Interleaved Coding for Secrecy with a Hidden Key

Dinis Sarmento*, João P. Vilela§, Willie K. Harrison‡, Marco Gomes*
*Instituto de Telecomunicações, Department of Electrical and Computer Engineering
University of Coimbra, Coimbra, Portugal
Email: dinis.pereira@student.uc.pt, marco@co.it.pt
§CISUC and Department of Informatics Engineering, University of Coimbra, Coimbra, Portugal
Email: jpvilela@dei.uc.pt
‡Department of Electrical and Computer Engineering
University of Colorado Colorado Springs, Colorado Springs, CO, 80923
Email: wharriso@uccs.edu

***Abstract*—We propose a coding scheme based on the combination of interleaving with systematic channel codes for secrecy. The basic idea consists of generating a random interleaving key that is used to shuffle/interleave information at the source. The message and the interleaving key are then both encoded with a systematic code and the part related to the interleaving key is removed/punctured before being sent to the channel, hence operating as a hidden key for any receiver (legitimate or not) that needs to deinterleave the message. Successfully obtaining the original message then depends on determining the interleaving key, which can only be done through the parity bits that result from jointly encoding the interleaving key and the message. We provide a method to determine the necessary signal-to-noise ratio difference that enables successful reception at the legitimate receiver without the eavesdropper having access to the message. In addition, we provide evidence that this scheme may also be used to turn a realistic channel into a discrete memoryless channel, thus providing a first practical implementation of an abstract channel that can be employed with a wiretap code to provide information-theoretic security guarantees.**

***Index Terms*—wireless, secrecy, coding, interleaving, physical-layer security.**

I. Introduction

The resurgence of physical-layer security, after early contributions from the seventies stemming from information-theoretic security concepts [1], is tied to recent advances related to wireless networks and coding techniques. While some works have looked to the effect of intrinsic wireless phenomena such as fading [2] on the secrecy level of these networks, other works consider active approaches whereby cooperative users (either relays [3] or friendly jammers [4]) are available to improve security by providing an advantage over eavesdroppers, an underlying assumption of most works.

In terms of coding for secrecy techniques [5], it was already shown by Wyner in 1975 [6] that there exist codes (wiretap codes) simultaneously guaranteeing reliable communication to Bob and secrecy against Eve. A great amount of work has recently been developed to provide code constructions that satisfy information-theoretic security constraints [7], [8]. However, these code constructions exist only for discrete memoryless wiretap channels, and require either a noiseless channel for Bob or a degraded wiretap channel for Eve [5]. In order to utilize these code constructions in real-world scenarios, it becomes relevant to design coding schemes that aim to produce an effective wiretap channel over which these codes can be applied.

Explicit constructions for more realistic channel models include puncturing for secrecy [9], where Klinc et al. propose a coding scheme in which messages are transmitted over punctured bits to hide information from eavesdroppers, thus leading to a small security gap (i.e. the ratio between Bob and Eve's channel quality required to achieve a desired level of physical-layer security). It was later proposed [10] to avoid directly exposing the secret information bits by using scrambling techniques over blocks of concatenated frames under the assumption that the eavesdropper's channel is noisier than the legitimate communications channel. When Eve's channel is not worse than Bob's channel, a feedback automatic repeat request (ARQ) mechanism is shown to provide secrecy at the cost of retransmissions and increased latency.

For more simplistic channel models, codes have been developed/evaluated with traditional information-theoretic measures, such as equivocation, mutual information, secrecy capacity, and variants thereof. While these metrics provide strong secrecy guarantees, information-theoretical analysis over more realistic channel models in short blocklength regimes is in general intractable. This has led to more operational secrecy metrics, such as the bit-error rate and its security gap [9] variant that are applicable to more realistic scenarios, yet do not satisfy information-theoretic security requirements. We proposed [11] the use of two metrics that strengthen the BER analysis by considering the entire distribution (cumulative distribution function (CDF)) of possible errors. The bit-error CDF (BE-CDF^{bc}) analyzes the probability of error before a code (hence the superscript bc) while the bit-error rate CDF (BER-CDF^{ac}) does the same, but after decoding.

