

Keyed Polar Coding for Physical-Layer Security without Channel State Information

Thyago M. S. Pinto*, João P. Vilela[†], Marco A. C. Gomes*, Willie K. Harrison[‡]

*Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, Portugal.

[†]CRACS/INESCTEC, CISUC and Department of Computer Science, Faculty of Sciences, University of Porto, Portugal.

[‡]Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT, 84602.

Emails: thypi@fotonik.dtu.dk, jvilela@fc.up.pt, marco@co.it.pt, willie.harrison@byu.edu

Abstract—Polar codes have been shown to provide an effective mechanism for achieving physical-layer security over various wiretap channels. A majority of these schemes require channel state information (CSI) at the encoder for both intended receivers and eavesdroppers. In this paper, we consider a polar coding scheme for secrecy over a Gaussian wiretap channel when no CSI is available. We show that the availability of a shared keystream between friendly parties allows polar codes to be used for both secure and reliable communications, even when the eavesdropper knows a large fraction of the keystream. The scheme relies on a predetermined strategy for partitioning the bits to be encoded into a set of frozen bits and a set of information bits. The frozen bits are filled with bits from the keystream, and we evaluate the security gap when the cyclic redundancy check-aided successive cancellation list decoder is used at both receivers in the wiretap channel model.

I. INTRODUCTION

Physical-layer security has emerged as a viable technique for providing joint error-control and secrecy in modern communication networks [1], [2]. The security obtained from efforts at the physical layer need not be standalone, as physical-layer security has been shown to effectively complement security efforts from other layers, such as cryptography at the application layer of the network [3]. Physical-layer security uses the inherent characteristics of the environment to protect the information of a transmitted message from being leaked to eavesdropping devices, making the technology particularly applicable for wireless transmissions due to their broadcast nature and ease of interception by eavesdroppers. The general model utilized for the design of physical-layer security schemes is the wiretap channel model [4], in which a transmitter (Alice) aims to send a message to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve) who is trying to intercept and decode the private data. A variety of coding techniques exist for secure and reliable communications over several wiretap model variants [5], and polar codes [6] have provided a number of approaches to coding over the wiretap channel [7], [8].

This work was funded by the European Regional Development Fund (FEDER), through the Regional Operational Programme of Centre (CENTRO 2020) of the Portugal 2020 framework and FCT under the MIT Portugal Program [Project SNOB-5G with Nr. 045929 (CENTRO-01-0247-FEDER-045929)], and by FCT/MCTES through national funds and when applicable co-funded EU funds under the projects UIDB/EEA/50008/2020, and PES3N (SAICT-45-2017-POCI-01-0145-FEDER-030629).

In their original form [6], polar codes were designed to achieve the capacity of binary input memoryless symmetric channels. The encoder is comprised of a rate-one mapping taking n bits at the input and producing n coded bits at the output; however, only a fraction of the input bits are carrying information, while the remainder are *frozen*. Frozen bits are traditionally set to zero (although they may be set to any known values), and knowledge of those bits at the receiver allows one to decode using a successive cancellation approach also laid out in the original polar coding work [6]. The selection of frozen bits and information bits must be made as a function of the channel state information (CSI) between the transmitter and receiver, and the successive cancellation decoder was designed to remove errors from the system as long as the code matches the channel. The known value of the frozen bits effectively allows the receiver to remove all uncertainty at the decoder, thus guaranteeing reliable communications [6].

When these codes were first adapted to the wiretap channel [7], it became necessary to sort the input bits of the encoder into three bins: (1) random bits for bit-channels that are reliable for both Bob and Eve, (2) information bits for bit-channels that are reliable only for Bob, and (3) frozen bits for bit-channels that are reliable for neither Bob nor Eve. It was assumed that Eve's channel was worse than Bob's channel in this first work, which was shown to be sufficient to guarantee that no bit-channels exist that are reliable for Eve but not for Bob [7]. Successive cancellation easily guarantees reliable communication between Alice and Bob using this approach, and the random bits introduce sufficient uncertainty to guarantee information theoretic security against Eve. The downside is that this technique requires explicit knowledge of the CSI of both the Alice-to-Bob channel and the Alice-to-Eve channel, which may not be attainable in practice.

