Adaptive Physical-Layer Security through Punctured Coding for Secrecy

Miguel Carreira[*], Thyago Monteiro[*], Marco Gomes[*], João P. Vilela[§], Willie K. Harrison[‡]
[*]Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, Portugal.
[§]CISUC and Department of Informatics Engineering, University of Coimbra, Portugal.
[‡]Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT, 84602.
Emails: uc2012152271@student.uc.pt, thyago.pinto@co.it.pt, marco@co.it.pt, jpvilela@dei.uc.pt, willie.harrison@byu.edu

***Abstract*—We propose a coding methodology for physical layer security with adaptive characteristics, whereby adaptive we mean that the system must be tunable to different operational points/signal-to-noise ratio levels of both the legitimate receiver and the eavesdropper. Based on interleaving and scrambling as techniques that shuffle the original message before transmission, we consider puncturing over an interleaving/scrambling key and/or over the message as a mechanism to provide the required adaptability to channel conditions. The proposed techniques have shown suitable adaptability to different channel quality levels of the legitimate receiver and eavesdropper, while still guaranteeing the desired reliability for the legitimate receiver and secrecy against the eavesdropper.**

Index Terms- Adaptive physical-layer security, scrambling, interleaving, puncturing, coding for secrecy.

I. Introduction

The wiretap channel is a reference model for secrecy evaluation in transmission schemes. Its structure is represented by a communication model dedicated to providing information for a legitimate receiver (Bob) in the presence of an eavesdropper (Eve) trying to identify the message [1]. In a general formulation of the problem, the illegitimate receiver is assumed to have no ability to process the data and discover the final message, due to an inferior signal to noise ratio (SNR). Therefore, to accomplish reliability to Bob and secrecy against Eve, several approaches have been investigated in the literature, such as based on information theory [2], cryptography [3] and physical-layer security (PLS) [4]. Considering the wireless channel, the main aspect of using PLS is to explore the inherent transmission randomness, and in such scenarios, scrambling, interleaving, and puncturing have shown to be appropriate techniques to achieve secrecy [5]. Current PLS works include [6]–[10]. Some of these follow a more theoretical approach, resorting to classical fundamental metrics such as mutual information and strong secrecy [6], while others target security from a system's perspective considering metrics such as bit error ratio (BER) and security gap (SG) [7]–[10]. However, most of these setups aim to provide secrecy and possibly reliability in an agnostic manner to the operation regions of the legitimate receiver and the eavesdropper. This is a major deficit of current schemes since there is no adjustment to different SNR levels of the involved parties.

Some recent works address the adaptive PLS nature as in [11] where is explored a setup with a cooperative jammer (CJ) sending a private message for a specific receiver with optimal transmission power and concurrently interfering with an eavesdropper. This scenario is expanded in [12] by letting the transmitter send information with artificial noise (AN), and as in [11] the CJ takes place when certain constraints are encountered. In [13] an adaptive link scheduling resource allocation was analyzed using a repeater between the transmitter and the receiver, and in [14] an adaptive interleaver is used to sort N sub-channels of an orthogonal frequency division multiplexing (OFDM) system with a frequency selective fading channel, estimating the best angle to transmit the symbols based on channel conditions. Additionally, in [15], an adjustable setup based on several code rates in concatenated polar codes and low-density-parity-check (LDPC) codes is considered.

Setups in [11]–[13] target flexibility in terms of optimal power distribution and mechanisms for secure and reliable communication based on secrecy rate, power allocation ratio and effective energy criteria, changing the transmit power and requiring an additional CJ device to provide defense against the eavesdropper. Concurrently, in [14] the adaptable characteristic is taken considering a specific fading channel, while in [15] changes in operation points for secrecy come at the cost of useful data rate by altering the code rate.