In this work, we present a coding scheme that relies on keyed interleaving and channel encoding for the transmission of secret information. In essence, the key and the interleaved

This work was partially funded by the Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) under project UID/EEA/50008/2013 - C00356 (WINCE - Wireless Interference and Coding for Secrecy) conducted at Instituto de Telecomunicações, and project PTDC/EEI-TEL/3684/2014 (SWING2 - Securing Wireless Networks with Coding and Jamming). It was also partly supported by project iCIS under grant CENTRO-07-ST24-FEDER-002003.

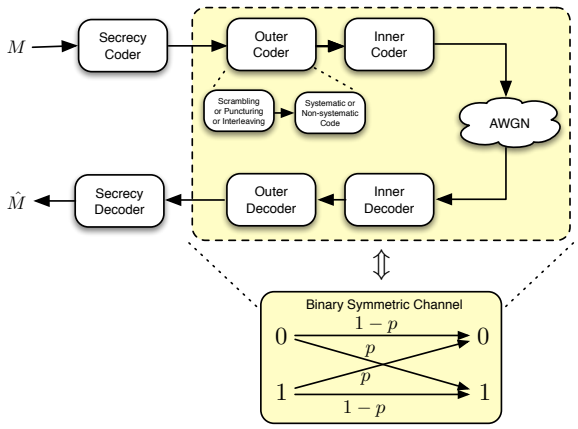

Fig. 1. A concatenated coding scheme may be utilized to emulate a binary symmetric channel (BSC) over which known secrecy codes may operate for information-theoretic security.

message are concatenated and then encoded into a single systematic codeword, whereupon the systematic bits associated with the key are punctured prior to transmission over a Gaussian wiretap channel. We show that this scheme can be used for secret communication, and also highlight an additional use case where the scheme can be used to turn a realistic wiretap channel (i.e. the Gaussian wiretap channel) into an effective discrete memoryless wiretap channel. This coding scheme can then be concatenated with a wiretap code that can achieve strong secrecy (in the information-theoretic sense) over a discrete memoryless channel (e.g. [12]) to effectively provide information theoretic security over the realistic wiretap channel without the need for a degraded channel model or a noise-free legitimate communications channel, as implied by Fig. 1.

The rest of the paper is organized as follows. First, we describe our system setup and more thoroughly describe relevant metrics in Section II. We then describe our coding scheme and resort to relevant metrics to assess its performance in Section III. In Section IV we show how this scheme effectively models a BSC for use with wiretap codes, and Section V concludes the paper.

II. System Model

We consider a wiretap channel system model, where the transmitter Alice wants to send a message M to the legitimate receiver Bob while an eavesdropper Eve is overhearing information. It is assumed throughout that M is a random binary message with equally likely independent and identically distributed bits, although in practice, the scheme may still be useful for real messages. As proposed in [13], an interleaving key K is used at the encoder to shuffle data before being appended to the interleaved message and encoded using a systematic code. Much of the codeword is then transmitted through a Gaussian wiretap channel to Bob and Eve.[1] however, the interleaving key K is not transmitted and, hence is hidden from the receivers (both Bob and Eve). The only information transmitted about the key is given indirectly through the parity bits in the transmitted codeword. Additional details of the encoders and decoders are given in Section III.

Let $\dot{X}$ represent a block of data X that has been decoded once. M^m represents a message of size m, while M_i^m corresponds to its shuffled/interleaved counterpart. Shuffling/interleaving is performed with a key K^k of size k, and P_b corresponds to the parity bits of an encoded message. Estimates of a message M after decoding are represented by $\hat{M}$ and $\tilde{M}$.

We consider an eavesdropper with the same type of soft-decoder as the legitimate receiver, as described in Section III.

A. Metrics

Due to the difficulty in the analytical study of coding schemes for secrecy over realistic channel models [14], security evaluation typically comes in the form of either bit error rate (BER) or security gap. In terms of BER, it is desirable to reach a low enough level (e.g. 10^{-5}) to the legitimate receiver, while assuring a BER as close as possible to 0.5 for the eavesdropper. The security gap [9] measures the required signal-to-noise ratio (SNR) advantage over an eavesdropper to operate at prescribed BER levels for Bob and Eve. It is calculated as the ratio between the minimum SNR threshold that achieves an acceptable reliability error rate for transmission to Bob $SNR_{B,min}$, and the maximum SNR threshold at which Eve operates with a minimum error rate level $SNR_{E,max}$.

