Abstract—This paper investigates the problem of ensuring secure communication through error-correcting coding methods. A practical structured secure coding design is considered for a general wiretap channel, in which the main channel and the eavesdropper channel are binary-input symmetric-output memoryless (BISOM) channels. The proposed secure error-correcting code has a nested code structure. The nesting is based on cosets of a capacity-achieving sequence for binary erasure channels (BECs). The corresponding achievable secrecy rate is derived based on an erasure decomposition for the eavesdropper channel and an Bhattacharyya-equivalent channel construction for the main channel. Those two techniques allow a “degraded” erasure wiretap channel to be built and, hence, significantly simplify the practical coding design for secure transmission.

I. INTRODUCTION

Rapid advances in wireless technology are quickly taking us toward a pervasively connected world in which a vast array of wireless devices, from iPhones to biosensors, seamlessly communicate with one another. However, wireless communication is particularly susceptible to eavesdropping due to its broadcast nature. Security and privacy issues have become critical for wireless providers and enterprise networks. The need for reliable and secure data communication over wireless networks is more important than ever before. The goal of this paper is to study practical coding schemes at the very basic physical layer level to secure wireless communication systems.

Physical-layer security techniques have a rather long history starting with the work of Shannon [1] and Wyner [2]. Shannon provided the first truly scientific treatment of secrecy in [1], in which a secret key is considered to protect confidential messages. The ingenuity of his remarkable work lies not only in the method used therein but also in the incisive formulation that Shannon made of the secrecy problem based on information-theoretic concepts. Wyner proposed an alternative approach to secure communication schemes in his seminal paper [2], where he introduced the so-called wiretap channel model. As shown in Fig. 1, the confidential communication via a discrete memoryless main channel is eavesdropped upon by a wiretapper, who has access to the degraded channel output. Wyner demonstrated that secure communication is possible without sharing a secret key and determined the secrecy capacity for a wiretap channel. Construction of explicit and practical secure encoders and decoders whose performance is as good as promised by Wyner is still an unsolved problem in the general case except for the type II wiretap channel [3] and the binary erasure wiretap channel [4].

![Fig. 1. Wiretap channel model.](image)

We note that channel coding and secrecy coding are closely related. Roughly speaking, the goal of channel coding is to send a message with sufficient redundancy so that it can be understood by the receiver; whereas the goal of secrecy coding is to provide sufficient randomness so that the message can not be understood by anyone else. In modern communication networks, error-correcting codes have traditionally been designed to ensure communication reliability. Various coding techniques have been thoroughly developed and tested for ensuring reliability of virtually all current, point-to-point physical channels. However, only very limited work has considered using error-correcting codes to ensure security as well. In [3], Ozarow and Wyner considered error-correcting code design for a type II binary erasure wiretap channel based on a coset coding scheme. This problem was further studied in connection with the generalized Hamming weights in [6]. More recently, low-density parity-check (LDPC) based coding design has been studied for binary erasure wiretap channels in [4] and type II wiretap channels in [5]. In another line of recent related work, secret key agreement protocols based on powerful LDPC codes have been studied by several authors [7]–[9]. Designing practical secure coding schemes for general wiretap channels is still an open problem.

In this work, we focus on secure coding for a class of wiretap channels, in which the main channel and the eavesdropper channel are binary-input symmetric-output memoryless (BISOM) channels. We first review and summarize the prior results of [2]–[4]. Inspired by [10], we propose a more general secure nested code structure. Next, we propose a secure nested code sequence for the BISOM wiretap channel. The nesting is based on cosets of a capacity-achieving sequence for binary erasure channels (BECs). We derive the corresponding achievable secrecy rate based on an erasure decomposition for the
eavesdropper channel and a Bhattacharyya-equivalent channel construction for the main channel. Those two techniques allow a “degraded” erasure wiretap channel to be built and, hence, significantly simplify practical coding design for secure transmission.

The remainder of the paper is organized as follows. Section II introduces the wiretap channel model and preliminaries. Section III states our main result on the design of secure nested codes for wiretap channels. The paper is concluded in Section IV. A detailed proof of our main result is provided in the Appendix.

