Journal of Advanced Computer Science & Technology, 4 (1) (2015) 90-94
www.sciencepubco.com/index.php/JACST
©Science Publishing Corporation
doi: 10.14419/jacst.v4i1.4163
Research Paper

New method for combining the channel coding with polar coding-based encryption

Mohammad Kenarkouhi [1]*, Hassan Tavakoli [2]

[1] *MSc Student, Guilan University, Rasht Branch , Iran*
[2] *Assistant Professor in Department of Electrical Engineering, Faculty of Technology & Engineering, Guilan University, Rasht Branch , Iran*
**Corresponding author E-mail: mohammad_k_g@yahoo.com*

Abstract

In this paper, polar codes recently presented by Arikan are introduced. Polar codes have a number of channels with high capacity where information is located. In addition, these codes are composed of a number of channels with low capacity called frozen bits. In the first proposed design, we optimally use frozen and useless bits of the polar code and insert the encryption key on all the bits of the design (information bits and frozen bits). In fact, in Arkian's proposed 8-bit design, we use 8 encryption keys. Then, in the rest of the article, a method is presented through which the number of encryption keys applied can be reduced. Because, the encryption system is effective and desired in which in addition to the high complexity and the lack of correlation between bits, the minimum number of encryption keys are used.

Keywords: *Encryption; Channel Coding; the Combination of Encryption and Coding; Polar Code; Complexity.*

1. Introduction

Encryption is a science which studies and recognizes the principles and methods of transfering or saving information safely. Encryption is using mathematical techniques for establishing information security. In principle, encryption is the science of changing the message or information text using the encryption key or is the use of an encryption algorithm, but in a way that only a person who knows the key and algorithm can extract main information from encoded information and a person who does not know one or both of them cannot access to information [1]. For accessing a secure telecommunication and transferring information without error, error control codes must be used. Using error control codes is called "channel coding" [2]. Functional forms which perform channel coding are channel encoder and channel detector. Channel encoder systematically adds some figures to the sent message figures. Although these additional figures do not carry information, they make the error detection and correction in sent data possible leading to the system total error reduction. Another reason for the channel coding is to deal with destructive noises on the sent message. Today, in selecting telecommunication systems for overcoming the problem, the channel coding structure is used. As mentioned, for dealing with the enemy attacks and reducing noise effects on the message, the combination between encryption and coding is studied leading to the reduction of error and maintenance of the main structure of the message. The simultaneous use of channel coding and encryption is shown in figure 1. The combined and simultaneous use of both channel coding and encryption blocks for encrypted messages on the side of transmitter and their decryption on the side of receptor lead to the improvement of security and maintenance of the message structure.