While these more operational metrics simplify system analysis and design over practical (short blocklength) channels, high error rates to the eavesdropper do not necessarily mean that information has not been leaked. Therefore, rather than calculating simple averages (as in the BER), we make use of knowledge of the entire distribution of BER values to make stronger guarantees about the performance of codes in the short blocklength regime [11]. Moreover, instead of using these metrics for secrecy purposes, we do it to emulate a BSC with as high an error probability as desired. For that we will resort to the bit error-cumulative distribution function (BE-CDF) and bit error rate-cumulative distribution function (BER-CDF) so as to make lower bound probabilistic guarantees on error rates over short blocklengths both preceding and following a given code, as depicted in Fig. 2. These metrics are defined as follows.

Definition 1 (Bit Error Cumulative Distribution Function [11]): The bit error cumulative distribution function, BE-CDF^{bc}(t, SNR, $\mathcal{S}_m$, $\mathcal{C}_i$), gives 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 *inner* code).

Working with the distribution of the number of errors allows us to overcome some of the shortcomings of the BER. For example, simply assuming a uniform error distribution and using the BER measured before the outer decoder to evaluate the likelihood of decoder failure is not a reliable method because, when the blocklength is short, errors are not guaranteed to occur so uniformly.

[1] Our scheme enables the exact determination of the needed advantage between Bob and Eve (example in Section III);

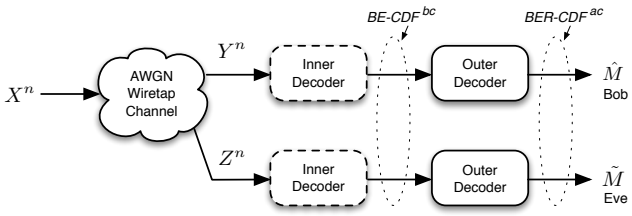

Fig. 2. Wiretap channel model assuming a concatenated coding scheme, where the outer code is for secrecy and the inner for reliability. The application points of the proposed new metrics are illustrated.

The BE-CDF^{bc} provides useful information when choosing possible SNR operation points for the legitimate user and the eavesdropper, by evaluating the effect of the channel. On the other hand, if Bob and Eve are expected to operate at given SNR values, this metric can also be used to provide information about which t-error correcting codes (of the BCH class for example) could be used as an outer code, to fit the given restraints [13].

Definition 2 (Bit Error Rate Cumulative Distribution Function [11]): The bit error rate cumulative distribution function, BER-CDF$^{ac}(\delta,\ E_b/N_0,\ \mathcal{S}_b,\ \mathcal{C})$ is the quantity

$$\Pr(\hat{P}_b > 0.5 - \delta) \tag{1}$$

calculated over $\mathcal{S}_b$ estimated message bits for a code $\mathcal{C}$ as a function of the energy per bit to noise power spectral density ratio E_b/N_0, where $\mathcal{C}$ may be the concatenation of an (optional) inner code $\mathcal{C}_i$ and an outer code $\mathcal{C}_o$, and $\hat{P}_b$ is the proportion of errors measured over $\mathcal{S}_b$ message bits at the output of the outer decoder.

This BER-CDF metric measures the probability of having a decoder failure that generates a BER close to 0.5 in the estimated message bits. In some sense, it can also be used to estimate a lower bound on the possible error rate at the output of the decoder over $\mathcal{S}_b$ bits, i.e. if $\Pr(\hat{P}_b > 0.5-\delta) \approx 1$, then a BER below $(0.5-\delta)$ over $\mathcal{S}_b$ bits occurs with probability approximately zero.

Note that the BER-CDF^{ac} is actually the complement of the CDF, but the nomenclature is chosen to be consistent with that of the BE-CDF^{bc}. Also, because we are calculating this metric after the decoder, it makes sense to use E_b/N_0, rather than SNR, although the conversion can be made if desired. The superscripts bc and ac indicate that the metrics are measure respectively *before* and *after* the outer decoder.