II. PRELIMINARIES

We review here some definitions and results from [2]–[4] and propose a secure nested coding structure, which serves as preliminary material for the rest of the paper.

A. Wiretap Channel Model

We consider the classic wiretap channel [2] illustrated in Fig. 1, where the transmitter sends a confidential message to a legitimate receiver via a main channel in the presence of an eavesdropper channel. Both the main and the eavesdropper channels are discrete memoryless and, in particular, the eavesdropper channel is a degraded version of the main channel. A confidential message \( w \in W \) is mapped into a channel input sequence \( x = [x_1, x_2, \ldots, x_n] \) of length \( n \), where \( W = \{1, \ldots, M\} \) and \( M \) is the number of distinct confidential messages that may be transmitted. The outputs from the main channel and the eavesdropper channel are \( y \) and \( z \), respectively. The level of ignorance of the eavesdropper with respect to the confidential message is measured by the equivocation \( H(W|Z) \). A rate-equivocation pair \((R, R_e)\) is achievable if there exists a rate-\( R \) code sequence with the average probability of error \( P_e \to 0\) as the code length \( n \) goes to infinity and with the equivocation rate \( R_e \) satisfying

\[
R_e \leq \lim_{n \to \infty} \frac{H(W|Z)}{n}.
\]

Perfect secrecy requires that, for any \( \epsilon_0 > 0 \) there exists a sufficiently large \( n \) so that the normalized equivocation satisfies

\[
H(W|Z)/n \geq H(W)/n - \epsilon_0.
\]

Hence, perfect secrecy happens when \( R_e = R \), i.e., all the information transmitted over the main channel is secret. The capacity-equivocation region of the wiretap channel \( X \to (Y, Z) \) contains all rate-equivocation pairs \((R, R_e)\) that satisfy

\[
R_e \leq R \leq I(X;Y)
\]

and

\[
0 \leq R_e \leq I(X;Y) - I(X;Z).
\]

B. Wyner Codes and Secrecy Bins

It is instructive to review first the problem of unstructured secure code design in terms of the stochastic encoding scheme introduced by Wyner [2]. As demonstrated in [2], the secrecy capacity of the wiretap channel is achieved by using a stochastic encoder, where a mother codebook \( C_0(n) \) of length \( n \) is randomly partitioned into “secret bins” or sub-codes \( \{C_1(n), C_2(n), \ldots, C_M(n)\} \). A message \( w \) is associated with a sub-code \( C_w(n) \) and the transmitted codeword is randomly selected within the sub-code. Such a codebook allows for decomposing the twofold objective of achieving both reliability and secrecy into two separate objectives. The mother code \( C_0(n) \) provides enough redundancy so that the legitimate receiver can decode the message reliably, whereas each sub-code is sufficiently large and, hence, introduces enough randomness so that the eavesdropper’s uncertainty about the transmitted message can be guaranteed.

Even though [2] does not describe a structured coding scheme, it does suggest that encoding for reliability and confidentiality would be achieved by partitioning the mother code into sub-codes. This idea has been extended to structured or semi-structured codes by using coset codes in [3], [4].

C. Secure Nested Codes

In the following, we construct secure error-correcting codes with the nested code structure [10].

We consider a nested linear code pair \((C_0(n), C_1(n))\), where \( C_0(n) \) is a fine code of rate \( R_0 \), and \( C_1(n) \) a coarse code of rate \( R_1 \). We use the fine code \( C_0(n) \) as the mother code, which is partitioned into \( M \) sub-codes consisting of the coarse code \( C_1(n) \) and its cosets. Each coset corresponds to a confidential message. The transmitter encodes a message \( w \in W \) into an \( n \)-tuple of coded symbols randomly selected within the corresponding coset \( C_w(n) \). By determining the coset of the transmitted codeword, the legitimate receiver can retrieve the confidential message \( w \). The redundancies provided by each coset are used to confuse the eavesdropper who has full knowledge about the code and its cosets. We refer to a code structured in this manner as a secure nested code. We note that the code \( C_1(n) \) and its cosets have the same (Hamming) distance properties. Hence, the secure coding design problem is to find a suitable nested code pair \((C_0(n), C_1(n))\) that satisfies both confidentiality and reliability requirements. Denote by \( \{C(n)\} \) a sequence of binary linear codes, where \( C(n) \) is an \((n, k_n)\) code having a common rate \( R_e = k_n/n \). Now, we define the secure nested code sequence as follows.

