CrossMark

Analysis of short blocklength codes for secrecy

Willie K. Harrison[1*] , Dinis Sarmento[2], João P. Vilela[3] and Marco A. C. Gomes[2]

Abstract

In this paper, we provide secrecy metrics applicable to physical-layer coding techniques with finite blocklengths over Gaussian and fading wiretap channel models and analyze their secrecy performance over several cases of concatenated code designs. Our metrics go beyond some of the known practical secrecy measures, such as bit error rate and security gap, so as to make lower bound probabilistic guarantees on error rates over short blocklengths both preceding and following a secrecy decoder. Our techniques are especially useful in cases where application of traditional information-theoretic security measures is either impractical or simply not yet understood. The metrics can aid both practical system analysis, including cryptanalysis, and practical system design when concatenated codes are used for physical-layer security. Furthermore, these new measures fill a void in the current landscape of practical security measures for physical-layer security coding and may assist in the wide-scale adoption of physical-layer techniques for security in real-world systems. We also show how the new metrics provide techniques for reducing realistic channel models to simpler discrete memoryless wiretap channel equivalents over which existing secrecy code designs may achieve information-theoretic security.

Keywords: Physical-layer security, Security measures, Wiretap channel

1 Introduction

Physical-layer security has attracted much attention of late as a means to provide a keyless layer of security using error-control coding and other physical-layer techniques such as intentional jamming [1, 2]. While traditional information-theoretic secrecy measures have been the preferred vehicles for proving the worth of physical-layer security coding schemes, some channel models remain elusive to this type of analysis [3]. In this paper, we provide two new security metrics that apply when blocklengths are finite (and especially when they are short) and when channel models are more representative of real-world environments.

Coding techniques exist that can achieve strong secrecy and even semantic secrecy over the binary erasure wiretap channel [4], but in the face of fading, jamming, and otherwise Gaussian noise, there remains a dearth of useful secrecy metrics beyond simple bit error rates (BER). The one exception is the security gap [5], which provides

a measure on the required signal-to-noise ratio (SNR) advantage over an eavesdropper to operate at acceptable error rates for friendly parties with an acceptable amount of security over illegitimate receivers.

In this paper, we present metrics for secrecy and reliability within a general framework of concatenated coding. These metrics were originally presented in [6], but with reference to only one specific coding scheme. In this work, we introduce a general framework of concatenated codes for which our metrics apply. This enables the application of our metrics to general coding schemes, of which the scheme presented in [6] is one specific use-case. Other examples are given throughout this paper to show the broader applicability of the new metrics. Furthermore, in this paper, we discuss the landscape of security metrics for physical-layer security and justify the existence of the new practical measures by highlighting their pros and cons with reference to existing metrics. Our metrics go beyond security gap, so as to identify operable regions of SNR for which bit error rates, even over a short number of bits, are guaranteed to be near 0.5. The basic premise of our techniques is to evaluate *the distribution of error rates over a small number of bits, such as might*

*Correspondence: willie.harrison@byu.edu
[1]Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT, USA
Full list of author information is available at the end of the article

be transmitted over a single packet, or within a single coded word, and to make guarantees not only on the mean of the distribution, but rather on, e.g., the 10th percentile or even the 1st percentile of the distribution. For very large blocklength codes, laws of large numbers guarantee performance near the mean, but for shorter blocklengths, we need to consider the entire distribution to make security guarantees. A proper tool that allows us to make these claims is the well-known cumulative distribution function (CDF) of the error rate over short blocklengths. As one considers percentiles closer to zero, the guarantees of our secrecy metrics are such that every small block of transmitted data either fails to be decoded (for the first metric) or achieves decoder output bit error rates greater than $0.5 - \delta$ for some δ in the range of $[0, 0.5]$ (for the second metric). These metrics fill a void in the current landscape of security measures for secrecy codes and find immediate application in real-world environments.

Consider the wiretap setup as depicted in Fig. 1, where the receiver chains for both a legitimate receiver Bob and an eavesdropper Eve are pictured. We consider here a possibly concatenated coding system, where the outer code is for security (and may consist of any number of coding operations as indicated) and the inner code is for reliability. Based on early work over the wiretap channel [7, 8], we know that there exists a supremum of achievable rates such that both security and reliability can be attained. This rate is called the *secrecy capacity* C_s. The first explicit code constructions to achieve information-theoretic security can be found in [9], and several variants soon followed, such as [10–12]. Many of these early works achieve security but only at coding rates below C_s and often in isolation from achieving any reliability constraint for friendly parties. In fact, many techniques require the legitimate receiver's channel to be noiseless. Other techniques specify that the eavesdropper's channel be physically or stochastically degraded [13] with respect to the main legitimate receiver's channel, and

all known information-theoretically secure coding techniques achieve security guarantees only for cases where all channels are discrete memoryless channels [1, 4].

One possible framework for extending these results is to employ a concatenated coding scheme as we illustrate in Fig. 1. It should be noted that the inner code in this figure is marked as *optional*, and if it is removed, then the model reduces to the traditional wiretap channel model [7]. Thus, although we are considering our new metrics in cases where concatenated codes are used, they remain applicable to the general wiretap case. We note the transmitter Alice encodes a message through all stages of the encoder to produce a length-n codeword X^n, which is transmitted over the wiretap channel. Bob and Eve observe their respective signals Y^n and Z^n, and both attempt to decode the message, perhaps producing respective message estimates $\hat{M}$ and $\tilde{M}$.

1.1 An example

As a simple example, consider the case where the outer code is just a scrambler, implemented by multiplying the binary length-k message M by a $k \times k$ binary matrix that is invertible in $GF(2)$ at the encoder and its inverse at the decoder (note that scrambling for physical-layer security was first studied in [14, 15], and many other works on the subject exist). Let us assume that the inner code is a t-error correcting code, such as a BCH code. If the channel is a Gaussian or a fading channel, then an information-theoretic security analysis may prove difficult. The alternative is to simulate the concatenated coding scheme at the decoder so as to obtain some guarantee on BER. When this is done, simulations are typically averaged over thousands of runs to obtain an average BER, and although the analysis is simulation driven, the results still only hold asymptotically as blocklengths become very large, just as in an information-theoretic analysis (if it is even possible).

We wish to provide probabilistic guarantees of decoder failure and guarantees of low statistical dependence between the message M and an eavesdropper's decoder
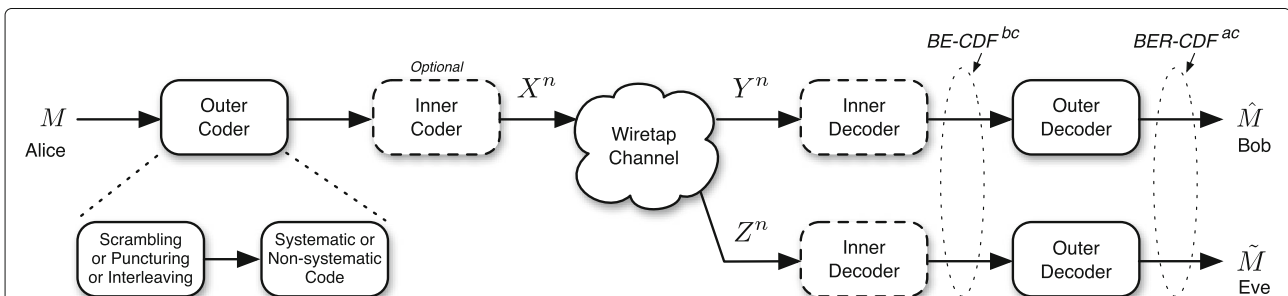

