n}}\right) \cap o\left(\frac{1}{\log n}\right)$, a sequence of integers

$\{b_n\}_{n\in\mathbb{D}} \in \omega(\log n) \cap o\left(\frac{1}{\beta_n}\right) \cap o(n)$, and we set $N = \frac{2^{n\alpha_n^2}}{\beta_n \alpha_n^2}$. Finally, we consider a vanishing entropy rate source $q_{X^{1:n}Y^{1:n}Z^{1:n}} \sim \Pi_{\alpha_n}^{\otimes n} W_{Y|X}^{\otimes n} W_{Z|X}^{\otimes n}$ (the marginal $q_{Z^{1:n}}^{\otimes n}$ is $Q_{\alpha_n}^{\otimes n}$) and we define the sets

$$\mathcal{V}_X(\delta_n) \triangleq \{j \in [\![1,n]\!] : \quad H(U_j|U^{1:j-1}) > 1-\delta_n\} \tag{16}$$

$$\mathcal{H}_{X|Y}(\delta_n) \triangleq \{j \in [\![1,n]\!] : \quad H(U_j|U^{1:j-1}Y^{1:n}) > \delta_n\} \tag{17}$$

$$\mathcal{V}_{X|Z}(\delta_n) \triangleq \{j \in [\![1,n]\!] : \quad H(U_j|U^{1:j-1}Z^{1:n}) > 1-\delta_n\}, \tag{18}$$

where all entropies should be computed based on $q_{X^{1:n}Y^{1:n}Z^{1:n}}$. To alleviate the notation, we drop the dependence on δ_n in the sets from now on, and write for instance $\mathcal{V}_X$ in place of $\mathcal{V}_X(\delta_n)$. We also write $H(X)$ and $H(X|Y)$ although these quantities should be understood for the independent and identically distributed (i.i.d.) random variables obtained as marginals of $q_{X^{1:n}Y^{1:n}Z^{1:n}}$. As illustrated in Figure 3a, the construction is based on the following sets:

- $\mathcal{V}_C \triangleq \mathcal{H}_{X|Y} \cap \mathcal{V}_{X|Z}$, which will contain uniformly distributed bits C representing the code;
- $\mathcal{V}_{C'} \triangleq \mathcal{H}_{X|Y} \cap \mathcal{V}_X^c$, which will contain non-uniformly distributed bits C' computed from the other bits;
- $\mathcal{V}_{W'}$, the largest subset of $\mathcal{H}_{X|Y}^c \cap \mathcal{V}_{X|Z}$ such that $|\mathcal{V}_{W'}| \leq |\mathcal{H}_{X|Y} \cap \mathcal{V}_{X|Z}^c \cap \mathcal{V}_X|$, which will contain uniformly distributed messages W';
- $\mathcal{V}_W \triangleq (\mathcal{H}_{X|Y}^c \cap \mathcal{V}_X) \setminus \mathcal{V}_{W'}$, which will contain additional uniformly distributed messages W;
- $\mathcal{V}_{S'}$, any subset of $\mathcal{H}_{X|Y} \cap \mathcal{V}_{X|Z}^c \cap \mathcal{V}_X$ such that $|\mathcal{V}_{S'}| = |\mathcal{V}_{W'}|$, which will use messages W' transmitted in the previous transmission window as a key;
- $\mathcal{V}_S = (\mathcal{H}_{X|Y} \cap \mathcal{V}_{X|Z}^c \cap \mathcal{V}_X) \setminus \mathcal{V}_{S'}$, which will contain uniformly distributed secret key symbols S.

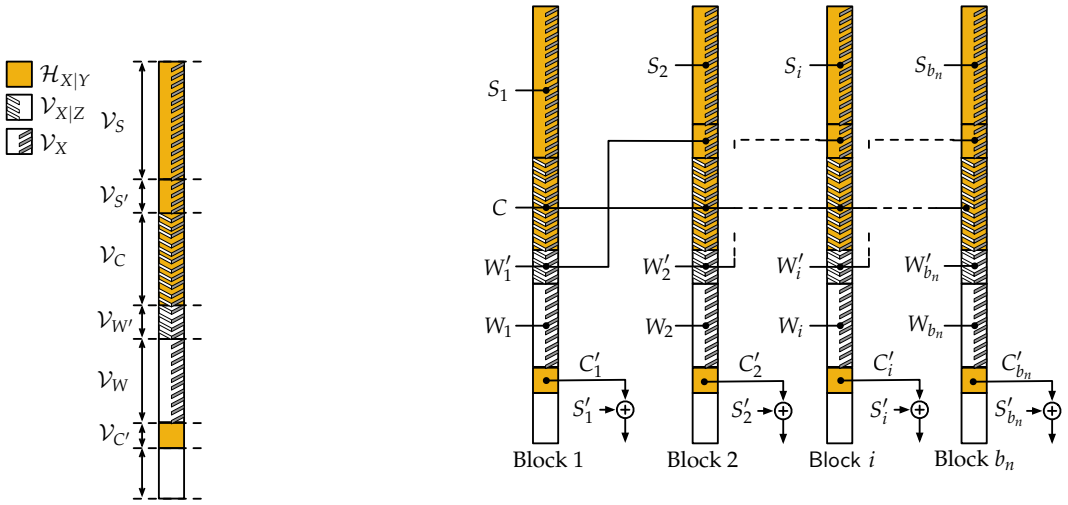

Figure 3. Illustration of polar coding scheme. (**a**) Sets used in polar coding scheme assuming $|\mathcal{H}_{X|Y}^c \cap \mathcal{V}_{X|Z}| \leq |\mathcal{H}_{X|Y} \cap \mathcal{V}_{X|Z}^c \cap \mathcal{V}_X|$; (**b**) Chaining construction.