The basic perspective in this work is to establish an adaptive PLS transmission scheme that is able to provide reliability for Bob and secrecy against Eve, with both operating at different and varying operation points/SNR levels. The proposed methodology comes from varying the number of punctured bits of scrambling and interleaving for secrecy schemes, where a key is used to scramble/interleave the original message before transmission. The goal is to determine the most suitable puncturing pattern to guarantee operation adaptability while ensuring reliability for Bob and secrecy against Eve. The remainder of this paper is organized as follows. In Section II, the background of the mentioned schemes will be explored, followed by the main metrics for performance evaluation. Con-

This work was partially funded by the following entities and projects: the US National Science Foundation (Grant Award Number 1761280), the FLAD project INCISE (Interference and Coding for Secrecy), project SWING2 (PTDC/EEI-TEL/3684/2014), funded by Fundos Europeus Estruturais e de Investimento (FEEI) through Programa Operacional Competitividade e Internacionalização - COMPETE 2020 and by National Funds from FCT - Fundação para a Ciência e a Tecnologia, through projects POCI-01-0145-FEDER-016753 and UID/EEA/50008/2013.

cept definition, transmission results on the proposed adaptive scheme and discussions appear in Section III. In Section IV, the major contributions of this paper are summarized.

II. Background

A. Wiretap Channel

The approach for evaluating secrecy in PLS is generally based on the wiretap channel proposed by Aaron Wyner [1] and presented in Fig. 1. This model establishes the communication between a transmitter (Alice) and a legitimate receiver (Bob) over a perfect channel in the presence of an eavesdropper (Eve) trying to intercept the message through a degraded channel. Here, the data M sent by Alice is encoded into X^n and sent through the channel. Bob receives $\hat{Z}$ and decodes it into an estimation of M, $\hat{M}$. Meanwhile, Eve is listening and also receives a word $\tilde{Z}$, which is decoded into an estimation of M, $\tilde{M}$. The situation of Eve discovering the private information, i.e., $\tilde{M} = M$, is not desirable and Wyner proved it to be possible to design error correction schemes to simultaneously guarantee secrecy and reliability for the communication model [1]. Furthermore, with the increasing number of services diffused by the wireless channel, a medium susceptible to interference, it becomes mandatory for certain applications to guarantee privacy, and several transmission schemes have been researched for this purpose. In this work, a wireless environment is considered and both links in Fig. 1 are assumed to be additive white Gaussian noise (AWGN) channels. Moreover, Eve's channel is assumed noisier when compared with Bob's connection, and passive, which means she does not interfere and is not noticed by Alice. In terms of computational processing and knowledge of decoding algorithms, the eavesdropper also owns the same capabilities as Bob.

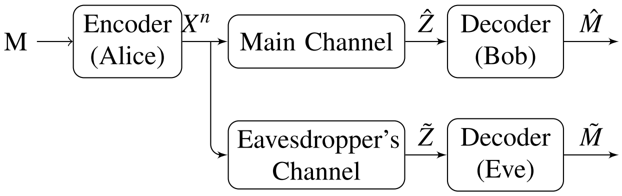


Fig. 1: Wiretap channel.

B. Coding for Secrecy with Hidden Key Schemes

Despite the obstacles faced in information transmission, errors introduced by a noisy channel can many times be detected and corrected by error correcting codes such as LDPC [10], turbo and convolutional codes. When they occur in long sequences, it is usual to employ techniques to spread them over the blocklength and facilitate the process of decoding. Interleaving is one of the methodologies employed with this purpose, allowing errors to be shuffled based on a known pattern or key. In the design of a system for secrecy, interleaving is utilized as an external code with the goal of increasing confusion to the eavesdropper as explored at the Interleaved Coding for Secrecy with a Hidden Key (ICSHK) scheme in [9] and depicted in Fig. 2. In this setup, a random key K is generated per message M and utilized to shuffle M into the resulting interleaved word M_i. Next, K and M_i are concatenated and the resulting vector $[K\ M_i]$ is encoded into a codeword X using a systematic inner code C_i with size $(l,(l_k+l_m))$, where l_k, l_m, and l are respectively the lengths of K, M and the word generated by C_i. Before passing through the channel, K or M_i are partially or completely erased, and the non-punctured bits X_p are sent. Eliminated bits remain hidden from both receivers, being retrievable from its parity bits introduced by the inner code. At the receiver, the decoding process is made in inverse order, starting by decoding to obtain an estimation of the interleaved message $\dot{M}_i$ and key $\dot{K}$, which is utilized for deshuffling $\dot{M}_i$ and estimating the message $\hat{M}$. For very good SNR conditions, zero errors occurrences in $\dot{M}_i$, $\dot{K}$ and $\hat{M}$ are expected. The existence of errors over $\dot{K}$ will lead to an incorrect recovery of M, increasing estimation failures but also secrecy in face of an eavesdropper. Interleaving can be implemented based on block, convolutional, and random methods, but for maximizing uncertainty given a blocklength code, this last was preferred through the development of this work.