Fig. 1 Wiretap channel model assuming a concatenated coding scheme, where the outer code is for secrecy and the inner code is for reliability. Note that the inner code is marked as optional, and if it is removed, then this model reduces to the traditional wiretap channel model. The new metrics presented in this work are BE-CDF^{bc} (where *bc* indicates *before code*) and BER-CDF^{ac} (where *ac* indicates *after code*)

output message $\tilde{M}$. Despite the fact that BER has several shortcomings as a security metric, it can still be used effectively to estimate decoder outputs when the eavesdropper's attack strategy is known. Our metrics strengthen this approach by considering the entire distribution of possible error rates. In Fig. 2, we show the BER both before and after the scrambler in a receiver, and as expected, the descrambling operation propagates errors into the message estimate. However, if we would like to guarantee error rates close to 0.5 in all k-bit message estimates at the eavesdropper, it is necessary to consider the entire distribution of error rates over a blocklength of data. We see curves for $\Pr(\hat{P}_b > 0.5 - \delta)$ in the figure, where $\hat{P}_b$ can be used to model the proportion of bits in error over one block of k bits either at the input or at the output of the outer decoder and is a point estimator of the true bit error rate P_b. To be more specific, let B be a random variable that represents the number of bits in error over k bits either at the input or the output of the outer decoder. Then,

$$\hat{P}_b = \frac{B}{k}, \tag{1}$$

and is coincidentally the maximum likelihood estimator for the bit error rate P_b given k independent observations [16]. While the errors in k received bits comprising a single transmitted codeword are likely not independent at the output of a decoder, we will address this concern later in Section 3.2. Notice in Fig. 2 that if we want $\Pr(\hat{P}_b > 0.5 - \delta)$ after the decoder to get close to one, then we need to allow $\delta > 0.15$ for this scheme and somehow ensure that Eve's E_b/N_0 is no better than 3 dB. These two facts together indicate that the scheme under investigation may not be appropriate for secure communications. Restricting Eve's E_b/N_0 may be possible for controlled

physical environments, but $\delta > 0.15$ may not be acceptable, as it indicates that some blocks of data will exist at the output of the decoder with only 35% bit error rate, even as Eve's channel continues to degrade in quality. We use this simple example to showcase the general applicability of the new metrics, as comparing distributions of error rates before and after the outer decoder for fixed blocklength schemes gives one method for quantifying the security contribution of a code. Furthermore, we see that the metrics allow system designers to identify ranges of values that are achievable for δ and P_b, which then imply bounds on worst-case error rates in any single block of data.

1.2 Outline

Throughout this paper, we will let SNR designate the signal-to-noise ratio as measured by the channel, meaning the energy per transmitted bit over the noise power spectral density N_0. E_b/N_0 will be the energy per information bit divided by N_0. The two are related by the overall rate R of the concatenated coding scheme so that SNR $= RE_b/N_0$ for binary phase shift keying (BPSK) transmission.

The rest of the paper is organized as follows. First, we survey the landscape of secrecy metrics for physical-layer security coding schemes in Section 2. We then point out some shortcomings and motivate the need for additional practical metrics, and finally highlight the cases for which our metrics are superior to both information-theoretic and BER-based existing metrics, while also pointing out their limitations. Section 3 discusses the methodology behind our new metrics BE-CDF^{bc} and BER-CDF^{ac}, with definitions and clarifying examples. We show a use case of these metrics in a more complicated concatenated coding scheme in Section 4 and indicate how the scheme may
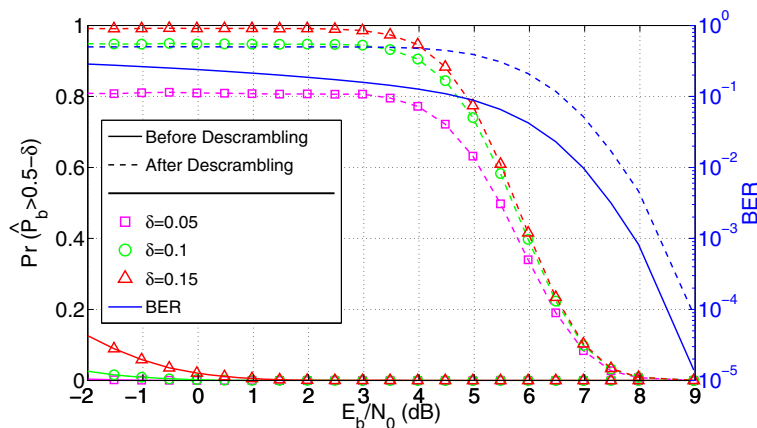

Fig. 2 New security metrics for a simple system where the outer code is a scrambler and the inner code is a BCH(127, 64) code. BER curves are given in blue with no markers, and $\Pr\left(\hat{P}_b > 0.5 - \delta\right)$ curves are given with markers as indicated to identify the values of δ. Solid lines indicate the location is before the outer coder, while dashed lines indicate the location is after the outer coder

be used directly for secrecy or used to provide a discrete memoryless wiretap channel equivalent over which additional secrecy codes may be used to achieve information-theoretic security. The scheme in this section uses a friendly jammer and illustrates the broad utility of the new metrics. We also compare and contrast our new metrics with traditional cryptographic strength and perform basic cryptanalysis both before and after the outer decoder for the nested coding framework. We offer some comments by way of conclusion in Section 5.

2 Discussion

2.1 Secrecy metrics

The secrecy metric space has progressively become more dense, particularly over the last few decades. The initial secrecy coding metric posed by Shannon in the late 1940s was that of *perfect secrecy* [17]. A code is said to achieve perfect secrecy if

$$I(M; X^n) = 0, \tag{2}$$

or, alternatively, if the equivocation $H(M|X^n)$ is equal to the entropy of the message $H(M)$. Perfect secrecy indicates that the coded message tells you nothing about the message itself. Shannon introduced the notion through the coding scheme of the one-time pad and promptly proved that it was impossible to achieve perfect secrecy in a scheme where the entropy of a secret key is not at least as much as the entropy of the message itself. Thus, it is known that perfect secrecy is completely impractical.

In the mid-1970s, Wyner [7] introduced an additional metric for secrecy that is known today as *weak secrecy*. A scheme is said to achieve weak secrecy if

$$\lim_{n \to \infty} \frac{1}{n} I(M; Z^n) = 0. \tag{3}$$

This metric introduced the idea of coding for secrecy in earnest because the results indicated that it was actually possible to achieve weak secrecy in a practical system. After all, this criterion does not require that the coded message X^n leaks no information about M, but rather that the eavesdropper's observation Z^n must leak a sufficiently small amount of information about M such that the $1/n$ factor can still drive the quantity to zero. With this new notion of secrecy came the idea of secrecy capacity C_s which was originally defined as the supremum of coding rates that can achieve weak secrecy against a passive eavesdropper as a function of the wiretap channel parameters, while maintaining arbitrarily low probability of decoding error at the legitimate receiver. As long as the legitimate parties are able to leverage an advantage over the eavesdropper so that the effective main channel is *less noisy* [8] than the eavesdropper's channel, then $C_s > 0$, which indicates that private communications are theoretically possible.

Weak secrecy was shown to be insufficient in many cases [13], and Maurer later defined a stronger metric known as *strong secrecy* [18], where a scheme is said to achieve strong secrecy if

$$\lim_{n \to \infty} I(M; Z^n) = 0. \tag{4}$$

It was recently noted in [19] that even strong secrecy may not be sufficient for some applications because the assumption is often made that message symbols are random and uniformly distributed over the message alphabet. Of course, in cryptographic scenarios, the messages are never perfectly random and uniform, and it is known that in practice there really is no universal compression algorithm that can provide such messages at the input of secrecy encoders. Thus, we have an even stronger notion of secrecy called *mutual information security* which is achieved if

$$\lim_{n \to \infty} \max_{p_M} \{I(M; Z^n)\} = 0. \tag{5}$$

Here, we maximize $I(M; Z^n)$ over all possible message distributions p_M. It is also shown in [19] that this notion of secrecy is equivalent to *distinguishing security* and *semantic security*.

Although it took over 30 years after Wyner introduced weak secrecy for an explicit code design to emerge that could achieve it [9], it has already been shown that codes exist that can achieve both strong and semantic secrecy, albeit over simple wiretap channel models [4, 19]. Surprisingly, the secrecy capacity defined using strong or semantic security is provably the same as that defined by the weak secrecy metric [20].

Although this list of information-theoretic measures is impressive and useful, there remain several wiretap channel models that have proved elusive to explicit code designs where information-theoretic security can be guaranteed. Thus, over channels that are more representative of real-world communications, such as the Gaussian wiretap channel or fading channel scenarios, there have been additional security metrics developed. For example, the authors in [5, 15] used bit error rate (BER) at the output of a decoder as a more practical security measure. This metric can be simulated in a straightforward manner, just as is done for traditional error-correcting codes. The authors in [5] developed a new secrecy metric by identifying a target BER for the legitimate receiver, as well as a target BER for an eavesdropper, and found the SNRs that would achieve each of these targets. The *security gap* was then defined as the difference between these two SNR values in decibels (or a ratio of the two linear values). The security gap tells a designer what the required advantage is for obtaining the desired security and reliability performance, and threshold operating points for achieving both. The metric has been well studied [5, 15, 21].

Authors in [22] studied coding mechanisms that provided *degrees of freedom* in an eavesdropper's decoder output, where no information about certain bits could be obtained, forcing an attacker to guess the bits associated with the degrees of freedom in the decoder. This notion was similar to an information-theoretic security approach in the sense that the information could not be attained through any degree of processing but was also very much unlike an information-theoretic security approach because it restricted an attacker to a specific attack strategy.