Alice's encoder is formally provided in Algorithm 1 while Bob's decoder is provided in Algorithm 2, but the chaining of the transmission windows over b_n blocks is illustrated in Figure 3b and we discuss here the salient features of the algorithms. In every block $i \in [\![1, b_n]\!]$, a message W_i is transmitted with the assistance of a secret key S_i as expected from the model of Section 2.2. In addition, the chaining exploits the property that the bits in $\mathcal{V}_{W'}$ are held secret from Willie and can therefore be used as a secret key in the next block, which is formally proved in Section 4.5; this chaining allows us to transmit an additional message W'_i in every block, which is crucial to achieve the scalings of Proposition 2 as shown in Section 4.3. The chaining also relies on the secrecy of the bits in $\mathcal{V}_C$, which allows us to reuse the same random bits C across all blocks. Finally, some bits of shared randomness

C'_i must be transmitted secretly, covertly, and reliably to the receiver. As we show in Section 4.3, the number of such bits is negligible compared to the number of covert bits transmitted; we therefore ensure their secrecy by performing a one time pad $C'_i \oplus S'_i$ with another secret key S'_i, and we ensure reliability and covertness in a single additional block at the end, e.g., using the somewhat inefficient scheme of [1]. In the remainder, we will ignore this last block for simplicity and assume that $C'_i \oplus S'_i$ is made available to the decoder "for free".

Ultimately, the messages transmitted consist of the messages W_i and W'_i transmitted in every block i; the keys required consist of the keys S_i, S'_i, S''_i used in every block i, as well as the bits C.

Remark 1. *The proposed chaining scheme could be further modified as follows. First, since the bits of C are secret from the perspective of Willie, they could be publicly disclosed and not counted as part of the secret keys, without compromising the performance. We have opted to count C as part of the key to make the analysis slightly more concise. Second, the bits of $C'_i \oplus S'_i$ could be chained by sacrificing part of the message W_i; since their amount is negligible, this would again not affect performance. We have opted to avoid this chaining since a last transmission for the bits $C'_{b_n} \oplus S'_{b_n}$ would be necessary anyway.*

Remark 2. *Because of the stochastic encoding in Algorithm 1, our codes are neither linear codes nor cosets of linear codes. In that regard, calling our codes "polar codes" is a slight abuse of terminology but follows standard practice [11,18,20]. Strictly speaking, our codes are only "polarization-based".*

4.3. Analysis of Normalized Set Sizes

We start by analyzing the normalized set sizes of the proposed scheme. Specifically, we are interested in characterizing the asymptotic total number of message bits $\log M_n$ and total number of key bits $\log K_n$, normalized by $nb_n\alpha_n$.

Over b_n transmission windows, the total number of message bits consists of those in $\mathcal{V}_W$ and $\mathcal{V}_{W'}$ in every transmission window. Hence, for every $n \in \mathbb{D}$, $\log M_n = b_n |\mathcal{V}_W| + b_n |\mathcal{V}_{W'}|$. Similarly, the total number of key bits consists of those in $\mathcal{V}_S$ (except for the first block which requires $\mathcal{V}_S + \mathcal{V}_{S'}$), the bits for the one time pad in $\mathcal{V}_{C'}$, the bits required to identify the codeword window within the transmission window, and the bits in $\mathcal{V}_C$, so that $\log K_n = b_n |\mathcal{V}_S| + |\mathcal{V}_{S'}| + b_n |\mathcal{V}_{C'}| + b_n \log N + |\mathcal{V}_C|$.

Lemma 4.

$$\lim_{n \in \mathbb{D} \to \infty} \frac{\log M_n}{nb_n\alpha_n} = \mathbb{D}(P_1 \| P_0).$$

Proof. By definition,

$$\frac{\log M_n}{nb_n\alpha_n} = \frac{(|\mathcal{V}_W| + |\mathcal{V}_{W'}|)}{n\alpha_n} = \frac{|\mathcal{H}^c_{X|Y} \cap \mathcal{V}_X|}{n\alpha_n}.$$

Introducing $\mathcal{H}^c_{X|Y} \subset \mathcal{V}^c_{X|Y}$, we obtain

$$\left|\mathcal{H}^c_{X|Y} \cap \mathcal{V}_X\right| = \left|\mathcal{V}^c_{X|Y} \cap \mathcal{V}_X\right| - \left|\mathcal{H}_{X|Y} \cap \mathcal{V}^c_{X|Y} \cap \mathcal{V}_X\right| \tag{19}$$

Since, $\mathcal{V}_{X|Y} \subset \mathcal{V}_X$, we have $|\mathcal{V}^c_{X|Y} \cap \mathcal{V}_X| = |\mathcal{V}_X| - |\mathcal{V}_{X|Y}|$ and, in addition, $0 \leq |\mathcal{H}_{X|Y} \cap \mathcal{V}^c_{X|Y} \cap \mathcal{V}_X| \leq |\mathcal{H}_{X|Y} \cap \mathcal{V}^c_{X|Y}|$. Using Proposition 3 to bound $|\mathcal{V}_X|$, $|\mathcal{V}_{X|Y}|$, and $|\mathcal{H}_{X|Y} \cap \mathcal{V}^c_{X|Y}|$, we obtain

$$\frac{\log M_n}{nb_n\alpha_n} \geq \frac{H(X) - H(X|Y)}{\alpha_n} - \frac{\delta_n}{\alpha_n} - 2\frac{A}{n^\kappa \alpha_n}. \tag{20}$$

Since $H(X) - H(X|Y) = I(X;Y) = \alpha_n \mathbb{D}(P_1 \| P_0) + o(\alpha_n)$ (Lemma 1, [3]), and remembering the choice of α_n, δ_n earlier, we obtain the desired result (note that we use $\alpha_n \in \omega(\frac{1}{n^\kappa}) \cap o(1)$ here). □

Lemma 5.

$$\lim_{n\in\mathbb{D}\to\infty} \frac{\log K_n}{nb_n\alpha_n} = [\mathbb{D}(Q_1\|Q_0) - \mathbb{D}(P_1\|P_0)]^+.$$