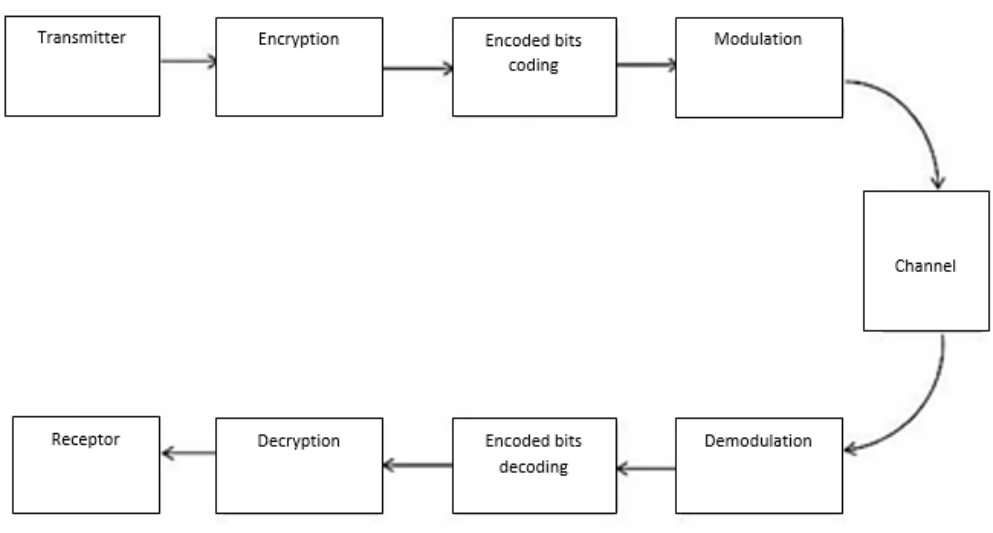

Fig. 1: The Structure of a Typical Telecommunication Transmitter and Receptor

2. Combination of encryption and coding

In any telecommunication, according to the transfer of information through a channel noisy, we need error detection and correction operations. This need is different in networks with wired and wireless infrastructure. The reason is the possibility of different errors of two channels. In the security of sent information, there are critical differences between wired and wireless networks. In wired networks, only in case of the access of enemy to information transfer environment, switch centers and infrastructures, the system security is distorted. In contrast, due to the use of open-space channel, the possibility of information eavesdropping, forging and repetition of the message by the enemy in wireless systems is more than wired ones. Therefore, in wireless communication, using encryption algorithms for security and validity is necessary as a basic need [3]. The existing systems use channel coding and encryption blocks separately for meeting the aforementioned demands. In the channel coding block, by adding redundancy bits to the main ones, it will be possible to do the error detection and correction in the receptor using these bits. These bits are called parity check bits. In the encryption block, as each bit of the encoded text can provide information about the key to the enemy, it is attempted to prevent from the information dissemination during the encryption process [4], [5]. The security section is mostly placed in the upper layers of transfer protocols, while error correction codes are used in the lower layers of these protocols. Therefore, sent information encrypted in the transmitter may face different error correction codes in passing different interfaces based on the protocols used between central interfaces, but it is only decrypted in the final destination. According to the computational load and the time required in each encryption and decryption operation in public key encryption algorithms, the issue of security and validity is a critical challenge. For this reason, encryption systems based on the coding theory are better than other encryption systems [6], [7], [8].

3. Polar coding

One of the block codes is the polar coding. Polar codes are recently introduced by Arikan [9] and are the first family of verifiable codes for binary discrete memoryless channels (B-DMC). The main idea of polar coding is the creation of a coding system in which any channel with W_N (i) coordinate can be accessed separately and data can be transferred only through this channel [10]. Polar codes have special designs for each channel, i.e. a polar code relating to a channel cannot be used for another one. Polar codes are linear ones, i.e. any linear combination of code words is another code word of the code. The polar transfer is using G^n_2 transfer which is the nth Kronecker of $G_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ to a block of $N=2^n$ ^{bit} V. The polar code is a natural coding design for transferring information bits on good channels, i.e. V_I is an information bit if $I(V, Y^N, V^{i-1})$ is close to 1; otherwise, we have a frozen bit. We optimally use frozen bits in the proposed design. Considering R<I (W), the polar coding is based on a set of matrix $G_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^n$ in order to form matrix $2^n R \times 2^n$ which is used in the channel coding as the matrix generator. The channel polarization method is provided for creating the code sequence in order to obtain I (W) symmetric capacity from any determined value of W relating to B-DMC [11]. The symmetric capacity of the highest accessible rate is an issue which uses bits entering the channel with an equal probability [12]. The channel polarization mentions the fact that there is the possibility to combine the second set of N from binary channel $\left\{W_N^{(i)}: 1 \le i \le N\right\}$ of N independent copy of a determined channel relating to B-DMC.

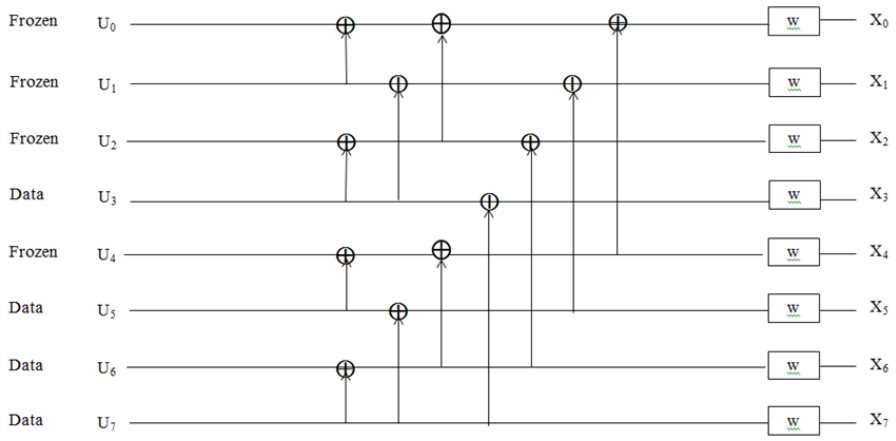

Fig. 2: The 8-Bit Structure of the Polar Code in Arikan's Design.