**Definition 1 (secure code sequence):** \( \{C_0(n), C_1(n)\} \) is a secure nested code sequence if \( C_0(n) \) is a (mother) fine code of rate \( R_0 \), and \( C_1(n) \) is a coarse code of rate \( R_1 \) so that \( C_1(n) \subseteq C_0(n) \) and \( R_1 \leq R_0 \). The information rate of this code sequence is \( R_0 - R_1 \).

D. Good Code, Capacity-Achieving Codes and Noise Thresholds

Following MacKay [11], we say that a code sequence \( \{C(n)\} \) is good if it achieves arbitrarily small word (bit) error probability when transmitted over a noisy channel at a nonzero rate \( R_e \). Capacity-achieving codes are good codes whose rate \( R_e \) is equal to the channel capacity. The class of good codes

\[1\]

In this paper, we consider binary-input wiretap channels and nested linear codes. This idea can be extended to nested lattice codes for channels with continuous inputs.
includes, for example, turbo, LDPC, and repeat-accumulate codes, whose performance is characterized by a threshold behavior in a single channel model [12].

**Definition 2 (noise threshold):** For a (single) channel model described by a single parameter, the noise threshold of a code sequence \{C(n)\} is defined as the worst case channel parameter value at which the word (bit) error probability decays to zero as the codeword length \(n\) increases.

For example, the noise threshold is described in terms of the erasure rate threshold \(\delta^*\) for a binary erasure channel (BEC) and the SNR threshold \(\lambda^*\) for a binary-input additive white Gaussian noise (AWGN) channel. Noise thresholds associated with good codes and the corresponding maximum-likelihood (ML), “typical pair”, and iterative decoding algorithms have been studied in [13]–[15].

Two capacity-achieving LDPC code sequences for BECs have been described in [16], called the Tornado sequence \(C_T(n)\) and the right-regular sequence \(C_R(n)\). For both of these sequences, the erasure rate threshold \(\delta^* = 1 - R_c = \epsilon\).

**E. Erasure Wiretap Channel**

Let BEC-WT\(\epsilon_0, \epsilon_1\) denote a binary erasure wiretap channel with the erasure rate \(\epsilon_0\) on the main channel and the erasure rate \(\epsilon_1\) on the eavesdropper channel. By employing the capacity-achieving code as the coarse code in the secure nested code structure, we reorganize the results of [4] in the following lemma.

**Lemma 1:** Consider a nested LDPC code sequence \((C_0(n), C_1(n))\), where the fine code \(C_0(n)\) of rate \(R_0\) has an erasure rate threshold \(\delta_0\) and the coarse code \(C_1(n)\) of rate \(R_1\) is a capacity-achieving LDPC code sequence for the binary erasure channel. Suppose that the secure nested code sequence \((C_0(n), C_1(n))\) is transmitted over a BEC-WT\(\epsilon_0, \epsilon_1\). If

\[
\delta_0 \geq \epsilon_0 \quad \text{and} \quad R_1 \leq 1 - \epsilon_1,
\]

then the code sequence can be successfully transmitted over the erasure wiretap channel with perfect secrecy.

**III. DESIGN SECURE NESTED CODES FOR WIRETAP CHANNELS**

In this section, we consider practical coding design for secure communication over the BISOM wiretap channel. We note that, even for a general binary-input channel without a secrecy constraint, designing practical capacity-achieving codes is still an open problem. Hence, to satisfy the perfect secrecy requirement, we allow a nonzero gap between the transmission rate and the secrecy capacity.

The basic idea of our approach is as follows. Since it is hard to directly design secure codes for such a channel, alternatively, we consider a “degraded” erasure wiretap channel described using the approach from Fig. 2 and described in the following.

**Fig. 2.** An equivalent degraded erasure wiretap channel.

**A. \(\gamma\)-Equivalent Main Channel**

The Bhattacharyya parameter is widely used to characterize the “noisiness” of the channel in coding theory. For a BISOM channel, the Bhattacharyya parameter \(\gamma\) can be expressed in terms of the channel transition probability \(p(x|y)\) as follows

\[
\gamma = \sum_{y \in Y} \sqrt{p(y|1)p(-y|1)}.
\]

We say that two binary-input symmetric-output memoryless channels are \(\gamma\)-equivalent if they have the same Bhattacharyya parameter \(\gamma\).