The literature on polar coding over wiretap channels now includes many additional approaches to physical-layer security. The original three-way binning technique was used to achieve the secrecy capacity under the weak secrecy criterion for degraded wiretap channels in [7], [9]. A clever concealment of small secret keys in each coded block using a chaining technique was shown to allow one to overcome the requirement for Bob to maintain a channel advantage over Eve and also extended the security condition to strong information theoretic

secrecy [10]–[12].

The main problem remains the lack of ability to design a polar code for secrecy without explicit CSI of all links in the wiretap channel model, despite recent results that appear to be moving in that direction [13]. Furthermore, most results for polar coding over wiretap channels are restricted to discrete memoryless channels, leaving explicit coding over the Gaussian wiretap channel as an open problem despite some theoretical results indicating the existence of such codes [14], [15].

In this work, we show that a predetermined strategy for partitioning a polar code based on an efficient rate-matching scheme [16] can be effective in achieving a prescribed level of physical-layer security over the Gaussian wiretap channel, as shown via a security gap analysis [17]. This technique does not require CSI from any of the channels in the network, but rather takes the traditional error-control coding route of choosing a coding rate and analyzing the performance of the resulting codes as a function of signal-to-noise ratio [18]. Our scheme requires a keystream known only to Alice and Bob, although we analyze the effectiveness of the scheme even when Eve knows large fractions of the key bits. Results indicate that even a small fraction of unknown key bits is sufficient to drastically affect the output of the cyclic redundancy check-aided successive cancellation list (CA-SCL) decoder, which represents the current state of the art in polar decoding.

The remainder of this paper is organized as follows. In Section II, we present the channel model for the paper, basic encoding and decoding for polar codes, the bit-channel sorting technique used in the paper, and some notes on the literature surrounding secret key agreement. Our scheme for polar coding with a shared key is then presented in Section III, with numerical results showcasing the effectiveness of the scheme being given in Section IV. We then conclude the paper in Section V.

II. BACKGROUND

A. Gaussian Wiretap Channel with a Shared Key

The communication model considered in this work is presented in Fig. 1. In this system, Alice intends to transmit a private message U to Bob in the presence of the eavesdropper Eve. Both channels depicted are Gaussian channels, i.e., $f(y^n|x^n)$ and $f(z^n|x^n)$ are n -dimensional Gaussian distributions with mean vectors equal to the modulated symbols that correspond to the bits in x^n and variance $N_0/2$. The signal-to-noise ratio at both receivers is measured according to the energy per information bit E_b/N_0 . Alice and Bob have a shared key K , that is used to encode and decode. Bob and Eves' estimates of U are \hat{U} and \tilde{U} , respectively, and both Bob and Eve are assumed to use the best available decoder. The system should be designed to reliably deliver the message to Bob so that $P(U \neq \hat{U})$ is small, and at the same time avoid any significant leakage of U to Eve.

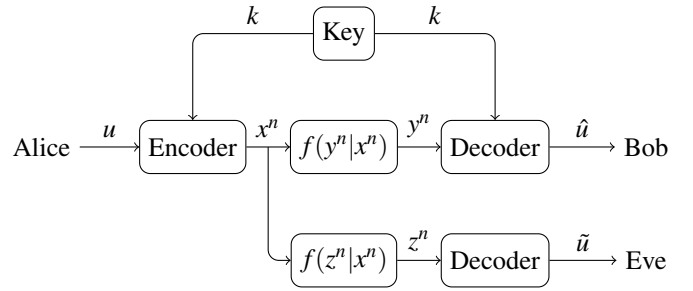


Fig. 1: Secrecy coding with a shared key over the Gaussian wiretap channel.

