entropy

MDPI

Article

Implications of Coding Layers on Physical-Layer Security: A Secrecy Benefit Approach

Willie K. Harrison [1,*], Elise Beard [1], Scott Dye [1], Erin Holmes [2], Kaela Nelson [1], Marco A. C. Gomes [3] and João P. Vilela [4]

[1] Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT 84602, USA
[2] Department of Mathematics and Computer Science, Colorado College, Colorado Springs, CO 80903, USA
[3] Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, 3004-531 Coimbra, Portugal
[4] CISUC and Department of Informatics Engineering, University of Coimbra, 3004-531 Coimbra, Portugal
* Correspondence: willie.harrison@byu.edu; Tel.: +1-801-422-4355

Received: 20 June 2019; Accepted: 30 July 2019; Published: 1 August 2019

Abstract: In this work, we consider the pros and cons of using various layers of keyless coding to achieve secure and reliable communication over the Gaussian wiretap channel. We define a new approach to information theoretic security, called practical secrecy and the secrecy benefit, to be used over real-world channels and finite blocklength instantiations of coding layers, and use this new approach to show the fundamental reliability and security implications of several coding mechanisms that have traditionally been used for physical-layer security. We perform a systematic/structured analysis of the effect of error-control coding, scrambling, interleaving, and coset coding, as coding layers of a secrecy system. Using this new approach, scrambling and interleaving are shown to be of no effect in increasing information theoretic security, even when measuring the effect at the output of the eavesdropper's decoder. Error control coding is shown to present a trade-off between secrecy and reliability that is dictated by the chosen code and the signal-to-noise ratios at the legitimate and eavesdropping receivers. Finally, the benefits of secrecy coding are highlighted, and it is shown how one can shape the secrecy benefit according to system specifications using combinations of different layers of coding to achieve both reliable and secure throughput.

Keywords: physical-layer security; equivocation; Gaussian wiretap channel; concatenated coding

1. Introduction

Physical-layer security [1] is currently undergoing a resurgence of interest and activity, specifically regarding progressing towards real-world application of information theoretic security principles [2–4]. Some of the early works in information theoretic security [5–7] laid the foundations of secrecy capacity for various versions of the wiretap channel. Secrecy coding constructions to date [8,9] are known explicitly, however, only for discrete memoryless versions of the wiretap channel, and, hence, appear to fall short of solving the practical security issues for real channels.

Since explicit secrecy code constructions that achieve information theoretic security over the Gaussian wiretap channel are still missing [10,11], non-information theoretic security metrics have arisen to address practical concerns, e.g., the security gap [12,13], degrees of freedom in decoders [14], etc. Although some of these security metrics allow for analysis over any wiretap channel model, they have met resistance due to their weaker security guarantees. These approaches are typically based on probability of error analysis at the eavesdropper assuming a specific decoder, rather than information theoretic analysis that would hold regardless of the chosen decoder. More recently, however, an additional information theoretic security approach has begun to take shape, where the eavesdropper's decoder outputs are used to estimate the security of a system [10,15,16]. This allows one to precisely and efficiently conduct the security analysis of systems over any wiretap channel variation through Monte Carlo simulation [4]. Since this new technique must also choose a specific decoder for the eavesdropper, it therefore requires one to assume that the eavesdropper will use the best (and hopefully provably best) decoder available. In this paper, we formalize the new information theoretic security definition and say that a code *achieves practical secrecy* if the entropy of the message given the best known decoder output can be shown to be approximately equal to the entropy of the message at the eavesdropper. Since the metric is a practical one, its application to finite blocklength codes with known explicit constructions is highlighted herein. Along with this new security metric, we present the idea of a code's *secrecy benefit*, which, over the Gaussian wiretap channel, shows the increase in confusion at the eavesdropper for the coded scenario over the uncoded scenario as a function of signal-to-noise ratio.

In addition to presenting these new metrics, we showcase their application in analyzing various coding approaches over the Gaussian wiretap channel. Although explicit code constructions exist that can both correct errors for legitimate parties and keep secrets from eavesdroppers over discrete memoryless wiretap channels [8,9,17], some works have sought solutions to tandem secrecy and reliability coding for real-world channels using a layered, or concatenated, coding approach [10,18,19]. The contributions of this paper include a systematic and structured analysis of error-control coding, interleaving, scrambling, and coset-based secrecy coding, as layers in a physical-layer security coding system. We chose these layers so as to represent fundamentally different approaches to coding for secrecy over the Gaussian wiretap channel, and leave additional layers of coding, such as other constructions of wiretap codes [8,9], for future work. Note also that scrambling and interleaving have been considered as keyed layers of coding as well [18,19], although herein we only consider keyless versions of these. The analysis of both reliability and security is carried out for each of the layers in isolation, as well as for various combinations of layers of coding. Benefits and drawbacks are provided for the inclusion of each layer in a concatenated coding system for physical-layer security. Among them, we show that keyless layers of scrambling and interleaving provide no secrecy benefit over the uncoded case, error-control coding layers can be used to increase security or reliability depending on the signal-to-noise ratios at the legitimate and eavesdropping receivers, and the secrecy benefit of coset-based secrecy codes can be shaped using error-control coding.

The rest of the paper is organized as follows. Section 2 provides the setup for the paper, including the system model and the metrics that define our new approach to information theoretic security. In Section 3, we consider layers of coding for reliable data transfer between legitimate nodes in a network, and show how error-control coding must leak information in the strictest sense of security, but, with the new approach, it may be considered a help to security efforts for a range of signal-to-noise ratios at the eavesdropper's receiver. Layers of secure coding are considered in Section 4, where we start with simpler (and more controversial) layers of coding such as interleaving and scrambling, and move on to wiretap coding. Several combinations of layers of coding are then analyzed and discussed in Section 5, and conclusions are made in Section 6.

2. Setup

In this section, we establish the system model and discuss metrics for quantifying both reliability and security. For notation, we assign capital letters to random variables and matrices, lowercase letters to realizations of random variables, calligraphic letters to ranges of random variables, superscripts to indicate the size of vectors and matrices, and subscripts to index the elements of vectors and matrices.

2.1. System Model

In this paper, we consider the Gaussian wiretap channel model, as portrayed in Figure 1, where Alice wishes to send a message M chosen uniformly at random from $\mathcal{M} = \{0, 1, \ldots, 2^k - 1\}$ to Bob in the presence of an eavesdropper named Eve. Alice encodes the message to produce a length-n binary codeword, which is modulated to produce a set of n source symbols X^n, which are then transmitted over two parallel independent Gaussian channels. The main channel of communications dictates Bob's received signal, and we call the set of Bob's decision variables Y^n, which are then decoded to produce Bob's estimate of the message $\hat{M}$. Eve's received signal is obtained over the eavesdropper's channel, and the set of Eve's decision variables are denoted Z^n. Eve may choose to attempt to decode the data as well. If she does, then her estimate of the message is called $\tilde{M}$. When considering $\tilde{M}$ in this paper, we assume that Eve uses the best known decoder to produce her estimate of the message. Additive white circularly symmetric zero-mean Gaussian noise processes at the main and eavesdropper's channels are denoted N_B^n and N_E^n, respectively, and thus,

$$Y^n = X^n + N_B^n, \tag{1}$$
$$Z^n = X^n + N_E^n. \tag{2}$$

The respective variances in all dimensions of the signal space for noise processes N_B^n and N_E^n are denoted σ_B^2 and σ_E^2.

