Polar Coding for Physical-layer Security without Knowledge of the Eavesdropper's Channel

Thyago Monteiro*, Marco Gomes*, João P. Vilela§, Willie K. Harrison‡
*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, UT, USA.
Emails: thyago.pinto@co.it.pt, marco@co.it.pt, jpvilela@dei.uc.pt, willie.harrison@byu.edu

***Abstract*—We propose an adaptive secrecy scheme using polar codes with random frozen bits for a general wiretap channel, in which to protect the data from a potential eavesdropper, part or all of the frozen bits are randomly generated per message. To assess the secrecy level of the proposed scheme, three types of decoding strategies are evaluated: a matching decoder which knows the positions of all inserted bits inside the blocklength and tries to estimate them using the same decoding techniques, a blind decoder which treats all the frozen bits as the same value, and a random decoder which considers those dynamic bits as random at the receiver. Results are presented in terms of the system security gap, assuming an adaptive decoding strategy. It is shown that the system achieves combined secrecy and reliability. The proposed scheme does not assume knowledge of the eavesdropper's channel when defining the indices of information and frozen bits.**

Index Terms- Polar codes, wiretap channel, security gap, physical layer security.

I. Introduction

Polar codes have been adopted by the 3rd Generation Partnership Project (3GPP) as the coding technique for uplink and downlink control information for the enhanced mobile broadband (eMBB) communication service on the 5th generation of wireless systems (5G) [1], and this has created considerable attention to the encoding and decoding methodology. The concept was introduced by Arıkan [2] and proved to achieve the capacity for the binary input memoryless symmetric channel (BIMSC). Since then, polar codes have been considered for several applications, including secrecy scenarios, more specifically the wiretap channel [3]–[8]. In this communication model, a private message from a transmitter (Alice) must be sent to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve), and the main designer goal is to allow the information to be delivered to the proper receiver without leakage to any unauthorized device. Moreover, secrecy scenarios with integrated polar codes usually rely on information theoretical analyses, with evaluation based on criteria like weak secrecy [4] and strong secrecy, while assuming code lengths tending to infinity. However, finite blocklength coding schemes employing polar codes for secrecy are still not fully understood.

The encoding methodology is based on N uses of the channel W, where part of these sub-channels achieve capacity and are selected to transmit data, while the remaining F positions (group $\mathfrak{F}$) are noisy and used to send frozen-bits, i.e., they carry a value known by all participants of the system. There are several methods for selecting $\mathfrak{F}$, and the most common is the Bhattacharyya parameter [2], which is signal-to-noise ratio (SNR) dependent. In this context, the basic approach for works involving polar codes with wiretap channels is inserting random bits on the most reliable sub-channel indices for the eavesdropper's channel to confuse the decoding. Since the Bhattacharyya parameter is based on channel estimation [3] and assuming Eve has a stochastically degraded link (lower SNR compared to Bob), the transmitter can use a bit allocation strategy of sending the message in sub-channels only good for Bob and bad for Eve, insert random bits in indices good for Eve and bad for Bob, and put frozen bits on the remaining positions [3]–[5], [8].

In a practical transmission scenario, Alice should have knowledge of both channels, what could be possible with feedback from Bob, but it is unrealistic for a passive eavesdropper's channel to be learned by the transmitter. Another assumption of this approach is that Eve bases her decoding on her own SNR, while the attacker strategy could be based on an estimation of Bob's conditions. To overcome the need for these assumptions over the eavesdropper's conditions and basing evaluation on a practical transmission setup, we propose and analyze the use of polar codes for secrecy when part (or all) of the frozen bit indices receive random data, i.e., they are dynamic positions, but with a selection of sub-channels not based on SNR but using the partial weight (PW) technique [9] developed by 3GPP. Moreover, the system is analyzed based on three strategies: a matching decoder (MD) with knowledge of all the random bit positions that uses this information to try to estimate the bit values, a blind decoder (BD) assuming all frozen bits have a pre-defined value, and a random decoder (RD) that puts random bits at the dynamic positions but without calculating their content.