Proof. We first assume that $|\mathcal{H}^c_{X|Y} \cap \mathcal{V}_{X|Z}| \leq |\mathcal{H}_{X|Y} \cap \mathcal{V}^c_{X|Z} \cap \mathcal{V}_X|$. By definition,

$$\begin{aligned}\frac{\log M_n + \log K_n}{nb_n\alpha_n} &= \frac{b_n\left|\mathcal{V}_W\right| + b_n\left|\mathcal{V}_S\right| + (b_n+1)\left|\mathcal{V}_{S'}\right| + b_n\left|\mathcal{V}_{C'}\right| + b_n\log N + |\mathcal{V}_C|}{nb_n\alpha_n}\\ &= \frac{\left|\mathcal{V}_W\right| + |\mathcal{V}_S| + \left|\mathcal{V}_{S'}\right| + \left|\mathcal{V}_{C'}\right|}{n\alpha_n} + \frac{\left|\mathcal{V}_{S'}\right| + \left|\mathcal{V}_C\right|}{nb_n\alpha_n} + \frac{\log N}{n\alpha_n}.\end{aligned}$$

We analyze the terms on the right hand side in order. First, since $\mathcal{V}_{X|Z} \subset \mathcal{V}_X$, we have $\left|\mathcal{V}_W\right| + |\mathcal{V}_S| + \left|\mathcal{V}_{S'}\right| = |\mathcal{V}^c_{X|Z} \cap \mathcal{V}_X| = |\mathcal{V}_X| - |\mathcal{V}_{X|Z}|$, and by Proposition 3 applied to the vanishing entropy rate sources $q_{X^{1:n}}$ and $q_{X^{1:n}Z^{1:n}}$

$$\frac{\left|\mathcal{V}_W\right| + |\mathcal{V}_S| + \left|\mathcal{V}_{S'}\right|}{n\alpha_n} \geq \frac{H(X) - H(X|Z)}{\alpha_n} - \frac{\delta_n}{\alpha_n} - \frac{A}{n^\kappa\alpha_n}. \tag{21}$$

Since $H(X) - H(X|Z) = I(X;Z) = \alpha_n\mathbb{D}(Q_1\|Q_0) + o(\alpha_n)$ (Lemma 1, [3]) and remembering the choice of α_n, δ_n earlier, it follows that $\frac{\left|\mathcal{V}_W\right|+|\mathcal{V}_S|+\left|\mathcal{V}_{S'}\right|}{n\alpha_n} = \mathbb{D}(Q_1\|Q_0) + o(1)$. This also implies that $\frac{\left|\mathcal{V}_{S'}\right|}{nb_n\alpha_n} = o(1)$. Next, since $\mathcal{V}^c_X \subset \mathcal{V}^c_{X|Y}$, we have with Proposition 3 that

$$\frac{\left|\mathcal{V}_{C'}\right|}{n\alpha_n} \leq \frac{\left|\mathcal{H}_{X|Y} \cap \mathcal{V}^c_{X|Y}\right|}{n\alpha_n} \leq \frac{A}{n^\kappa\alpha_n}, \tag{22}$$

which vanishes by definition of α_n. Similarly, since $\mathcal{V}_C \subset \mathcal{H}_X$, Proposition 3 applied to the vanishing entropy rate source $q_{Z^{1:n}}$ ensures that

$$\frac{|\mathcal{V}_C|}{nb_n\alpha_n} \leq \frac{H(X^{1:n})}{nb_n\alpha_n} + \frac{A}{n^\kappa b_n\alpha_n} = -\frac{\log\alpha_n}{b_n} - \frac{(1-\alpha_n)\log(1-\alpha_n)}{b_n\alpha_n} + \frac{A}{n^\kappa b_n\alpha_n}, \tag{23}$$

which vanishes with our choice of α_n and b_n (note that we use the condition $b_n = \omega(\log n)$ here). Finally, since $N = \frac{2^{n\alpha_n^2}}{\beta_n\alpha_n^2}$, we have

$$\frac{\log N}{n\alpha_n} = \alpha_n - \frac{\log\beta_n}{n\alpha_n} - \frac{2\log\alpha_n}{n\alpha_n}, \tag{24}$$

which vanishes with the choice of α_n, β_n (note that we use the condition $\beta_n \in \omega\left(2^{-\frac{n\alpha_n}{\log n}}\right)$ here).

We finally assume that $|\mathcal{H}^c_{X|Y} \cap \mathcal{V}_{X|Z}| > |\mathcal{H}_{X|Y} \cap \mathcal{V}^c_{X|Z} \cap \mathcal{V}_X|$, which is equivalent to assuming that $|\mathcal{V}_X \cap \mathcal{H}^c_{X|Y}| > |\mathcal{V}_X \cap \mathcal{V}^c_{X|Z}|$. With Proposition 3 and Lemma 1 of [3], this implies that $\mathbb{D}(P_1\|P_0) > \mathbb{D}(Q_1\|Q_0) + o(1)$. Since we have $\mathcal{V}_S = \emptyset$ in this case, following the same steps as earlier we now obtain $\lim_{n\in\mathbb{D}\to\infty} \frac{\log K_n}{nb_n\alpha_n} = 0$, which is the desired result. □

4.4. Reliability Analysis

In this section, we prove that the proposed scheme ensures reliable communication. To avoid any confusion between the distribution induced by the algorithms and the underlying vanishing entropy rate source, we denote the distribution induced by Algorithm 1 by $\tilde{p}$; accordingly, all random variables generated according to this distribution have a tilde, e.g., $\tilde{X}$ has distribution $\tilde{p}_X$. The estimates obtained from Algorithm 2 are denoted with a hat, e.g., $\widehat{X}$. Since the location of the transmission window is

known to the legitimate receiver, it is sufficient to show that $\lim_{n\to\infty} \mathbb{P}\left[\widehat{X}_{1:b_n}^{1:n} \neq \widetilde{X}_{1:b_n}^{1:n}\right] = 0$. We proceed to prove this with a series of lemmas.

Lemma 6. *For any transmission window $i \in [\![1, b_n]\!]$*

$$\mathbb{D}\left(q_{X^{1:n}Y^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}Y_i^{1:n}}\right) = \mathbb{D}\left(q_{X^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}}\right) \leq \delta_n^{(1)} \tag{25}$$

where $\delta_n^{(1)} \triangleq n\delta_n$.