The two presented metrics can be applied as a pair to help in the design of systems that aim to provide both reliability and secrecy. The BE-CDF^{bc} can be used to identify regions of operation for Bob, in terms of SNR, that provide a high probability of decoding success and therefore, reliability. It also provides information of acceptable regions of operation for Eve that guarantee a high probability of decoder failure. The BER-CDF^{ac} can then be used to evaluate the contribution of the outer code in terms of generating a considerable BER when decoder failure occurs, which is desired at the eavesdropper's receiver.

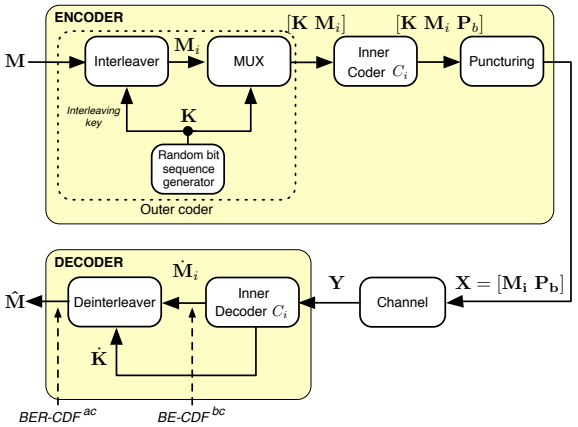

Fig. 3. Encoder and decoder processes of the described scheme. Note that the bits of K at the output of the inner coder are not transmitted onto the channel. P_b refers to the parity bits of the codeword at the output of C_i.

III. Interleaved Coding Scheme with a Hidden Key

Figure 3 illustrates our proposed scheme. At the beginning, a word K^k is randomly generated and used as a permutation key to interleave the message M^m, giving origin to a shuffled message M_i^m. Then, the key is concatenated to the interleaved message and coded by the inner coder, a systematic code C_i of size $(n, k+m)$. This scheme allows each length-m message to have it's own separate key. After the encoder process, only the last $n-k$ bits from the obtained codeword are transmitted onto the channel. This means that the bits of K, from the codeword at the output of the encoder C_i, are not transmitted, and hence hidden from both Bob an Eve. Information on those bits is only present within the transmitted parity bits. This can be seen as a limiting case of the scheme proposed in [13] where intentional friendly jamming was used only when data associated with K was transmitted so as to hide information about the key from eavesdroppers. If we consider an infinite jamming power over the key, then we ensure an eavesdropper obtains no information about K, just as in this case where the key is not transmitted. On the decoder end we apply a state-of-the art soft inner decoder followed by a deinterleaver, as depicted in Fig. 3. The goal of the inner code is to strike a balance so that the punctured key bits can be retrieved over Bob's channel, but not over Eve's channel.

A. Performance analysis

Let us consider, for illustration purposes, a powerful systematic inner LDPC code of dimensions (1536,1280), that resorts to the sum-product algorithm for decoding. To identify regions of operation for Bob and Eve as a function of the SNR and the size of the key (k), we consider the BE-CDF^{bc} applied over the bits of K at the output of the inner decoder. Since we are interested in assessing the likelihood of Bob and Eve retrieving the key without errors, we consider the parameter $t = 0$, and therefore, Fig. 4 represents $\Pr(E = 0)$, where E is a random variable that indicates the number of errors in the decoded key bits at the output of the LDPC decoder.

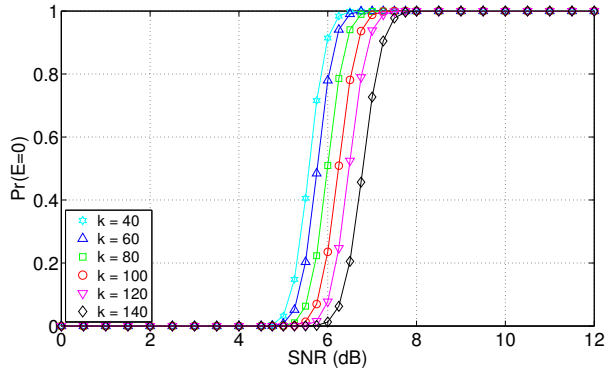

Fig. 4. BE-CDF^{bc} for the first k bits coded by a LDPC$(1536, 1280)$. These bits are not transmitted. The remainder of the codeword is transmitted onto a AWGN channel using BPSK modulation.