The remainder of this paper is organized as follows. In Section II, the background explored in the proposed scheme will be detailed, followed by the main metrics for performance

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.

evaluation, while results and discussions appear in Section III. In Section IV, the major contributions of this paper are summarized.

II. Background

A. Polar Coding and Decoding

The first step on the encoding process using the polar codes technique is to sort the N sub-channels and determine the positions selected to transmit information or frozen bits, with N being the length of the encoded word. For this, some known techniques are the Bhattacharyya parameter [2] and the density evolution Gaussian approximation (DE/GA) [10] or, more recently, the partial weight (PW) sequence [9], explored by 3GPP when polar codes are used in the context of 5G. For not requiring any SNR dependence and for purposes of this work, PW was chosen as the method for selecting frozen bits, with the weights P_i for each sub-channel i ($1 \leq i \leq N$) calculated as

$$P_i = \sum_{j}^{B} b_j \times 2^{(j/4)} \tag{1}$$

where b_j is the bit value in position j of the reversed binary representation of i and B is the number of bits in it. For example, the position 8 becomes 100, reversed 001 and with weight $0 \times 2^{1/4} + 0 \times 2^{2/4} + 1 \times 2^{3/4} = 1.68$. In this way, a table of P_i with length N is achieved, and the M higher values for $i \in \mathfrak{F}^C$ are selected as indices to transmit the data $m = [m_1\ m_2\ \cdots\ m_M]$. The remaining $N-M$ positions ($i \in \mathfrak{F}$) are used to transport frozen bits that take on a value known by all players in the communication system. By this, the data to be encoded is defined as $u = [u_1\ u_2\ \cdots u_N]$, where u_i means the bit in position i. Moreover, the encoded word is given by the product $c = u \times G$ with $G = F^{\otimes n}$, F being the polarization matrix

$$F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{2}$$

and $\otimes$ the n-th Kronecker power.

At the decoder side, bits recovery can be made using successive cancellation (SC) based on the received log-likelihood ratio (LLR) calculated by the formula [11]

$$L_i \triangleq \ln\left(\frac{W_i(y, [\hat{u_1}\ \hat{u_2} \cdots\ \hat{u_{i-1}}]|0)}{W_i(y, [\hat{u_1}\hat{u_2} \cdot\ \cdots\ \hat{u_{i-1}}]|1)}\right), \tag{3}$$

where L_i is the LLR value for the sub-channel i, W_i is the channel probability density function (pdf), y is the received vector and $[\hat{u_1}\ \hat{u_2} \cdots\ \hat{u_{i-1}}]$ is the vector of estimated bits until index $i-1$. Due to its structure, the conventional polar decoding is made in $S = \log_2(N)$ stages, and the internal LLRs from y until the decision layer are calculated as [11]

$$L_{\{2i,\ s\}} = f_1(L_{\{2i-[d_s],\ s-1\}}, L_{\{2^s+2i-[d_s],\ s-1\}}), \tag{4}$$

$$L_{\{2i+1,\ s\}} = f_2(L_{\{2i-[d_s],\ s-1\}}, L_{\{2^s+2i-[d_s],\ s-1\}},\ \hat{u}_{2i,s}), \tag{5}$$

with $L_{\{i,s\}}$ the LLR value at layer s and bit index i and $d_s = i \bmod 2^{s-1}$. The functions f_1 and f_2 are defined as [11]

$$f_1(\alpha, \beta) \triangleq \ln\left(\frac{\exp\alpha + \beta + 1}{\exp\alpha + \exp\beta}\right), \tag{6}$$

$$f_2(\alpha, \beta, \lambda) \triangleq (-1)^{\lambda}\alpha + \beta. \tag{7}$$

In addition, to avoid computational complexity, (6) can be replaced by an approximation [11]

$$f_1(\alpha, \beta) \approx \tilde{f_1}(\alpha, \beta) = \text{sign}(\alpha)\text{sign}(\beta)\min|\alpha||\beta|. \tag{8}$$