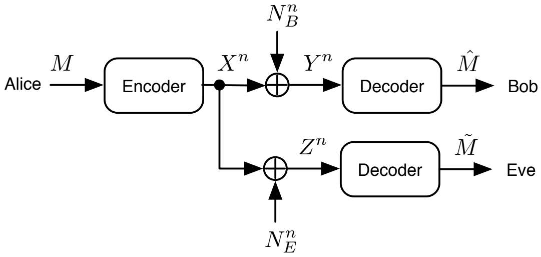


Figure 1. The Gaussian wiretap channel model.

The encoder and decoder may be comprised of several layers of coding, as shown in Figure 2. All codes are block codes. The dimension of each encoding layer is equal to the number of input bits required at the layer to do a single encoding operation, while the blocklength of each encoding layer is equal to the number of output bits produced by the layer in a single encoding operation. Unless otherwise stated, it is assumed that each symbol of the message M is encoded separately at each layer. That is, the dimension of the Layer i encoder matches exactly the blocklength of the Layer $(i-1)$ encoder for $i = 2, 3, \ldots, L$. Thus, there is no need to buffer codewords at any layer of the encoding or decoding process to perform the operations. For the Layer 1 encoder, a message symbol from M is first mapped to k bits, and k is the dimension of Layer 1. All codes are assumed to be binary, and coding operations are computed in $\mathbb{F}_2$. The rate of each coding layer is simply given as the ratio of the layer's dimension over its blocklength. The digital modulator and demodulator are assumed to be in place [20], but are not depicted as *layers* in Figure 2.

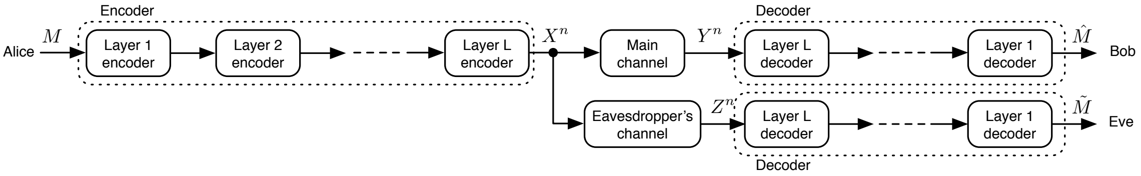


Figure 2. Portrayal of a layered, or concatenated, coding approach to physical-layer security.

2.2. Metrics

The equivocation $\mathbb{H}(M|Z^n)$ is now a standard metric to consider when analyzing security over the wiretap channel model. If

$$\mathbb{H}(M|Z^n) = \mathbb{H}(M), \tag{3}$$

we may say the system achieves *perfect secrecy* in some sense, although the original Shannon definition of perfect secrecy [21] required that $\mathbb{H}(M|X^n) = \mathbb{H}(M)$. If we can only state that for a sequence of codes with blocklength n

$$\lim_{n\to\infty} \frac{1}{n}\mathbb{H}(M|Z^n) = \mathbb{H}(M), \tag{4}$$

then the system is said to achieve *weak secrecy*, while

$$\lim_{n\to\infty} \mathbb{H}(M|Z^n) = \mathbb{H}(M) \tag{5}$$

indicates that a system achieves *strong secrecy*. Each of these security definitions assumes that messages are chosen uniformly at random from $\mathcal{M}$. If the strong secrecy condition can be shown to hold for any possible distribution on the messages, then we may state that the system achieves *semantic secrecy*. Of note to this work is that it has been shown recently in [11] that lattice codes can be used to achieve semantic secrecy over the Gaussian wiretap channel, and yet knowledge of how to build such codes is still forthcoming. Assuming we could find constructions to achieve information theoretic security in any sense over the Gaussian wiretap channel, we also note that, other than for perfect secrecy, the security analysis requires blocklength to grow in the limit to infinity. It remains unclear as to how these security measures should or should not be changed for finite blocklength codes, although the problem has been addressed using various approaches [4,22–24].

While the general trend has been to employ stricter definitions of secrecy over time as codes have been discovered that achieve weak, then strong, then semantic secrecy, albeit only for discrete memoryless wiretap channel model variants [8,9], in this paper, we move in the opposite direction in order to formulate a security metric that has immediate application over real-world channels when finite blocklength codes are deployed. The new metric is more practical than many of the traditional metrics, and is to be computed for specific codes of specific blocklengths. The metric also returns a feel for the operational level of security, seeing as any real system will require the eavesdropper to attempt to decode the message. Some suggest that security metrics based on bit-error rate (BER) may be of use [12,13] when information theoretical metrics prove difficult to use, since in practice we really only care if Eve can decode and obtain the secret message. However, it is still desirable to root even practical metrics in information theory, even if we must analyze Eve's decoder outputs rather than Z^n.

Definition 1. *We say that a finite blocklength coding system achieves* practical secrecy *at a level of δ_s if, for the best known decoding algorithm,*

$$\mathbb{H}(M|\tilde{M}) - \mathbb{H}(M) < \delta_s. \tag{6}$$

In other words, we'd like $\mathbb{H}(M|\tilde{M}) \approx \mathbb{H}(M)$. This notion of secrecy has been used over the Gaussian wiretap channel in a few previous works [10,15,16]. One of the main reasons this notion of secrecy is so attractive is that, when Eve is forced to decode, a continuous random variable Z^n is transformed into a discrete random variable $\tilde{M}$, which makes the entropy calculation straightforward. Note that, when the code's error properties are not a function of the choice of $m \in \mathcal{M}$, then

$$\begin{aligned}
\mathbb{H}(M|\tilde{M}) &= -\sum_{\tilde{m}\in\mathcal{M}}\sum_{m\in\mathcal{M}} p_{M,\tilde{M}}(m,\tilde{m}) \log_2 p_{M|\tilde{M}}(m|\tilde{m}) && (7)\\
&= -\sum_{m\in\mathcal{M}} p_M(m) \sum_{\tilde{m}\in\mathcal{M}} p_{\tilde{M}|M}(\tilde{m}|m) \log_2 \frac{p_{\tilde{M}|M}(\tilde{m}|m)p_M(m)}{p_{\tilde{M}}(\tilde{m})} && (8)\\
&= -\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\sum_{\tilde{m}\in\mathcal{M}} p_{\tilde{M}|M}(\tilde{m}|m) \log_2 p_{\tilde{M}|M}(\tilde{m}|m) && (9)\\
&= -\sum_{\tilde{m}\in\mathcal{M}} p_{\tilde{M}|M}(\tilde{m}|m) \log_2 p_{\tilde{M}|M}(\tilde{m}|m), && (10)
\end{aligned}$$

for any choice of $m \in \mathcal{M}$. If $|\mathcal{M}|$ is small enough, this quantity can be estimated through Monte Carlo simulation of the encoding and decoding layers [4,10].