Now we consider the following \(\gamma\)-equivalent channel lemma established in [17].

**Lemma 2:** [17, Theorem 4.2] Suppose a binary erasure channel with an erasure rate \(\delta\) is within the iterative decoding (density evolution) threshold of an ensemble of codes. Then so is any other BISOM with a Bhattacharyya parameter \(\gamma \leq \delta\).

Lemma 2 states that if a code ensemble can be successfully transmitted over a BEC, then it can be universally communicated over any \(\gamma\)-equivalent BISOM channel in a reliable manner. Hence, we can focus on the code design for a \(\gamma\)-equivalent erasure channel, as shown in Fig. 2, instead of for the original main channel.

Any BISOM channel with the same Bhattacharyya parameter as a BEC must have a higher capacity, which has been formally proved in [18]. In this sense, we say that the \(\gamma\)-equivalent BEC channel is less capable than the original main channel.

**B. Enhanced Eavesdropper Channel**

Here, we will construct an “enhanced” eavesdropper channel based on the following erasure decomposition Lemma.

**Lemma 3:** Consider a BISOM channel \(X \rightarrow Z\) with the channel transition distribution

\[
f(z) \triangleq p(z|X = 1).
\]

Let us define

\[
\epsilon \triangleq \int_{-\infty}^{\infty} \min[f(z), f(-z)]\, dz.
\]

Then, the channel \(X \rightarrow Z\) can be represented as the concatenation of a binary erasure channel \(X \rightarrow Z'\) with erasure probability \(\epsilon\) and a memoryless ternary-input symmetric-output channel \(Z' \rightarrow Z\).

**Proof:** This Lemma follows from [19]. We provide a proof in Appendix A for the sake of completeness.
Lemma 3 illustrates that the original channel $X \rightarrow Z$ is a physical degraded version of the BEC $X \rightarrow Z'$ and, hence, we can consider security issues via the enhanced erasure eavesdropper channel.

### C. Main Result

the $\gamma$-equivalent main channel and the enhanced eavesdropper channel together form a “degraded” erasure wiretap channel, $X \rightarrow Y' \rightarrow Z'$ as shown in Fig. 2. The code design for BISOM channels based on the secure nested code LDPC sequence for the degraded erasure wiretap channel is summarized in the following theorem.

**Theorem 1:** Consider a nested LDPC code sequence $(C_0(n), C_1(n))$, where the fine code $C_0(n)$ of rate $R_0$ has an erasure rate threshold $\delta_0$ and the coarse code $C_1(n)$ of rate $R_1$ is a capacity-achieving LDPC code sequence for the binary erasure channel. Let $X \rightarrow Y \rightarrow Z$ denote a BISOM wiretap channel with channel transition distribution $p(z, y|x)$, let $\gamma$ denote the Bhattacharyya parameter of the main channel defined in (2), and let $\epsilon$ denote the erasure rate of the enhanced eavesdropper channel defined in (4). If

$$\delta_0 \geq \gamma, \quad R_1 = 1 - \epsilon \tag{5}$$

and

$$\gamma < \epsilon, \quad R_1 \tag{6}$$

then the LDPC nested code sequence can be successfully transmitted over the wiretap channel with perfect secrecy.

### IV. Conclusion

In this paper, we have addressed the problem of secure coding design for a binary-input symmetric-output memoryless wiretap channel. We have proposed a secure error-correcting code in terms of a nested code structure. We have studied the secure nested coding scheme based on cosets of a capacity-achieving LDPC sequence for BECs. In order to derive the corresponding achievable secrecy rate, we have introduced a framework based on the erasure decomposition for the eavesdropper channel and the $\gamma$-equivalent channel construction for the main channel. The proposed approach has allowed us to build a “degraded” binary erasure wiretap channel and, hence, has significantly simplified the practical coding design for secure transmission.