From (3), the SC decoder establishes the decision of bit $\hat{u_i}$ depending on all previous decisions $[\hat{u_1}\ \hat{u_2} \cdot \cdots\ \hat{u_{i-1}}]$ of lower indices. In case of an erroneous estimation, the error propagates and can lead to a decoding degradation. To overcome this issue, an alternative is for each index i to consider the two alternatives (zero or one), save each in a new vector $\hat{u}_{\{i,l\}} = [\hat{u_1}\ \hat{u_2} \cdots\ \hat{u_{i-1}}]$, attribute a path metric (PM) for them and prune the list when the size H is reached. This type of decoder is called a successive cancellation list (SCL) decoder [12] and is implemented in [11] based on LLRs, with PM calculated as

$$PM_{\{i,l\}} \triangleq \phi(PM_{\{i-1,l\}},\ L_{\{i,l\}},\ \hat{u}_{\{i,l\}}), \tag{9}$$

where $PM_{\{i,l\}}$, $L_{\{i,l\}}$ and $\hat{u}_{\{i,l\}}$ are the path metric, the LLR value and the estimated message for sub-channel i and list index l, respectively. Also ϕ is defined as

$$\phi(\theta, \zeta, \sigma) = \theta + \ln(1 + \exp(-(1-2\sigma)\zeta)) \tag{10}$$

or by its approximation

$$\tilde{\phi}(\theta, \zeta, \sigma) \triangleq \begin{cases} \theta, & \text{if } \sigma = \frac{1}{2}[1 - \text{sign}(\zeta)] \\ \theta + \zeta, & \text{if otherwise.} \end{cases} \tag{11}$$

At the end of the decoding process, the vector with the higher path metric is selected, and larger values of H result in more precise decoding but at the cost of higher computational demand. In this direction, [13] observed that when the algorithm does not converge into the right transmitted information, the correct message is probably inside the list. To help convergence, an auxiliary cyclic redundancy check (CRC) code is utilized for verification, concatenated with the data, and extracted at the decoder side. By doing this, the vector compatible with the CRC polynomial is selected even if the PM leads to another result. This technique is called CRC-aided SCL (CA-SCL) proved capable of outperform the current low-density parity check (LDPC) codes [14] of the 4th communication generation (4G).

B. Polar Coding for the General Wiretap Channel

The approach for evaluating secrecy in PLS is generally based on the wiretap channel proposed by Aaron Wyner [15] and presented in Fig. 1. In this model, a transmitter (Alice) establishes communication with a legitimate receiver (Bob) over a channel in the presence of an eavesdropper (Eve) trying to intercept the message. The data $m = [m_1\ m_2 \cdots m_M]$ is encoded by Alice into $x = [x_1\ x_2 \cdots x_N]$ and sent through the channel. At the receiver, Bob receives $\hat{z} = [\hat{z_1}\ \hat{z_2} \cdots \hat{z_N}]$ and decodes it into an estimation of m, $\hat{m} = [\hat{m_1}\ \hat{m_2} \cdots \hat{m_M}]$. Meanwhile, Eve is listening and also receives a word $\tilde{z} = [\tilde{z}_1\ \tilde{z}_2 \cdots \tilde{z}_M]$, which is decoded into an estimation of m, $\tilde{m} = [\tilde{m_1}\ \tilde{m_2} \cdots \tilde{m_M}]$. The situation of Eve discovering the private information, i.e., $\tilde{m} = m$ is not desirable, and Wyner proved it is possible to design coding schemes that simultaneously guarantee secrecy and reliability for the communication model [15].