2.2 Shortcomings of current security metrics

The metrics of the previous section give many techniques for analyzing the security achieved by specific coding schemes. Developing wiretap codes that are able to reach the envisioned secrecy capacity for more practical channel models remains a formidable challenge, and performing the information-theoretic analysis is oftentimes deemed intractable. The information-theoretic measures are still the most desirable where possible to apply, but they also have another weakness in the sense that they lead to codes that are designed to meet a secrecy criterion in an asymptotic blocklength regime only, thus limiting their applicability in real systems that require short blocklength codes. Some work has been done recently in an attempt to expand information-theoretic security measures to finite blocklengths, but thus far, these attempts are either directed only at discrete memoryless channel models [23] or provide only bounds on the information leakage that are very loose for short blocklength codes [24, 25].

One should be careful when performing security analysis that relies only on BER-based measures, because high error rates do not necessarily indicate that some information has not been leaked. On the other hand, modern cryptography is based on computational security that does leak the information about the message. These systems work not because of an information-theoretic guarantee, but rather due to there being no known computationally efficient algorithm that can find the solution in any reasonable amount of time with any realistic amount of computing power unless the key is known. Thus, we see that despite not achieving an information-theoretic security measure, cryptosystems remain useful because they attain security in a more practical/applied sense. In a similar way, BER security analysis assumes the best known decoder/attack and makes calculations assuming an eavesdropper uses that attack. While BER may provide some useful information about the quality of the received data or the decoder output at the eavesdropper, BER calculations are still made by averaging large amounts of data and are therefore only reliable as blocklengths get large.

The metrics we introduce over the next two sections of this paper take a BER approach but rather than calculating simple averages, make use of our knowledge of the CDF of bit error rates over small blocks of data to provide lower bounds on error rates through the receiver decoder chain, where the highest BER considered is 0.5. Making this fundamental change in how BER is used to analyze security in a system allows us to make stronger guarantees about the performance of secrecy codes in the short blocklength regime without the need for laws of large numbers. This is something that none of the metrics in Section 2.1 can provide due to the way the analysis is completed either as blocklength goes to infinity or as simulations are averaged over thousands of independent runs. Using the new metrics, we also maintain the ease of simulation-based characterization of security (which is particularly helpful when realistic channel models are considered, where it is not known how to provide an information-theoretic analysis). Table 1 outlines the utility of each currently known physical-layer security metric [1, 4] and indicates the contribution of our new metrics lies in ease of computation and providing the strongest guarantee yet for analyzing finite blocklength code designs.

3 Methods

3.1 The bit error cumulative distribution function

Let us consider an additive white Gaussian noise (AWGN) channel with BPSK modulation, for which the BER (depicted in Fig. 3) is given by [26]

$$P_b = \frac{1}{2}\text{erfc}\left(\sqrt{\text{SNR}}\right). \tag{6}$$

A t-error correcting code of length 127 that is able to correct up to 10 errors can recover from a BER of $\frac{10}{127} \approx 0.079$ assuming uniform error distribution, but errors over short blocks of data are not guaranteed to occur so uniformly. Let E be the number of bit errors in a block of n bits. For a transmitted word of size n with independent bit errors, the probability of having fewer than or equal to t errors $\Pr(E \leq t)$ can be straightforwardly obtained from (6) as

$$\Pr(E \leq t) = \sum_{i=0}^{t} \binom{n}{i} P_b{}^i (1 - P_b)^{n-i}. \tag{7}$$

Let us now consider two operating points of Fig. 3: (a) SNR = 0 dB that leads to a BER close to the 0.079 that the code supports and (b) SNR = -3 dB, that leads to a BER ≈ 0.16. Looking at $\Pr(E \leq 10)$ in the same figure, for SNR = 0 dB, we have $\Pr(E \leq 10) \approx 0.58$, meaning that the code would still succeed more than half of the time. For SNR = -3 dB, we get $\Pr(E \leq 10) \approx 0.006$, which indicates that the decoder will fail over 99% of the time, yet with a BER far from 0.5. Also note that the curve for $\Pr(E \leq 10)$ approaches zero for low SNR values, with

Table 1 Summary of current physical-layer security metrics, highlighting some of their pros and cons

Class	Metric	Directly applicable to short codes	Easily computable in general	Information-theoretic secrecy guarantees	Strongest in class	Known how to achieve in practice
Impractical	Perfect secrecy	Yes	No	Yes	Yes	No
Info-theoretic	Weak secrecy	No	No	Yes	No	Yes (only for DMCs)
Info-theoretic	Strong secrecy	No	No	Yes	No	Yes (only for DMCs)
Info-theoretic	Semantic secrecy	No	No	Yes	Yes	Yes (only for DMCs)
Error rate	BER	No	Yes	No	No	Yes (BER $\approx$ 0.5)
Error rate	Security gap	No	Yes	No	No	Yes (security gap < 0 dB)
Error rate	BE-CDF^{bc}	Yes	Yes	No	No	Yes (decoder failure w. p. $\approx$ 1)
Error rate	BER-CDF^{ac}	Yes	Yes	No	Yes	Yes (high error rates w. p. $\approx$ 1)

Here we see that although our new metrics cannot provide information-theoretic security, they are best in class among the error-rate secrecy metrics. Note: w.p. means *with probability*

the BER still far from the idealized 0.5 value. With this in mind, the question arises of how close to BER = 0.5 is close enough for security purposes.

To address this issue, we look to the distribution of errors of transmitted data and propose the first of two new secrecy metrics.

Definition 1 (Bit error cumulative distribution function) *The bit error cumulative distribution function, BE-CDF^{bc}(t, SNR, $\mathcal{S}_m$, $\mathcal{C}_i$), gives us the probability of having t or less errors,* $\Pr(E \leq t)$, *as a function of the SNR for a message of size $\mathcal{S}_m$, encoded with a code $\mathcal{C}_i$ (refers to the optional inner code).*

From this metric, we can deduce the probability of having more than t errors in a block of data, giving us the power to predict the likelihood of decoder failure when

the code is a t-error correcting code such as a Bose-Chaudhuri-Hocquenghem (BCH) code. This information is useful for identifying acceptable SNR operating points for both friendly parties and eavesdroppers [6]. Notice from Fig. 1 that we measure this metric *before* the outer *code* (hence the superscript *bc*) in a concatenated coding scheme, i.e., prior to the secrecy code. Because of this, we choose to use SNR, rather than E_b/N_0 to show the results, although the conversion can be made if desired.

3.1.1 Analysis
This metric can also be used to fine-tune the security and reliability levels of a coding scheme that relies on t-error correcting codes. For example, if we assume no inner code and set the outer code to a BCH(127, 64) code that corrects up to 10 errors, and if we want a reliability level of $\Pr(E \leq 10) > 0.99$, Bob would have to operate at
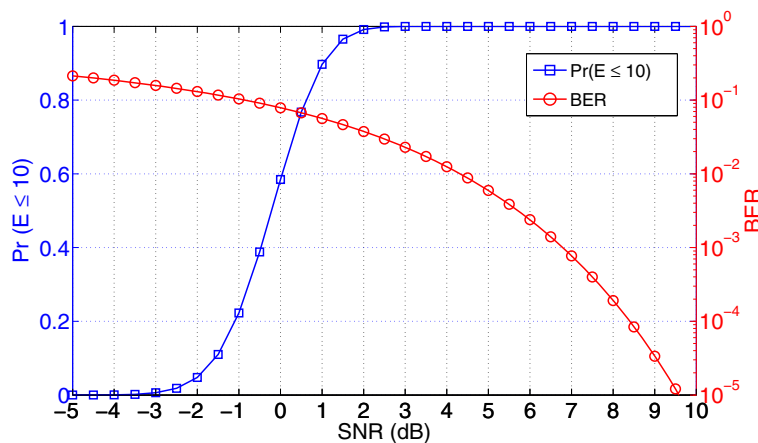

Fig. 3 Bit error probability and probability of having fewer than or equal to 10 errors out of 127 bits for an AWGN channel with BPSK modulation

an SNR above 1.95 dB as indicated in Fig. 3. For a confidentiality level of 0.99, i.e., $\Pr(E \leq 10) < 0.01$, Eve would need to operate at SNR below -2.78 dB.

While relevant reliability and confidentiality levels with a reasonable SNR gap between Bob and Eve may seem illusive with simple coding schemes such as the mentioned BCH code, this metric enables the selection of t-error correcting codes that can be used in more evolved concatenated coding schemes combined with the generation of interference [6] to provide desired levels of reliability and confidentiality, as will be described in Section 4.1.