The goals of communication over the Gaussian wiretap channel for this paper are then to analyze and test specific layers of coding to ascertain whether they can be used to achieve both of the following constraints in a layered coding architecture: (i) $\Pr(M \neq \hat{M}) < \delta_r$ (the reliability constraint), and (ii) $\mathbb{H}(M|\tilde{M}) - \mathbb{H}(M) < \delta_s$ (the practical secrecy constraint), for positive δ_r and δ_s as small as possible and fixed n.

We will find it useful to compare several various coded cases with the uncoded case in terms of reliability and secrecy. A new mechanism for showcasing the usefulness of a coding technique for physical-layer security can help.

Definition 2. *Let $\mathbb{H}_U(M|\tilde{M})$ be the practical secrecy when no coding layers are employed in the layered coding system of Figure 2, and let $\mathbb{H}_{\mathcal{C}}(M|\tilde{M})$ be the practical secrecy measure when code $\mathcal{C}$ is employed in the system, where $\mathcal{C}$ may comprise one or more layers of coding. Then the* secrecy benefit *of $\mathcal{C}$ is defined as*

$$\mathcal{B}(\mathcal{C}) = \mathbb{H}_{\mathcal{C}}(M|\tilde{M}) - \mathbb{H}_U(M|\tilde{M}), \tag{11}$$

which measures the uncertainty about M added at a receiving node over and above the uncertainty level of uncoded transmissions.

We will find it useful to plot the secrecy benefit of many codes as a function of the signal-to-noise ratio in the eavesdropper's channel.

3. Layers of Coding for Reliable Data Transfer

In this section, we discuss the general effects of adding a layer of error-control coding at Layer L in Figure 2. If the binary input to this encoder is k bits and the binary output is n bits, then we say the rate of the code is $R = k/n$. The overhead of the code is used to detect and correct errors [25]. Intuitively, we may decide to add a code of this nature to fine tune the reliability measure for Bob over the main channel, with the goal to retain as much security against Eve as possible. This approach has been highlighted in the recent works [24,26], where the eavesdropper's channel state is assumed to be unknown. Rather than worry about achieving information theoretic security against Eve, one may instead decide to use the best existing code for secrecy to maximize the equivocation subject to the reliability constraint. In this way, coding for secrecy becomes an optimization problem rather than a strict security problem, and security endeavors at other layers in the protocol stack, e.g., cryptography, fill in to help when needed.

3.1. Error-Control Coding Leaks Information

First, let us consider the effect of adding an error-control code at Layer L in terms of $\mathbb{H}(M|Z^n)$ when the eavesdropper's channel is a binary symmetric channel (BSC), and no layers of coding are used besides the one layer of error-control coding. The BSC flips bits at Eve's receiver independently with probability p. Let us consider only a three bit transmission over this channel, where bits A and B are chosen independently at random, and bit

$$C = A \oplus B, \tag{12}$$

where $\oplus$ indicates addition in $\mathbb{F}_2$. Bit C is then generated by one of the simplest parity-check equations possible for error control over bits A and B. Let the corresponding outputs from the channel for A, B, and C, be given as

$$A' = A \oplus E_A, \tag{13}$$

$$B' = B \oplus E_B, \tag{14}$$

$$C' = C \oplus E_C, \tag{15}$$

respectively, where

$$E_X = \begin{cases} 1, \text{ with probability } p, \\ 0, \text{ with probability } 1-p, \end{cases} \tag{16}$$

for each of the three independent cases: $X = A, B, C$.

We wish to calculate $\mathbb{H}(A|A',B',C')$ and compare the quantity to $\mathbb{H}(A|A') = \mathbb{H}_2(p)$ to see the secrecy effect brought on by this simplest of codes, where $\mathbb{H}_2(p)$ is the binary entropy function evaluated at p. First, note that

$$\mathbb{H}(A|A',B',C') = -\sum_{a,a',b',c' \in \{0,1\}} p(a',b',c'|a)p(a)\log_2 \frac{p(a',b',c'|a)p(a)}{p(a',b',c')}. \tag{17}$$

It can be shown that

$$p(a',b',c') = \begin{cases} \frac{1}{4}(1-p)^3 + \frac{3}{4}p^2(1-p), & \text{if } a' \oplus b' = c', \\ \frac{3}{4}p(1-p)^2 + \frac{1}{4}p^3, & \text{if } a' \oplus b' \neq c'. \end{cases} \tag{18}$$

Note that $a' \oplus b' = c'$ when there are an even number of bit flips through the BSC since $a \oplus b = c$ at the transmitter, but $a' \oplus b' \neq c'$ when there are an odd number of bit flips through the BSC for the same reason. Similarly,

$$p(a',b',c'|a) = \begin{cases} \frac{1}{2}p^2(1-p) + \frac{1}{2}(1-p)^3, & \text{if } a' \oplus b' = c', a = a', \\ p^2(1-p), & \text{if } a' \oplus b' = c', a \neq a', \\ p(1-p)^2, & \text{if } a' \oplus b' \neq c', a = a', \\ \frac{1}{2}p(1-p)^2 + \frac{1}{2}p^3, & \text{if } a' \oplus b' \neq c', a \neq a'. \end{cases} \tag{19}$$

When we put this all together noting that $p(a) = p(a') = \frac{1}{2}$, then $\mathbb{H}(A|A',B',C') < \mathbb{H}(A|A')$ for all p except for the three trivial cases where $p \in \{0, 0.5, 1\}$ as shown in Figure 3. The implication is that the introduction of a check sum that involves the bit A reduces the entropy of A at the receiver as long as the channel is not perfectly clean or perfectly noisy. This effect gets larger with the introduction of more checksums involving A.