Alternatively, the Scrambled Coding for Secrecy with a Hidden-Key (SCSHK) scheme [16] is implemented using the same architecture of Fig. 2 but replacing interleaving by a scrambler as an external code. The purpose remains the same, shuffling M and making it difficult for an eavesdropper to capture the information. While interleaving keeps message bits unchanged, just altering their positions within the blocklength, the scrambler generates an equivalent scrambled message M_i, where each bit is a linear combination of the original bits in M. A general scrambler model is presented in Fig. 3, constructed based on states $[m_{n-1}\ m_{n-2}\ \cdots\ m_{n-l_k-1}\ m_{n-l_k}]$ and l_k shift registers defined by a polynomial $[1+k_1z^{-1}+k_2z^{-2}+...k_{l_k}z^{l_k}]$ indicating which values influence the output as in

$$m_n^s = m_n \oplus \sum_{j=1}^{l_k} \oplus k_j m_{n-j}, \tag{1}$$

where $\sum\oplus$ represents mod 2 operation, and m_n and m_n^s are the scrambler input and output, respectively. In each interaction, the register values are shifted and the last position discarded. At the reception side, the descrambler reverts the scrambler impositions, i.e., the output at instant m_n is the result of the difference between the received symbol $m_n^{(s)}$ and the linear combination of l_k previously computed values. Mathematically, this means

$$m_n = m_n^s - \sum_{j=1}^{l_k} \oplus k_j m_{n-j}^s. \tag{2}$$

For secrecy, scrambling is utilized for error propagation in operation points with low-reliability performance, reinforcing the secure area against an eavesdropper. Since m_n^s is highly dependent on the l_k registers, its implementation in the Fig.

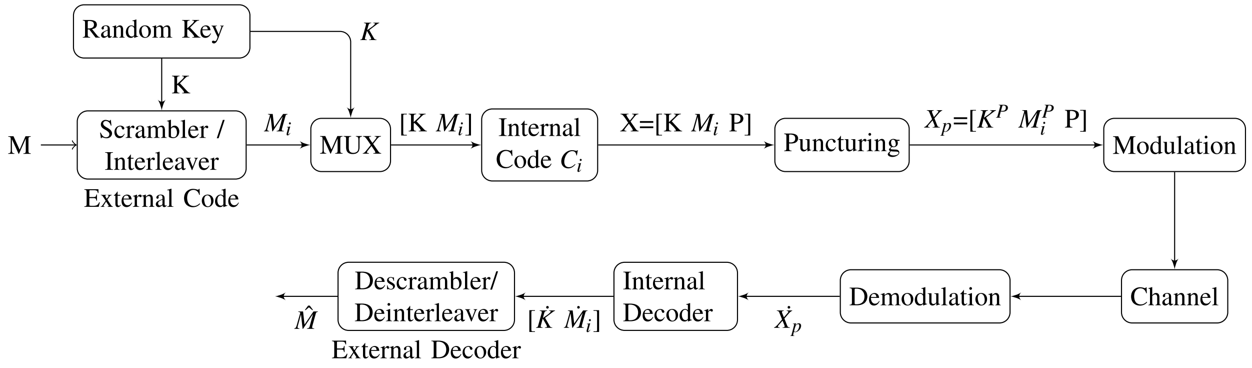


Fig. 2: Scrambler\ Interleaving for secrecy with hidden key scheme.

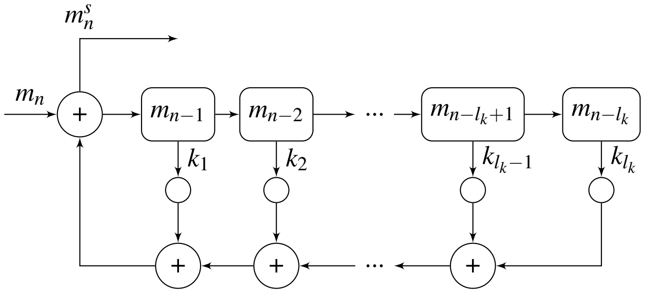


Fig. 3: Scrambler with l_k shift registers.

2 setup uses K as the connection polynomial instead of the initial state in order to improve its coding effects.