Proof. We have

$$\begin{aligned}
\mathbb{D}\left(q_{X^{1:n}Y^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}Y_i^{1:n}}\right) &= \mathbb{D}\left(q_{X^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}}\right) + \mathbb{E}_{q_{X^{1:n}}}\left[\mathbb{D}\left(q_{Y^{1:n}|X^{1:n}} \middle\| \tilde{p}_{Y_i^{1:n}|X_i^{1:n}}\right)\right] && (26)\\
&= \mathbb{D}\left(q_{X^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}}\right) && (27)\\
&= \mathbb{D}\left(q_{U^{1:n}} \middle\| \tilde{p}_{U_i^{1:n}}\right) && (28)\\
&= \sum_{j=1}^{n} \mathbb{E}_{q_{U^{1:j-1}}}\left[\mathbb{D}\left(q_{U^j|U^{1:j-1}} \middle\| \tilde{p}_{U_i^j|U_i^{1:j-1}}\right)\right] && (29)\\
&= \sum_{j\in\mathcal{V}_X} \mathbb{E}_{q_{U^{1:j-1}}}\left[\mathbb{D}\left(q_{U^j|U^{1:j-1}} \middle\| \tilde{p}_{U_i^j|U_i^{1:j-1}}\right)\right] && (30)\\
&= \sum_{j\in\mathcal{V}_X} \left(1 - H\left(U^j|U^{1:j-1}\right)\right) && (31)\\
&\leq |\mathcal{V}_X|\,\delta_n && (32)\\
&\leq n\delta_n && (33)
\end{aligned}$$

where (26) comes from the chain rule of divergence, (27) comes from

$$\mathbb{E}_{q_{X^{1:n}}}\left[\mathbb{D}\left(q_{Y^{1:n}|X^{1:n}} \middle\| \tilde{p}_{Y_i^{1:n}|X_i^{1:n}}\right)\right] = \mathbb{E}_{q_{X^{1:n}}}\left[\mathbb{D}\left(W_{Y|X}^{\otimes n} \middle\| W_{Y|X}^{\otimes n}\right)\right] = 0 \tag{34}$$

Equation (28) comes from the invertibility of $X^{1:n} = U^{1:n}G^{\otimes\nu}$ and $\widetilde{X}^{1:n} = \widetilde{U}^{1:n}G^{\otimes\nu}$, (29) comes from the chain rule of divergence, (30) comes from the definition of the encoder for $j \in \mathcal{V}_X^c$ in (4), (31) comes from the uniformity of the symbols in $\mathcal{V}_X$, (32) comes from the definition of $\mathcal{V}_X$. □

Lemma 7. *For any transmission window $i \in [\![1, b_n]\!]$, define the event*

$$\mathcal{E}_i \triangleq \left\{\widehat{X}_i^{1:n} \neq \widetilde{X}_i^{1:n}\right\} \tag{35}$$

Then,

$$\mathbb{P}\left[\mathcal{E}_i | \mathcal{E}_{i-1}^c\right] = \mathbb{P}\left[\widehat{X}_i^{1:n} \neq \widetilde{X}_i^{1:n} | \widehat{X}_{i-1}^{1:n} = \widetilde{X}_{i-1}^{1:n}\right] \leq \delta_n^{(2)} \tag{36}$$

where $\delta_n^{(2)} = O\left(n^{1/2}\delta_n^{1/2}\right)$.

Proof. For $i \in [\![1, b_n]\!]$, define the event that the sequence produced by the polar encoder differs from the actual one:

$$\mathcal{E}_i^{(XY)} \triangleq \left\{\left(\widetilde{X}_i^{1:n}, \widetilde{Y}_i^{1:n}\right) \neq \left(X^{1:n}, Y^{1:n}\right)\right\} \tag{37}$$

and define an optimal coupling such that

$$\mathbb{P}\left[\mathcal{E}_i^{(XY)}\right] = \mathbb{V}\left(q_{X^{1:n}Y^{1:n}}, \tilde{p}_{X_i^{1:n}Y_i^{1:n}}\right) \leq \sqrt{\mathbb{D}\left(q_{X^{1:n}Y^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}Y_i^{1:n}}\right)} \leq \sqrt{\delta_n^{(1)}} \tag{38}$$

by Pinsker's inequality and Lemma 6. Then, we have

$$\begin{aligned}
\mathbb{P}\left[\mathcal{E}_i|\mathcal{E}_{i-1}^c\right] &= \mathbb{P}\left[\mathcal{E}_i|\mathcal{E}_i^{(XY)c} \cap \mathcal{E}_{i-1}^c\right]\mathbb{P}\left[\mathcal{E}_i^{(XY)c}\right] + \mathbb{P}\left[\mathcal{E}_i|\mathcal{E}_i^{(XY)} \cap \mathcal{E}_{i-1}^c\right]\mathbb{P}\left[\mathcal{E}_i^{(XY)}\right] && (39)\\
&\leq \mathbb{P}\left[\mathcal{E}_i|\mathcal{E}_i^{(XY)c} \cap \mathcal{E}_{i-1}^c\right] + \mathbb{P}\left[\mathcal{E}_i^{(XY)}\right] && (40)\\
&\leq O(n\delta_n) + \sqrt{\delta_n^{(1)}} && (41)
\end{aligned}$$

where (39) comes from the law of total probabilities, (40) from $\mathbb{P}\left[\mathcal{E}_i^{(XY)c}\right] \leq 1$, $\mathbb{P}\left[\mathcal{E}_i|\mathcal{E}_i^{(XY)} \cap \mathcal{E}_{i-1}^c\right] \leq 1$, and (41) from Lemma 1 and the optimal coupling. □

Lemma 8. *We have*

$$\mathbb{P}\left[\widehat{X}_{1:b_n}^{1:n} \neq \widetilde{X}_{1:b_n}^{1:n}\right] \leq \delta_n^{(3)} \tag{42}$$

where $\delta_n^{(3)} = O\left(b_n n^{1/2} \delta_n^{1/2}\right)$.