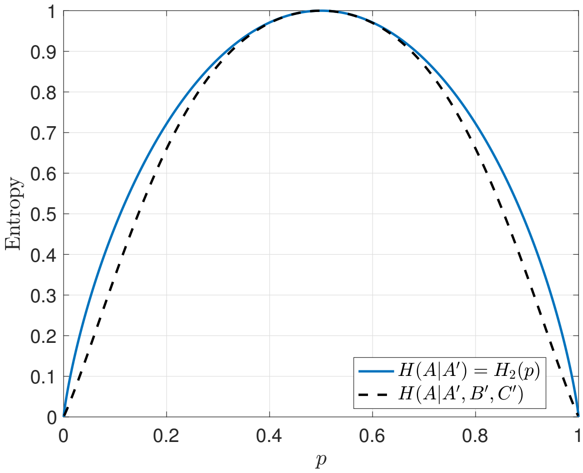
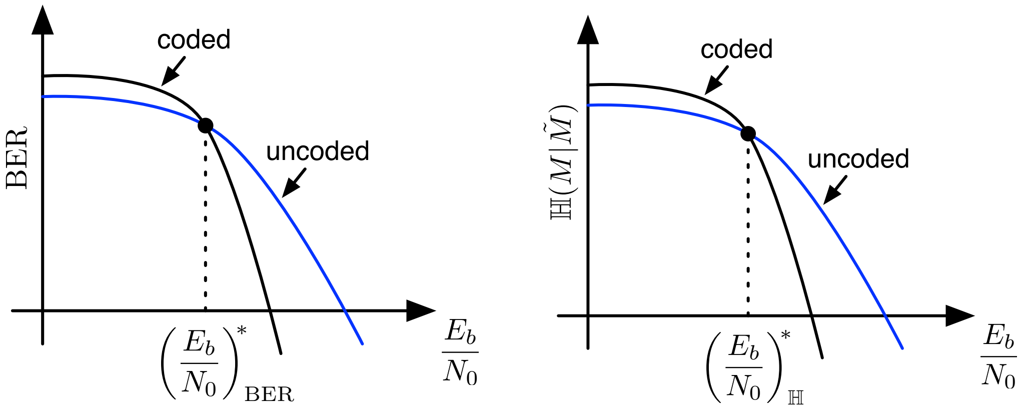


Figure 3. Conditional entropy of a message bit at the receiver for the uncoded and error-control coded case. Curves indicate that even a simple parity check leaks information compared to the uncoded case.

3.2. Error-Control Coding Shapes Practical Secrecy

It seems as if layers of error-control coding are doomed to leak information to the eavesdropper, and this is certainly true when secrecy is quantified using the traditional equivocation $\mathbb{H}(M|Z^n)$, as shown in the previous section. For the practical secrecy metric, however, $\mathbb{H}(M|\tilde{M})$ does not necessarily indicate the leakage of information for some signal-to-noise ratios. Let us consider uncoded binary phase shift keying (BPSK) as compared to coded BPSK over a Gaussian channel, where the coding is a simple layer of error control coding as before. Figure 4a illustrates BER curves for the two cases, and points out that there exists an $\frac{E_b}{N_0}$ threshold value, which we call $\left(\frac{E_b}{N_0}\right)^*_{\text{BER}}$, where the bit-error rates of the two cases are equivalent. For $\frac{E_b}{N_0}$ below this threshold, the coded case exhibits a higher error rate compared to the uncoded case, while for $\frac{E_b}{N_0}$ above this threshold, the coded case exhibits a lower error rate. Standard distance property arguments argue the existence of such a threshold for all possible error-control codes. Once the channel is degraded below a certain amount, errors in the channel are more likely to result in incorrect codewords at the output of the decoder than the correct codeword. What is not as obvious, although still somewhat intuitive, is that there also exists a threshold in $\frac{E_b}{N_0}$, which we call $\left(\frac{E_b}{N_0}\right)^*_{\mathbb{H}}$ for the $\mathbb{H}(M|\tilde{M})$ curve of a code, whereby $\frac{E_b}{N_0}$ below the threshold will result in a rise in practical secrecy and $\frac{E_b}{N_0}$ above the threshold will result in a decrease in practical secrecy. This idea is illustrated in Figure 4b.

It will be shown in Section 5 that the two threshold values $\left(\frac{E_b}{N_0}\right)^*_{\text{BER}}$ and $\left(\frac{E_b}{N_0}\right)^*_{\mathbb{H}}$ are not equal in many cases. Typically, we require worse signal-to-noise ratio at Eve's receiver to operate left of $\left(\frac{E_b}{N_0}\right)^*_{\mathbb{H}}$ than we do to operate to the left of $\left(\frac{E_b}{N_0}\right)^*_{\text{BER}}$, which satisfies our intuition that practical secrecy based on $\mathbb{H}(M|\tilde{M})$ should be easier to achieve than weak or strong secrecy based on $\mathbb{H}(M|Z^n)$, but harder to achieve than secrecy based only on bit-error rates. It is furthermore true that layers of error-control coding may be used to shape secrecy benefit curves $\mathcal{B}(\mathcal{C})$ for codes $\mathcal{C}$ at other layers. Examples of this idea are given in Section 5.



(**a**) (**b**)

Figure 4. (**a**) illustration of the $\frac{E_b}{N_0}$ crossover point $\left(\frac{E_b}{N_0}\right)^*_{\mathrm{BER}}$ in bit-error rate curves for coded and uncoded data; (**b**) illustration of the $\frac{E_b}{N_0}$ crossover point $\left(\frac{E_b}{N_0}\right)^*_{\mathbb{H}}$ in $\mathbb{H}(M|\hat{M})$ curves for coded and uncoded data, whose existence implies that error-control coding increases practical secrecy below the crossover point and decreases practical secrecy above the crossover point.

4. Layers of Coding for Secure Data Transfer

In this section, we consider several layers of coding that are meant to secure the message against eavesdropping, and analyze the utility of keyless scrambling (and interleaving as a special case), in addition to coset-based secrecy coding.

4.1. Practical Security Coding Layers

Simple rate-one layers of coding have been argued to fill practical roles of error propagation in numerous works including [13], and even some of our own past works [10,18,19]. While the BER may be affected by such layers of coding, we show in this section that $\mathbb{H}(M|\tilde{M})$ is unaffected by rate one bijective coding layers.

Let S be a rate one encoder in the form of a square $k \times k$ binary matrix, where the $1 \times k$ output of the encoder x_{out} is produced from the $1 \times k$ input of the encoder x_{in} by the encoding operation

$$x_{\mathrm{out}} = x_{\mathrm{in}} S. \tag{20}$$

Suppose that S^{-1} is the decoder so that

$$x_{\mathrm{in}} = x_{\mathrm{out}} S^{-1} \tag{21}$$

for all possible x_{in}. Notice that S and S^{-1} define a bijection between $\mathbb{F}_2^k$ and itself, and constitute a layer of rate-one coding.