C. Puncturing

The main typical function of puncturing bits is to increase the code rate and suppressing redundancy at the encoded word. In SCSHK and ICSHK schemes, the puncturing stage means the elimination of total or partial key and message bits depending on system design, thus altering the code rate to

$$R = \frac{l_m}{l - N_{punct}}, \tag{3}$$

where N_{punct} is the number of erased bits. As a systematic inner code is applied, original bits from the key and the message are embedded in X, and it is possible to distinguish them. Considering this in the setup of Fig. 2, puncturing is performed designing if bits will be eliminated from K or M or both, but making the choice of bits randomly. For example, considering $l_k = 100$ and $N_{punct} = 50$ over K, the function will erase half of K bits present at X, and the same quantity will be eliminated from M if the project establishes puncturing over the message instead. The erased information can be recovered at the reception side by parity bits inserted by the inner code. Since the focus in this work is to analyze adaptability characteristics for the transmission setup, punctured indices are assumed transparent and known by all parties in the system of Fig. 1, and from a reception point of view, they are assumed to be zero.

D. BER and BER-CDF

Metrics for evaluating secrecy in communication systems conventionally rely on information theoretic concepts like weak secrecy [1], strong secrecy [17], perfect secrecy [18], and semantic secrecy [19]. Although these provide strong guarantees, they have limited applicability in practical channels where the analytical calculation of mutual information is impractical and the restriction of encoded word tending to infinity cannot be satisfied, being an obstacle when short and medium blocklength transmissions are investigated [5]. This way, metrics like BER, SG, block error ratio (BLER) and frame error rate (FER) are usually preferred for evaluating secrecy and reliability in a practical physical layer scenario.

To establish a secure zone to transmit data, the SG concept is utilized, corresponding to the difference between a reception level SNR_{min}^{Bob} for which the message can be correctly decoded by a legitimate receiver and a level SNR_{max}^{Eve} in which an eavesdropper is incapable of decoding it. The conventional security gap definition in dB can be described mathematically as

$$\text{SG}_{conv} = \text{SNR}_{min}^{Bob} - \text{SNR}_{max}^{Eve}. \tag{4}$$

Obviously, (4) presupposes a power advantage, and usually relies on observing the BER curve at reception, designing a low BER to the legitimate receiver BER_{max}^{Bob}, i.e., a reliability threshold imposing that Bob senses a $\text{BER}<\text{BER}_{max}^{Bob}$ and a high value to the eavesdropper (generally near 0.5) BER_{min}^{Eve}, meaning a security bound $\text{BER}_{min}^{Eve} > 0.5$. Moreover, the interval SG_{conv} can be calculated using extracted values at the BER curve in the points of SNRs or E_b/N_o corresponding to the thresholds BER_{min}^{Eve} and BER_{max}^{Bob}. This way, (4) can be rewritten as

$$\text{SG}_{conv} = f_{SNR}(\text{BER}_{max}^{Bob}) - f_{SNR}(\text{BER}_{min}^{Eve}), \tag{5}$$

with $f_{SNR}(\text{BER}_{max}^{Bob})$ meaning the SNR value at the point BER_{max}^{Bob}, and $f_{SNR}(\text{BER}_{min}^{Eve})$ the SNR value at the point BER_{min}^{Eve}.

Despite the BER being a consistent metric for reliability purposes, its evaluation in terms of secrecy does not necessarily implicate no information leakage since it represents an average value of estimation failures, meaning it can cover their distribution. Furthermore, the BER is assumed to have a uniform distribution, which is not realistic for short blocklength codes. To overcome this phenomenon, an alternative is to analyze not only the BER but its behavior before and after the external decoder in Fig. 2.

As a different perspective to improve secrecy requirements, in [5] and [7], BER distribution analysis for short blocklength transmission is made and the bit error ratio cumulative distribution function BER-CDF$^{ac}(E_b/N_o, \delta, S_b, C)$ (after external decoder) is introduced and calculated using the parameters: points of energy per bit to spectral noise density ratio E_b/N_o, error tolerance δ, decoded message bits S_b and C utilized code. The BER-CDF allows the probability analysis of the proportion of bit errors per codeword, $\hat{P}_b$, to be superior to $0.5-\delta$ when $\delta << 0.5$. Mathematically, this means

$$Pr(\hat{P}_b > 0.5-\delta). \tag{6}$$

By taking the BER-CDF^{ac} into consideration, we redefine the SG concept for further secrecy guarantees when applied to the scenario of Fig. 2. This way, the SNR$_{max}$ for secrecy is then obtained considering error distribution after an external decoder or BER-CDF^{ac}, while reliability is still based on BER, i.e.,

$$\text{SG}_{new} = f_{SNR}(\text{BER}^{Bob}_{max}) - f_{SNR}(\text{BER}-\text{CDF}^{ac}). \tag{7}$$