Proof. We have the following partition

$$\bigcup_{i=1}^{b_n} \mathcal{E}_i = \bigcup_{i=1}^{b_n} \left(\mathcal{E}_i \cap \left(\bigcup_{j=1}^{i-1} \mathcal{E}_j\right)^c\right). \tag{43}$$

Thus,

$$\begin{aligned}
\mathbb{P}\left[\widehat{X}_{1:b_n}^{1:n} \neq \widetilde{X}_{1:b_n}^{1:n}\right] = \mathbb{P}\left[\bigcup_{i=1}^{b_n} \mathcal{E}_i\right] &= \mathbb{P}\left[\bigcup_{i=1}^{b_n} \mathcal{E}_i \cap \left(\bigcup_{j=1}^{i-1} \mathcal{E}_j\right)^c\right] && (44)\\
&= \sum_{i=1}^{b_n} \mathbb{P}\left[\mathcal{E}_i \cap \left(\bigcup_{j=1}^{i-1} \mathcal{E}_j\right)^c\right] && (45)\\
&\leq \sum_{i=1}^{b_n} \mathbb{P}\left[\mathcal{E}_i \cap \mathcal{E}_{i-1}^c\right] && (46)\\
&= \sum_{i=1}^{b_n} \mathbb{P}\left[\mathcal{E}_i|\mathcal{E}_{i-1}^c\right]\mathbb{P}\left[\mathcal{E}_{i-1}^c\right] && (47)\\
&\leq \sum_{i=1}^{b_n} \mathbb{P}\left[\mathcal{E}_i|\mathcal{E}_{i-1}^c\right] && (48)\\
&\leq O(b_n n\delta_n) + b_n\sqrt{\delta_n^{(1)}} && (49)
\end{aligned}$$

where (45) comes from the probability of the partition, (46) from $\mathcal{E}_{i-1} \subseteq \bigcup_{j=1}^{i-1} \mathcal{E}_j$, (47) from the definition of conditional probability, (48) from $\mathbb{P}\left[\mathcal{E}_{i-1}^c\right] \leq 1$, and (49) from Lemma 7. The choice $b_n = o(n)$ ensures that $\mathbb{P}\left[\widehat{X}_{1:b_n}^{1:n} \neq \widetilde{X}_{1:b_n}^{1:n}\right]$ vanishes. □

4.5. Covertness Analysis

In this section, we prove that the proposed scheme is covert in the sense that $\lim_{n\in\mathbb{D}\to\infty} \mathbb{V}(\tilde{p}_{Z_{1:b_n}^{1:n}} \| q_{Z_{1:b_n}^{1:n}}) = 0$, where $q_{Z_{1:b_n}^{1:n}}(\mathbf{z}_1, \ldots, \mathbf{z}_{b_n}) \triangleq \prod_{i=1}^{b_n} Q_{\alpha_n}^{\otimes n}(\mathbf{z}_i)$.

Lemma 9. *For any transmission window $i \in [\![1, b_n]\!]$*

$$\mathbb{D}\left(q_{X^{1:n}Z^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}Z_i^{1:n}}\right) = \mathbb{D}\left(q_{X^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}}\right) \leq \delta_n^{(1)} \tag{50}$$

$$\mathbb{V}\left(\tilde{p}_{Z_i^{1:n}}, q_{Z^{1:n}}\right) \leq \mathbb{V}\left(\tilde{p}_{X_i^{1:n}Z_i^{1:n}}, q_{X^{1:n}Z^{1:n}}\right) \leq \delta_n^{(4)} \tag{51}$$

where $\delta_n^{(1)} \triangleq n\delta_n$ and $\delta_n^{(4)} = \sqrt{n\delta_n}$.

Proof. The proof of the divergence inequality is identical to Lemma 6. The proof of the total variation distance inequality follows from

$$\mathbb{V}\left(\tilde{p}_{Z_i^{1:n}}, q_{Z^{1:n}}\right) \leq \mathbb{V}\left(\tilde{p}_{X_i^{1:n}Z_i^{1:n}}, q_{X^{1:n}Z^{1:n}}\right) \tag{52}$$

$$\leq \sqrt{\mathbb{D}\left(q_{X^{1:n}Z^{1:n}} \middle\| \tilde{p}_{X_i^{1:n}Z_i^{1:n}}\right)} \tag{53}$$

$$\leq \sqrt{\delta_n^{(1)}} = \sqrt{n\delta_n} \tag{54}$$

where (52) comes from the total variation of marginal distributions, (53) from Pinsker's inequality, and (54) from the previous inequality. □

Lemma 10. *For $i \in [\![1, b_n]\!]$,*

$$I\left(\widetilde{Z}_i^{1:n}; CW_i'\right) \leq \delta_n^{(5)} \tag{55}$$

where $\delta_n^{(5)} = n\delta_n + 2\delta_n^{(4)}\left[n(1 + 2\log|\mathcal{Z}|) - 2\log 2\delta_n^{(4)}\right]$.

Proof. Let $i \in [\![2, b_n]\!]$.

$$H\left(U^{1:n}\left[\mathcal{V}_{X|Z}\right] \middle| Z^{1:n}\right) - H\left(\widetilde{U}_i^{1:n}\left[\mathcal{V}_{X|Z}\right] \middle| \widetilde{Z}_i^{1:n}\right) \tag{56}$$

$$= H\left(U^{1:n}\left[\mathcal{V}_{X|Z}\right], Z^{1:n}\right) - H\left(\widetilde{U}_i^{1:n}\left[\mathcal{V}_{X|Z}\right], \widetilde{Z}_i^{1:n}\right) + H\left(\widetilde{Z}_i^{1:n}\right) - H\left(Z^{1:n}\right) \tag{57}$$

$$\leq 2\mathbb{V}\left(\tilde{p}_{U_i^{1:n}[\mathcal{V}_{X|Z}],Z_i^{1:n}}, q_{U^{1:n}[\mathcal{V}_{X|Z}],Z^{1:n}}\right)\left[n\log\left(|\mathcal{X}||\mathcal{Z}|\right) - \log 2\mathbb{V}\left(\tilde{p}_{U_i^{1:n}[\mathcal{V}_{X|Z}],Z_i^{1:n}}, q_{U^{1:n}[\mathcal{V}_{X|Z}],Z^{1:n}}\right)\right] \tag{58}$$

$$+ 2\mathbb{V}\left(\tilde{p}_{Z_i^{1:n}}, q_{Z^{1:n}}\right)\left[n\log|\mathcal{Z}| - \log 2\mathbb{V}\left(\tilde{p}_{Z_i^{1:n}}, q_{Z^{1:n}}\right)\right] \tag{59}$$