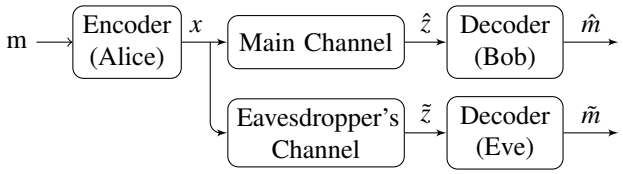

Fig. 1. Wiretap channel.

Furthermore, stochastically BIMSC wiretap models with polar coding are explored in [3], [4] generally reinforced by theoretical analysis in terms of criteria like weak secrecy and strong secrecy. The most applied method when using polar codes in this scenario is designing the selection of frozen bits positions based on channel conditions of Bob and Eve. For this, the N sub-channels used for encoding are categorized into three groups:

- The subset $\wp$ holds the channels only good for Bob and selected to transmit data;
- The subset ξ possesses the indices only good for Eve and used to transmit random bits;
- The remaining $\mathscr{F}$ positions are frozen bits and transport a value known by all parties of the system.

Practical evaluations of this scenario in terms of PLS are still a recent topic and appear in works like [5], although still assuming knowledge or an estimation of the eavesdropper channel when designing the positions of the random bits with the Bhattacharyya method. In this work, a wireless environment is considered and both channels in Fig. 1 are Additive white Gaussian noise (AWGN) channels, instead of BIMSC. The eavesdropper's channel is considered stochastically degraded with respect to Bob's, and Eve is passive, meaning she does not interfere and is not noticed by the system. In terms of computational processing and knowledge of decoding CA-SCL algorithms, list size (H), Eve is assumed to possess the same capabilities as Bob.

C. Security Gap

Metrics for evaluating secrecy in communication systems conventionally rely on information theoretic concepts like weak secrecy [15], strong secrecy [16], perfect secrecy [17], and semantic secrecy [18]. Although these provide strong guarantees, they have limited applicability in practical channels where an analytical calculation of mutual information is impractical and the restriction of an encoded word tending to infinity cannot be satisfied. This is particularly true when short and medium blocklength transmissions are investigated [19]. Therefore, metrics like bit error rate (BER), security gap (SG), block error rate (BLER) and frame error rate (FER) are sometimes preferred for evaluating secrecy and reliability in a PLS scenario.

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

$$SG = \text{SNR}_{min}^{Bob} - \text{SNR}_{max}^{Eve}. \tag{12}$$

In degraded stochastically channels, (12) 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 BER$<\text{BER}_{max}^{Bob}$ and a high value to the eavesdropper (something near 0.5) BER_{min}^{Eve}. Moreover, the SG interval 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, (12) can be rewritten as

$$SG = f_{SNR}(\text{BER}_{max}^{Bob}) - f_{SNR}(\text{BER}_{min}^{Eve}), \tag{13}$$

with $f_{SNR}(BER_{max}^{Bob})$ meaning the SNR value that achieves BER_{max}^{Bob}, and $f_{SNR}(BER_{min}^{Eve})$ the SNR value that achieves BER_{min}^{Eve}.

III. Polar Codes for Physical Layer Security

A. Polar Codes with Random Frozen Bits and Decoding Strategies

Considering the conventional encoding methodology and the setup in Fig. 1, the approach on this work for providing secrecy and reliability using polar codes is based on inserting random bits to be transmitted with the information but without any SNR dependence in the choice of message and frozen bit positions. After evaluating the sub-channels based on PW as in (1) and allocating the data on indices with higher P_i, a vector $k = [k_1\ k_2 \cdots k_K]$ with random bits and length K is generated per message and placed on the worst K channels. This way, the transmitter not only sends useful information but also an amount of data designed to confuse the eavesdropper. The encoder produces the concatenated vector $[m\ k]$, which is sent and decoded by both receivers in Fig. 1 after passing through the respective AWGN channels.

In order to evaluate the effectiveness of the proposed scheme, we consider and evaluate three distinct decoding strategies, with rationale as follows.

