Achieving Secure Communication over Wiretap Channels Using the Error Exponent of the Polar Code

Mohammad Reza Deylam Salehi, Hassan Tavakoli

***Abstract*—In this paper, the error exponent of a polar code generator matrix for data rate enhancement between two users is investigated. A new expression for optimal correlation coefficient between the error probability of the main and eavesdropper channel in Wyner's wiretap channel model introduced. By using this optimal correlation coefficient, a relationship between code length and the error exponent is defined. Moreover, to investigate the performance of the proposed formulation, an optimization based on Arikan and Korda's theory on the maximum value of the error exponent was conducted. It is shown that the new correlation coefficients significantly increase the decoding error probability in the wiretapper side for both of the theories. In addition, the Bhattacharyya parameter was also defined for the wiretap channel. Finally, by applying the optimized values to a binary erasure channel, the error probability for each scenario is calculated.**

***Index Terms*—Polar code, Wiretap channel, Error exponent, Generator matrix, Error probability, Bhattacharyya parameter.**

I. Introduction

Polar coding, i.e., a channel coding method, can achieve the capacity of binary symmetric channels (BSCs), i.e., binary erasure channels (BECs). Arikan introduced polar coding in 2009 [1]. Due to the complexity of both encoding and decoding with the order $O(N.\log N)$, this paper aims to enhance the secrecy capacity of the wiretap channel using the polar coding technique. In particular, the coefficient between the error probability of the main and wiretapper's channels is introduced using the order of successive cancellation (SC) decoding. For this purpose, Wyner's model is utilized [2]. Afterwards, we investigate the relationship between error exponent and code length in order to come up with an optimal coefficient, and then we construct a general matrix for polar code.

II. Wiretap channel

Wiretap channel was introduced by Wyner in 1975 [2]. In this channel transmitter, the main sender (i.e., Alice) wishes to send a message to the legitimate receiver (i.e., Bob) and prevent the leakage of the transmitted information to an eavesdropper (i.e., Eve). The communication channel between Alice and Bob is called the main channel, and the communication channel between Alice and the eavesdropper is called the wiretapper's channel. The wiretap channel model is illustrated in Fig. 1.

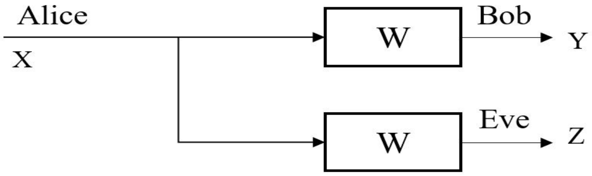

Fig. 1. Wiretap channel model which is drawn for this article.

$$C(W)=\left\{\begin{vmatrix} (R_e,R) \\ 0\le R\le C_m \\ 0\le R_e\le R \\ R_e\le C_m-C_w \end{vmatrix}\right\} \tag{1}$$

Equation (1) denotes the equivocation rate R_e as follows:

$$R_e=\frac{1}{n}H(W^n\mid Z^n) \tag{2}$$

where W, Z, and n denote a transmitted message, received data on the eavesdropper side, and code length, respectively. Regarding (1), the error probability of the wiretap channel must be higher than the value of the main channel. This is the primary assumption in this article.

III. Polar code

Polar codes are designed to achieve the capacity of binary-input discrete memoryless channels. The generator matrix of polar codes is demonstrated as (3) and (4):

$$G_2=\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{3}$$

$$G_2^{\otimes 1}=G_2\,,G_2=\begin{pmatrix} G_2^{\otimes(n-1)} & 0 \\ G_2^{\otimes(n-1)} & G_2^{\otimes(n-1)} \end{pmatrix} \tag{4}$$

where ⊗ is the Kronecker product. These codes produce the generator matrix, G_2^n, which is applied to the input of an $N=2^n$ input block. The result of this matrix multiplication,

Manuscript received November 09, 2020; revised December 14, 2021.