$$\leq 2\mathbb{V}\left(\tilde{p}_{X_i^{1:n}Z_i^{1:n}}, q_{X^{1:n}Z^{1:n}}\right)\left[n\log\left(|\mathcal{X}||\mathcal{Z}|\right) - \log 2\mathbb{V}\left(\tilde{p}_{X_i^{1:n},Z_i^{1:n}}, q_{X^{1:n},Z^{1:n}}\right)\right] \tag{60}$$

$$+ 2\mathbb{V}\left(\tilde{p}_{Z_i^{1:n}}, q_{Z^{1:n}}\right)\left[n\log|\mathcal{Z}| - \log 2\mathbb{V}\left(\tilde{p}_{Z_i^{1:n}}, q_{Z^{1:n}}\right)\right] \tag{61}$$

$$\leq 2\delta_n^{(4)}\left[n\log\left(|\mathcal{X}||\mathcal{Z}|\right) - \log 2\delta_n^{(4)}\right] + 2\delta_n^{(4)}\left[n\log|\mathcal{Z}| - \log 2\delta_n^{(4)}\right] \tag{62}$$

$$= 2\delta_n^{(4)}\left[n(1 + 2\log|\mathcal{Z}|) - 2\log 2\delta_n^{(4)}\right] \tag{63}$$

$$\triangleq \delta_n^{(XZ)} \tag{64}$$

where (57) comes from the chain rule of entropy, (58) and (59) from Lemma 2.7 of [21] with n large enough, (60) and (61) from the total variation of marginal distributions, the invertibility of $X^{1:n} = U^{1:n}G^{\otimes\nu}$ and $\widetilde{X}^{1:n} = \widetilde{U}^{1:n}G^{\otimes\nu}$ and that the function $x \mapsto x(1 - \log x)$ is monotonically increasing, and (62) from Lemma 9. Hence for $i \in [\![2, b_n]\!]$,

$$
\begin{aligned}
I\left(\widetilde{Z}_i^{1:n}; CW_i'\right) &\leq I\left(\widetilde{Z}_i^{1:n}; \widetilde{U}_i^{1:n}\left[\mathcal{V}_{X|Z}\right]\right) && (65)\\
&= H\left(\widetilde{U}_i^{1:n}\left[\mathcal{V}_{X|Z}\right]\right) - H\left(\widetilde{U}_i^{1:n}\left[\mathcal{V}_{X|Z}\right]|\widetilde{Z}_i^{1:n}\right) && (66)\\
&= |\mathcal{V}_{X|Z}| - H\left(\widetilde{U}_i^{1:n}\left[\mathcal{V}_{X|Z}\right]|\widetilde{Z}_i^{1:n}\right) && (67)\\
&\leq |\mathcal{V}_{X|Z}| - H\left(U^{1:n}\left[\mathcal{V}_{X|Z}\right]|Z^{1:n}\right) + \delta_n^{(XZ)} && (68)\\
&\leq |\mathcal{V}_{X|Z}| - \sum_{j\in\mathcal{V}_{X|Z}} H(U^j|U^{1:j-1}Z^{1:n}) + \delta_n^{(XZ)} && (69)\\
&\leq |\mathcal{V}_{X|Z}| - |\mathcal{V}_{X|Z}|(1-\delta_n) + \delta_n^{(XZ)} && (70)\\
&\leq n\delta_n + \delta_n^{(XZ)} && (71)
\end{aligned}
$$

where (66) come the definition of mutual information, (65) and (70) from the definition of the set $\mathcal{V}_{X|Z}$, (67) from the uniformity of symbols in $\mathcal{V}_{X|Z}$, (68) comes from (64), and (69) from the chain rule of entropy and conditioning. □

Lemma 11. *The outputs of all blocks are asymptotically independent in the sense that*

$$
\mathbb{V}\left(\tilde{p}_{Z_{1:b_n}^{1:n}}, \prod_{i=1}^{b_n}\tilde{p}_{Z_i^{1:n}}\right) \leq b_n\sqrt{\delta_n^{(5)}}. \tag{72}
$$

Proof. We have

$$
\begin{aligned}
\mathbb{V}\left(\tilde{p}_{Z_{1:b_n}^{1:n}}, \prod_{i=1}^{b_n}\tilde{p}_{Z_i^{1:n}}\right) &\leq \sum_{i=1}^{b_n}\mathbb{E}_{\tilde{p}_{Z_{1:i-1}^{1:n}}}\left[\mathbb{V}\left(\tilde{p}_{Z_i^{1:n}|Z_{1:i-1}^{1:n}}, \tilde{p}_{Z_i^{1:n}}\right)\right] && (73)\\
&= \sum_{i=1}^{b_n}\mathbb{V}\left(\tilde{p}_{Z_{1:i}^{1:n}}, \tilde{p}_{Z_{1:i-1}^{1:n}}\tilde{p}_{Z_i^{1:n}}\right) && (74)\\
&\leq \sum_{i=1}^{b_n}\mathbb{V}\left(\tilde{p}_{Z_{1:i}^{1:n}CW_i'}, \tilde{p}_{Z_{1:i-1}^{1:n}CW_i'}\tilde{p}_{Z_i^{1:n}}\right) && (75)\\
&\leq \sum_{i=1}^{b_n}\sqrt{\mathbb{D}\left(\tilde{p}_{Z_{1:i}^{1:n}CW_i'}\|\tilde{p}_{Z_{1:i-1}^{1:n}CW_i'}\tilde{p}_{Z_i^{1:n}}\right)}. && (76)
\end{aligned}
$$

where (73) follows from the chain rule of total variation. Note that

$$
\begin{aligned}
\mathbb{D}\left(\tilde{p}_{Z_{1:i}^{1:n}CW_i'}\|\tilde{p}_{Z_{1:i-1}^{1:n}CW_i'}\tilde{p}_{Z_i^{1:n}}\right) &= I\left(\widetilde{Z}_{1:i-1}CW_i'; \widetilde{Z}_i^{1:n}\right) && (77)\\
&= I\left(CW_i'; \widetilde{Z}_i^{1:n}\right) + I\left(\widetilde{Z}_{1:i-1}; \widetilde{Z}_i^{1:n}|CW_i'\right) && (78)\\
&= I\left(CW_i'; \widetilde{Z}_i^{1:n}\right), && (79)
\end{aligned}
$$

where we have used the Markov chain $Z_{1:i-1}^{1:n} - CW_i' - Z_i^{1:n}$. The result then follows by Lemma 10. □

Lemma 12. *We have*

$$
\mathbb{V}\left(\tilde{p}_{Z_{1:b_n}^{1:n}}, q_{Z_{1:b_n}^{1:n}}\right) \leq \delta_n^{(6)} \tag{80}
$$

where $\delta_n^{(6)} = b_n(\sqrt{\delta_n^{(5)}} + \delta_n^{(4)})$.