- A matching decoder (MD), which presupposes knowledge over ξ positions inside the encoded word c and the application of the same CA-SCL decoder to estimate the data in these positions, but discarding it when evaluating the CRC polynomial.
- A blind decoder (BD), which has no information about ξ and assumes all the frozen bits as a pre-defined value, without loss of generality, in this work they are considered to be 0.
- A random decoder (RD), which knows ξ but assumes random values with an equal probability of being zero or one, instead of calculating or setting them to zero.

B. Results

For evaluating the scenario in Fig. 1, we consider a transmission of a relativaly small (512, 256) polar code and a randomly generated k per message with lengths $K = [10, 20, 30, 40, 50]$. The selection of information and frozen bit sub-channels is made using the PW method, and the encoded word is modulated using the binary phase shift keying (BPSK) scheme, with the resulting constellation symbols transmitted over an AWGN channel. At the legitimate receiver, the demodulated signal is sent to an internal decoder responsible to estimate m using the CA-SCL algorithm with list size $H = 32$, CRC polynomial $g(x) = b^{11} + b^{10} + b^9 + b^5 + b^4 + b^3 + 1$ and the approximated function in (8). All the techniques, RD, BD, and MD are evaluated as decoding methods to extract the information sent.

For this code size, the behavior for several K lengths is shown in Fig. 2, where a changing performance is observable when increasing K since E_b/N_o for reliability and secrecy are shifted from the reference curve, which represents a polar encoding without k. As K increases, the BD and RD present similar behaviors, leading to the conclusion that assuming the k bits as zero or as random bits are equivalent strategies. On the other hand, the MD shows less sensitivity in terms of reliability, especially for a large K, although requiring information about ξ.

Assuming a secrecy parameter in terms of $\text{BER}_{Eve}^{min} > 0.2$ and reliability when $\text{BER}_{Bob}^{max} < 0.001$, graphics in Fig. 2 can be read in terms of SG as in (13) and depicted in Table I. These data are graphically exposed in Fig. 3 and an increasing SG as a function of K is observed for all explored decoding methodologies. In terms of secrecy against an eavesdropper, all the techniques lead to a small variation when considering the same K, although, for different sizes of this parameter, a significant interval is achieved. The MD has a slightly better performance in terms of reliability, bringing an inferior SG as presented in Fig. 3. At the extreme situation of changing all frozen bits for a random vector of size $K = 256$ as shown in Fig. 2, a huge shift at the secrecy point is achieved when using an MD. In this work we only considered small/medium sizes of K when compared to the length of the encoded word N.

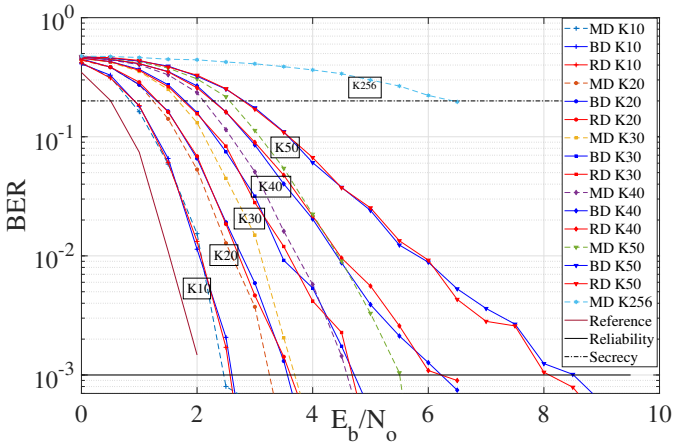

Fig. 2. Polar decoding strategies evaluation for short blocklength codes (512, 256) with K random frozen bits in a wiretap channel.

TABLE I
SECRECY AND RELIABILITY EVALUATION FOR A SHORT BLOCKLENGTH POLAR CODING (512,256) WITH RANDOM FROZEN BITS TRANSMISSION.