Theorem 1. *A rate-one encoding function S that forms a bijection between $\mathbb{F}_2^k$ and itself for any positive integer k, has secrecy benefit $\mathcal{B}(S) = 0$ over a discrete memoryless symmetric eavesdropper's channel.*

Proof. Recall that

$$\mathcal{B}(S) = \mathbb{H}_S(M|\tilde{M}) - \mathbb{H}_U(M|\tilde{M}), \tag{22}$$

where M is coded with S to produce X, which is transmitted over the eavesdropper's channel to produce Z. Since the channel is symmetric, then its noise properties are independent of the choice of $x \in \mathcal{X}$. Z is then mapped to $\tilde{M}$ via S^{-1}. Note the transition probabilities $p_{\tilde{M}|M}(\tilde{m}|m)$ for this encoding, and recognize that fixing $m \in \mathcal{M}$ produces $|\mathcal{M}|$ probabilities whose order is dependent on the choice of m, but whose collection of values are independent of the choice of m, as in (10). Since S and S^{-1} define a bijection on $\mathbb{F}_2^k$, these probabilities are identical to the collection of probabilities $p_{Z|X}(z|x)$ that define hard decisions over the eavesdropper's channel. Thus,

$$-\sum_{\tilde{m}\in\mathcal{M}} p(\tilde{m}|m)\log_2 p(\tilde{m}|m) = -\sum_{z\in\mathcal{Z}} p(z|x)\log_2 p(z|x), \tag{23}$$

which implies that

$$\mathbb{H}_S(M|\tilde{M}) = \mathbb{H}_U(M|\tilde{M}), \tag{24}$$

by application of (10). □

The implications of this theorem are that keyless layers of scrambling and interleaving (which is a special case of scrambling) provide no secrecy benefit in terms of $\mathbb{H}(M|\tilde{M})$. We give the following as a corollary to Theorem 1.

Corollary 1. *Let M be encoded to produce X, which is transmitted over a discrete memoryless channel resulting in Z, which is decoded to produce $\tilde{M}$. If the encoding function S is a rate-one bijective function between $\mathbb{F}_2^k$ and itself for any positive integer k, then*

$$\mathbb{H}(X|Z) = \mathbb{H}(M|Z^n) = \mathbb{H}(M|\tilde{M}). \tag{25}$$

This indicates that the stricter form of the secrecy benefit calculated as $\mathbb{H}(M|Z^n) - \mathbb{H}_U(M|\tilde{M})$ is also zero.

Proof. Two uses of the data processing theorem result in

$$\mathbb{I}(X;Z) \geq \mathbb{I}(M;Z) \geq \mathbb{I}(M;\tilde{M}), \tag{26}$$

which can be rewritten in terms of equivocations as

$$\mathbb{H}(X|Z) \leq \mathbb{H}(M|Z) \leq \mathbb{H}(M|\tilde{M}). \tag{27}$$

Thus, the corollary is proved by Theorem 1. □

Note that these results hold only for encoding functions S that form a bijection over $\mathbb{F}_2^k$, which is not true if multiple coded blocks are interleaved or scrambled together. Thus, there may still be some benefit to inter-block rate-one encoding functions, although intra-block rate-one encoding functions appear to have no effect of increasing the information theoretic security.

4.2. Information Theoretic Security Coding Layers

In this section, we contrast the simple rate-one encoding schemes from the previous section with coset codes for the wiretap channel [5,27]. While it was shown that rate-one codes are of no effect over symmetric discrete memoryless channels (and hence, hard decision Gaussian channels), wiretap codes, on the other hand, are of immense effect in increasing the practical secrecy.

Let G be the $(n-k)\times n$ generator matrix of an $(n, n-k)$ binary linear block code $\mathcal{C}$. Then, let G' be a $k\times n$ matrix such that $G^* = \begin{bmatrix} G \\ G' \end{bmatrix}$ is a full rank $n\times n$ matrix in $\mathbb{F}_2$. Let H be the $k\times n$ parity check matrix associated with $\mathcal{C}$. Then, the encoding function of a coset wiretap code computes a codeword as

$$x^n = \begin{bmatrix} m' & m \end{bmatrix} G^*, \tag{28}$$

where m' is a randomly chosen $1\times(n-k)$ vector in $\mathbb{F}_2^{n-k}$. Note that this encoding function picks a specific element of a coset of $\mathcal{C}$ as the codeword x^n, where m chooses the coset of $\mathcal{C}$ and m' chooses the codeword within the coset. Codes such as these were originally showcased in [5], and have been used in many wiretap code constructions [8]. Confusion about the message is achieved as an eavesdropper uncertainty of the proper coset is increased. Errors in the eavesdropper's channel facilitate this confusion. Note that such a code has a secrecy rate of $R = k/n$, but the overhead of the code is used to cause confusion, rather than error correction. Since all codewords in the same coset have the same syndrome [25], codewords can be mapped back to messages via the calculation

$$s = rH^T, \tag{29}$$

where r is the received word at the receiver, and s is the syndrome of that word. Although it can be made so that $m = s$ as in [4], storing the mapping from s to m is sufficient for decoding. These codes have been analyzed in great depth, and variants of them have been proposed to achieve weak, strong, and semantic secrecy [9] over various discrete memoryless wiretap channel models. In this work, we apply them as the Layer 1 code in Figure 2, and show how other layers combine to shape the secrecy benefit of these codes. We will also show in Section 5 that these codes are the only layers of this study with any significant help to achieving secure throughput.

5. Results and Discussion

In this section, we consider several different combinations of layers of coding, and show the BER curves, the practical secrecy $\mathbb{H}(M|\tilde{M})$ curves, and the secrecy benefit $\mathcal{B}(\mathcal{C})$ curves. Here, $\mathcal{C}$ denotes the coding operation inclusive of all deployed layers. This set of results is presented for two different sets of parameters on the coding layers to showcase the general effect first using small algebraic codes and then that the trends hold for slightly larger codes. The following cases are all presented as combinations of coding layers for both sets of coding parameters:

- Zero layers of coding (uncoded case);
- One layer: error-control coding (ECC);
- One layer: scrambling;
- One layer: interleaving (special case of scrambling);
- One layer: coset coding;
- Two layers: scrambling, then ECC;
- Two layers: interleaving, then ECC;
- Two layers: coset coding, then ECC;
- Three layers: coset coding, then scrambling, then ECC.

BPSK modulation is applied to all Layer L encoding outputs.

5.1. Algebraic Code Examples with Inter-Block Processing

In this section, we use the $(7, 4)$ Hamming code. ECC layers use the Hamming code for error correction, while the coset coding layer is chosen to have the same rate of $R = 4/7$. The dual of the Hamming code (the $(7, 3)$ simplex code) is used as the base linear code for the coset coding to accomplish this. Scramblers and interleavers are applied at the smallest block level; thus, S is a 4×4 binary matrix with inverse S^{-1} in $\mathbb{F}_2$. Although all analysis to this point has only allowed for block-by-block processing, we allow inter-block processing to match the dimensions of the chosen codes. This requires buffering between encoders and decoders in practice. All decoders are hard-decision in this section, and decoding the ECC layers is performed using the syndrome method [25]. We employ state-of-the-art decoders in the next section of examples.