M. R. Deylam Salehi is a Graduated M.Sc. of the Guilan University in the Department of Telecommunication Engineering, Rasht, Iran (e-mail: Reza.deylamsalehi@gmail.com).
H. Tavakoli is an assistant professor of the Department of Telecommunication Engineering, Guilan University, Rasht, Iran (e-mail: hasantavakoli1983@gmail.com & htavakoli@guilan.ac.ir).

known as *P*, will be transmitted through independent copies of the binary-input discrete memoryless channel (B-DMC). When the number of n-independent channels increases, the channel becomes more polarized; then, we have two main channel statuses, noiseless (good channel) and pure noisy (bad channel). For $i \in [N]$, $[N] = \{1, 2, ..., N\}$, and $P_N^{(i)}$ is the i-th polarized channel, which is defined by the following transition probability shown in (5):

$$P_N^{(i)}(y_1^N, u_1^{i-1} \mid u_i) = \sum_{u_{i+1}^N} \frac{1}{2^{N-1}} P_N(y_1^N, u_1^N) \tag{5}$$

For any $\beta < 0.5$, the reliability of polar codes calculated from the block error probability under SC yields the following error probability complexity:

$$P_e \le \sum_{i \in A} Z(P_N^{(i)}) = O(2^{-(N)^\beta}) \tag{6}$$

By considering the error probability in (6), this paper seeks to design a wiretap channel to achieve secrecy capacity.

IV. Security Coefficient for the Wiretap Channel

The paper outlines some methods of securing data transition in wiretap channels. In order to achieve this, the error probability of the main channel as well as the wiretapper's channel is estimated by polar coding technique. Based on (6), in polar codes, the decoding error probability of the channel converges to $O\left(2^{-(N)^\beta}\right)$ complexity. For any $\beta < 0.5$, the block error probability determines the reliability of polar codes under SC.

$$G = [g_{i,j}]_{n \times n} \tag{7}$$

(8) and (9) show the polar code generator matrices at the main and wiretapper's channels in the wiretap model:

$$G \rightarrow P_e\left(AB\right) \simeq 2^{-N^\beta} \tag{8}$$

$$G' \rightarrow P_e\left(AE\right) \simeq 2^{-N^{\beta'}} \tag{9}$$

A. Code design based on error exponent

In the ideal wiretap channel that allows Alice and Bob to secure their communication, the wiretapper's channel would show a higher error probability value than the main channel.

Definition (transmission over a secure channel): when a transmission is secure, the error probability of the main and wiretapper's channel calculated as follows:

$$P_e(AE) = mP_e(AB) \tag{10}$$

Equation (10) shows the advantages of a legitimate sender and the differences between receivers. The coefficient *m* is a parameter used to generate generator matrices and simulate the wiretap model, and represents the difference between the decoding error probability on Bob's and Eve's side. Taking logarithm of (10) in two stages, the error exponent of each channel is achieved.

$$\log_N(-\log_2 P_e(AB)) = \beta \tag{11}$$

$$\log_N(-\log_2 P_e(AE)) = \beta' \tag{12}$$

Taking the logarithm of each side of (10), we get:

$$(-\log_2 P_e(AE)) = N^{\beta'} = -\log_2 m - \log_2 P_e(AB) \tag{13}$$

$$\log_N \left[(-\log_2(P_e(AE))) = (-\log_2 m - \log_2(P_e(AB)))\right] \tag{14}$$

$$\log_N(-\log_2(P_e(AE))) = \log_N(-\log_2 m - \log_2(P_e(AB))) \tag{15}$$

The correlation between the error exponent of the main and wiretapper's channels is extracted from (16):

$$\beta' = \log_N(-\log_2 m + N^\beta) \tag{16}$$

$$\beta' = \beta + \log_N(1 - (\frac{\log_2 m}{N^\beta})) \tag{17}$$

A logarithmic expression reduces complexity by (18):

$$\forall x \ll 1, \log(1-x) \simeq x \tag{18}$$

As a result of (17), the error exponent for the wiretapper's channel is:

$$\beta' = \beta - \frac{\log_2 m}{N^\beta} \tag{19}$$

By definition, the value of β (the error exponent) is in the range $[0, 0.5]$. β' falls in the same range:

$$0 \le \beta - \frac{\log_2 m}{N^\beta} \le \alpha \tag{20}$$

where the maximum value of β' is 0.5, which optimizes the coefficient between the error parameters. Considering the equations mentioned earlier, we approximate an optimal coefficient between the error probability of the main and wiretapper's channels. An inequality that limited *m* can be expressed as (21):

$$1 \le m \le 2^{(\alpha-\beta)N^\beta} \tag{21}$$

To consider it secure, the lower bound should be set to 1. In addition, when β takes its maximum value in (21), 0.5, *m* equals 1. This equation was added to an optimal function circumstance named particle swarm optimization (PSO). This function gives us the maximum value for *m*, with $N = 1000$ and $\beta = 0.355$.

$$m = 3.2453 \tag{22}$$

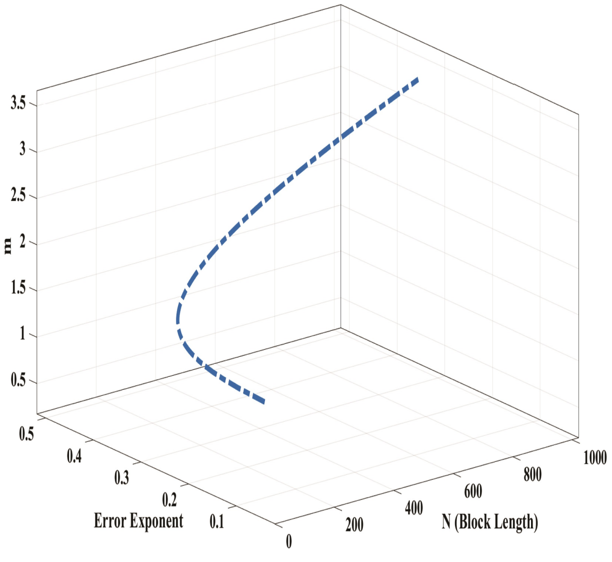

Fig. 2. The relationship between M, N, and β

The error probability of thbe main and wiretapper's channels is calculated to design an optimal scenario for the wiretap channel. In our optimization program, N should be considered at its maximum value of 1000 to achieve an optimal state:

$$P_e(AB) = 2^{-N^{\beta}} = 2^{-1000^{0.355}} = 0.0003189 \tag{23}$$

Theorem 1: The optimal point of (21), which gives maximum m, is:

$$\beta = \frac{1}{a} - \frac{1}{\ln N} \tag{24}$$

Proof: The error probability of the wiretapper's channel is calculated as follows:

$$P_e(AE) = 2^{-N^{\beta}} = mP_e(AB) = 0.001035 \tag{25}$$

Taking the derivative of (21):

$$m = 2^{(a-\beta)N^{\beta}}$$

$$\frac{\partial m}{\partial \beta} = ((-N^{\beta} + (\frac{1}{a} - \beta)N^{\beta}\ln N)2^{(0.5-\beta)N^{\beta}}) \tag{26}$$

$$\frac{\partial m}{\partial \beta} = 0 = -N^{\beta} + (\frac{1}{a} - \beta)N^{\beta}\ln N \tag{27}$$

$$\beta = \frac{1}{a} - \frac{1}{\ln N} \qquad \blacksquare$$

Remark: To have the highest coefficient (m), we set $a = 1/2$:

$$\beta = 1/2 - 1/(\ln N) \tag{28}$$

B. *Error exponent of $l \times l$ matrix: Korada's work*

The assumption presented in the previous section is based on Arikan's determination of the error exponent that takes values in the range of $0 \le \beta \le 1/2$. Korada showed any $l{\times}l$ matrices that none of the column permutations is upper triangular polarizes binary-input memoryless channel [3]. In this paper they proved that any invertible G can be used as a building block to construct polar codes. They then showed that the error exponent of the $l \times l$ generator matrix exceeds 0.5, and discussed the relation between polar codes and Read-Muller (RM) in construction. One of the main reasons we realized the coefficient m could be higher was due to this approach.

