The ISC Int'l Journal of Information Security
ISeCure

July 2017, Volume 9, Number 2 (pp. 111–118)
http://www.isecure-journal.org

An Efficient Secure Channel Coding Scheme based on Polar Codes

Behnam Mafakheri [1], Taraneh Eghlidos [2,*], and Hossein Pilaram [1]
[1] *Sharif University of Technology, Department of Electrical Engineering, Iran, Tehran*
[2] *Sharif University of Technology, Electronics Research Institute, Iran, Tehran*

ARTICLE INFO.

Article history:
Received: 24 April 2017
Revised: 22 July 2017
Accepted: 26 July 2017
Published Online: 30 July 2017

Keywords:
Code Based Cryptography, Rao-Nam Cryptosystem, Channel Coding, Polar Codes, Shannon Capacity.

ABSTRACT

In this paper, we propose a new framework for joint encryption encoding scheme based on polar codes, namely efficient and secure joint secret key encryption channel coding scheme. The issue of using new coding structure, i.e. polar codes in Rao-Nam (RN) like schemes is addressed. Cryptanalysis methods show that the proposed scheme has an acceptable level of security with a relatively smaller key size in comparison with the previous works. The results indicate that the scheme provides an efficient error performance and benefits from a higher code rate which can approach the channel capacity for large enough polar codes. The most important property of the proposed scheme is that if we increase the block length of the code, we can have a higher code rate and higher level of security without significant changes in the key size of the scheme. The resulting characteristics of the proposed scheme make it suitable for high-speed communications, such as deep space communication systems.

1 Introduction

The main challenges of satellite communications are in short security, error performance, energy efficiency and implementation costs. A solution to the shortcomings raised from these challenges to some extent is using joint encryption-channel coding scheme appropriately [1]. In 1978, McEliece proposed a public-key cryptosystem based on algebraic coding theory [2] that revealed to be very secure. The McEliece cryptosystem is based on the difficulty of decoding a large linear code, which is known to be an NP-complete problem [3]. This system is two or three orders of magnitude faster than RSA. A variant of the McEliece cryptosystem, according to Niederreiter [4], is even faster. The McEliece scheme employs probabilistic encryption [5]. However, because of the large size of the public key and a low code rate, this cryptosystem is not used widely. To remove these two imperfections in McEliece cryptosystem, several modifications are presented [6–10], so far.

In 1984, Rao used the McEliece public-key cryptosystem as a symmetric key cryptosystem [11]. Rao and Nam modified this cryptosystem to reduce the key size and increase the information rate [12]. However, this cryptosystem is insecure against chosen plaintext attacks [13, 14]. In the last decade, capacity approaching codes have been widely used. Turbo codes have been employed in two different symmetric-key secure channel coding schemes in [15, 16]. Some other schemes have been proposed to use Low Den-

* Corresponding author.
Email addresses: mafakheri_behnam@ee.sharif.edu (B. Mafakher), teghlidos@sharif.edu (T. Eghlidos), h_pilaram@ee.sharif.edu (H. Pilaram)
ISSN: 2008-2045

sity Parity Check (LDPC) codes in the McEliece-cryptosystem [10, 17–19]. In [20] Baldi, Bianchi and Chiaraluce tried to optimize and fill the gap between the density of the parity check matrices used in QC-LDPC code-based variants of the McEliece cryptosystem. In [21], the authors have proposed a secret key encryption scheme based on 1-level QC-LDPC lattices. In [22] the authors employ punctured QC-LDPC codes obtained from Extended Difference Families (EDFs). Security analysis shows that if the code employed is revealed, the scheme remains secure. A secure channel coding scheme proposed in[23] in which randomly inserts and deletes some bits in a codeword of a QC-LDPC code and it is shown that the error performance of the code after the insertions and deletions is better than a random LDPC code with similar parameters. Moreover, the idea of applying non-systematic polar codes in the structure of secure channel coding schemes is introduced in [24].

Polar codes were introduced by Arikan in 2009 [25]. These are the first low complexity linear block code which provably achieve the capacity for a fairly wide class of channels. The original paper of Arikan proved that these codes can achieve the capacity of binary symmetric channels as well as arbitrary discrete memoryless channels [26–28]. Some modifications of the original structure were proposed and it was shown that these codes are optimal for lossless and lossy source coding [29–31].