3.2 The bit error rate cumulative distribution function

The BE-CDF^{bc} allows us to guarantee failed decoding with high probability over certain SNR regions for t-error correcting codes. However, a failed decoder does not necessarily imply that the eavesdropper cannot obtain most of the message bits at the output. Hence, in this section, we introduce a metric that can guarantee decoder failure with BER close to 0.5 in the estimated message bits to strengthen the security guarantee. For this section, let $\hat{P}_b$ be the measured proportion of bit errors at the output of an error-correcting decoder measured over $\mathcal{S}_b$ decoded message bits. For the case where the code being used is a block (n, k) code, it makes sense to let $\mathcal{S}_b$ be an integer multiple of k. The metric we propose in this section allows a user to specify a required error rate at the output of the eavesdropper's error-control decoder over $\mathcal{S}_b$ bits using the probability that $\hat{P}_b > 0.5 - \delta$ for any δ desired.

Definition 2 (Bit error rate cumulative distribution function) *The bit error rate cumulative distribution function, BER-CDF$^{ac}(\delta, E_b/N_0, \mathcal{S}_b, \mathcal{C})$ is the quantity*

$$\Pr\left(\hat{P}_b > 0.5 - \delta\right) \qquad (8)$$

calculated over $\mathcal{S}_b$ estimated message bits for a code $\mathcal{C}$ as a function of E_b/N_0, where $\mathcal{C}$ may be the concatenation of an (optional) inner code $\mathcal{C}_i$ and an outer code $\mathcal{C}_o$.

We note that the *ac* exponent indicates that the metric is measured *after the code*. Since the inner code is shown to be optional in Fig. 1, this is referring to the outer (secrecy) code. Also, because we are calculating this metric after the decoder, it makes sense to use E_b/N_0, rather than SNR. Finally, we should note that this metric is actually the complement to the CDF, but we choose to use a consistent nomenclature to that of the BE-CDF^{bc}. These two metrics packaged in a pair provide valuable design information so as to achieve both reliability and secrecy.

3.2.1 Analysis

The BER-CDF^{ac} allows us to guarantee decoder failure with high probability in addition to high BER (near 0.5) over short blocks of $\mathcal{S}_b$ bits at the output of the decoder.

Although the metric is not information-theoretic, it comes much closer to the information-theoretic definitions of secrecy than the BE-CDF^{bc} by limiting the amount of useful information to an eavesdropper (as tends to happen with high BER). That is, for a scheme that guarantees high BER using the BER-CDF^{ac} metric, it is unlikely that the decoder will fail and yet provide small BER at the output. Notice that this metric is also much more robust than simply considering the average BER, and examples are shown in the following section of the paper. Similarly as with our BE-CDF^{bc} metric, we now ensure that the entire distribution of BER values for a specific length of text $\mathcal{S}_b$ is within an acceptable security region.

Recall that $\hat{P}_b$ is the estimator of the error rate P_b at the output of the final decoder over a short blocklength of $\mathcal{S}_b$ bits. If we assume that each bit at the output of the decoder is in error independently with probability P_b, then the random variable $P_n = \mathcal{S}_b \hat{P}_b$ models the number of errors in a block of $\mathcal{S}_b$ bits and is distributed according to the binomial distribution with parameters $\mu = P_b$ and $\sigma^2 = \mathcal{S}_b P_b (1 - P_b)$. This means we can calculate the metric exactly as

$$\Pr(\hat{P}_b > 0.5 - \delta) = \Pr[P_n > \mathcal{S}_b(0.5 - \delta)]$$
$$= 1 - \sum_{x=0}^{\lfloor \mathcal{S}_b(0.5-\delta) \rfloor} \binom{\mathcal{S}_b}{x} P_b^x (1 - P_b)^{\mathcal{S}_b - x}. \qquad (9)$$

Although the exact expression can be derived in this case, the assumption of i.i.d. errors is not likely to hold in practice, P_b may be unknown, and the calculation itself would be time intensive or require approximation using the Gaussian distribution [16]. Thus, in practice, it makes more sense to calculate the metric using straightforward Monte Carlo simulations.

By way of example, consider $\Pr\left(\hat{P}_b > 0.5 - \delta\right)$ as plotted for a BCH(127, 92) code as the outer code with several varying sets of parameters as portrayed in Fig. 4. Each case presented uses $\mathcal{S}_b = 92 \times 2 = 184$ so as to allow an $L = 4$ order modulation scheme without zero padding. The modulation scheme was chosen arbitrarily to be differential phase shift keying (DPSK) and is either binary or quaternary as indicated in the legend. Beyond this, we consider different δ values as shown. Although there exist E_b/N_0 values for which the decoder fails with probability close to one, unless the resultant BER is greater than $(0.5 - \delta)$ with high probability, the metric will not approach one in the limit as $E_b/N_0 \to -\infty$.

Notice that the value the BER-CDF^{ac} approaches as $E_b/N_0 \to -\infty$ is strongly linked to δ, which makes perfect sense. As δ grows, it is more possible to fit the entire distribution of BER above the $(0.5 - \delta)$ threshold. This observation indicates that for any particular coding scenario, there may in fact exist a minimum δ for which the
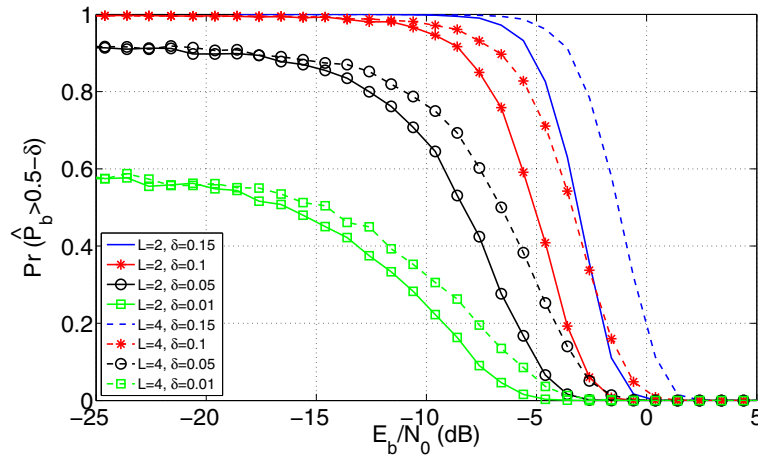
Fig. 4 Depiction of the BER-CDF^{ac} metric $\mathrm{Pr}\left(\hat{P}_b > 0.5 - \delta\right)$ for the BCH(127, 92) code for $\mathcal{S}_b = 2 \times 92 = 184$ using L-order DPSK modulation. Notice that for some δ values, the BER-CDF^{ac} approaches one, where other curves appear to be bounded away from one

BER-CDF^{ac} can be made to go to one as $E_b/N_0 \rightarrow -\infty$. Also notice in Fig. 4 that increasing the order of the digital modulation scheme can bring about an effective shift towards better security. When $\mathrm{Pr}\left(\hat{P}_b > 0.5 - \delta\right)$ is bounded away from one, we are viewing the random corrective capabilities of the code even when the signal is completely overwhelmed by noise. Certainly, we can do better by increasing $\mathcal{S}_b$ or the dimensions of the code as well, but the utility of this metric is that we can get a clear picture for what happens when $\mathcal{S}_b$ is small, thus providing small blocklength security analysis in practical physical-layer security system designs.

Exploring the metric in the limit as channel quality deteriorates is accomplished in the following lemma.

Lemma 1 *The limiting value of the BER-CDF^{ac} (δ, E_b/N_0, $\mathcal{S}_b$, $\mathcal{C}$) as $E_b/N_0 \rightarrow -\infty$ is*

$$\lim_{E_b/N_0 \rightarrow -\infty} \mathrm{Pr}(\hat{P}_b > 0.5 - \delta) = Q\left(-2\delta\sqrt{\mathcal{S}_b}\right). \quad (10)$$

Proof Clearly this quantity is a function of δ and $\mathcal{S}_b$ and can be calculated by recognizing that $\hat{P}_b$ is a sample mean of Bernoulli random variables X_i where

$$X_i = \begin{cases} 1 & \text{if bit } i \text{ is in error,} \\ 0 & \text{otherwise.} \end{cases} \quad (11)$$

Since we are evaluating the BER-CDF^{ac} as $E_b/N_0 \rightarrow -\infty$, we can assume that all of the X_i random variables are effectively independent. In essence, the independence of the relatively high-power noise masks any potential dependence of the underlying data as channel quality deteriorates. Let $\mathrm{Pr}(X_i = 1) = P_b$ as before. Then specifically,

$$\hat{P}_b = \frac{1}{\mathcal{S}_b} \sum_{i=1}^{\mathcal{S}_b} X_i, \quad (12)$$

and by the central limit theorem $\hat{P}_b \sim \mathcal{N}\left(P_b, \frac{P_b(1-P_b)}{\mathcal{S}_b}\right)$. Clearly, this is true in the limit as $\mathcal{S}_b$ gets large, but even for small and moderate blocklength sizes, the central limit theorem still provides a good approximate distribution. In the limit as $E_b/N_0 \rightarrow -\infty$, we also have $P_b \rightarrow 0.5$ and $\hat{P}_b \sim \mathcal{N}\left(0.5, \frac{0.25}{\mathcal{S}_b}\right)$. Using the classic Gaussian standardization technique [16], we find that the lemma is proved. □

This limiting value of the BER-CDF^{ac} is shown in Fig. 5 over a range of δ and $\mathcal{S}_b$ values. These results can aid system designers in choosing $\mathcal{S}_b$ (or k) in outer codes appropriately so as to supply a desired BER-CDF^{ac}. Once $\mathcal{S}_b$ is chosen, we also have a best possible value for the metric over which any coding scheme can be compared. One characteristic of good secrecy codes is that they will transition from zero to the limiting value in this metric over a very short range of E_b/N_0.