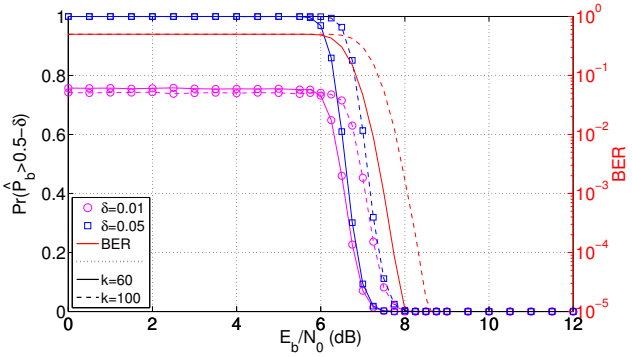

Fig. 5. BER-CDF^{ac} and BER for the coding for secrecy scheme presented on Section III, when the inner code is a LDPC$(1536, 1280)$ and using a key with k bits.

Examining Fig. 4, it is easy to identify, for each curve, the SNR region that displays a probability close to 1 of obtaining a key with errors, and the SNR region where getting an errorless key is guaranteed with high probability. These will be the regions of operation for Eve and Bob, respectively. The gap ($\approx$ 2.5dB) between the thresholds of these regions of SNR corresponds to a rough estimation on the minimum advantage Bob needs to possess over Eve in terms of channel quality, which seems to not vary much with the key size according to the results in the figure. The security criteria could be made stronger by enforcing that Eve is affected by a minimum number of errors N, i.e. $\Pr(E < N) \to 0$, which would widen the required SNR gap to Bob, but would make it harder to correct errors by exhaustively testing all possible error patterns.

The BE-CDF^{bc} gives us an idea on the advantage in terms of SNR Bob needs to maintain over Eve. In order to get a more precise value for this gap of SNR and have more closure on the security brought by this scheme, we will analyze the BER-CDF^{ac} and BER, depicted in Fig. 5. For illustration, we picked the cases in which the key is composed of 60 and 100 bits. We also consider the transmission secure if the eavesdropper's decoding generates a $\Pr(\hat{P}_b > 0.45) \geq 0.999$, i.e. the security restriction would be fulfilled if Eve operates at $E_b/N_0 \leq 5.5$ dB for $k = 60$, and at $E_b/N_0 \leq 6$ dB for $k = 100$. This restriction could be made closer to $\hat{P}_b = 0.5$ and with greater

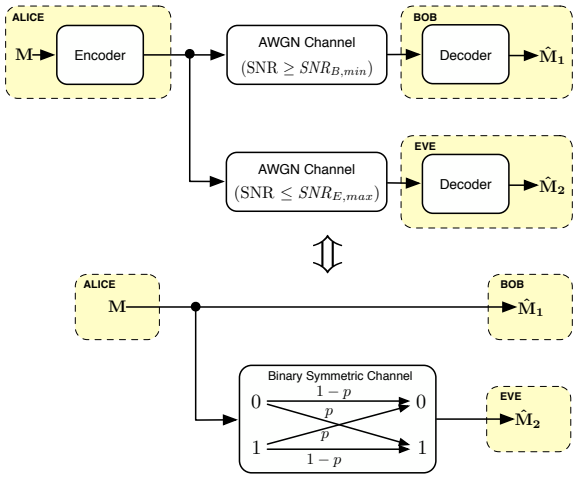

Fig. 6. Using the encoder and decoder from Fig. 3 a perfect channel is emulated for Bob when having a AWGN channel and operating at a value of SNR $\geq SNR_{B,min}$. For Eve a BSC is emulated when having a AWGN channel and operating at a value of SNR $\leq SNR_{E,max}$.

probability with a corresponding reduction in the acceptable E_b/N_0 level for Eve. If we recognize the transmission as reliable if the BER over the message bits is below 10^{-5}, Bob would have to operate at $E_b/N_0 \geq 8$ dB and $E_b/N_0 \geq 8.6$ dB for keys of size 60 and 100, respectively. From here on we will refer to $SNR_{B,min}$ and $SNR_{E,max}$ as the threshold values of SNR that limit the regions of operation of Bob and Eve, respectively.