In this paper, we propose a secure channel coding scheme using polar codes. This scheme is designed to be secure against the previous known attacks. To the best of our knowledge, the code rate is much more than that of the previous schemes, and the key size is reduced to 1.6kbits, which is lower than that of the smallest key size of the previously proposed schemes, to the best of our knowledge (i.e. 2.191Kbits in [22]). The proposed scheme avoids the weaknesses of Rao-Nam (RN) scheme. The most important property of the proposed scheme is that if we increase the block length of the code, we could have a higher code rate and a higher level of security without significant changes in the key size of the scheme. These make our cryptosystem much more desirable in satellite communications.

The rest of this paper is organized as follows: In Section 2 we consider the basic polar code construction. The new symmetric cryptosystem based on polar codes is addressed in Section 3. Section 4 deals with the security and the efficiency of the proposed scheme. Finally, Section 5 concludes the paper.

2 Introduction to Polar Codes

In [32] Shannon proved the achievability part of noisy channel coding theorem using random-coding. He showed the existence of a code that achieves capacity. Polar codes are an explicit construction that achieve channel capacity with low complexity of encoding and decoding [25]. This section gives an overview of channel polarization and polar coding.

2.1 Channel Polarization

The process of channel polarization is a transformation in which one synthesizes a set of N channels $W_N^{(i)} : 1 \leq i \leq N$ from N independent copies of a given binary discrete memoryless channel (B-DMC) W, such that, as N becomes larger, for all but a vanishing subset of indices i, the symmetric capacity terms, $I(W_N^{(i)})$, tend towards 0 or 1 [33]. This process consists of two dependent steps: channel combining phase and channel splitting phase.

Channel Combining: In this phase we combine N copies of DMC W recursively to produce a vector channel $W_N : X^N \to Y^N$, where $N = 2^n$. Figure 1 shows how to construct channel W_2 with the probability of

$$W_2(y_1, y_2|u_1, u_2) = W(y_1|u_1 \oplus u_2).W(y_2|u_2) \quad (1)$$

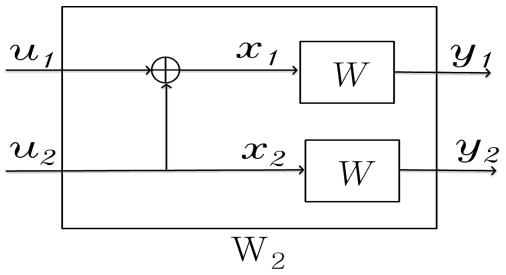

Figure 1. The Channel W_2.

Figure 2 shows the general form of channel combining, where two copies of $W_{\frac{N}{2}}$ are combined to produce the channel W_N. The block R_N is a permutation operator, known as the reverse shuffle operation, which converts its inputs s_1^N to $v_1^N = (s_1, s_3, \ldots, s_{N-1}, s_2, s_4, \ldots, s_N)$. In fact, polar code is similar to Reed-Muller (RM) code which is a class of linear codes [34, 35].

Channel Splitting: Here, we want to split channel W_N to construct N channels $W_N^{(i)} : X \to Y^N \times X^{i-1}$, defined by the following transition probability

$$W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) \triangleq \sum_{u_{i+1}^N \in X^{N-i}} \frac{1}{2^{N-1}} W_N(y_1^N|u_1^N) \quad (2)$$

It can be shown that the generator matrix G_N equals $B_N F^{\otimes n}$ for any $N = 2^n$, $n \geq 0$, where B_N is a