Finally, we end this section with a word of caution regarding these new metrics. As implied in Section 2.2, any BER-based security analysis is, by its very nature, incomplete. Information-theoretic security guarantees will always be preferred, as they consider information (including correlation of errors in decoded data) that cannot be quantified using error rates. Since explicit coding schemes that deliver information-theoretic security over the Gaussian wiretap channel are still unknown, we must address practical security questions when choosing to use BER-based measures. In Section 4, we consider the utility
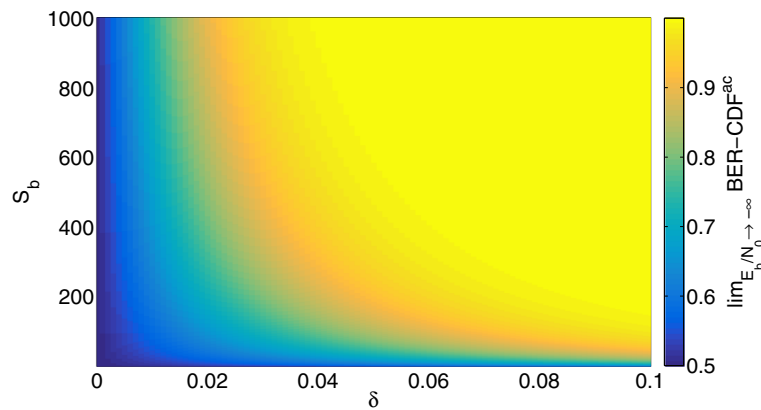
Fig. 5 Limiting value of the BER-CDF^{ac} metric as E_b/N_0 goes to $-\infty$ as a function of δ and $\mathcal{S}_b$

of log-likelihood ratios (LLRs) in determining error locations at the output of an iterative decoder and perform simple cryptanalysis to accompany the use of our metrics in a more complex coding scheme.

4 Results

4.1 Application

In this section, we show how the concatenated coding system from [6] measures up using the two new metrics and discuss the utility of the system as a result of its BE-CDF^{bc} and its BER-CDF^{ac} curves. It should also be noted that [6] goes through a design process based on the BE-CDF^{bc} for this coding scheme. Although we do briefly outline the scheme and one possible design process here, the interested reader is directed to the original work for further details. It is of note that the scheme highlighted in this section requires a friendly jammer, and the scheme is chosen for presentation partly for this reason. Although the simpler examples shown in the previous sections of the paper apply to the general wiretap channel (Fig. 1), our framework, and our metrics, are broad enough to consider more complicated cases as shown with this use case. For an additional concatenated coding example without the use of a friendly jammer, the reader is directed to [27]. Finally, we indicate how our new metrics may be combined with this coding scheme to provide *effective* discrete memoryless wiretap channel equivalents over which other secrecy coding schemes may be implemented to achieve information-theoretic security.

4.1.1 System setup

The system analyzed in this section follows the general concatenated coding framework outlined in Fig. 1. The outer code can actually be considered as two encodings, where the message is interleaved according to a secret key K (drawn at random from the space of possible permutations on $\mathcal{S}_m$ input message bits), and the key is encoded

separately from the message using a BCH(127, 64) code that is capable of correcting 10 errors. The interleaved message and the encoded key are then appended together, and this constitutes the outer code. An LDPC(1056, 880) code is then used as the inner code, which is applied to the appended message and key to form a codeword suitable for transmission over a noisy channel. Recall from Fig. 1 that the general concatenated framework is such that the outer code is intended to achieve the secrecy requirements of the system, while the inner code is used to achieve reliability for Bob.

In this system, however, there is more at play than just the coding schemes. When the encoded data that are associated with the key K are transmitted over the channel, they are intentionally jammed by some friendly network user with jamming power equal to a fraction α of Alice's transmit power. The idea is to give Bob an advantage because of his location or knowledge of the jamming signal so that the jamming affects him only minimally, while an eavesdropper has no information about the jamming signal and/or is positioned in a geographic location that does not afford her the same advantage as Bob [6, 28, 29]. Since the jamming is only applied to the encoded bits associated with the interleaving key, reliability in the system also stems from Bob being able to recover the key for deinterleaving, while security in the system depends on Eve being unable to recover the interleaving key. Data are transmitted over a Gaussian wiretap channel using BPSK modulation.

The receiving decoders at Bob and Eve apply a soft-decoding algorithm for the low-density parity-check (LDPC) code, and the BCH decoder can then correct no more than 10 errors in the key bits. The goal is to reliably keep the errors at the output of the LDPC decoder at no more than 10 for Bob and above 10 for Eve for each transmitted key block, as the key bits must be used to deinterleave the message bits at the final step of the

decoder. The mapping of keys to interleavers is such that any errors in the estimated key result in high error rates in the deinterleaved message, even when the interleaved message bits are recovered exactly [6].

4.1.2 Direct results

Our two new metrics paint a complete picture of how this system will respond for both Bob and Eve, thus providing security analysis and system design constraints. The BE-CDF^{bc} will show us the operating point for Bob to attain any desired level of reliability and will also show us how Eve's decoding capability breaks down. The BER-CDF^{ac} will then further enlighten us as to where we truly wish Eve to operate so as to guarantee (with probability essentially one) high BER near 0.5 at the output of her decoder. Coincidentally, this analysis also allows us to identify the jamming power advantage required during key transmission for the system to be successfully deployed [6].

Let us assume that the effective jamming to Bob is $\alpha_B = 0.2$, while the effective jamming to Eve is $\alpha_E = 0.7$ (we also include $\alpha = 1$ in the figures for instructional purposes). The BE-CDF^{bc} results apply to the BCH-encoded key bits and are given in Fig. 6, where we see that if Bob wishes to attain an overall BER around 10^{-3}, the system must be designed to guarantee a BE-CDF^{bc} value no lower than 0.9975. The interpretation of this value is that less than one fourth of 1% of the transmitted key blocks should be decoded in error for Bob. Also according to Fig. 6, Bob achieves this performance if the SNR over his Gaussian channel is 6.5 dB or greater. We also note that the BE-CDF^{bc} for Eve at an SNR of 4 dB is equal to 0.0048, meaning less than one half of 1% of the time Eve will receive a key block for which she can correct all the errors if this BE-CDF^{bc} value can be maintained.

To get the true feel for how Eve is affected by this scheme, however, we need to track the distribution of error proportion in Eve's guess of the message bits as a function of E_b/N_0 using the BER-CDF^{ac} as depicted in Fig. 7. Here we see that for $\delta = 0.05$, we can attain $\Pr\left(\hat{P}_b > 0.5 - \delta\right) = 0.995$ at roughly $E_b/N_0 = 4.7$ dB, which corresponds to an SNR value of approximately 4 dB. The limiting values of the BER-CDF^{ac} are also shown in the figure, as given by (10). These results indicate that for this scheme, insuring that Eve cannot correct all errors in the key is in fact sufficient for insuring a high proportion of errors in Eve's estimate of each short blocklength of message bits at the output of her decoder, which is exactly what we'd like to see in a practical physical-layer security scheme. For the sake of referring back to Fig. 5 for the limiting value of the BER-CDF^{ac} metric $\mathcal{S}_b$ for this scheme is the dimension of the LDPC code (880 bits) minus the blocklength of the BCH code (127 bits), because the BCH code only encodes the key bits, and the remainder of the bits in the dimension of the LDPC code are dedicated to the message. This yields $\mathcal{S}_b = 753$ bits.