Theorem2 (Exponent from a partial distance): For any B-DMC and any $l{\times}l$ polarizing matrix G, the error exponent is computed with $\{D_i\}_{i=1}^{l}$ partial distance as follows:

$$E(G) = \frac{1}{l}\sum_{i=1}^{l}\log_i D_i \tag{29}$$

Example: For the generator matrix G, the partial distances, and the error exponent, is calculated as follows:

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \tag{30}$$

The partial distances, therefore, the error exponent will be:

$$d_1 = 1, d_2 = 2, d_3 = 2,$$

$$E(G) = \beta = \frac{1}{3}(\log_3 1 + \log_3 2 + \log_3 2) = 0.42062 \tag{31}$$

The upper bound and the lower bound in the error exponent were determined by Korada as follows:

$$E_l \le \frac{1}{l}\sum_{i=1}^{l}\log_1 d(l, l-i+1) \tag{32}$$

$d(N,k)$ denotes the largest possible minimum distance of a binary code of length N and dimension k. The lower bound is as follows:

$$E_l \ge \frac{1}{l}\sum_{i=1}^{l}\log_l D_i \tag{33}$$

The upper bound on the error exponent will also change by considering [4].

$$0 \le \beta \le 1 \tag{34}$$

$$1 \le m \le 2^{(1-\beta)N^{\beta}} \tag{35}$$

Moreover, the relationship between the error exponent and code length will be changed, and the new equation is shown as:

$$\beta = 1 - (1/\ln N) \tag{36}$$

Fig. 3 shows the relationship between error exponent and code length, that was shown in (24). a is the maximum value of error exponent in each scenario.

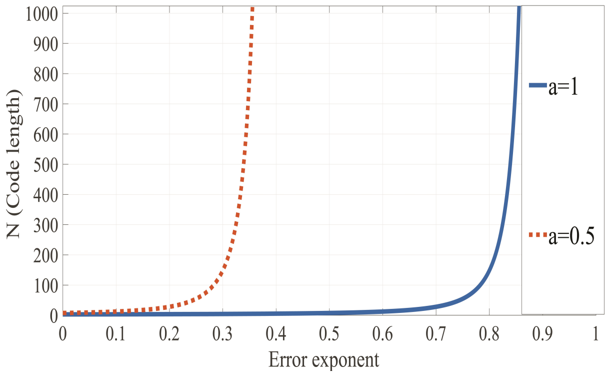

Fig. 3. The correlation between code length and error exponent.

m will be different subsequently. Considering (19) and (36), the coefficient will increase significantly. In code length $N = 1024$, for the generator matrix with $\beta = 0.8526$, we have the optimal coefficient as $m = 2.272e^{16}$.

Then, the error exponent for the eavesdropper is computed using (19).

$$\beta' = \beta - (\log_2 m / N^{\beta}) = 0.70520035806 \tag{37}$$

Fig. 4 shows the difference between the coefficient and the irregular generator matrix. Using m and (37), the coding error probability for this assumption is calculated as follows:

$$P_e(AB) = 2^{-(N)^{\beta}} = 2^{-(1024)^{0.8526}} = 1.080427e^{-111} \tag{38}$$

$$P_e(AE) = 2^{-(N)^{\beta'}} = 2^{-1024^{0.70520035}} = 1.1321467e^{-40} \tag{39}$$

To design a wiretap, a polar code generator matrix needs to be defined for each channel individually.

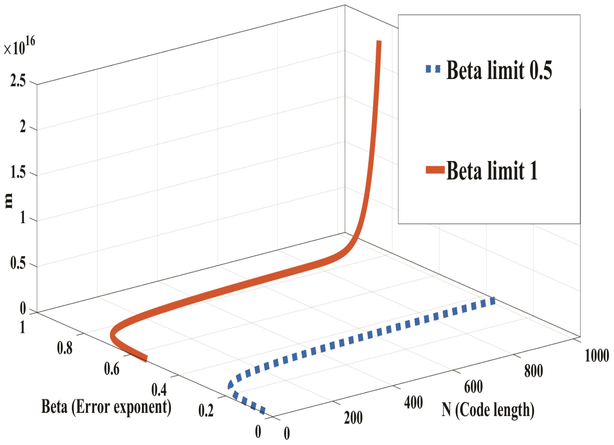

Fig. 4. The difference between coefficients for the $l \times l$ matrix.