As a first step to the analysis, consider the BER curves in Figure 5. Note that the single layer of interleaving does not even affect the BER curve, as it lays directly over the uncoded curve. This is true since an error prior to deinterleaving remains only one error in the deinterleaver output, even though its location has changed. The ECC curves exhibit a crossover point $\left(\frac{E_b}{N_0}\right)^*_{\text{BER}}$ around 6 dB. As expected, scrambling does appear to increase the BER, and the cases with wiretap codes in play have much higher error rates.

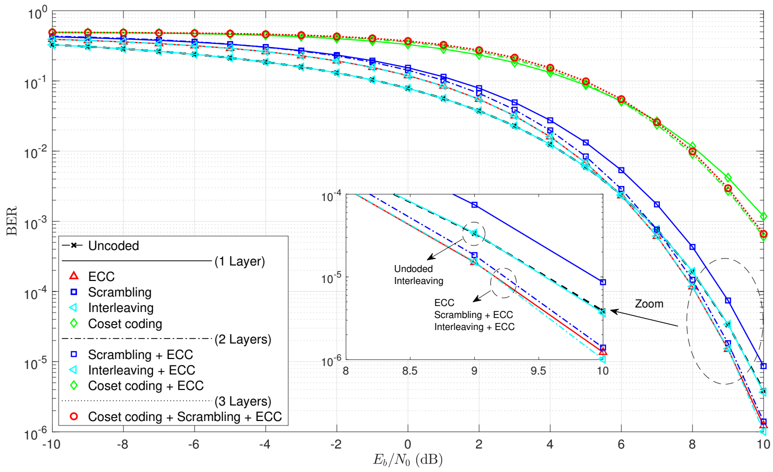
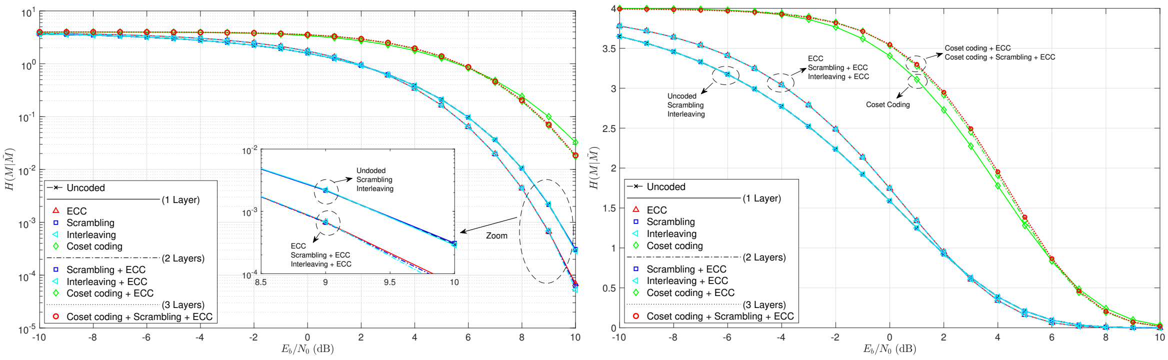


Figure 5. Bit-error rate curves for various combinations of coding layers and the set of algebraic code examples.

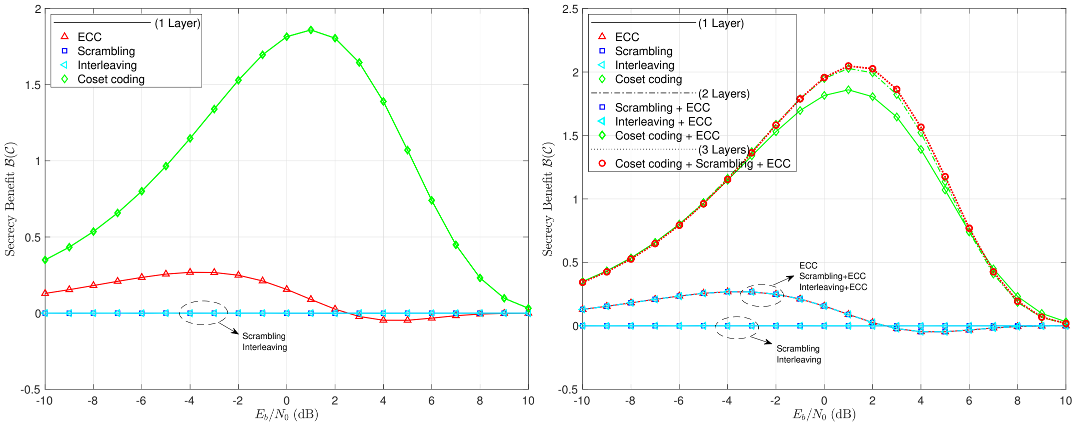
The practical secrecy curves for these same coding scenarios are given in Figure 6 on both a log scale and a linear scale. We see here much less difference between the several cases for $\mathbb{H}(M|\tilde{M})$ than we saw for BER in Figure 5. When considering the BER, we had seven unique curves between the nine tested scenarios. Only interleaving appeared not to make a difference in the curves. Now, when considering $\mathbb{H}(M|\tilde{M})$ curves, however, there appear to only be four unique curves. Scrambling and interleaving are both shown to be of no effect as predicted. The four unique cases are essentially the uncoded case, the ECC single layer case, the coset coding single layer case, and the coset coding plus ECC double layer case. We see the threshold $\left(\frac{E_b}{N_0}\right)^*_{\mathbb{H}}$ at around 2.5 dB, which, as predicted is much less than $\left(\frac{E_b}{N_0}\right)^*_{\text{BER}}$. This implies that practical secrecy is harder to achieve than secrecy based on BER, as discussed previously.



(**a**) (**b**)

Figure 6. (**a**) practical secrecy $\mathbb{H}(M|\tilde{M})$ curves as a function of $\frac{E_b}{N_0}$ on a log scale for the algebraic code examples; (**b**) practical secrecy $\mathbb{H}(M|\tilde{M})$ curves as a function of $\frac{E_b}{N_0}$ on a linear scale for the algebraic code examples.

Finally, we explore the secrecy benefit of the many cases in Figure 7. Of greatest interest is that even coset coding only provides a positive secrecy benefit when compared to the uncoded case for a range of $\frac{E_b}{N_0}$ around the usual operating points of radio receivers (roughly −10 dB to +10 dB). For lower $\frac{E_b}{N_0}$, the channel is so bad that the uncoded case is essentially secure on its own, while, for higher $\frac{E_b}{N_0}$, even the coset coding communicates the information error free. In either case, the code cannot be deemed to be helping the situation. The ECC layer has a positive secrecy benefit up until $\left(\frac{E_b}{N_0}\right)^*_{\mathbb{H}}$, and a negative secrecy benefit afterwards. The secrecy benefits of scrambling and interleaving are shown to be zero as expected. When we consider multi-layer coding, it appears that more is going on. Scrambling appears to help, although we need to remember that we have allowed inter-block scrambling for this case. Essentially, the only significantly different secrecy benefit curve in the multi-layer coding schemes is the one that combines ECC with coset coding. We see hints of a shaping effect of $\mathcal{B}(\mathcal{C})$, where the ECC can be used to affect the secure and reliable regions of signal-to-noise ratio, even when codes are small.