4.1.3 Creating a discrete memoryless channel

Explicit secrecy code constructions exist that can provide information-theoretic security, however, only for discrete memoryless wiretap channels [1, 4]. As mentioned previously, some of these currently known designs require either a noiseless main channel for legitimate communication or a degraded wiretap channel for the eavesdropper. Thus, we have two possible research directions for making information-theoretically secure coding designs more practical to real end users. First, effort can be placed to design secrecy codes that operate over more realistic channels [3], and second, coding and/or signaling techniques may be leveraged to produce an *effective* wiretap
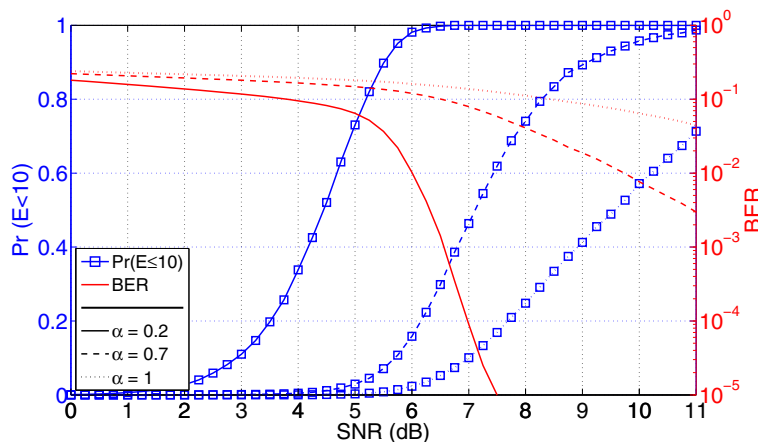

Fig. 6 BE-CDF^{bc} calculated when $t = 10$ for three different effective jamming powers. These results anticipate the likelihood of decoder failure for Eve at $\alpha = 0.7$ for a BCH(127, 64) code at around 0.9952 when Eve's Gaussian channel has SNR = 4 dB. If Bob experiences an effective $\alpha = 0.2$, then he can operate with BE-CDF$^{bc} = 0.9975$ at 6.5 dB
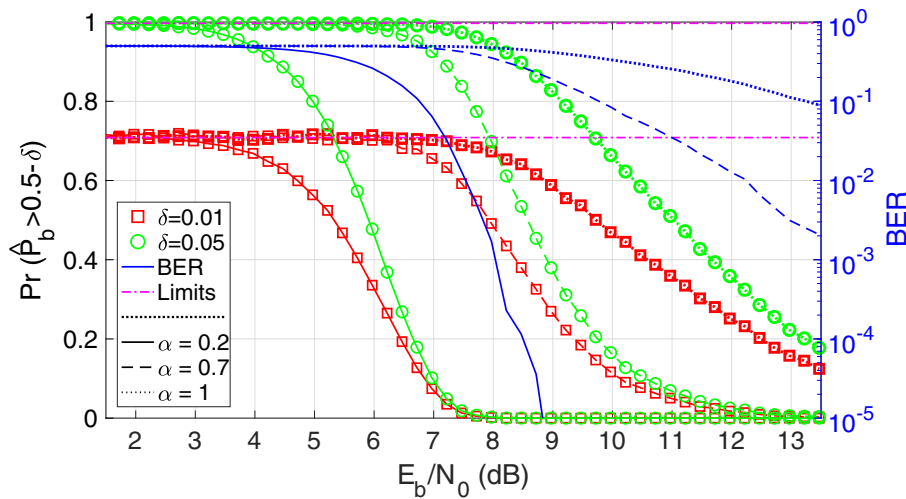
Fig. 7 BER-CDF^{ac} given for two delta values along with the BER. These three curves are given for three different effective jamming powers and show that if Eve experiences jamming power $\alpha_E = 0.7$, then her BER over 753 message bits is guaranteed to be within $\delta = 0.05$ of 0.5 with high probability as long as her E_b/N_0 is no greater than 4.7 dB. This corresponds to an SNR value of approximately 4 dB. The lines marked as *limits* are the limiting expressions given from (10) for the two different δ values

channel [30] over which we already know how to code for information-theoretic security. In this section, we outline how our new metrics and the coding scheme explained in Section 4.1.1 can be used to produce an effective discrete memoryless wiretap channel.

Consider again the results shown in Fig. 7 that indicate an eavesdropper experiencing jamming power $\alpha_E = 0.7$ and $E_b/N_0 = 4.7$ dB over a Gaussian channel can expect error rates over 753-bit messages to have BER greater than 0.45 with probability very close to one. Since the analysis was conducted over short blocklengths, we offer not just an average BER, but rather a low estimate of the BER over the channel. We now consider applying one more code on the outside of the entire scheme described in Section 4.1.1, as depicted in Fig. 8, and modeling the remaining blocks as an effective binary symmetric channel (BSC). The additional code added is one that can leverage this effective channel to bring about an information-theoretic security result (e.g., [31]).

In order to claim that the interior blocks in Fig. 8 can truly be modeled as a BSC, we need to verify three main properties of the BSC in our system: (1) each bit should be flipped independently from all other bits, (2) the probability p of flipping each bit over the channel should be identical and we need to identify its value, and (3) we need to ensure that soft information about the bit is either not available or impossible to use at the secrecy decoder.

To ensure that bits within message blocks retain their independence of being in error, as required by the BSC model, we need to apply an inter-block interleaver as the first subcode in the outer coder block in Fig. 8 to spread information around as in [22, 30] and many other works.

Although there may exist some correlations between flipped bits over the same transmitted packet, since all bits from every secrecy codeword are transmitted in different packets over the channel, we effectively deliver independence between the bits at the secrecy codeword level, which is where we need independence for the secrecy code to work properly.

In terms of identifying the probability p that corresponds to the flipping of each bit over the channel, we will use the lower bound given by BER-CDF^{ac} as indicated above. By so doing, we provide an even stronger guarantee than identifying an average probability, since even short blocklengths maintain this probability of bit error with probability close to one. Bit error locations within secrecy codewords are kept uniformly random as a byproduct of the inter-codeword interleaving at the output of the secrecy encoder.

Finally, we need to address this issue of soft information at the input of the secrecy decoder. Although soft information is technically available here, we must deduce whether or not the information is actually worth anything. In other words, what do LLRs look like when the overall bit error rates at the output of an LDPC decoder are close to 0.5? LLRs can be approximated by Gaussian distributions with means centered at positive values if the bits should have a value of 0 and at negative values if the bits should have a value of 1. The Gaussian approximation rule-of-thumb stems from the central limit theorem for likelihood ratios, where sums of random variables are calculated to give the ratio's next iteration [26, 32]. The distribution of LLRs corresponding to bits in error is always symmetric and centered at zero since the decision threshold at the
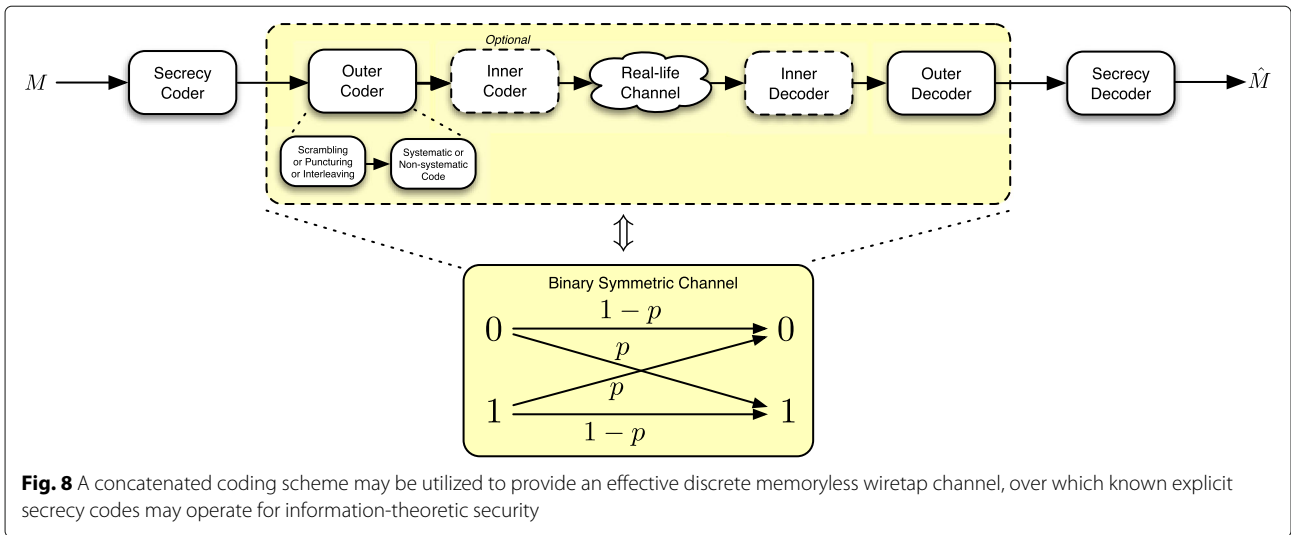
Fig. 8 A concatenated coding scheme may be utilized to provide an effective discrete memoryless wiretap channel, over which known explicit secrecy codes may operate for information-theoretic security