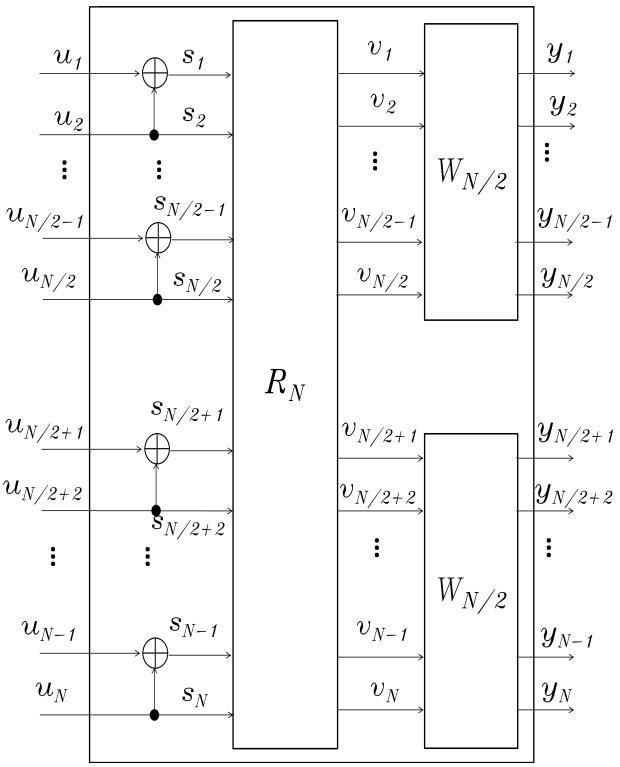

Figure 2. Recursive construction of W_N from two copies of $W_{N/2}$.

permutation matrix known as bit reversal and $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Now, we convey two remarkable theorems on channel polarization.

Theorem 1. [25] For any B-DMC W, the channels $W_N^{(i)}$ are polarized in the sense that, for any fixed $\delta \in (0,1)$, as N goes to infinity through powers of two, the fraction of indices $i \in \{1,2,\ldots,N\}$ for which $I(W_N^{(i)}) \in (1-\delta, 1]$ goes to $I(W)$ and the fraction for which $I(W_N^{(i)}) \in [0,\delta)$ goes to $1 - I(W)$.

Theorem 2. [25] For any B-DMC W with $I(W) > 0$, and any fixed $R < I(W)$, there exists a sequence of sets $A_N \subset \{1,\ldots,N\}$, $N \in \{1,2,...,2^n,...\}$, such that $|A_N| \geq NR$ and $Z(W_N^{(i)}) \leq O(N^{-5/4})$ for $i \in A_N$.

where $Z(W_N^{(i)})$ denotes the Bhattacharyya parameter of channel $W_N^{(i)}$.

2.2 Polar Coding

We use the channel polarization to construct polar codes that achieve channel capacity based on the idea that we only send data through those channels $W_N^{(i)}$ for which $Z(W_N^{(i)})$ is close to 0and equivalently $I(W_N^{(i)})$ is close to 1.

G_N-Coset Codes: This set is a class of block codes, with the following encoding process:

$$x_1^N = u_1^N G_N = u_A G_N(A) + u_{A^c} G_N(A^c) \quad (3)$$

where G_N is the generator matrix and A is a K-element subset of $\{1,2,...,N\}$ and u_1^N is the input vector which is divided into two vectors, u_A and u_{A^c}, according to the index set A. The vector u_A is known as the input to the good channels and u_{A^c} is the input to the bad channels. By fixing the index set A, pointing the information set, and the frozen bits u_{A^c}, the G_N-Coset Code is determined by (N, K, A, u_{A^c}), where K is the code dimension. Polar codes suggest a particular rule for choosing the index set A which is the indices of those rows from the generator matrix which are known as the information set (also called the indices of good channels).

A Successive Cancellation (SC) Decoder: For a G_N-coset code, the decoder decides on y_1^N and estimates $\hat{u}_1^N$ as the transmitted data. A block error is occurred if $\hat{u}_1^N \neq u_1^N$. SC decision functions are similar to ML decision functions, but these functions consider the frozen bits as random variables instead of the fixed bits. However, the loss of performance due to this suboptimum decoding is negligible and the symmetric capacity is still achievable. Notice that ML decoding is an efficient decoding algorithm for short length codes of polar codes but its complexity is large [25, 36]. The SC decoder generates $\hat{u}_1^N$ by computing

$$\hat{u}_i = \begin{cases} u_i & \text{for } i \in A^c \\ h_i(y_1^N, \hat{u}_1^{i-1}) & \text{for } i \in A \end{cases} \quad (4)$$

where

$$h_i(y_1^N, \hat{u}_1^{i-1}) = \begin{cases} 0, & \text{if } \frac{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|0)}{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|1)} \geq 1 \\ 1, & \text{otherwise} \end{cases} \quad (5)$$

Code Performance: It can be shown that for any B-DMC W and any choices of (N, K, A) code the probability of block error for this code under SC decoding, $P_e(N, K, A, u_{A^c})$ is bounded as follows:

$$P_e(N, K, A, u_{A^c}) \leq \sum_{i \in A} Z(W_N^i) \quad (6)$$

This suggests that we should choose A from all K-element subsets of $\{1,...,N\}$ such that it minimizes the right hand side of Equation 6.