B. Ranking the Bit-Channels for Polar Codes

Let $G = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, and let $G^{\otimes m}$ be the m th Kronecker power of G . Also, let P_n be the $n \times n$ bit-reversal permutation matrix (see, e.g., [7]), where $n = 2^m$ is the blocklength of the code. Then n input bits to the polar encoder v^n are encoded as

$$x^n = v^n P_n G^{\otimes m}, \quad (1)$$

calculated in the binary finite field \mathbb{F}_2 .

In a general polar code, the bits of the vector v^n are comprised of information (message) bits and frozen bits (usually set to zero). In essence, the rows corresponding to the indices of the information bits in v^n of $P_n G^{\otimes m}$ form a generator matrix for a linear block code. Such a code can be decoded using successive cancellation techniques, and the code achieves capacity over certain channels as long as the bits of v^n are properly assigned, according to the channel properties, into the sets of information bits and frozen bits [6]. The *bit-channels* are effectively measured from the input to the encoder to the output of the decoder, and the reliability of these channels polarizes when successive cancellation is used so that each channel is essentially perfect, or perfectly random. The noise is effectively “collected” in the perfectly random bit-channels, and it can be removed if the bits transmitted over those channels are known at the decoder. These bits make up the frozen bit set.

Usually the allocation of bit-channels to be used for the transmission of either information bits or frozen bits is a function of the CSI between Alice and Bob. Bit-channels are then sorted into *good* channels and *bad* channels, where information bits are sent over the good channels and frozen bits are sent over the bad channels [6]. When an eavesdropper is added to the network, the bins are more complicated. If Bob’s overall channel is better than Eve’s, then bit-channels that are good for both Bob and Eve can be assigned random bits, bit-channels that are good for Bob and bad for Eve can be assigned information bits, and bit-channels that are bad for both Bob and Eve can be assigned frozen bits. The assignment of bit-channels in this case is a function of the CSI in the Alice-to-Bob channel and the Alice-to-Eve channel [7], [19], [20]. In this work, however, we are assuming no CSI is

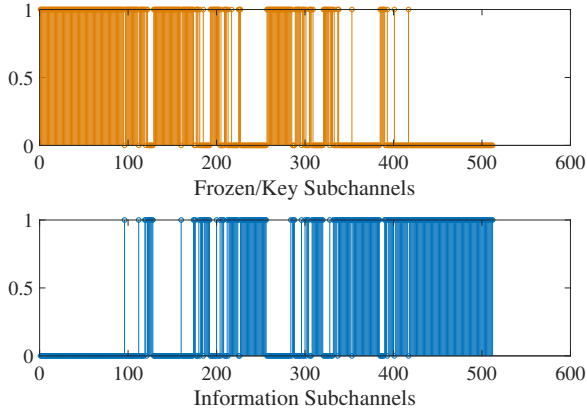


Fig. 2: Bin assignments according to the partial weights for the $n = 512$, $R = 1/2$ polar code.

available at the transmitter, meaning we need a new approach to make the assignments of bit-channels.

To avoid assumptions over the receivers' CSI, an alternative is to use the bit-channel-ranking technique found in [16]. We do not assume that Bob's channel is superior to Eve's channel in this work, and we only sort the bit-channels into two bins.

Let the integers from zero to $n - 1$ be expanded into their binary form. For example, let the integer $i = b_{m-1}b_{m-2} \dots b_0$, where the left-most bit b_{m-1} is the most significant bit. Then let p_i be the *partial weight* for the i th bit-channel ($0 \leq i \leq n - 1$) be calculated as

$$p_i = \sum_{j=0}^{m-1} b_j \times 2^{(j/4)}. \quad (2)$$

Recall here that $m = \log_2 n$. Let the bin of indices associated with the information-bit-carrying bit-channels be called Υ , and the frozen-bit-carrying bit-channels be called κ . Let R be the design rate of the code. We then sort the partial weights from highest to lowest, and assign the indices with the highest $R \times n$ partial weights to Υ , and the remainder to κ . We can assume that $R \times n$ is an integer, since R and n are design parameters of the code, and can be chosen with this constraint in mind. In Fig. 2, we plot the bin assignments for the polar code with $n = 512$ and $R = 1/2$ as an example.