3.1. Channel polarization

Theorem: *For any binary symmetric discrete channel W, channel* $\{W_N^{(i)}\}$ *is called polarized. It means that for any* $\varepsilon\in(0,1)$*, with the increase of N and tendency toward infinity with exponent 2, a fraction of indices* $(i\in\{1,\ldots,N\})$ *where* $I(W_N^{(i)})\in(1-\delta,1]$ *tends toward I(W) (Clean and noise-free channels) and a fraction where* $I(W_N^{(i)})\in[0,\delta)$ *tends toward 1-I(W) (noise channels).*

Proof: [13], [14].
For BEC channel, $I(W_N^{(i)})$ is calculated by the following recurrence relation:
$I(W_N^{(2n-1)}) = I(W_{n/2}^{(i)})^2$
$I(W_n^{(2i)}) = 2I(W_{n/2}^{(i)}) - I(W_{n/2}^{(i)})^2$

4. The proposed method

In the encryption system, the information section must be hidden from the enemy. In other words, the enemy must not know a section of information. For example, in a design, bits demonstrated in Arikan's design can be considered as a key. In Arikan's proposed design, the possibility of error occurrence is 1/2. We send zero, but we are not aware whether zero is received in the receptor or one. Then, we send bit 1 and we are still unaware whether zero is received in the receptor or one.

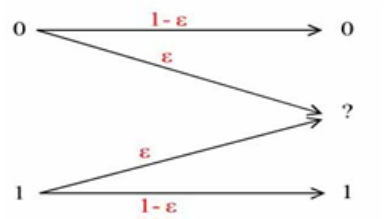

Fig. 3: The Typical Benchmarking Channel W

In this case, the capacity of one channel is increased and the capacity of another one is reduced. After two polarization stages, the capacity of one channel is continuously increased and the capacity of another one is continuously reduced. It depends on the number of polarization stages. In figure 4, the upper channel was accompanied with the capacity reduction, but the lower one was accompanied the capacity increase. In this case, more appropriate information can be sent using the lower channel.

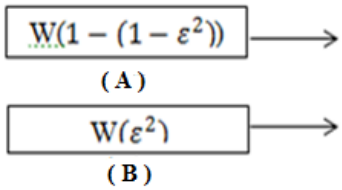

Fig. 4: The Equivalent Polar Code.

(A) The low-capacity channel, (B) The high-capacity channel

In the structure of polar codes, the capacity of bits is obvious; a series has high capacity and another series has low one which accordingly, the capacity of links (channels) is increased or reduced. In fact, the capacity of a series of channels is increased and the capacity of some channels is reduced and will be close to zero. In Arikan's design, information is placed on links with high capacity and links with low capacity close to one are considered as the frozen bits.
The structure of figure (5) is considered as follows:

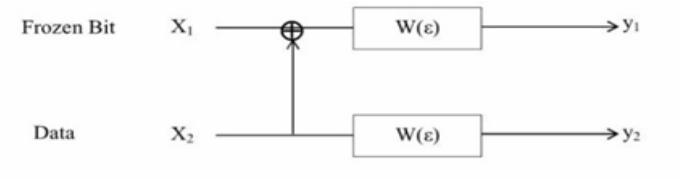

Fig. 5: The Typical Polar Code

The above system has weakness in security and it cannot be used for encryption because first, the information bit is placed on the channel without any encryption key and in fact, no encryption is done on it. Second, without any replacement on the information bit and the frozen bit, it is easy for the enemy to distinguish between these bits. Therefore, there is a need for the key bit for encrypting bits and performing replacement on them through a replacement box before entering the channel. There is also a need for the increase of security in the system.
In the system and the first proposed design, 3 actions are done on bits as follows:

1. Adding a key bit to the information bit
2. Considering the frozen bit as the encryption key. (Adding a key bit to the frozen bit)
3. Performing replacement on output bits before entering the channel

In the simplest case, after adding the encryption key to the information bit and frozen bit:

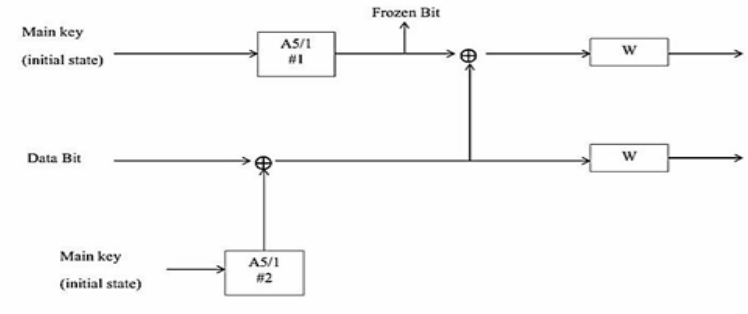

Fig. 6: Adding the Encryption Key on Bits

Now, consider Arikan's 8-bit structure. As it is shown in the figure, LFSR A5/1 is placed on each frozen bit. In fact, the frozen bit is used as the encryption key. LFSR was added to all frozen bits. As mentioned, A5/1 algorithm is used in the proposed design.