Polar Codes: In polar codes the subset A is chosen such that $Z(W_N^i) \leq Z(W_N^j)$ for all $i \in A$, $j \in A^c$. The channels with indices in A and A^c are called good and bad channels, respectively. The main coding result is given below.

Theorem 3. [25] For any given B-DMC W and fixed $R < I(W)$, the block error probability for polar coding under successive cancellation decoding satisfies:

$$P_e(N,R) = O(N^{-\frac{1}{4}}) \tag{7}$$

Furthermore, it can be shown that the encoding and decoding (SC) complexities of polar codes are both of order $O(NlogN)$[17]. Therefore, the general complexity of the system (both encoder and decoder) for polar codes is less than that of LDPC codes (the best capacity approaching code before the birth of polar codes) and this makes the polar codes much more of practical interests.

3 The Proposed Symmetric Scheme Based on Polar Codes

In this section, we introduce our proposed secure channel coding scheme. As the fundamental component of our scheme, we construct a polar code as described in Section 2 according to the parameters used for the channel. For this purpose, we construct the generator matrix of length N for encoding purpose. Then we select the indices of bad channels according to the polar codes construction algorithm, explained in section II-B, which determines how to choose the index set A based on Bhattacharyya parameter. We also choose the frozen bits randomly. Note that we do not set the frozen bits as all zero bits As another component of the scheme, we choose a random quasi-cyclic block diagonal permutation matrix P, constructed by submatrix $\pi_{l\times l}$ as below [17]:

$$\begin{pmatrix} \pi_{l\times l} & 0 & \dots & 0 \\ 0 & \pi_{l\times l} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \pi_{l\times l} \end{pmatrix} \tag{8}$$

It is obvious that this method reduces the key size which we are going to discuss in Section 4.1. As it was mentioned in Section 2 the code parameters depend on the channel parameters. So, we randomly select the values of both frozen bits and the input of some other bad channels, namely v_s, which is given by inequalities (12) and (13) in Section 4.1 according to the coding rate, and keep them secret. Note that the secret key set would be $\{P, e_s, u_{A^c}, v_s\}$. Even though by this construction, we distance from the channel capacity to some extent, we obtain a more reliable communications as it will be discussed in Section 4.1.

3.1 Encryption-Encoding

For our secure channel coding scheme, the sender computes

$$u = (mG + e_s)P, \tag{9}$$

where m is the plaintext message, e_s is the perturbation vector, and G is the generator matrix of the polar code.

3.2 Decryption-Decoding

The legitimate receiver receives the following vector:

$$c' = (mG + e_s)P + e_{ch} \tag{10}$$

Using the secret key $\{P, e_s, u_{A^c}, v_s\}$ he can decrypt c' according to the following algorithm:

1. Multiply Equation (1) by P^{-1} and obtain

$$c'' = c'P^{-1} = mG + e_s + e_{ch}P^{-1} \tag{11}$$

2. Subtract the error vector from Equation (11) and obtain $mG + e_{ch}P^{-1}$.

3. Recover m, using SC algorithm with the input parameters u_{A^c} and v_s.

Notice that $e_{ch}P^{-1}$ has the same Hamming weight as that of e_{ch}. This is because $P^{-1} = P^T$ is a permutation matrix and does not change the Hamming weight of the vector.

Thus far, we have developed a secure channel coding scheme which can be interpreted as a joint symmetric encryption-encoding cryptosystem. In the ensuing part we are going to evaluate the efficiency and security of the proposed scheme.

4 Efficiency and Security

In this section, we evaluate the efficiency and the security of the proposed scheme, where we choose $N = 2048$.

4.1 Efficiency

The efficiency of the proposed scheme is discussed from the viewpoints of encryption/decryption complexity, bit error rate, code rate and key size.

4.1.1 Complexity

Here, we discuss the implementation complexity of the proposed scheme. Since we use the codes with large block lengths for satellite communications[37], we should give evidence for applicability of our scheme with low complexity.

In the proposed scheme there is no precomputation phase. In the computation phase, the complexity of the scheme corresponds only to the encoding and decoding processes. According to Section 2, both encoding and decoding complexities have the same order $O(NlogN)$. We observe that the complexity of the proposed scheme is lower than that of capacity approaching codes, which is indeed more desirable for satellite communications.