end of the soft iterative decoding algorithm is positioned directly between the distributions of LLRs corresponding to differing bit values. When the SNR is small enough that the code does not correct all the errors, distributions corresponding to bits in error and correct bits start to look very similar. In fact, when the noise completely overwhelms the coding scheme, each of these distributions tends to an approximate Gaussian distribution with mean zero and identical variances. It is this property that supplies an effective decoding *threshold* for iteratively decodable codes [26]. Finally, as the BER approaches 0.5, the statistical difference between the distributions of LLRs for correct bits and bits in error becomes negligible. To demonstrate this, we show through simulation that the Kullback-Leibler (K-L) divergence [33] between the two distributions approaches 0 as the BER approaches 0.5, where the K-L divergence is given as

$$D(p||q) = \int\limits_x p(x) \log_2 \frac{p(x)}{q(x)} \, \mathrm{d}x, \qquad (13)$$

and $p(x)$ represents the distribution of LLRs for correct bits while $q(x)$ represents the distribution of LLRs for bits in error at the output of a soft-information LDPC decoder. These results are given in Fig. 9, where we observe $D(p||q)$ going to zero with increasing BER. Recognize that $D(p||q) = 0$ implies that there is no statistical difference between $p(x)$ and $q(x)$ or that the *distance* between the two distributions is zero. It can be argued then, that as long as $D(p||q)$ is small enough, soft information at the output of an iterative decoder is unusable as it does not accurately depict any type of relationship between a bit's likelihood of being correct or in error.

The end result is that our new metrics mixed with the scheme from [6] can provide the effective channel model

necessary for these information-theoretic designs to succeed. We see in [1] that one type of secrecy code that may be able to offer secrecy over this channel is that given in [31], where known advantageous (good for Bob and bad for Eve) polarizations of synthesized bit channels in polar codes are used to transmit secret information over a symmetric eavesdropper's channel. This coding scheme is known to achieve strong secrecy at information rates approaching the secrecy capacity when the legitimate channel can be modeled as noiseless. For our case (where we have assumed that $\alpha_E = 0.7$, $\alpha_B = 0.2$, Bob's SNR ≥ 6.5 dB and Eve's SNR ≤ 4 dB), supplying a probability of a flipped bit $p \geq 0.45$ over an effective BSC to an eavesdropper while maintaining an effectively noiseless main channel results in secrecy capacity $C_s = C_m - C_w = p$ bits per channel use, where C_m and C_w signify the channel capacities of the main and wiretap channel, respectively [7, 8, 33].

The approach outlined here, where we manufacture a wiretap channel over which additional secrecy codes can be utilized, can be extended to produce other effective discrete memoryless wiretap channels as well that may form ideal backdrops for other code designs to operate in more realistic environments.

4.2 Cryptographic strength of new metrics
In this section, we consider implications of our new security metrics in light of current acceptable levels of computational security for modern cryptography. According to the US National Institute of Standards and Technology (NIST), "approved security strengths for federal applications are 112, 128, 192, and 256 bits [34]." As may be expected, the required strength of an applied security algorithm is set according to the importance of the data to be encrypted. For example, low-impact information
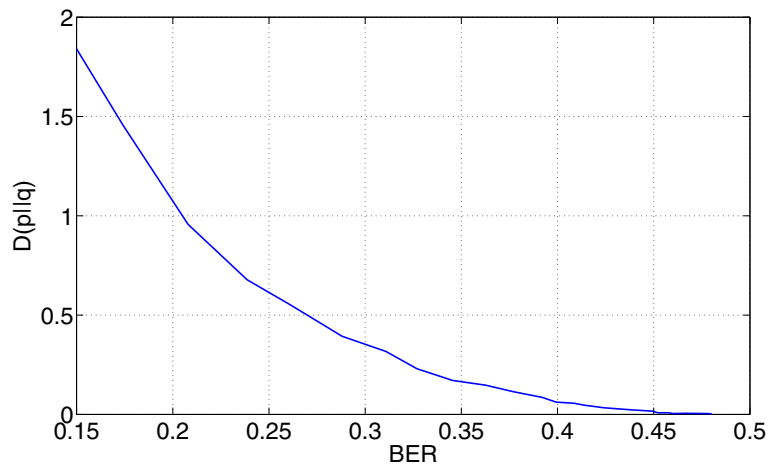
Fig. 9 Kullback-Leibler divergence between distributions of LLRs that correspond to bits in error and LLRs that correspond to correct bits at the output of an LDPC soft decoder, as a function of the hard-decision BER at the output of the decoder. As the BER approaches 0.5, the distributions become more alike, to the point where detecting a correct bit or a bit in error is impossible, even with soft information

that is communicated over wireless links may only be required to be encrypted using algorithms deemed to achieve cryptographic strength at the 112-bit level, while high-impact information would require the 192-bit level [34]. The cryptographic strength of an algorithm can be measured in many ways, including the length of any secret keys used during encryption/decryption and the complexity/running time of the best known attack against the algorithm [34, 35]. Algorithms that achieve N bits of security are those where all known attacks require effort equivalent to a brute-force attack for guessing a key of length N bits.

When considering the new security metrics presented in this paper in light of cryptographic strength, we note that the metrics cannot adequately classify algorithms without additional cryptanalysis; however, we also note that physical-layer security has been shown to improve cryptographic strength when the two techniques (physical-layer security and cryptography) are used in tandem [36–38]. In cases like these, the role of physical-layer security is to introduce confusion regarding the true values of bits of ciphertext, thus requiring attackers to consider a noisy ciphertext model when formulating an attack [38].

If we assume that a nested coding technique as illustrated in Fig. 1 is used without cryptography at the application layer of the communication protocol stack, then parameters for both new metrics should be chosen to deliver the desired amount of security. In other words, cryptanalysis at the input to the outer decoder (see Fig. 1) would require us to calculate BE-CDF$^{bc}(t^*, \text{SNR}, \mathcal{S}_m, \mathcal{C}_i)$, where t^* is no longer the threshold of correct decoding for code $\mathcal{C}_i$, but rather the threshold that guarantees computational complexity in the attack to be at least at the

level of N bits. If N bits of security are not possible at an acceptable value of SNR for the eavesdropper, then the message size $\mathcal{S}_m$ and code $\mathcal{C}_i$ would need to be changed to allow the desired level of security.

Cryptanalysis at the output of the outer decoder could be achieved by considering BER-CDF$^{ac}(\delta, E_b/N_0, \mathcal{S}_b, \mathcal{C})$ for δ small enough to render attacks at this stage ineffective. An upper bound on the strength of the outer code can be calculated by considering $(0.5 - \delta)$ as the proportion of bits in error of $\mathcal{S}_b$ total bits at the eavesdropper's operating E_b/N_0 point. If we assume the eavesdropper knows the number of errors

$$N_e \approx (0.5 - \delta)\mathcal{S}_b, \tag{14}$$

then the eavesdropper would still have to cycle through $\binom{\mathcal{S}_b}{N_e}$ possible combinations of error locations to guess the plaintext, assuming there is no additional statistical information about the message the eavesdropper can leverage. Thus, in the absence of a smarter attack at the decoder's output, to achieve N-bit security at this stage for every block of data, a sufficient condition is that

$$\log_2 \binom{\mathcal{S}_b}{N_e} \geq N. \tag{15}$$

For the example scheme given in Section 4.1.1, $\mathcal{S}_b = 753$. If Eve operates in the flat area of the BER-CDF^{ac} curve so that all blocks of data have at least an error proportion of $(0.5 - \delta)$, then the scheme yields $\log_2 \binom{753}{(0.5-\delta) \times 753}$ bits of cryptographic strength when analyzed after the final decoder. Even for fairly large δ values, the strength at this point in the scheme is considerable. From this analysis, it also becomes clear that the weak spot for the eavesdropper to try to attack the system is before the final decoder, rather than after the final decoder.

5 Conclusions

In this paper, we have discussed the landscape of physical-layer security coding metrics. We note that most measures in use today rely on information-theoretic analysis as blocklengths tend to infinity or use mean BER, both of which give asymptotic results that have limited meaning for short blocklength codes. We have proposed two new metrics that effectively employ CDFs to provide a lower bound on the security levels based on BER. Such an approach provides a stronger guarantee of secrecy over realistic channel models than simply using mean BER to estimate performance, and yet, our metrics retain their simplicity of calculation making them directly adaptable to real-world communication systems. The metrics apply generally to cases where concatenated codes are used to provide confidentiality, which includes as a special case the generic wiretap channel model. We have also shown how these new metrics may be used to reduce realistic channel model environments to simpler models over which known secrecy codes may be implemented to achieve information-theoretic security and have used them in performing basic cryptanalysis to aid system design.