(**a**) (**b**)

Figure 7. (**a**) secrecy benefit to coding $\mathcal{B}(\mathcal{C})$ for single layer codes; (**b**) secrecy benefit to coding $\mathcal{B}(\mathcal{C})$ for all coding scenarios tested.

5.2. Code Examples with Intra-Block Processing Only

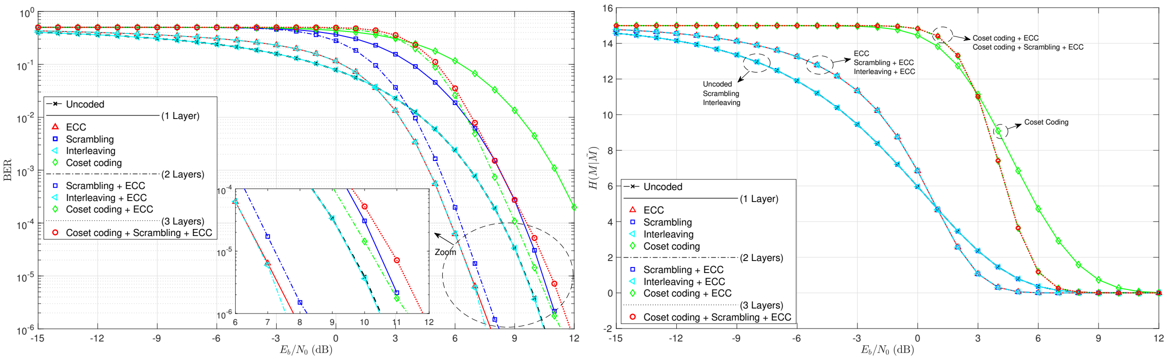
In this section, we are more strict as to ensuring that each message block is processed independently. That is, the dimensions of Layer 2 and Layer 3 codes are set equal to the blocklengths of Layer 1 and Layer 2 codes, respectively. We also increase the dimension of the Layer 1 encoder from 4 in the last section to 15 in this section. While the dimension is still small, it is necessary to present high fidelity simulation results with the new metrics, and even the small size shows the benefit of each layer and how combinations of layers can work together to achieve specific effects. All ECC and coset coding layers are encoded at $R = 1/2$. The parity-check matrix that governs ECC layers is chosen using the socket approach to irregular low-density parity-check (LDPC) code construction [28] with the edge-perspective degree distribution pair [25]

$$\lambda(x) = 0.3157x^2 + 0.41672x^3 + 0.4381x^7, \tag{30}$$

$$\rho(x) = 0.4381x^6 + 0.5619x^7. \tag{31}$$

This same code is used as the base linear code for the coset coding. Finally, soft-decision decoding is used whenever possible, although some layers require hard decisions to do the decoding operations, e.g., scrambling and coset decoding. Soft demodulation and soft-information belief propagation at the ECC decoder are both used.

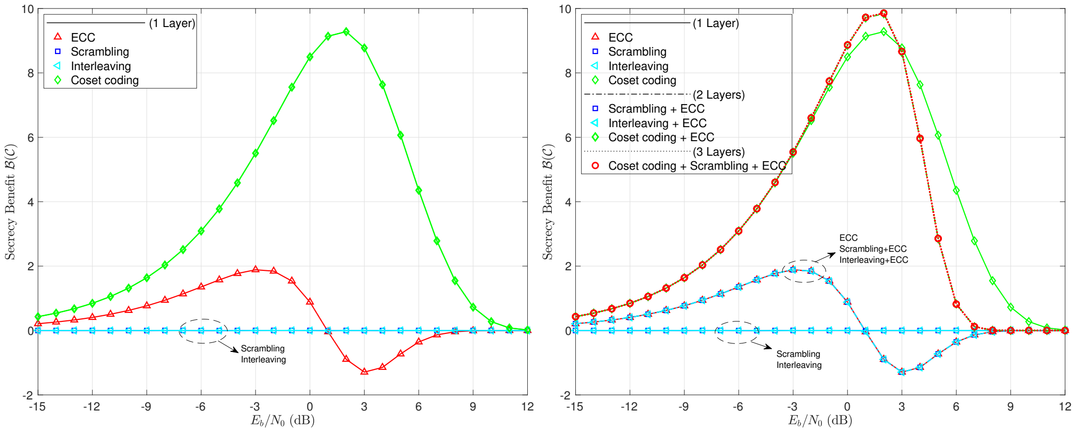
This new set of code parameters give very similar results as those given by the algebraic set of codes based on Hamming and simplex codes. Note in Figure 8 the BER and practical secrecy curves. Again, we see plenty of differences across the coding layer combinations for BER, but only four cases for $\mathbb{H}(M|\tilde{M})$. Only ECC and coset codes make any difference in practical secrecy. The thresholds of crossover come in around $\left(\frac{E_b}{N_0}\right)^*_{\text{BER}} \approx 2$ dB and $\left(\frac{E_b}{N_0}\right)^*_{\mathbb{H}} \approx 1$ dB, again indicating that it is harder to make a code help the secrecy cause when using $\mathbb{H}(M|\tilde{M})$ as the measuring stick, rather than BER.



(**a**) (**b**)

Figure 8. (**a**) bit-error rate curves for various combinations of coding layers and the set of irregular coding examples; (**b**) practical secrecy $\mathbb{H}(M|\tilde{M})$ curves as a function of $\frac{E_b}{N_0}$ on a linear scale for the irregular code examples.

The secrecy benefit curves are given in Figure 9, where we see again that scrambling and interleaving are of no effect when measuring practical secrecy. The notion of using a layer of ECC to shape the secrecy benefit of a coset code is a bit more believable when looking at the multi-layer coding schemes here. Note that the combination of these two layers increases the peak secrecy benefit, moves its location slightly to the left, and brings about a reliable region of operating signal-to-noise ratios sooner than the coset coding only case. Scrambling and interleaving, once again, prove to be useless in increasing the practical secrecy or secrecy benefit in any way.



(**a**) (**b**)

Figure 9. (**a**) secrecy benefit to coding $\mathcal{B}(\mathcal{C})$ for single layer codes; (**b**) secrecy benefit to coding $\mathcal{B}(\mathcal{C})$ for all coding scenarios tested.

6. Conclusions

In conclusion, this paper provides a fresh approach to information theoretic security over the Gaussian wiretap channel for finite blocklength codes. It is shown how to quantify the practical secrecy and the secrecy benefit of a code, and this approach is used to systematically analyze the effects of various combinations of layers of coding in a concatenated coding scheme. Scrambling and interleaving are shown to have no effect on the practical secrecy, and thereby achieve zero secrecy benefit. On the other hand, error-control coding and wiretap coding are shown to have a significant secrecy benefit over uncoded transmissions. Layers of error-control coding may be used to shape the secrecy benefit of wiretap coding when concatenated coding schemes are employed.