### APPENDIX

#### A. Proof of Lemma 3

**Proof:** We consider a binary-input channel

$$X \rightarrow (Z', Z)$$

with the joint channel transition probabilities satisfying

$$p(z, z'|X = 1) = \begin{cases} [f(z) - f(-z)]^+ & z' = 1 \\ \min[f(z), f(-z)] & z' = 0 \\ 0 & z' = -1 \end{cases} \tag{7}$$

and

$$p(z, z'|X = -1) = \begin{cases} 0 & z' = 1 \\ \min[f(z), f(-z)] & z' = 0 \\ [f(-z) - f(z)]^+ & z' = -1 \end{cases} \tag{8}$$

where $x \in \{-1, +1\}$, $z' \in \{-1, 0, 1\}$, and $[a]^+ = \max(0, a)$. Based on the definitions in (4), (7) and (8), we can verify that

$$p(z'|x) = \begin{cases} 1 - \epsilon & z' = x \\ \epsilon & z' = 0 \\ 0 & z' \neq x \end{cases} \tag{9}$$

and

$$p(z|x) = \begin{cases} f(z) & x = 1 \\ f(-z) & x = -1 \end{cases} \tag{10}$$

i.e., the channel $X \rightarrow Z'$ is a BEC with the erasure rate $\epsilon$ and the channel $X \rightarrow Z$ is the original BISOM channel. Furthermore, note that

$$p(z|Z' = 1) = \frac{[f(z) - f(-z)]^+}{1 - \epsilon} = p(z|Z' = 1, x)$$

$$p(z|Z' = 0) = \min[f(z), f(-z)] = p(z|Z' = 0, x)$$

and

$$p(z|Z' = -1) = \frac{[f(-z) - f(z)]^+}{1 - \epsilon} = p(z|Z' = -1, x). \tag{11}$$

The channel output $Z$ is a physically degraded version of the output $Z'$ and, hence, we have the desired result. ■

#### B. Proof of Theorem 1

**Proof:** We divide our proof into two steps.

**Step 1—binary erasure main channel:** We first consider the special case where the main channel is a BEC channel with an erasure rate $\epsilon_0$ and the eavesdropper channel is a BISOM channel with the channel transition probability

$$f(z) = p(z|X = 1).$$

To develop the achievable secrecy rate, we enhance the eavesdropper channel based on Lemma 3, and, thus, the new channel $X \rightarrow (Y, Z')$ is a binary erasure wiretap channel BEC-WT($\epsilon_0, \epsilon_1$), where

$$\epsilon_1 = \epsilon = \int_{-\infty}^{\infty} \min[f(z), f(-z)] \, dz.$$  

Based on the Bhattacharyya parameter definition (2) and the condition (6), we have the following relationship between the erasure rate pair

$$\epsilon_0 = \gamma < \epsilon = \epsilon_1.$$  

Now, by applying Lemma 1, we can design a sequence of LDPC nested codes $(C_0(n), C_1(n))$, which satisfy the condition (5) and can be successfully transmitted over the erasure wiretap channel BEC-WT($\epsilon_0, \epsilon_1$) with perfect secrecy. Note that the confidential message $W$, the enhanced eavesdropper BEC output $Z'$, and the received signal at the eavesdropper $Z$ satisfy the Markov relationship

$$W \leftrightarrow Z' \leftrightarrow Z.$$
The data processing inequality [20] implies that the normalized equivocation can be bounded as 
\[ H(W|Z)/n \geq H(W'|Z)/n. \]

Hence, the requirement of perfect secrecy can also be achieved in the original wiretap channel \( X \to (Y,Z) \).

**Step 2—BISOM main channel:** Next, we consider the general case where both the main channel and the eavesdropper channel are BISOM channels. Let \( \gamma \) denote the Bhattacharyya parameter of the main channel defined in (2). Based on the result in step 1, the sequence of LDPC nested codes \( (C_0(n), C_1(n)) \) can achieve the requirement of perfect secrecy. Here, we need only to consider the reliability requirement for the main channel. However, Lemma 2 implies that if a code ensemble can be successfully transmitted over a BEC, then it can be universally communicated over any \( \gamma \)-equivalent BISOM channel in a reliable manner. This completes the proof of Theorem 1.

**REFERENCES**