With Bob and Eve operating at $SNR_{B,min}$ and $SNR_{E,max}$, respectively, of the previously defined operating regions, the advantage of E_b/N_0 (or SNR) Bob needs over Eve for assuring reliability and security is 2.5 dB for $k = 60$ and 2.6 dB for $k = 100$. The similarity of these values is interesting, because it introduces the notion of selecting the most appropriate key size (i.e. the one that assures reliability and has the highest possible value of $SNR_{E,max}$), when applying this security scheme to a scenario where Bob's expected SNR is characterized.

IV. Generation of a Discrete Memoryless Channel

Now that we have an idea of how this scheme performs in terms of acceptable SNR thresholds for Bob and Eve, let us move on to a possible use case, which is the concept of using our coding scheme to emulate a discrete memoryless channel, more specifically, a BSC. The availability of an error-free channel to the legitimate receiver and a discrete memoryless channel to the eavesdropper enables the applicability of existing wiretap code constructions [5], [11].

We will now make the necessary deliberations for showing that the previously introduced scheme can emulate this situation, when Bob and Eve receive data through an AWGN channel with a SNR greater than $SNR_{B,min}$ and less than $SNR_{E,max}$, respectively, as illustrated in Fig. 6.

Let us start by defining the bounds for the emulated channels. For illustrative purposes, Bob's channel will be considered as perfect if the probability of having errors on

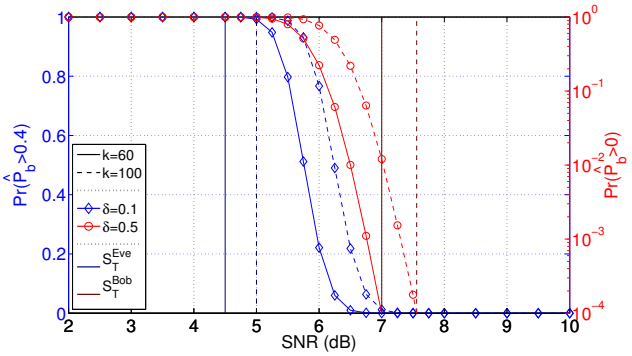

Fig. 7. BER-CDF^{ac} for the coding for secrecy scheme presented on Section III, when the inner code is a LDPC$(1536, 1280)$ and using a key with k bits. The thresholds values of operation for Bob and Eve are also included.

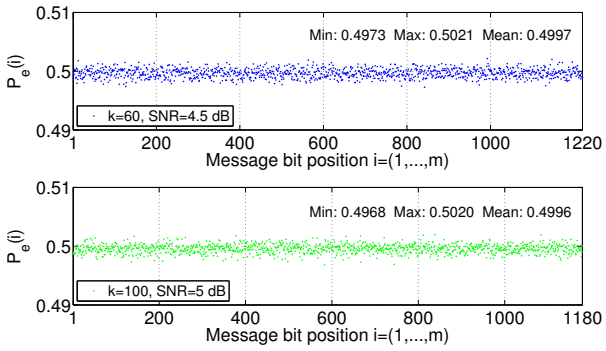

Fig. 8. Probability of error of a bit from a decoded message, P_e, as a function of n, which represents the position of the bit on the message word of size $1280 - k$.

the message bits after the decoding of a block is at least fewer than 10^{-4}, i.e. $1 - P(E_X = 0) \leq 10^{-4}$, where E_X represents the number of errors in the message bits. The BER-CDF^{ac} with $\delta = 0.5$ allows us to evaluate this probability, i.e. $1 - P(E_X = 0) = \Pr(\hat{P}_b > 0)$. On a similar fashion, Eve's channel will be considered as a BSC, if the probability of it possessing the properties of a BSC, for the transmission of a block, is at least 0.9999.

The properties that need to be verified for considering that Eve's channel is modeled as an effective BSC are:

1) the probability p of flipping each bit over the channel should be identical for all bits;
2) each bit should be flipped independently from all other bits;
3) soft information about bit values should be unavailable to attackers.