With this new SG definition, more strict privacy guarantees with respect to the eavesdropper are endured, by looking at the entire distribution of errors (BER-CDF) other than the BER alone, while reliability is measured as usual through the BER. An example of (7) is graphically represented in Fig. 4 by the BER and BER-CDF^{ac} curves, respectively, in Fig. 4a and 4b, for the transmission setup of Fig. 2 with interleaving as the external code, $l_K = 100$, $N_{punct} = 75$ and $\delta = 0.05$. Reliability is taken at BER =10^{-4}, corresponding to $E_b/N_o = 8.12$ dB, and secrecy was based on $Pr(\hat{P}_b > 0.5-\delta) > 0.99$ achieved at $E_b/N_o = 6.12$ dB. The difference of these values extracted in each graphics results in the SG using (7), in this case, 2 dB (Fig. 4c). This means that an SNR gap of 2 dB between the legitimate receiver and the eavesdropper is sufficient to provide the prescribed reliability level for Bob and secrecy limit against Eve.

III. Adaptive Physical-layer Security through Punctured Coding

In this work, a transmission setup with operation point adjustment to establish a private communication is investigated. Adaptability is achieved considering puncturing patterns, and flexibility of the SG so as to encompass several SNR or E_b/N_o values for both receivers in Fig. 1. The system analyzed is based on ICSHK and SCSHK schemes described in Section II-B. Basically, observing the system performance, the transmitter changes N_{punct} in the encoded word and the area of action, erasing key or information bits. By this, BER and BER-CDF curves (Fig. 4a and 4b) are shifted and also the corresponding SG limits in a way to provide adaptable secrecy to the operation points of Bob and Eve.

A. System Configuration

The proposed adaptive system in terms of puncturing pattern over key and message bits for SCSHK or ICSHK schemes is presented in Fig. 2. We consider two setups, one with a medium-sized (1536,1280) LDPC code and another with a smaller (256,128) LDPC code. The randomly generated key has length $l_k = 100$ bits for the medium-sized blocklength code and $l_k = 64$ bits for the short LDPC code, and is used to interleave/scramble the data in the external coding stage. The concatenated vector $[K\ M_i]$ passes through the systematic inner LDPC code, then puncturing is performed over the key, the message, or both, with $N_{punct} = \{50, 100, 150\}$. Non-erased bits are modulated using the binary phase shift keying (BPSK) scheme and the resulting constellation is transmitted over an AWGN channel modeled as an additive noise. The received symbol is demodulated and sent to an internal decoder responsible to estimate K and M_i based on its parity bits. Vectors $\dot{K}$ and $\dot{M}_i$ pass through an external decoder and $\hat{M}$ is deinterleaved/descrambled based on $\dot{K}$.

B. Puncturing over the Key or the Message?

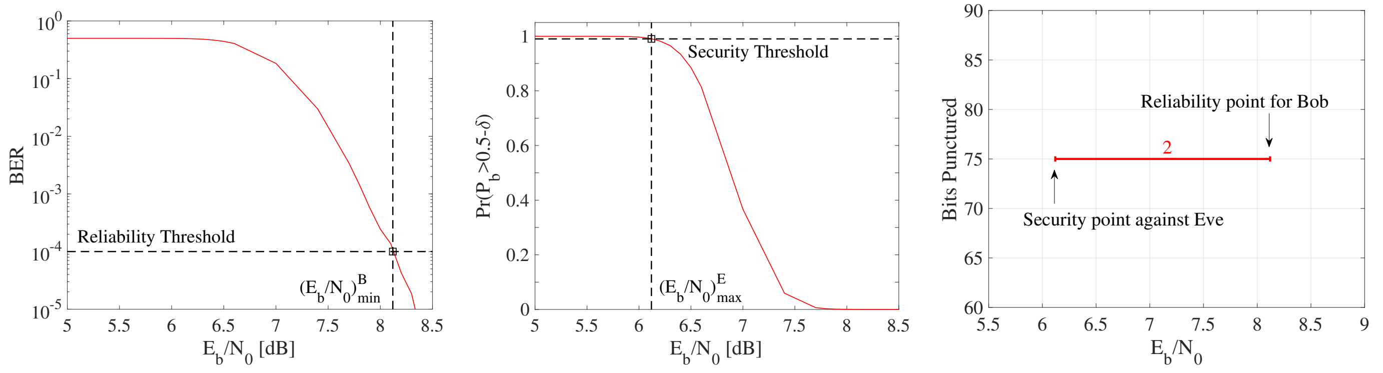
Considering the setup in Fig. 2, results were obtained by Monte Carlo simulations for several puncturing patterns following the notation X^K_P k X^M_P m, with X^K_P as the number of punctured bits of the key K, and X^M_P the number of punctured bits of the message M. For example, the notation "100k50m" means that 100 bits of K and 50 bits of M will be erased. So for each defined pattern, BER and BER-CDF curves behavior were generated like in Fig. 4 and we obtained the E_b/N_o values for reliability (BER=10^{-4}) and secrecy (BER-CDF=0.99), as summarized in Table I.