	E_b/N_o (dB) at BER=10^{-3}			E_b/N_o (dB) at BER=0.02		
K	MD	RD	BD	MD	RD	BD
10	2.462	2.517	2.605	0.84	0.915	0.915
20	3.25	3.56	3.6	1.24	1.312	1.304
30	3.69	4.684	4.73	1.67	1.76	1.79
40	4.59	6.223	6.224	2.11	2.27	2.29
50	5.5	8.1	8.5	2.55	2.8	2.82

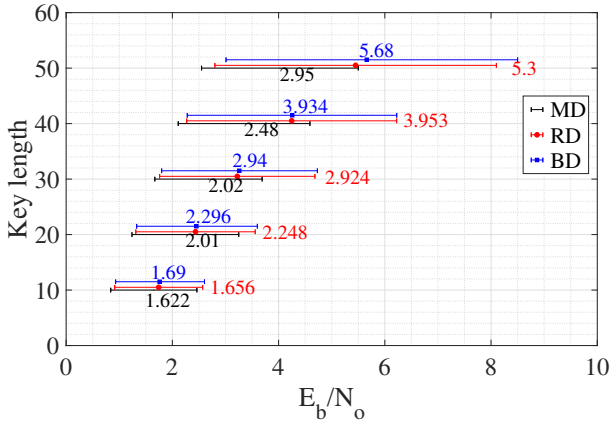

Fig. 3. Security gap behavior of short blocklength polar coding (512, 256) with K random frozen bits for a secrecy scheme. The left-most point on each line corresponds to the security threshold for Eve, while the right-most point to the reliability threshold for Bob, with the difference between the two being the security gap.

The same analysis for a medium blocklength (1024, 512) code is depicted in Fig. 4. In this scenario, the three types of decoders give almost the same behavior for small K. However, differently from the short-sized blocklength code, RD and BD have a slighter better performance than the MD for small values of K. Moreover, inserting k almost does not change the secrecy threshold among all approaches for the same value of

K, but does affect the reliability criterion. The three techniques RD and BD show similar results, and for all the cases the MD leads to inferior values of the reliability threshold when compared with the remaining methods. These results motivate an adaptive PLS as a function of K for short and medium-sized blocklength codes, whereby the transmitter is able to adjust secrecy in the system by sensing channel conditions with its legitimate receiver and changing the size of K so as to minimize leakage under the constrainy of reliable throughput to Bob.

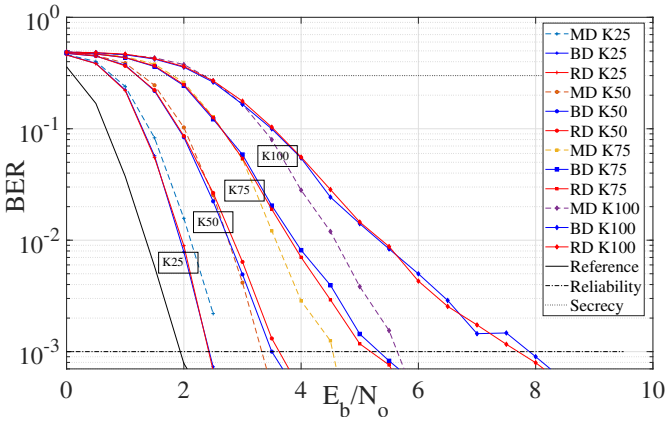

Fig. 4. Polar decoding strategies evaluation for medium-sized blocklength codes (1024, 512) with K random frozen bits in a wiretap channel.

TABLE II
SECRECY AND RELIABILITY EVALUATION FOR A MEDIUM-SIZED BLOCKLENGTH (1024, 512) POLAR CODING WITH RANDOM FROZEN BITS.