Author Contributions: Conceptualization, funding acquisition, methodology, project administration, and supervision, W.K.H., M.A.C.G. and J.P.V.; formal analysis, W.K.H. and E.H.; investigation, W.K.H., E.B., S.D., E.H. and K.N.; software, W.K.H., E.B., S.D. and K.N.; validation, W.K.H.; visualization, W.K.H. and M.A.C.G., writing—original draft preparation, W.K.H.; writing—review and editing, all.

Funding: This research was funded by the following entities and projects: the US National Science Foundation (Grant Award Number 1761280), projects SWING2 (PTDC/EEI-TEL/3684/2014) and MobiWise (P2020 SAICTPAC/001/2015), funded by Fundos Europeus Estruturais e de Investimento (FEEI) through Programa Operacional Competitividade e Internacionalização—COMPETE 2020, and by National Funds from FCT—Fundação para a Ciência e a Tecnologia, through projects POCI-01-0145-FEDER-016753 and UID/EEA/50008/2019, and European Union's ERDF (European Regional Development Fund).

Acknowledgments: The authors wish to acknowledge the help of Ximena Briceno, who altered code to run various simulations in the research phase of the project, and Jack Pfister, who helped plot some of the functions in Section 3.1.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

BPSK	binary phase shift keying
BER	bit-error rate
BSC	binary symmetric channel
LDPC	low-density parity-check

References

1. Bloch, M.; Barros, J. *Physical Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011.
2. Jensen, B.; Clark, B.; Flanary, D.; Norman, K.; Rice, M.; Harrison, W.K. Physical-Layer Security: Does it Work in a Real Environment? In Proceedings of the 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7.
3. Flanary, D.; Jensen, B.; Clark, B.; Norman, K.; Nelson, N.; Rice, M.; Harrison, W.K. Manufacturing an Erasure Wiretap Channel from Channel Sounding Measurements. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; pp. 1–5.
4. Pfister, J.; Gomes, M.; Vilela, J.P.; Harrison, W.K. Quantifying Equivocation for Finite Blocklength Wiretap Codes. In Proceedings of the IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
5. Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
6. Csiszár, I.; Körner, J. Broadcast Channels with Confidential Messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [CrossRef]
7. Leung-Yan-Cheong, S.K.; Hellman, M.E. The Gaussian Wire-tap Channel. *IEEE Trans. Inf. Theory* **1978**, *IT-24*, 451–456. [CrossRef]
8. Harrison, W.K.; Almeida, J.; Bloch, M.R.; McLaughlin, S.W.; Barros, J. Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security. *IEEE Signal Process. Mag.* **2013**, *30*, 41–50. [CrossRef]
9. Bloch, M.R.; Hayashi, M.; Thangaraj, A. Error-Control Coding for Physical-Layer Secrecy. *Proc. IEEE* **2015**, *103*, 1725–1746. [CrossRef]
10. Harrison, W.K.; Fernandes, T.; Gomes, M.A.C.; Vilela, J.P. Generating a Binary Symmetric Channel for Wiretap Codes. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2128–2138. [CrossRef]
11. Ling, C.; Luzzi, L.; Belfiore, J.C.; Stehlé, D. Semantically Secure Lattice Codes for the Gaussian Wiretap Channel. *IEEE Trans. Inf. Theory* **2014**, *60*, 6399–6416. [CrossRef]
12. Klinc, D.; Ha, J.; McLaughlin, S.W.; Barros, J.; Kwak, B.J. LDPC Codes for the Gaussian Wiretap Channel. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 532–540. [CrossRef]

13. Baldi, M.; Bianchi, M.; Chiaraluce, F. Coding With Scrambling, Concatenation, and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analysis. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 883–894. [CrossRef]
14. Harrison, W.K.; Almeida, J.; McLaughlin, S.W.; Barros, J. Coding for Cryptographic Security Enhancement Using Stopping Sets. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 575–584. [CrossRef]
15. Fritschek, R.; Schaefer, R.F.; Wunder, G. Deep Learning for the Gaussian Wiretap Channel. In Proceedings of the 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
16. Dryer, Z.; Nickerl, A.; Gomes, M.A.C.; Vilela, J.P.; Harrison, W.K. Full-Duplex Jamming for Enhanced Hidden-Key Secrecy. In Proceedings of the 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7.
17. Rathi, V.; Andersson, M.; Thobaben, R.; Kliewer, J.; Skoglund, M. Performance Analysis and Design of Two Edge-Type LDPC Codes for the BEC Wiretap Channel. *IEEE Trans. Inf. Theory* **2013**, *59*, 1048–1064. [CrossRef]
18. Vilela, J.P.; Gomes, M.; Harrison, W.K.; Sarmento, D.; Dias, F. Interleaved Concatenated Coding for Secrecy in the Finite Blocklength Regime. *IEEE Signal Process. Lett.* **2016**, *23*, 356–360. [CrossRef]
19. Sarmento, D.; Vilela, J.; Harrison, W.K.; Gomes, M. Interleaved Coding for Secrecy with a Hidden Key. In Proceedings of the 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [CrossRef]
20. Rice, M. *Digital Communications: A Discrete-Time Approach*; Pearson/Prentice Hall: Upper Saddle River, NJ, USA, 2009.
21. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
22. Al-Hassan, S.; Ahmed, M.Z.; Tomlinson, M. New best equivocation codes for syndrome coding. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Busan, Korea, 22–24 October 2014; pp. 669–674. [CrossRef]
23. Zhang, K.; Tomlinson, M.; Ahmed, M.Z.; Ambroze, M.; Rodrigues, M.R.D. Best binary equivocation code construction for syndrome coding. *IET Commun.* **2014**, *8*, 1696–1704. [CrossRef]
24. Harrison, W.K.; Bloch, M.R. On Dual Relationships of Secrecy Codes. In Proceedings of the 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2–5 October 2018; pp. 366–372. [CrossRef]
25. Moon, T.K. *Error Correction Coding: Mathematical Methods And Algorithms*; John Wiley & Sons: Hoboken, NJ, USA, 2005.
26. Harrison, W.K.; Bloch, M.R. Attributes of Generators for Best Finite Blocklength Coset Wiretap Codes over Erasure Channels. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; pp. 1–5.
27. Thangaraj, A.; Dihidar, S.; Calderbank, A.R.; McLaughlin, S.W.; Merolla, J.M. Applications of LDPC Codes to the Wiretap Channels. *IEEE Trans. Inf. Theory* **2007**, *53*, 2933–2945. [CrossRef]
28. Burshtein, D.; Miller, G. Efficient maximum-likelihood decoding of LDPC codes over the binary erasure channel. *IEEE Trans. Inf. Theory* **2004**, *50*, 2837–2844. [CrossRef]