C. Cyclic Redundancy Check-Aided Successive Cancellation List Decoding

The cyclic redundancy check-aided successive cancellation list (CA-SCL) decoder [21]–[23] is used in this work. The decoder requires log-likelihood ratios (LLR) under successive cancellation decoding and a list of depth specified by the user. The LLR for the bit transmitted over the i th bit-channel is calculated as

$$L_i \triangleq \ln \left(\frac{W_i(y^n, [\hat{v}_0 \ \hat{v}_1 \ \dots \ \hat{v}_{i-1}] | v_i = 0)}{W_i(y^n, [\hat{v}_0 \ \hat{u}_1 \ \dots \ \hat{v}_{i-1}] | v_i = 1)} \right), \quad (3)$$

where W_i is the probability density function (pdf) that governs the i th bit-channel and $[\hat{v}_0 \ \hat{v}_1 \ \dots \ \hat{v}_{i-1}]$ is the vector

of estimated bits in the decoder through index $i - 1$. This decoder was chosen for its superior performance over other potential options [24], and represents the state-of-the-art in polar decoding. The decoder rule works as follows:

$$\hat{v}_i = \begin{cases} 0, & \text{if } L_i \geq 0 \text{ and } i \in \Upsilon, \\ 1, & \text{if } L_i < 0 \text{ and } i \in \Upsilon, \\ \lambda, & \text{if } i \in \kappa, \end{cases} \quad (4)$$

where λ is equal to the value of the frozen bit.

D. Key Agreement Techniques

The use of a shared key is a well-investigated topic in secrecy communication schemes, especially for cryptography and information reconciliation. In terms of physical-layer security, a key-agreement system based on simultaneous channel probing by Alice and Bob is explored in [25]. Schemes using polar codes with key-agreement are proposed in [10], [26], [27] where the basic idea is to send a seed with the message to be used only for the next transmitted codeword and [10], [27] proved theoretically that a scheme with a combined key can achieve the secret-key capacity under the strong secrecy criterion, although relying upon a selection of frozen bits based on previous knowledge of the eavesdropper's channel. In [28], a key establishment based on physical unclonable functions is evaluated, translating the unique randomness of specific devices into a shared key. Furthermore, in [29], secret-key generation is performed by expansion-combination-interleaving of an initial seed combined with advanced encryption standard (AES) to protect private data.

For this particular work, it is assumed that the mechanism for distributing the key is used in combination with cryptography. The shared key can then be used to enhance physical-layer security. In this way, a level of integration is required between layers of the protocol stack, and physical-layer security combines with security efforts throughout the communication system. The seed (and consequently the dynamic frozen bits) are assumed to work without transmission limitations like reliability, misinformation or synchronization, for example. The key is assumed to be shared using protocols (e.g., Diffie-Hellman key exchange) at upper-layers of the protocol stack, and the main analysis here is focused on the secrecy and reliability of the message with the assumption that the secret key is in place.

III. POLAR CODES FOR SECRECY WITH SHARED KEY

The idea for our scheme is straightforward. We use the shared keystream to supply the bits for the frozen bit-channels in κ , and transmit each block with new key bits. Information bits are assigned to the bit-channels in Υ . The sets κ and Υ decide the locations of frozen bits and information bits in each block, and these sets are fixed according to the partial weights and the design rate of the code. We can then apply the CA-SCL decoder and characterize the performance for a set of receivers as a function of E_b/N_0 .