From the results of Table I, it is observed that the lowest E_b/N_o values for reliability (BER=10^{-4}) occur when puncturing first over the key, and only afterward over the message, namely for the "k50", "k100", and "100k50m" cases. This indicates that it is advantageous to primarily erase K to deliver the private message with a lower SNR. For secrecy, this behavior no longer holds and higher E_b/N_o are achieved for a combined action of X^K_P and X^M_P punctured bits, especially for cases when more M bits are eliminated.

In a combined analysis in terms of minimum SG, in general, higher X^K_P key punctured bits showed to be a more beneficial methodology, and puncturing first bits of the key was the selected approach for the remaining results. For example, if puncturing $N_{punct} = 50$ bits and with a key of size $l_k = 100$ bits, then half of the key bits will be eliminated, but if puncturing is realized over 120 bits, K will be entirely erased and the remaining 20 bits shall be removed over the message.

C. Puncturing for Adaptive Security

Based on a puncturing strategy of always erasing key bits first, the SG behavior for the system of Fig. 2 is given in Fig. 5 for both uses of interleaving and scrambling, an inner code with dimension (1536,1280), and calculating SG as expressed in (7). The leftmost E_b/N_o point in each line corresponds to secrecy threshold against an eavesdropper, while the rightmost



(a) Reliability analysis.

(b) Secrecy analysis.

(c) SG calculus.

Fig. 4: SG analysis for ICSHK scheme, $l = 1536$, $l_K = 100$ and N_{punct}=75.

TABLE I: Effect of puncturing pattern in terms of E_b/N_o for ICSHK and SCSHK schemes with reliability threshold at point BER=10^{-4} and secrecy threshold at BER-CDF=0.99.

	E_b/N_o (dB) at BER=10^{-4}		E_b/N_o (dB) at BER-CDF=0.99		SG (dB)	
Pattern	ICS	SCS	ICS	SCS	ICS	SCS
13k37m	7.93	7.89	6.00	6.00	1.93	1.89
25k25m	7.94	7.94	6.03	5.95	1.91	1.99
38k12m	7.95	7.91	6.01	5.90	1.94	2.01
k50	7.87	7.87	5.93	5.95	1.94	1.92
m50	7.89	7.88	5.55	5.70	2.34	2.18
25k75m	8.70	8.64	6.50	6.30	2.20	2.34
50k50m	8.64	8.62	6.46	6.47	2.18	2.15
75k25m	8.43	8.40	6.35	6.27	2.08	2.13
k100	8.32	8.28	6.30	6.24	2.02	2.04
m100	8.62	8.63	5.40	5.30	3.22	2.33
20k130m	10.24	10.29	7.13	7.13	3.11	3.16
35k115m	10.20	10.25	7.16	7.07	3.04	3.18
50k100m	10.10	10.10	7.14	6.91	2.96	3.19
65k85m	9.90	9.85	7.08	6.80	2.82	2.95
80k70m	9.60	9.46	7.00	6.85	2.60	2.61
100k50m	9.20	9.19	6.82	6.83	2.38	2.36
150m	10.17	10.34	5.25	5.60	4.92	4.74

point represents the reliability threshold for the legitimate receiver.

We observe in Fig. 5 that as the number of punctured bits is increased and advance from over the key until the message, the SG is shifted and expanded, showing a capacity degradation in error correction. This behavior maps the secrecy region over different puncturing patterns and allows an adjustable selection of the operational point, considering an autonomous transmitter trying to avoid information leakage.