4.1.2 Error Performance

As it is mentioned in Section 2, polar codes provably achieve the capacity of the channel. In [38] Arikan and Telatar showed that for any rate $R < I(W)$ and any $\beta < \frac{1}{2}$, the block error probability is upper bounded by $2^{-N^{\beta}}$ for large enough N. Another problem is to determine the trade-off between the rate and the block length for a given error probability when we use successive cancellation decoder. In our scheme, because of the finite length of the blocks, we cannot use a rate equal to the channel capacity. For example, if the error probability of the BEC is 0.01, the channel capacity is 0.99 [39]. Thus, from[25] we know that, for $N = 2048$, the number of frozen bits is approximately equal to 21, but in this rate, we do not have reliable communications. Therefore, the rate should be reduced to obtain reliability. In [40, 41] the authors showed that for any BEC, W, with capacity $I(W)$, reliable communications require the rates that satisfy the following inequality:

$$R < I(W) - N^{-\frac{1}{\mu}} \tag{12}$$

where N is the block length and $\mu \approx 3.627$. In other words, if we want to have reliable communications, then the block length should be lower bounded by the following inequality:

$$N > (\frac{1}{I(W) - R})^{\mu} \tag{13}$$

In the proposed scheme, to make a comparison with the results obtained in other publications, the block length is considered to be 2048. Therefore, from Equation (12), if the coding rate is less than 0.87, a reliable communication is achieved. From this we can conclude that the number of fixed bits is approximately equal to $((I(W) - R) \times N) \approx 245$. Figure 3 shows the rate versus reliability trade-off for W using polar codes with $N = 2048$.

A comparison between the code rates of different RN-like secret key schemes with their recommended code parameters are given in Table 1.

Table 1. Code rate of the new scheme compared with other RN-like schemes.

scheme	code	rate
Rao[11]	C(1024, 524)	0.51
Rao-Nam [12]	C(72,64)	0.89
Struik-Tillburg [42]	C(72,64)	0.89
Barbero-Ytrehus [43]	C(30,20) over GF(2^8)	0.66
SobliAfshar-Eghlidos [17]	C(2044,1024)	0.5
Proposed Scheme	C(2048, 1781)	0.87

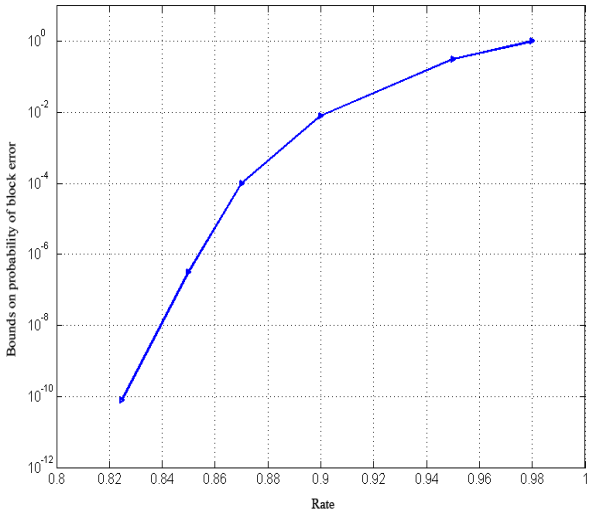

Figure 3. Rate vs. reliability for polar coding and SC decoding at block-lengths $N = 2^{11}$.

4.1.3 Key Size

Using a specific structure, we are able to reduce the key size to a reasonable level. Here, we discuss the key size of the proposed scheme. Then we compare the results with the previous ones.

In the proposed symmetric scheme, the secret key consists of three components: the frozen bits, the error vector and the permutation submatrix $\pi_{l\times l}$. As it was mentioned in Section 2 and 4.1.2, the number of frozen bits depends on the channel capacity, which in our scheme is $(|u_{A^c}|+|v_s|) = 21 + 245 = 266$bits, where u_{A^c} and v_s indicate the frozen bits and the fixed bits, respectively. To reduce the key size of this scheme, we use a certain procedure to store the permutation submatrix $\pi_{l\times l}$. The number of such permutation matrices is $l!$. Here, we use an efficient representation of this matrix which was first introduced by Barbero and Ytrehus [43]. By choosing $l = 64$, the permutation matrix P consists of 32 submatrices $\pi_{64\times 64}(2048 = 32 \times 64)$. To store the matrix $\pi_{64\times 64}$ we need 321 bits [43].