The key ingredient that provides the first two properties of the BSC is interleaving. The first property is true due to the keyed interleaving of the scheme. Since each codeword possesses its own interleaving key, as long as the interleaving keys are uniformly random, this property is guaranteed. The second property can be guaranteed by adding an additional interleaving operation prior to the inner code as in [15] and many other sources, where one bit from each of several interleaved message blocks is grouped at the input of the inner code. Thus a block error at C_i's decoder gives bit errors throughout several message blocks, and neighboring groups of message bits are independently in error at the output of the final deinterleaver. Finally, the third property has been shown in [11], where the Kullback-Leibler divergence between distributions of LLRs for bits in error and correct bits is shown to go to zero as the SNR in the channel degrades, indicating that the soft information becomes worthless for detecting errors.

We provide simulation results of some of these phenomena by considering the example from the last section, i.e. using a LDPC$(1536, 1280)$ code as the inner code and considering the key sizes of 60 and 100. Figure 7 represents the BER-CDF^{ac} for this scenario as a function of the SNR. The values of $\delta = 0.1$ and $\delta = 0.5$ were chosen for evaluating Eve's and Bob's performances, respectively. The vertical dark red lines indicate the minimum values of SNR, (7 dB for $k = 60$ and 7.56 dB for $k = 100$), that satisfy the previously stated requirement for considering Bob's channel as perfect. The values of $SNR_{E,max}$, (4.5 dB for $k = 60$ and 5 dB for $k = 100$), marked by the vertical dark blue lines, are the maximum SNR values that guarantee $\Pr(\hat{P}_b > 0.4) \geq 0.9999$. Recall that $\hat{P}_b$ is the proportion of estimated message bits in error over a single block of data, so this guarantee indicates that all blocks maintain at least a 40% error rate.

We will evaluate the first property for considering that Eve's channel is a BSC, when Eve operates at $SNR \leq SNR_{E,max}$, through the analysis of the probability of error of each message bit, for $SNR = SNR_{E,max}$. In Fig. 8, we see that for both cases, the probability of flipping each message bit over the channel is approximately identical for all message bits, with value $p \approx 0.5$. This result verifies the first stated property, and indicates that the effect of the deinterleaver on error-prone data is significant enough to drive the average error rate of any single bit to 0.5.

The second property can be given by inter-block interleaving as already specified, but we wish to see if the scheme may still provide the property in the absence of the additional interleaver. However, evaluating if each bit is flipped independently from all other bits proves to be a more difficult challenge. Let E_X be the random variable that defines the number of errors on a word of size m, received through a BSC with probability of flipping a bit P_f. Then, due to the errors being independent, $E_X \sim Bin(m, P_f)$, with $Bin(\cdot)$ representing the Binomial distribution with parameters m and P_f. Then, the probability of having x errors on a received word is given by:

$$\Pr(E_X = x) = \binom{m}{x} {P_f}^x (1 - P_f)^{m-x}. \quad (2)$$

When $P_f = 0.5$, which corresponds to the value of p we identified on Fig. 8, (2) can be simplified into:

$$\Pr(E_X = x) = \binom{m}{x} 0.5^m. \quad (3)$$

In Figs. 9 and 10 the PMFs that model the number of errors on the decoded message bits are obtained through simulation. For comparison, the two cases we are considering ($k = 60$ and $k = 100$) are depicted against the PMF of E_X for the respective values of m and P_f [2]. Although this comparison

[2]Due to the complexity of calculating (3) for large values of m, the curves on Figs. 9 and 10 were obtained by approximation to a normal distribution. The central limit theorem states that for large values of m and/or P_f close to 0.5, $E_X \sim B(m, P_f)$ approaches $E_X \sim \mathcal{N}(m \times P_f,\ m \times P_f(1 - P_f))$.

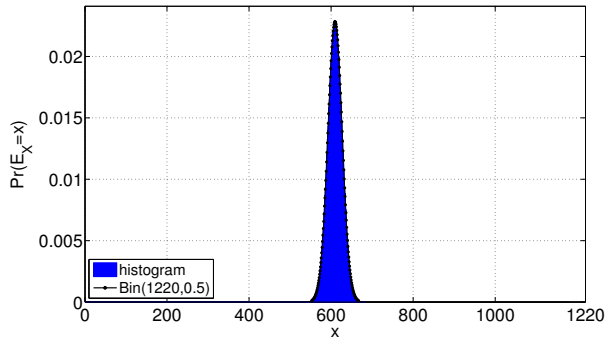

Fig. 9. Probability of having x errors on the decoded message, for the scheme presented on Section III when the inner code is a LDPC$(1536, 1280)$, k=60 bits and the SNR is 4.5 dB. The curve from (3) when $m = 1220$ is shown for comparison.