Considering the value from (37) and (38), the effectiveness of this coefficient in improving security can be understood. *E(G)* is the polarization rate exponent for generator matrix *G*, which is calculated using partial distance (Hamming distance) D_i. Furthermore, we have:

$$E(G) = \frac{1}{l}\sum_{i=1}^{l} \log_l D_i$$

β and $E(G)$ are similar. Therefore, we have:

$$\beta = \frac{1}{l}\sum_{i=1}^{l} \log_l D_i \tag{40}$$

A proper generator matrix is achieved for any error exponents using (40) and considering the upper bound in Korada's work, indicating the possibility of constructing such a code. By calculating the upper bound of the error exponent for $N = 1024$, we have:

$$E_l \le \frac{1}{l}\sum_{i=1}^{l} \log_1 d(l, l-i+1) \tag{41}$$

$$E_l \le \frac{1}{1024}\sum_{i=1}^{1024} \log_{1024} d(1024, 1024-i+1) \tag{42}$$

$E_l \le 0.8563$ proves that the error exponent calculated for $N = 1024$, is possible for the generator matrix with the mentioned characteristics.

The polar code with the error probability calculated in (38) is designed using [5], [6]. By employing the BEC for the main channel, channel parameters can be defined as follows:

$$C(W) = \sum_{y}\sum_{x\in\{0,1\}} \frac{1}{2} W(y \mid x) \log_2 \frac{W(y \mid x)}{\frac{1}{2}W(y \mid 0) + \frac{1}{2}W(y \mid 1)} \tag{43}$$

$$R_0(W) = 1 - \log_2\Big(1 + \sum_{y} \sqrt{W(y \mid 0)W(y \mid 1)}\Big) \tag{44}$$

The Bhattacharyya parameter for the BEC main channel with erasure probability ε is calculated based on the following theorem.

Theorem 2: Bhattacharyya parameter for the BEC is:

$$Z = \varepsilon \tag{45}$$

Proof:

$$Z = \sum_{y}\sqrt{W(y \mid 0)W(y \mid 1)} = \sqrt{W(1 \mid 0)W(1 \mid 1)} + \sqrt{W(0 \mid 1)W(0 \mid 0)} + \sqrt{W(\varepsilon \mid 1)W(\varepsilon \mid 0)} = \sqrt{\varepsilon^2} \tag{46}$$

All terms, except the last one, would be zero.

Theorem 3 (Bhattacharyya parameter of a wiretap channel): Taking into consideration that the main channel and wiretap channel, in general, are modulated by BEC channels, we can define the Bhattacharyya parameter the following way:

$$Z(P) = \sum_{y\in Y} \sqrt{p(y_1 y_2 \mid 0)\, p(y_1 y_2 \mid 1)} = \varepsilon_1 \varepsilon_2 \tag{47}$$

Proof

The states that were shown in Fig. 5, help us to calculate the Bhattacharyya parameter.

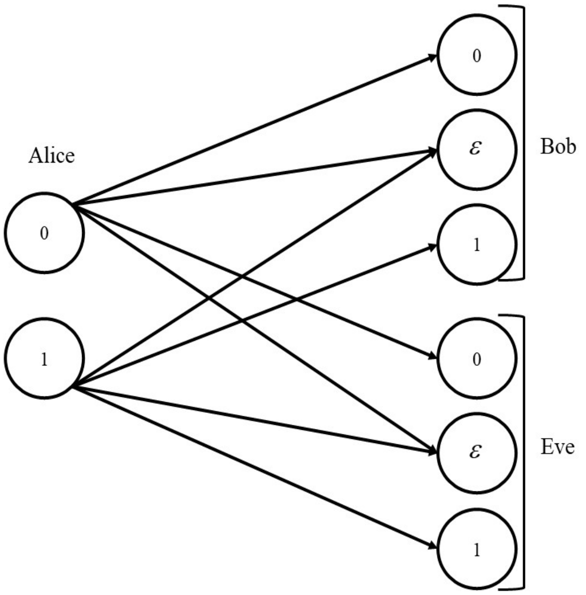

Fig. 5. The transmission states for a wiretap channel.