We first consider the intended receiver, for whom the keystream is also known. For this user, knowledge of the

frozen bits allows the decoder to operate as if the bits were set to zero in a general polar code [6], and performance is expected to be very good. We then consider eavesdroppers with knowledge of certain fractions of the keystream. In essence, we want to know how performance degrades as the keystream is revealed to an attacker. If we find that a small amount of unknown keystream is sufficient to degrade the performance to our liking, then this really implies that we can actually freeze many bits (say, set them to zero), and use the keystream for a smaller portion of bits at a negligible performance cost.

Successive cancellation decoders tend to rely on the correctness of previously decoded bits, and are capable of propagating errors even in the case of the CA-SLC decoder [22]. Thus, we may expect a significant degradation of performance without knowledge of the frozen bits in κ . At the very least, this may force eavesdroppers to consider other types of attacks. Luckily, a similar scheme was set forth in [30], wherein the authors took a cryptographic approach to security and considered a number of well-known attacks. Their system was shown to perform admirably in the face of these attacks, meaning we can still have confidence that the keystream can be kept secure (in terms of computational security), even if it is generated by a smaller seed as in [30].

The decision rule for Bob in the scheme of Fig. 1 is defined as

$$\hat{v}_i = \begin{cases} 0, & \text{if } L_i \geq 0 \text{ and } i \in \Upsilon, \\ 1, & \text{if } L_i < 0 \text{ and } i \in \Upsilon, \\ k_i, & \text{if } i \in \kappa, \end{cases} \quad (5)$$

where k_i is the bit value from the keystream assigned to v_i in the encoder. Since Eve is assumed to have no access to the keystream, she can try to use the same decoding rule as Bob's, but this would require her to estimate k_i for all bits in κ . Since this is likely to result in many bad estimates, she can simply apply the decision rule

$$\tilde{v}_i = \begin{cases} 0, & \text{if } L_i \geq 0 \\ 1, & \text{if } L_i < 0, \end{cases} \quad (6)$$

which requires the device to calculate the LLR for all bit-channels. Without knowledge of the key, this decision rule is the maximum-likelihood decoder.

In addition, the eavesdropper is presumed to have knowledge over the encoding and decoding techniques, including explicit knowledge of the sets Υ and κ . She has no computational restrictions when processing the data, and for the case with partial knowledge of the keystream, she is able to use Bob's decoder rule when she knows k_i . Again, partial knowledge of the keystream allows us to test how much key is really needed to degrade Eve's performance to our liking, as a function of her signal-to-noise ratio.

IV. SYSTEM EVALUATION

For evaluating the scenario in Fig. 1, we consider our scheme using two polar codes with medium sized parameters. The codes have size parameters (512, 256) and (1024, 512),

where the first parameter is the blocklength n , and the ratio of the second parameter to the first is the coding rate R . Codewords are modulated using binary phase shift keying (BPSK), and simulations are conducted assuming additive white Gaussian noise. At the legitimate receiver, the demodulated signal is sent to an internal decoder responsible for estimating the message U using the CA-SCL algorithm with list size $L = 32$ and CRC polynomial defined as $g(x) = x^{11} + x^{10} + x^9 + x^5 + x^4 + x^3 + 1$. At the eavesdropper's receiver, the decoding capabilities are considered equal with the legitimate receiver, except for the knowledge of K .

As discussed in [31], the best decoder strategy in a case where random bits are being transmitted with the message is to try to estimate the random bit values using the same decoding procedure as applied to the information bits, and this is the methodology chosen for evaluating the secrecy level of this system. Let Δ be the percentage of frozen bit values unknown to the receiver. Then $\Delta = 0\%$ gives the baseline polar code performance when frozen bits take on the value of zero. This case also matches the performance of Bob in our scheme, since the keystream is fully known at both Alice and Bob. Eavesdroppers of varying degrees are given for specific Δ values greater than 0% up to a full 100%, and several such operating points are evaluated in the following.