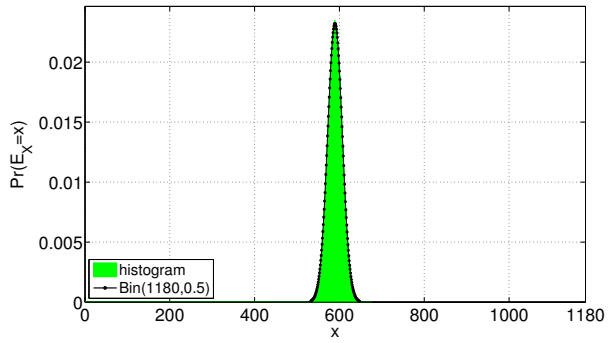

Fig. 10. Probability of having x errors on the decoded message, for the scheme presented on Section III when the inner code is a LDPC$(1536, 1280)$, k=100 bits and the SNR is 5 dB. The curve from (3) when $m = 1180$ is shown for comparison.

is not enough to claim that the second property is verified without the additional interleaver, it serves as an indicator of how our coding scheme approaches the behavior of a BSC for the example parameters evaluated, even without the addition of an inter-block interleaver.

It is well known that the mutual information over a BSC with $p = 0.5$ is zero and, therefore, if the probability of a flipped bit can indeed be assumed to be 0.5, then this scheme could provide secrecy by itself. However, we feel that the proper approach to achieving secrecy in practice is to apply a wiretap code on top of the emulated BSC, while assuming the lower bound of the error rate over smaller blocks of $p = 0.5 - \delta$, ($p = 0.4$ in this case) given by the BER-CDF^{ac}. Any secrecy codes appended to our system would then be designed to provide information-theoretic security on this lower bound p value, and would thus provide it in practice on every (possibly short) secrecy codeword since we have designed for the worst case error rate over a single small block of data.

We also point out that these results are more general than the specific code outlined in this section, and any code that leads to similar properties (steep waterfall region) could be applied to our scheme with the accompanying analysis to identify the required SNR gap between Bob and Eve.

V. Conclusions

We proposed a coding scheme that relies on a hidden interleaving key and a given signal-to-noise ratio advantage to conceal information from an eavesdropper. Through a systematic code, the interleaving key is encoded with the original message, but punctured/hidden before being sent through the channel, meaning that for any receiver the only information about the key is in the transmitted parity bits. The systematic code needs to be powerful enough and have enough parity bits to allow a receiver with a favorable signal-to-noise ratio to obtain an errorless key to decode and deinterleave the original message. Our methodology allows us to determine the exact signal-to-noise ratio advantage needed for a legitimate receiver to obtain the key (and consequently the message) without an eavesdropper being able to do so. We have also outlined arguments and given evidence for using this scheme to generate an effective discrete memoryless channel from a Gaussian wiretap channel. Therefore, the scheme can be concatenated with existing wiretap codes that require such a channel to provide information-theoretic security guarantees.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[3] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, September 2008.

[4] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, June 2011.

[5] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, September 2013.

[6] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[7] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Submitted to Proc. IEEE*, pp. 1–37, 2015.

[8] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, August 2007.

[9] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, Sept 2011.

[10] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and harq for the awgn wire-tap channel: A security gap analysis," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883–894, 2012.

[11] W. K. Harrison, D. Sarmento, J. P. Vilela, and M. Gomes, "Analysis of Short Blocklength Codes for Secrecy," *ArXiv e-prints*, Sep. 2015, [Online]. Available at http://arxiv.org/abs/1509.07092.

[12] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[13] J. P. Vilela, M. Gomes, W. Harrison, D. Sarmento, and F. Dias, "Interleaved Concatenated Coding for Secrecy in the Finite Blocklength Regime," *Submitted for publication*, 2015.

[14] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6399–6416, 2014.

[15] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs under passive and active attacks," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6692–6702, Oct. 2011.