$$\begin{aligned} Z(P) &= \sqrt{p(00|0)\,P(00|1)} + \sqrt{p(01|0)\,p(01|1)} \\ &+ \sqrt{p(10|0)\,P(10|1)} + \sqrt{p(11|0)\,P(11|1)} \\ &+ \sqrt{p(0? \mid 0)\,P(0? \mid 1)} + \sqrt{P(1? \mid 0)P(1? \mid 1)} \\ &+ \sqrt{p(?0|0)\,P(?0|1)} + \sqrt{p(?1 \mid 0)\,P(?1 \mid 1)} \\ &+ \sqrt{P(?? \mid 0)P(?? \mid 1)}. \end{aligned} \tag{48}$$

It should be noted that, in the right side of *Z(P)* all terms except the last one would be equal to zero.

$$Z(P) = \sqrt{P(?? \mid 0)P(?? \mid 1)} = \sqrt{(\varepsilon_1\varepsilon_2)(\varepsilon_1\varepsilon_2)} = \varepsilon_1\varepsilon_2 \tag{49} \blacksquare$$

The cutoff rate can be determined by (41). Arikan mentioned R_0 / C in [5] for the BSC channel, you can also calculate this parameter for the BEC. This ratio is derived from a cutoff rate and channel capacity, which for BSC is defined as follows:

$$\frac{R_0}{C} = \frac{1 - \log_2[1 + 2\sqrt{p(1-p)}]}{1 + p\log_2(p) + (1-p)\log_2(1-p)} \tag{50}$$

In order to determine this parameter for a BEC, first, one must determine the channel capacity and cutoff rate. These parameters are affected by the erasure probability.

$$C = 1 - \varepsilon \tag{51}$$

$$R_0 = 1 - \log_2(1+\varepsilon) \tag{52}$$

By using (51) and (52) the R_0 / C for BEC channel is defined as follows:

$$\frac{R_0}{C} = \frac{1-\log_2(1+\varepsilon)}{1-\varepsilon} \tag{53}$$

In Fig. 6, R_0 / C per erasure probability is depicted.

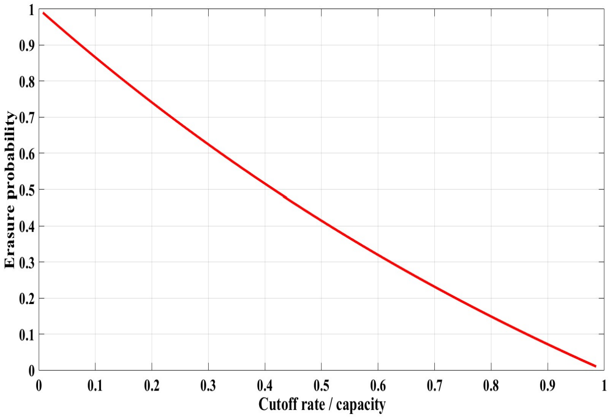

Fig. 6. The ratio of cutoff rate to capacity for the BEC.

The cutoff rates for both scenarios are calculated from [1]. According to (6), two lower bounds of the Bhattacharyya parameter are (25) and (38), respectively. The cutoff rate is calculated using (54):

$$R_0(W) = 1 - \log_2(1+Z) = 1 - \log_2(1+\varepsilon) \tag{54}$$

The cutoff rate for both tends to 1. The channel will be simulated with erasure probability (P_e) extracted in (23) and (38). The simulation results are shown in Figs. 7 and 8.