Proof. We have

$$\mathbb{V}\left(\tilde{p}_{Z_{1:b_n}^{1:n}}, q_{Z_{1:b_n}^{1:n}}\right) = \mathbb{V}\left(\tilde{p}_{Z_{1:b_n}^{1:n}}, \prod_{i=1}^{b_n} q_{Z^{1:n}}\right) \tag{81}$$

$$\leq \mathbb{V}\left(\tilde{p}_{Z_{1:b_n}^{1:n}}, \prod_{i=1}^{b_n} \tilde{p}_{Z_i^{1:n}}\right) + \mathbb{V}\left(\prod_{i=1}^{b_n} \tilde{p}_{Z_i^{1:n}}, \prod_{i=1}^{b_n} q_{Z^{1:n}}\right) \tag{82}$$

$$\leq \mathbb{V}\left(\tilde{p}_{Z_{1:b_n}^{1:n}}, \prod_{i=1}^{b_n} \tilde{p}_{Z_i^{1:n}}\right) + \sum_{i=1}^{b_n} \mathbb{V}\left(\tilde{p}_{Z_i^{1:n}}, q_{Z^{1:n}}\right) \tag{83}$$

$$\leq b_n \sqrt{\delta_n^{(5)}} + b_n \delta_n^{(4)} \tag{84}$$

where we have used the results of Lemmas 9 and 11. □

We finally conclude the proof of covertness as follows. We let $\{T_i\}_{i=1}^{b_n}$ be the independent uniform random variables denoting the choice of the start time in each of the chained b_n transmission windows. Note that the distribution $\widehat{Q}^{b_n N}$ induced by the code may be written as $\widehat{Q}^{b_n N}(\mathbf{z}) = \mathbb{E}_{T_1,\cdots,T_{b_n}}\left(\widehat{Q}^{b_n N}_{T_1,\cdots,T_n}(\mathbf{z})\right)$ where for $(t_1,\cdots,t_{b_n}) \in [\![1, N']\!]^{b_n}$

$$\widehat{Q}^{b_n N}_{t_1,\cdots,t_n}(\mathbf{z}) = \widehat{Q}^{b_n n}(\mathbf{z_t}) \prod_{i=1}^{b_n} \left(\prod_{k=1}^{t_i - 1} Q_0(z_{(i-1)N+k}) \prod_{k=t_i+n}^{N} Q_0(z_{(i-1)N+k}) \right) \tag{85}$$

and $\mathbf{z_t}$ contains the components $\{z_{(i-1)N+t_i-1+k}\}_{i\in[\![1,b_N]\!],k\in[\![1,n]\!]}$ corresponding to the positions where a code is used in every transmission window. This formulation allows us to isolate the distribution $\widehat{Q}^{b_n n}(\mathbf{z_t})$, which corresponds to the chained coded blocks of length n. We also define the process $Q_{\alpha_n}^{b_n N}$ as

$$Q_{\alpha_n}^{b_n N}(\mathbf{z}) \triangleq \mathbb{E}_{T_1,\cdots,T_{b_n}}\left(\prod_{i=1}^{b_n} Q_{\alpha_n,T_i}^N(\mathbf{z}_i)\right) = \prod_{i=1}^{b_n} \mathbb{E}_{T_i}\left(Q_{\alpha_n,T_i}^N(\mathbf{z}_i)\right), \tag{86}$$

where $\mathbf{z} = (\mathbf{z}_1, \ldots, \mathbf{z}_{b_n})$. We then bound $\mathbb{V}\left(\widehat{Q}^{b_n N}, Q_0^{\otimes b_n N}\right)$ as follows.

$$\mathbb{V}\left(\widehat{Q}^{b_n N}, Q_0^{\otimes b_n N}\right) \overset{(a)}{\leq} \mathbb{V}\left(\widehat{Q}^{b_n N}, Q_{\alpha_n}^{b_n N}\right) + \mathbb{V}\left(Q_{\alpha_n}^{b_n N}, Q_0^{\otimes b_n N}\right) \tag{87}$$

$$\overset{(b)}{\leq} \mathbb{V}\left(\mathbb{E}_{T_1,\cdots,T_{b_n}}\left(\widehat{Q}^{b_n N}_{T_1,\cdots,T_n}\right), \mathbb{E}_{T_1,\cdots,T_{b_n}}\left(\prod_{i=1}^{b_n} Q_{\alpha_n,T_i}^N\right)\right) + \sqrt{b_n \mathbb{D}\left(Q_{\alpha_n}^N \| Q_0^{\otimes N}\right)} \tag{88}$$

$$\overset{(c)}{\leq} \mathbb{E}_{T_1,\cdots,T_{b_n}}\left(\mathbb{V}\left(Q^{b_n N}_{T_1,\cdots,T_n}\right), \prod_{i=1}^{b_n} Q_{\alpha_n,T_i}^N\right) + O(\sqrt{b_n \beta_n}) \tag{89}$$

$$\overset{(d)}{=} \mathbb{V}\left(\widehat{Q}^{b_n n}, Q_{\alpha_n}^{\otimes b_n n}\right) + O(\sqrt{b_n \beta_n}) \tag{90}$$

$$\overset{(e)}{=} \mathbb{V}\left(\tilde{p}_{Z_{1:b_n}^{1:n}}, q_{Z_{1:b_n}^{1:n}}\right) + O(\sqrt{b_n \beta_n}) \tag{91}$$

$$\overset{(f)}{=} \delta_n^{(6)} + O(\sqrt{b_n \beta_n}), \tag{92}$$

where (a) follows by the triangle inequality; (b) follows from the definition of $\widehat{Q}^{b_n N}$ and $Q_{\alpha_n}^{b_n N}$, Pinsker's inequality, and the product form of $Q_{\alpha_n}^{b_n N}$ and $Q_0^{\otimes b_n N}$ over the b_n blocks; (c) follows from the convexity of total variation distance and Lemma 3; (d) follows from the definition of $\mathbb{V}\left(Q^{b_n N}_{T_1,\cdots,T_n}\right)$ and $\prod_{i=1}^{b_n} Q_{\alpha_n,T_i}^N$; (e) follows by substituting the notation used in the analysis of the chained scheme; (f) follows from