Finally, for this paper, we assume that a system designer would like Bob's bit-error rate (BER) no higher than $\text{BER}_{\max}^{\text{Bob}} = 10^{-3}$, and Eve's BER no lower than $\text{BER}_{\min}^{\text{Eve}} = 0.2$. These choices are somewhat arbitrary, and can be changed by any user. The security gap (SG) is then calculated as

$$\text{SG} = f_{\frac{E_b}{N_0}}(\text{BER}_{\max}^{\text{Bob}}) - f_{\frac{E_b}{N_0}}(\text{BER}_{\min}^{\text{Eve}}), \quad (7)$$

where $f_{\frac{E_b}{N_0}}(B)$ is the value of E_b/N_0 at which the system achieves an average BER of B .

Figs. 3 and 4 show BER curves for Bob and various Eves ($0\% < \Delta \leq 100\%$) for the two codes. Note that the Eve operating points tested tend to give very similar BER curves, although extra knowledge of the keystream tends to help Eve's efforts at high SNR. Bob's performance matches the expected performance of the polar code, which is quite good.

When Eve is operating at around $\Delta = 40\%$, the security gap is roughly -3 dB for the smaller code and -4 dB for the larger code. At $\Delta = 100\%$ (meaning, Eve has no knowledge of the keystream) the smaller code gives a security gap of roughly -4.5 dB, while the larger code gives a security gap around -5 dB.

If a stricter security requirement on Eve is desired, say $\text{BER}_{\min}^{\text{Eve}} = 0.4$, then the security gaps measured over Eve with $\Delta = 40\%$ are roughly -1 dB for the smaller code and -2 dB for the larger code. For $\Delta = 100\%$, security gaps are closer to -1 dB for the smaller code and -3.5 dB for the larger code. Either way, we see that the key-based scheme is capable of returning negative security gaps for a variety of scenarios, and we also see that depending on the desired level of security, one may be able to use less key bits (replacing them with frozen

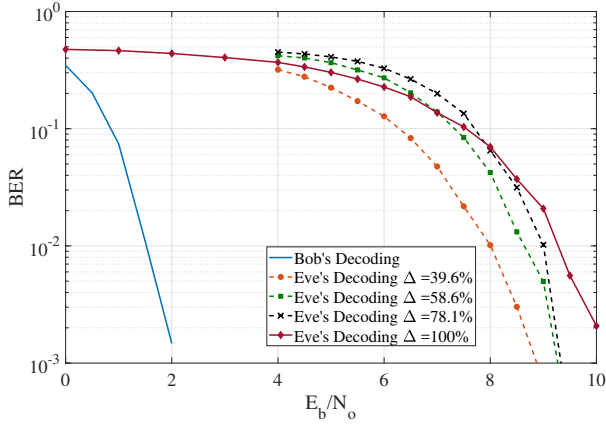


Fig. 3: Evaluation of (512, 256) polar code for a wiretap channel with shared key (Alice-Bob) and unknown frozen bits at the eavesdropper with Δ percentages.

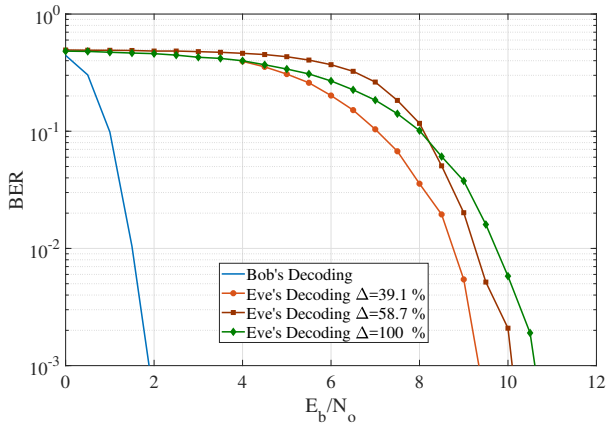


Fig. 4: Evaluation of (1024, 512) polar code for a wiretap channel with shared key (Alice-Bob) and unknown frozen bits at the eavesdropper with Δ percentages.

values of zero) while still maintaining reliable and secure communication.