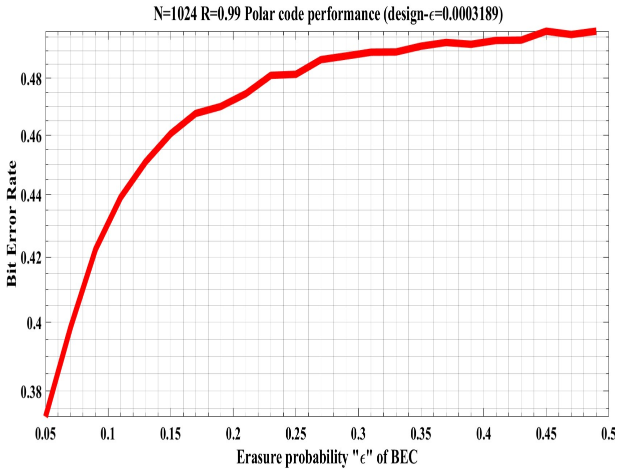

Fig. 7. Simulation of the BEC with error exponent limit 0.5.

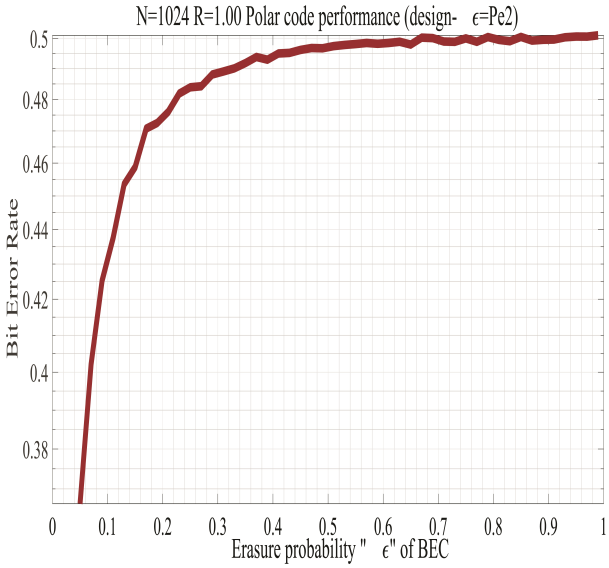

Fig. 8. Simulation of the BEC with error exponent limit 1.

V. Conclusion

This paper presents a novel technique that uses error exponents to improve security in wiretap channels. The order of complexity for decoding in polar codes was used to determine the relationship between code length and error exponent that provided secure coding and decoding. Our next goal was to find the optimal error exponent for a legitimate sender and generate a matrix of generators. Additionally, we calculated the decoding error probability for this generator matrix, which indicates that the wiretap channel has a higher error probability than the main channel. In our calculations for the $l \times l$ matrix, we applied Korada's assumption and displayed how it affected the error exponent. The process by which BEC simulated both states of the main channel and the BER was also discussed. It would be beneficial for future research to look into the multi-input, multi-output (MIMO) channel in order to enhance wiretap security.

References

[1] E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” vol. 55, no. 7, pp. 3051-3073, 2009.

[2] I. Csiszár and J. Korner, “Broadcast channels with confidential messages,” vol. 24, no. 3, pp. 339-348, 1978.

[3] A. Wyner, “The wiretap channel,” vol. 54, no. 8, pp. 1355-1387, 1975.

[4] S. B. Korada, E. Sasoglu, and R. Urbanke, “Polar codes: Characterization of exponent, bounds, and constructions,” vol. 56, no. 12, pp. 6253-6264, 2010.

[5] E. Arıkan, “From sequential decoding to channel polarization and back again,” arXiv preprint arXiv:1908.09594, 2019.

[6] Karbassian, Ghafouri-Shiraz, “Performance Analysis of Unipolar Code in Different Phase Modulations of Coherent Optical CDMA,” Engineering Letters, vol. 16, no.1, pp 50-55, 2008.

Date modification 28/08/2022

Change in the Affiliation part.
1.name of the university, change from Guilan University to University of Guilan.
2.M. R. Deylam Salehi is a Graduated M.Sc. of the Guilan University in the Department of Telecommunication Engineering, Rasht, Iran
Change to: M. R. Deylam Salehi is a PhD candidate at Eurecom, Sorbonne University in the Department of Communication System, Biot France.