Lemma 12. With our choice of β_n, b_n, and δ_n, note that $\lim_{n\to\infty} \delta_n^{(6)} = 0$ and $\lim_{n\to\infty} b_n\beta_n = 0$, hence establishing covertness (note that we use the condition $b_n \in o\left(\frac{1}{\beta_n}\right)$ here).

5. Conclusions

In this paper, we have proposed a coding scheme for covert communication based on polar codes. Although our scheme offers a first explicit solution of covert communication in a non-trivial regime, its performance is still far from that of random codes. The proven speed of polarization severely limits the rate at which the average weight of codewords can decay, and in particular we cannot approach the average codeword weight on the order of $\sqrt{n}$ required by the square root law. We have circumvented this issue by hiding the transmission window within a larger window as in [5,6], and at least in the regime for which our proofs hold, the proposed scheme achieves the best known rates. Several extensions and improvements are currently under investigation, particularly the refinement of Proposition 3 to improve the constant κ and the use of non-binary polar codes in conjunction with pulse-position modulation [22].

Supplementary Materials: The following are available online at www.mdpi.com/1099-4300/20/1/3/s1.

Acknowledgments: This work was supported in part by the National Science Foundation under award 1527387, the Agence Nationale pour la Recherche under award 13-BS03-0008, and a grant from the Région Lorraine.

Author Contributions: All authors contributed equally to the work, and have read and approved the final manuscript.

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

References

1. Bash, B.; Goeckel, D.; Towsley, D. Limits of reliable communication with low probability of detection on AWGN channels. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1921–1930.
2. Che, P.H.; Bakshi, M.; Jaggi, S. Reliable deniable communication: Hiding messages in noise. In Proceedings of the IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013; pp. 2945–2949.
3. Bloch, M.R. Covert communication over noisy channels: A resolvability perspective. *IEEE Trans. Inf. Theory* **2016**, *62*, 2334–2354.
4. Wang, L.; Wornell, G.W.; Zheng, L. Fundamental limits of communication with low probability of detection. *IEEE Trans. Inf. Theory* **2016**, *62*, 3493–3503.
5. Bash, B.; Goeckel, D.; Towsley, D. LPD communication when the warden does not know when. In Proceedings of the IEEE International Symposium on Information Theory, Honolulu, HI, USA, 29 June–4 July 2014; pp. 606–610.
6. Arumugam, K.S.K.; Bloch, M.R. Keyless asynchronous covert communication. In Proceedings of the IEEE Information Theory Workshop, Cambridge, UK, 11–14 September 2016; pp. 191–195.
7. Zhang, Q.; Bakshi, M.; Jaggi, S. Computationally efficient deniable communication. In Proceedings of the IEEE International Symposium on Information Theory, Barcelona, Spain, 10–15 July 2016; pp. 2234–2238.
8. Han, T.; Verdú, S. Approximation theory of output statistics. *IEEE Trans. Inf. Theory* **1993**, *39*, 752–772.
9. Bloch, M.R.; Hayashi, M.; Thangaraj, A. Error-control coding for physical-layer secrecy. *Proc. IEEE* **2015**, *103*, 1725–1746.
10. 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.
11. Chou, R.A.; Bloch, M.R. Polar coding for the broadcast channel with confidential messages: A random binning analogy. *IEEE Trans. Inf. Theory* **2016**, *62*, 2410–2429.
12. Guruswami, V.; Xia, P. Polar codes: Speed of polarization and polynomial gap to capacity. *IEEE Trans. Inf. Theory* **2015**, *61*, 3–16.
13. Hassani, S.H.; Alishahi, K.; Urbanke, R.L. Finite-length scaling for polar codes. *IEEE Trans. Inf. Theory* **2014**, *60*, 5875–5898.
14. Mondelli, M.; Hassani, S.H.; Urbanke, R.L. Unified scaling of polar codes: Error exponent, scaling exponent, moderate deviations, and error floors. *IEEE Trans. Inf. Theory* **2016**, *62*, 6698–6712.

15. Pfister, H.D.; Urbanke, R. Near-optimal finite-length scaling for polar codes over large alphabets. In Proceedings of the IEEE International Symposium on Information Theory, Barcelona, Spain, 10–15 July 2016; pp. 215–219.
16. Renes, J.; Renner, R. Noisy channel coding via privacy amplification and information reconciliation. *IEEE Trans. Inf. Theory* **2011**, *57*, 7377–7385.
17. Yassaee, M.; Aref, M.; Gohari, A. Achievability proof via output statistics of random binning. *IEEE Trans. Inf. Theory* **2014**, *60*, 6760–6786.
18. Mondelli, M.; Hassani, S.H.; Sason, I.; Urbanke, R.L. Achieving marton's region for broadcast channels using polar codes. *IEEE Trans. Inf. Theory* **2015**, *61*, 783–800.
19. Arikan, E. Source polarization. In Proceedings of the IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 899–903.
20. Chou, R.A.; Bloch, M.R.; Abbe, E. Polar coding for secret-key generation. *IEEE Trans. Inf. Theory* **2015**, *61*, 6213–6237.
21. Csiszár, I.; Körner, J. *Information Theory: Coding Theorems for Discrete Memoryless Systems*; Akademiai Kiado: Budapest, Hungary, 1981.
22. Bloch, M.R.; Guha, S. Optimal covert communications using pulse-position modulation. In Proceedings of the IEEE International Symposium on Information Theory, Aachen, Germany, 25–30 June 2017; pp. 2835–2839.