V. CONCLUSIONS

In this work, we proposed and evaluated the use of polar coding with a secret keystream in achieving tunable physical-layer security without the need for receiver CSI. The technique allows a system designer to specify the code rate, and then assigns bit-channels as information-carrying or frozen according to predetermined rankings using partial weights. Frozen bit channels are then filled with bits from the secret keystream. A security gap analysis shows that it is possible to achieve both security and reliability, even when an eavesdropper is more capable than the legitimate receiver (as indicated by the scheme achieving negative security gaps). The scheme can still achieve security gaps less than zero, even when the attacker knows a significant percentage of the keystream, indicating

that smaller amounts of key may be used if needed, where the remainder of the frozen bits may be set to an arbitrary value.

REFERENCES

- [1] 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.
- [2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.
- [3] W. K. Harrison and S. W. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *Proc. IEEE Int. Conf. Communications (ICC)*, Dresden, Germany, June 2009, pp. 1–5.
- [4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [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 Processing Magazine*, vol. 30, no. 5, pp. 41–50, Sept. 2013.
- [6] 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.
- [7] H. Mahdaviifar 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.
- [8] M. R. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.
- [9] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, 2012.
- [10] T. C. Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," *IEEE Transactions on Information Theory*, vol. 63, no. 2, pp. 1311–1324, 2016.
- [11] H. Wang, X. Tao, N. Li, and Z. Han, "Polar coding for the wiretap channel with shared key," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1351–1360, 2017.
- [12] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2410–2429, 2016.
- [13] R. A. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 2018, pp. 476–480.
- [14] E. Abbe and A. Barron, "Polar coding schemes for the AWGN channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 2011, pp. 194–198.
- [15] 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, Oct. 2014.
- [16] 3GPP, "Polar code design and rate matching," Gothenburg, Sweden: Huawei, HiSilicon, Report R1-167209, 2016.
- [17] 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.
- [18] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2005.
- [19] Y.-P. Wei and S. Ulukus, "Polar coding for the general wiretap channel," in *Proc. IEEE Information Theory Workshop (ITW)*, 2015, pp. 1–5.
- [20] A. Rajagopalan, A. Thangaraj, and S. Agrawal, "Wiretap polar codes in encryption schemes based on learning with errors problem," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 2018, pp. 1146–1150.
- [21] K. Niu and K. Chen, "CRC-aided decoding of polar codes," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1668–1671, 2012.
- [22] I. Tal and A. Vardy, "List decoding of polar codes," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 2011, pp. 1–5.
- [23] 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.
- [24] 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.

- [25] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.
- [26] E. Şaşıoğlu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 2013, pp. 1117–1121.
- [27] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.
- [28] B. Chen, T. Ignatenko, F. M. Willems, R. Maes, E. van der Sluis, and G. Selimis, "A robust SRAM-PUF key generation scheme based on polar codes," in *Proc. IEEE Global Communications Conf. (GLOBECOM)*, 2017, pp. 1–6.
- [29] H. Jin, R. Liu, and C. Zhang, "Low transmission overhead for polar coding physical-layer encryption," *IEEE China Communications*, vol. 16, no. 2, pp. 246–256, 2019.
- [30] R. Hooshmand, M. R. Aref, and T. Eghlidos, "Secret key cryptosystem based on non-systematic polar codes," *Wireless Personal Communications*, vol. 84, pp. 1345–1373, May 2015.
- [31] T. Pinto, M. Gomes, J. Vilela, and W. K. Harrison, "Polar coding for physical-layer security without knowledge of the eavesdropper's channel," in *Proc. IEEE 89th Vehicular Technology Conference (VTC Spring)*, 2019, pp. 1–5.