Comparing SCSHK and ICSHK techniques in Fig. 5, no significant SG difference is observed for using scrambling or interleaving, and both techniques show comparable performance when acting as the external code. Despite this, SCSHK presents an advantage over ICSHK since its hardware implementation requires only activation/deactivation of switches, while ICSHK demands storage of all shuffling sequences at the transmitter and receiver. In terms of SG behavior, observable secrecy points show a lower variation, while reliability results are dispersed and more sensitive to the puncturing pattern. Moreover, the SG presents small changes until approximately $N_{punct} = 100$ bits, which corresponds to the key size. After this point, the parameter increases faster since message bits are also being erased and information data is lost, thus requiring a higher E_b/N_o for reliability. This increase in the number of punctured bits past the key size shifts the reliability threshold faster than the secrecy threshold, thus increasing the security gap. This reinforces the validity of our choice to first puncture/erase bits of the key other than the message.

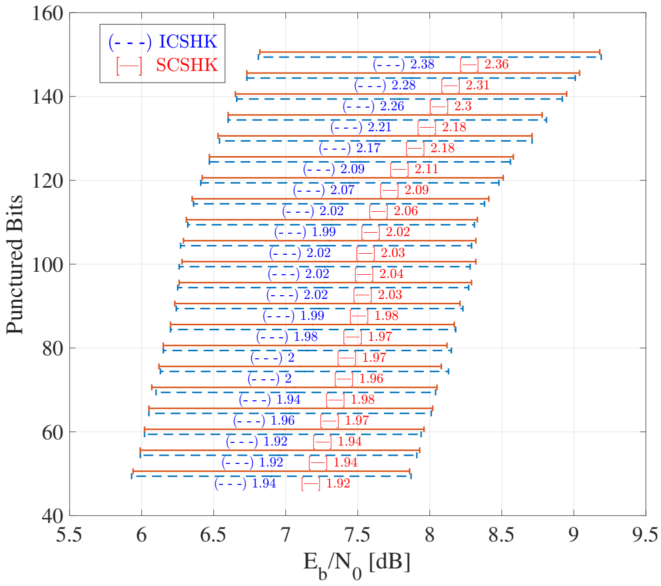


Fig. 5: Security gap behavior in ICSHK and SCSHK schemes with a code dimension (1536,1280) and puncturing first over the key.

Changing evaluation from a medium-long blocklength code (1536,1280) to a short LDPC code (256,128) with $l_k = 64$ bits as presented in Fig. 6, the behavior is maintained and SG pattern continues shifting as N_{punct} increases, although ICSHK presents a slightly better quantitative performance compared to SCSHK scheme. For a short blocklength code, the verified higher SG is due to the larger influence of the key since it has a length closer to the size of the message M, being a significant part of the encoded word. This explains why the SG starts to increase when the number of punctured bits is still smaller than the size of the key l_k, unlike what happened with the medium-sized code. This highlights the need for a proper balance between the size of the key and the size of the message, whereby a larger key relative to the size of the message will lead to a penalty both in terms of security gap as well as code rate.

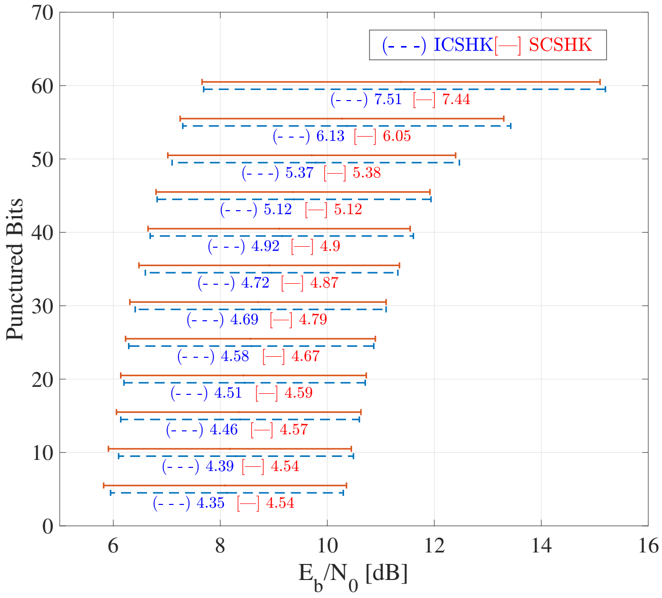


Fig. 6: Security gap behavior in ICSHK and SCSHK schemes with a code dimension (256,128) and puncturing first over the key.