Abbreviations
AWGN: Additive white Gaussian noise; BCH: Bose-Chaudhuri-Hocquenghem; BE-CDF^{bc}: Bit error cumulative distribution function; BER: Bit error rate; BER-CDF^{ac}: Bit error rate cumulative distribution function; BPSK: Binary phase shift keying; BSC: Binary symmetric channel; CDF: Cumulative distribution function; DMC: Discrete memoryless channel; DPSK: Differential phase shift keying; LDPC: Low-density parity-check; LLRs: Log-likelihood ratios; NIST: National Institute of Standards and Technology; SNR: Signal-to-noise ratio

Availability of data and materials
Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Authors' contributions
WKH conducted the review of existing research metrics, devised the second new metric, and drafted the manuscript. DS conducted the numerical studies in the Results section. JPV and MACG devised the first new metric, designed the scheme tested in the application section, and together with WKH considered the possibility that such a scheme may provide an effective BSC to eavesdroppers. All authors took an active role in the writing process of the document, and read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details
[1] Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT, USA. [2] Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, Coimbra, Portugal. [3] CISUC and Department of Informatics Engineering, University of Coimbra, Coimbra, Portugal.

References
1. W.K. Harrison, J. Almeida, M.R. Bloch, S.W. McLaughlin, J. Barros, Coding for secrecy: an overview of error-control coding techniques for physical-layer security. IEEE Signal Process. Mag. **30**(5), 41–50 (2013)
2. A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun. Surv. Tuts. **16**(3), 1550–1573 (2014)
3. C. Ling, L. Luzzi, J.-C. Belfiore, D. Stehle, Semantically secure lattice codes for the Gaussian wiretap channel. IEEE Trans. Inf. Theory. **60**(10), 6399–6416 (2014)
4. M. Bloch, M. Hayashi, A. Thangaraj, Error-control coding for physical-layer secrecy. Proc. IEEE. **103**(10), 1725–1746 (2015)
5. D. Klinc, J. Ha, S.W. McLaughlin, J. Barros, B.-J. Kwak, LDPC codes for the Gaussian wiretap channel. IEEE Trans. Inf. Forensics Secur. **6**(3), 532–540 (2011)
6. J.P. Vilela, M. Gomes, W.K. Harrison, D. Sarmento, F. Dias, Interleaved concatenated coding for secrecy in the finite blocklength regime. IEEE Sig. Process. Lett. **23**(3), 356–360 (2016)
7. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
8. I. Csiszar, J. Korner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory. **24**(3), 339–348 (1978)
9. A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin, J.-M. Merolla, Applications of LDPC codes to the wiretap channel. IEEE Trans. Inf. Theory. **53**(8), 2933–2945 (2007)
10. A.T. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, S.W. McLaughlin, in *Proc. IEEE Information Theory Workshop (ITW)*. Strong secrecy for erasure wiretap channels, (2010), pp. 1–5
11. A. Subramanian, A. Thangaraj, M. Bloch, S.W. McLaughlin, Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes. IEEE Trans. Inf. Forensics Secur. **6**(3), 585–594 (2011)
12. A.K. Pradhan, A. Subramanian, A. Thangaraj, in *Proc. IEEE Int. Symp. Information Theory (ISIT)*. Deterministic constructions for large girth protograph LDPC codes, (2013), pp. 1680–1684
13. M. Bloch, J. Barros, *Physical Layer Security: From Information Theory to Security Engineering*. (Cambridge University Press, 2011)
14. M. Baldi, M. Bianchi, F. Chiaraluce, in *Proc. IEEE Information Theory Workshop (ITW)*. Non-systematic codes for physical layer security, (2010), pp. 1–5
15. M. Baldi, M. Bianchi, F. Chiaraluce, Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: a security gap analysis. IEEE Trans. Inf. Forensic Secur. **7**(3), 883–894 (2012)
16. D.C. Montgomery, G.C. Runger, *Applied Statistics and Probability for Engineers*, 5th edn. (Wiley, Hoboken, 2011)
17. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
18. U.M. Maurer, in *Communications and Cryptography: Two Sides of One Tapestry*. The strong secret key rate of discrete random triples (Kluwer Academic Publishers, 1994), pp. 271–285
19. M. Bellare, S. Tessaro, A. Vardy, in *Advances in Cryptology – CRYPTO 2012*, ed. by R. Safavi-Naini, R. Canetti. Lecture Notes in Computer Science, vol 7417. Semantic security for the wiretap channel (Springer, 2012), pp. 294–311
20. U. Maure, S. Wolf, in *Advances in Cryptology — EUROCRYPT 2000*, ed. by B. Preneel. Lecture Notes in Computer Science, vol 1807. Information-theoretic key agreement: From weak to strong secrecy for free (Springer, 2000), pp. 351–368
21. M. Baldi, F. Chiaraluce, N. Maturo, S. Tomasin, in *Physical and Data-Link Security Techniques for Future Communication Systems*, ed. by M. Baldi, S. Tomasin. Lecture Notes in Electrical Engineering, vol. 358. Performance analysis of transmission over AWGN wiretap channels with practical codes (Springer, 2016), pp. 53–68

22. W.K. Harrison, J. Almeida, S.W. McLaughlin, J. Barros, Coding for cryptographic security enhancement using stopping sets. IEEE Trans. Inf. Forens. Security. **6**(3), 575–584 (2011)

23. J. Pfister, M.A.C. Gomes, J.P. Vilela, W.K. Harrison, in *Proc. IEEE International Conference on Communications (ICC)*. Quantifying equivocation for finite blocklength wiretap codes, (2017), pp. 1–6

24. C.W. Wong, T.F. Wong, J.M. Shea, in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*. LDPC code design for the BPSK-constrained Gaussian wiretap channel, (2011), pp. 898–902

25. M. Baldi, G. Ricciutelli, N. Maturo, F. Chiaraluce, in *Proc. IEEE International Conference on Communication Workshop (ICCW)*. Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel, (2015), pp. 435–440

26. T.K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. (Wiley, Hoboken, 2005)

27. D. Sarmento, J. Vilela, W.K. Harrison, M. Gomes, in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*. Interleaved coding for secrecy with a hidden key, (2015), pp. 1–6

28. J.P. Vilela, P.C. Pinto, J. Barros, Position-based jamming for enhanced wireless secrecy. IEEE Trans. Inf. Forensic Secur. **6**(3), 616–627 (2011)

29. J.P. Vilela, J. Barros, in *Proc. IEEE International Workshop on Data Security and PrivAcy in Wireless Networks (held Jointly with IEEE WoWMoM)*. Collision-free jamming for enhanced wireless secrecy, (Madrid, 2013)

30. Y. Liang, H.V. Poor, L. Ying, Secrecy throughput of MANETs under passive and active attacks. IEEE Trans. Inf. Theory. **57**(10), 6692–6702 (2011)

31. H. Mahdavifar, A. Vardy, Achieving the secrecy capacity of wiretap channels using polar codes. IEEE Trans. Inf. Theory. **57**(10), 6428–6443 (2011)

32. H. Zheng, W. Mav, Y. Choi, S. Zhang, Link performance abstraction for ML receivers based on RBIR metrics. Google Patents. US Patent App. 12/207,497 (2010). http://www.google.com/patents/US20100064185. Accessed Apr 2018

33. T. M. Cover, J.A. Thomas, *Elements of Information Theory*. (Wiley, Hoboken, 2006)

34. E. Barker, Guideline for using cryptographic standards in the federal government: cryptographic mechanisms. Technical report, National Institute of Standards and Technology (NIST) (2016). https://doi.org/10.6028/NIST.SP.800-175B. Accessed Apr 2018

35. N.D. Jorstad, L.T. Smith Jr., Cryptographic algorithm metrics. Technical report, Institute for Defense Analyses (IDA): Science and Technology Division (1997)

36. W.K. Harrison, S.W. McLaughlin, in *Proc. IEEE Int. Conf. Communications (ICC)*. Physical-layer security: combining error control coding and cryptography, (2009), pp. 1–5

37. W.K. Harrison, S.W. McLaughlin, in *Proc. IEEE Int. Symp. Information Theory (ISIT)*. Tandem coding and cryptography on wiretap channels: EXIT chart analysis, (2009), pp. 1939–1943

38. N.L. Gross, W.K. Harrison, in *Proc. IEEE Int. Conf. Communications (ICC)*. An analysis of an HMM-based attack on the substitution cipher with error-prone ciphertext, (2014), pp. 749–754