	E_b/N_o (dB) at BER=10^{-3}			E_b/N_o (dB) at BER=0.03		
K	MD	RD	BD	MD	RD	BD
25	2.7*	2.424	2.434	0.7825	0.722	0.731
50	3.33	3.63	3.5	1.28	1.2	1.2
75	4.54	5.19	5.327	1.813	1.76	1.73
100	5.64	7.7	7.9	2.341	2.318	2.28

IV. CONCLUSIONS

In this work, we evaluate the use of polar coding with partial random frozen bits in a wiretap channel, and by this, an adaptive physical layer security transmission scheme is proposed for increasing secrecy and reliability requirements. Three decoding strategies are presented, a blind decoder, a random decoder, and a matching decoder with different levels of knowledge over the random bit positions. Results show that from the methodologies employed to extract the data, estimating the random frozen bits leads to smalller SG values when compared with a blind and a random decoder.

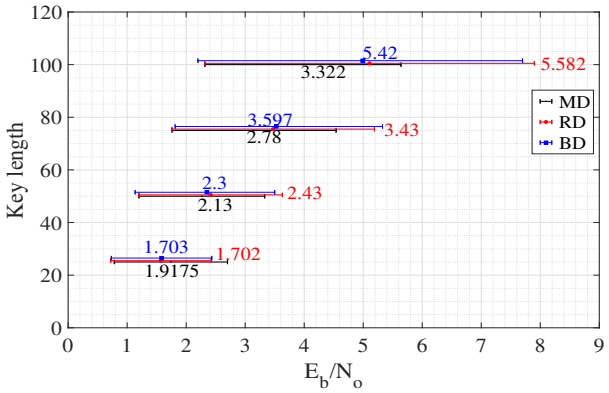

Fig. 5. Security gap behavior of medium-sized blocklength polar coding (1024, 512) with random frozen bits for a secrecy scheme. The left-most point on each line corresponds to the security threshold for Eve, while the right-most point to the reliability threshold for Bob, with the difference between the two being the security gap.

REFERENCES

[1] V. Bioglio, C. Condo, and I. Land, "Design of polar codes in 5g new radio," *arXiv preprint arXiv:1804.04389*, 2018.

[2] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[3] Y.-P. Wei and S. Ulukus, "Polar coding for the general wiretap channel," in *Information Theory Workshop (ITW), 2015 IEEE*. IEEE, 2015, pp. 1–5.

[4] 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.

[5] H. Bai, L. Jin, and M. Yi, "Artificial noise aided polar codes for physical layer security," *China Communications*, vol. 14, no. 12, pp. 15–24, 2017.

[6] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Information Theory Workshop (ITW), 2010 IEEE*. IEEE, 2010, pp. 1–5.

[7] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communications Letters*, vol. 14, no. 8, pp. 752–754, 2010.

[8] A. Rajagopalan, A. Thangaraj, and S. Agrawal, "Wiretap polar codes in encryption schemes based on learning with errors problem," in *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2018, pp. 1146–1150.

[9] R1-167209, "Polar code design and rate matching," *Huawei, 3GPP TSG RAN WG1 Meeting 86*.

[10] R. Mori and T. Tanaka, "Performance of polar codes with the construction using density evolution," *IEEE Communications Letters*, vol. 13, no. 7, 2009.

[11] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, "Llr-based successive cancellation list decoding of polar codes," *IEEE transactions on signal processing*, vol. 63, no. 19, pp. 5165–5179, 2015.

[12] I. Tal and A. Vardy, "List decoding of polar codes." in *ISIT*, 2011, pp. 1–5.

[13] K. Niu and K. Chen, "Crc-aided decoding of polar codes," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1668–1671, 2012.

[14] K. Niu, K. Chen, J. Lin, and Q. Zhang, "Polar codes: Primary concepts and practical decoding algorithms," *IEEE Communications magazine*, vol. 52, no. 7, pp. 192–203, 2014.

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

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

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

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

[19] W. K. Harrison, D. Sarmento, J. P. Vilela, and M. A. Gomes, "Analysis of short blocklength codes for secrecy," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 255, 2018.