Finally, the results of Fig. 5 and 6 illustrate the ability of our methodology to adjust to different operation points for Bob and Eve, thus providing the required adaptability of coding for secrecy schemes that must be able to operate with devices for which the SNR is expected to vary through time.

IV. Conclusions

In this work, we propose a methodology for adaptive physical-layer security, suitable to different operation points/signal-to-noise ratio levels of the legitimate receiver and the eavesdropper. The proposal is based on interleaving and scrambling as mechanisms that shuffle the original message before transmission, and considers different levels of puncturing over an interleaving/scrambling key and/or over the original message for adaptability. Considering the bit-error ratio (BER) as the reliability criterion and the bit-error ratio cumulative distribution function (BER-CDF) as the secrecy parameter, we establish and analyze the required security gap between the legitimate receiver and an eavesdropper at varying operational/SNR levels. Results show the benefit of puncturing over the interleaving/scrambling key first, to achieve the desired adaptability with little security gap penalty, while puncturing over the message was showed to provide further flexibility but at the cost of a higher SNR. For future work, we consider the evaluation of the system with different internal codes, such as polar codes. The implementation and evaluation in software-defined ratio platforms is also a possibility, taking channel quality as a reference for choosing the number of punctured bits.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] H. Mahdavifar and A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes,” *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[3] W. K. Harrison and S. W. McLaughlin, “Physical-layer security: Combining error control coding and cryptography,” in *Communications, 2009. ICC’09. IEEE International Conference on*. IEEE, 2009, pp. 1–5.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[5] W. K. Harrison, D. Sarmento, J. P. Vilela, and M. Gomes, “Analysis of short blocklength codes for secrecy,” *arXiv preprint arXiv:1509.07092*, 2015.

[6] 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.

[7] J. P. Vilela, M. Gomes, W. K. Harrison, D. Sarmento, and F. Dias, “Interleaved concatenated coding for secrecy in the finite blocklength regime,” *IEEE Signal Processing Letters*, vol. 23, no. 3, pp. 356–360, 2016.

[8] 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.

[9] D. Sarmento, J. Vilela, W. K. Harrison, and M. Gomes, “Interleaved coding for secrecy with a hidden key,” in *Globecom Workshops (GC Wkshps), 2015 IEEE*. IEEE, 2015, pp. 1–6.

[10] 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, 2011.

[11] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, “Adaptive secure transmission for physical layer security in cooperative wireless networks,” *IEEE Communications Letters*, vol. 21, no. 3, pp. 524–527, 2017.

[12] H. Song, H. Wen, L. Hu, Y. Chen, and R.-F. Liao, “Optimal power allocation for secrecy rate maximization in broadcast wiretap channels,” *IEEE Wireless Communications Letters*, 2018.

[13] K. T. Phan, Y. Hong, and E. Viterbo, “Adaptive resource allocation for secure two-hop communication,” in *Wireless Communications and Networking Conference (WCNC), 2018 IEEE*. IEEE, 2018, pp. 1–6.

[14] M. Yusuf and H. Arslan, “On signal space diversity: An adaptive interleaver for enhancing physical layer security in frequency selective fading channels,” *Physical Communication*, vol. 24, pp. 154–160, 2017.

[15] Y. Zhang, A. Liu, C. Gong, G. Yang, and S. Yang, “Polar-LDPC concatenated coding for the AWGN wiretap channel,” *IEEE Communications Letters*, vol. 18, no. 10, pp. 1683–1686, 2014.

[16] C. Martins, T. Fernandes, M. Gomes, and J. Vilela, “Testbed implementation and evaluation of interleaved and scrambled coding for physical-layer security,” in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE, 2018, pp. 1–6.

[17] U. M. Maurer, “The strong secret key rate of discrete random triples,” in *Communications and Cryptography*. Springer, 1994, pp. 271–285.

[18] C. E. Shannon, “Communication theory of secrecy systems,” *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[19] M. Bellare, S. Tessaro, and A. Vardy, “Semantic security for the wiretap channel,” in *Advances in Cryptology–CRYPTO 2012*. Springer, 2012, pp. 294–311.