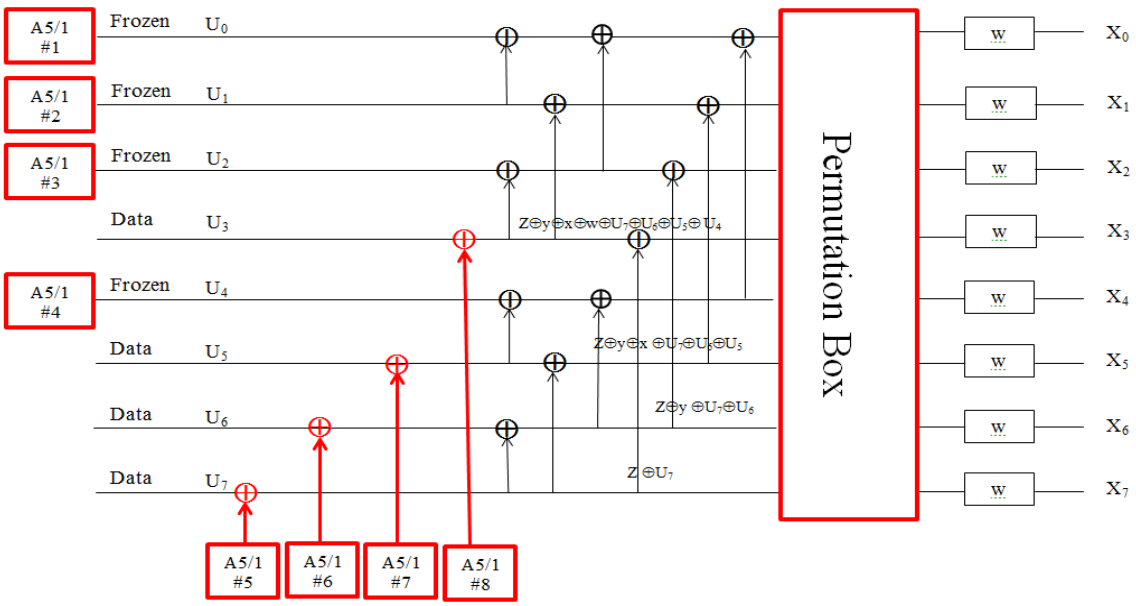

Fig. 7: Adding Lfsrs and Presenting the First Proposed Design

LFSR is applied to all information bits which are shown by #5, #6, #7 and #8 in the figure. The reason of using these LFSRs is that information bits are placed on the channel directly and without any change because in this case, it is simple for the enemy to access to and recall them. As shown in the figure, the output bits enter a replacement box before entering the channel. The replacement box changes the configuration and order of LFSR outputs before entering the channel in order to make it very difficult for the enemy to recall them. In the rest of the paper, we demonstrate that the expressed contents lead to the increase of security and complexity in Arikan's proposed system.
Before entering the channel, the encrypted bits must enter a system in order to change their order and layout. We place a replacement box in the system in order to replace the encrypted bits before they enter the channel. It leads to the increase of complexity in the system. The advantage of using the proposed replacement box (Π-Box) is that it is used for few number of bits (for example two and four bits) while other algorithms (such as AES algorithm) are not used for few number of bits. The mechanism of the proposed replacement box is that by replacing bits, the equivalent complexity of $\frac{\log(n!)}{\log 2}$ is added to the system. (n indicates the total number of bits per system).

5. Calculating complexity of the 8-bit system in the proposed design

Theorem 1: *The complexity of entire system in the 8-bit design is equal to O* ($2^{506.56}$).

Proof: In the proposed 8-bit design, 8 LFSR A5/1s are used. Each A5/1 equals to O ($2^{63.32}$); so, the total complexity of A5/1s is equal to O ($2^{506.56}$). As it was mentioned, a replacement box is used for replacing output bits in the system which applies n complexities to the system. n indicates the total number of bits. Therefore, the system total complexity equals to:

$|\chi|=2^{316.6}\times 2^{15.29}=2^{521.85}$

6. Conclusion

In this paper, after studying the polar coding presented by Arikan, a combined method was provided for the channel coding, replacement box-based block encryption system and A5/1 algorithm-based successive encryption system. The results of this algorithm show that in the combined system, in addition to the enemy's knowledge of A5/1 successive encryption algorithm keys, the channel breakdown and channel polarization help the encoder and provide the maximum ambiguity for the enemy. It is because not only the enemy faces the lack of a frozen bit key, but also faces ambiguity in the selection of the correct channel on which information is placed. The results of studying the ambiguity indicate the ability of this algorithm.

References

[1] Stallings w (2007).Cryptography and Network Security,fifth Editiom.
[2] Thomas M. Cover, Joy A. Thomas (2006).Elements of Information Theory.Second Edition.New jerky.
[3] R. J. McEliece, a Public-Key Cryptosystem Based on Algebraic Coding Theory, 1978.
[4] Berlekamp, Elwyn R.; McEliece, Robert J.; Van Tilborg, Henk C.A. (1978). "On the Inherent Intractability of Certain Coding Problems". IEEE Transactions on Information Theory. IT-24: 203–207.
[5] Giulian G.la Guardia, Nonbinary Convolutional Codes Drwed from group character, Discrete Mathematics, Vol 313, August 2013, PP. 2730-2736.
[6] Anne canteaut and Florent chabaud, "A new Algorithm for finding minimum-weight Words in a liner code: Application to McElieces Cryptosystem and a Narrow – sense BCH code of Lengh 511", IEEE Transaction on Information Theory, Vol 44,January 1998, PP.367-378.
[7] A.Canteaut and N. Sendrier, "Cryptanalysis of the original McEliece Cryptosystem," in Advances in Cryptology-ASIACRYPT 98, LNCS 1514,PP.187-199,1998.
[8] Hessam, Mohammad Hosseini, "Study of coding theory-based encryption systems", MSc seminar, Tarbiat Modares University, October 2005.
[9] Erdal Arikan, channel Polarization: a method for Construting Capacity Achiving codes, ISI, 2008. 10-N.Hussami, etal, performance of polar Code forchannel and source Coding, mag 2009.
[10] Duo Bin, et al., Achieving the Capacity of Half-duplex degraded relay channels using polar coding, Chinese Journal of Aeronautics, Vol. 27, 2014, pp. 584-592. http://dx.doi.org/10.1016/j.cja.2014.04.008.
[11] Erdal Arikan, channel Polarization: a method for construeting Capacity achiving code Symmetric binary-input memoryless channel, july 2009.
[12] Arikan, E. (July 2009). "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels". IEEE Transactions on Information Theory 55 (7): 3051–73. http://dx.doi.org/10.1109/TIT.2009.2021379.
[13] Michael Rose, Lattice-based cryptography: A practical implementation, A thesis submitted in Partial Fullfilment of the Requirements for the degree of Master of Computer Science, University of Wollongong, 2011.