As another component of the secret key, the error vector e_s has 2048 entries. This vector is generated using Feedback Shift Registers (FSRs); the seed to generate such pseudorandom vector must be at least 1024 bits. These yield the total secret key size of $1611bits \approx 1.6Kbits$ to be exchanged. One may choose $l = 32$ or $l = 128$ and the key size would be $\approx$ 1.4Kbits and 2Kbits, respectively. A comparison between the key sizes of various RN-like schemes and the proposed one is given in Table 2. It is observed that we are able to achieve a short key size. As we discuss in Section 4.2, we observe that our scheme enjoys a high security level.

Table 2. Key size of the new scheme compared with other RN-like schemes

Scheme	Code	Key Size
Rao [11]	C(1024, 524)	2Mbits
Rao-Nam [12]	C(72,64)	18Kbits
Struik-Tillburg [42]	C(72,64)	18Kbits
Barbero-Ytrehus [43]	C(30,20) over GF(2^8)	4.9Kbits
SobliAfshar-Eghlidos [17]	C(2044,1024)	2.5Kbits
Esmaeli-DG [22]	C(2048, 1536)	2.2Kbits
Proposed Scheme	C(2048, 1781)	1.6Kbits

It is noteworthy that by increasing the code length N, not only the key size of the proposed scheme remains constant, but also the security of the scheme increases. Thus, from Equation 12, one concludes that by increasing the code length, the code rate is increased without any change in the key size. As stated previously, this property is much more desirable in satellite communications.

4.2 Security

In this section, we discuss the security of the proposed scheme including the attacks already applied to the previous RN-like cryptosystems.

Brute Force Attack: In this kind of attack, the adversary aims to enumerate the code set, i.e. the set of equivalent codes; to determine the error vector and the permutation matrix. As mentioned in Section 2, decoding algorithm of polar codes is based on successive cancellation. Hence, the attacker must find all of the frozen bits and the fixed bits. In our scheme, the number of components of these vectors is at least 266 bits. Therefore, the number of such vectors is at least 2^{266}, which denotes an impractical amount of preliminary work.

For the pseudorandom error vector e_s of length N, there is a large number of non-zero vectors (i.e. $2^{N/2}-1$), because of the large code parameters.

The number of permutations P in a block diagonal form is $l!$, where l is the number of rows of the permutation submatrix $\pi_{l\times l}$ and l is a divisor of the code length N. It is recommended that l should be chosen such that the number of all possible permutations leads to a large amount of preliminary work with regard to the design parameters of the code. For instance, $l=32$, $l=64$, or $l=128$ yields $l!\geq 2^{117}$, $l!\geq 2^{295}$, and $l!\geq 2^{716}$, respectively. Thus, choosing each of these values for l makes the computation impractical. Therefore, one can choose $l=32$, to reduce the key size while having an acceptable level of security.

RN attack: The symmetric key scheme proposed by Rao [11] uses error vectors of weight $t\leq\lfloor\frac{d-1}{2}\rfloor$, where d is the minimum distance of the (n,k)-code. Rao and Nam showed that this cryptosystem is vulnerable to a majority voting attack [12]. However, a chosen-plaintext attack can only succeed when $\frac{t}{n}$ is small enough. In our scheme, the generated error vectors have a Hamming weight of at most N and $\frac{N}{2}$ on average. This makes our scheme resistant against this attack.

Struik-Tilburg Attack: One of the drawbacks of the McEliece scheme is the low code rate. The RN scheme was introduced to remove this defect. Rao and Nam used the error-correcting properties of the code to determine predefined error patterns [12]. The error patterns used in the RN scheme have an average Hamming weight equal to half of the code length. Rao and Nam claimed that determining the encryption matrix of their scheme in a chosen-plaintext attack has a work factor of at least $O(N^{2k})$ for the (N,k)-code [12]. However, Struik and Tilburg proposed a chosen-plaintext attack on RN cryptosystem that shows it is insecure [42]. All of these attacks were practical because of the small code parameters used by Rao. However, the size of the polar code used in our scheme is large enough (One may use $N=1024$ and have the same level of security while having lower data rates), so that such an attack is not practical.

5 Conclusions

In this paper, we have proposed a new scheme based on polar codes: A symmetric-key secure channel coding scheme. The scheme utilizes a specific form of permutation matrix, a random error vector and input bits of bad channels as the secret key. The security and efficiency of this scheme have been discussed; the proposed scheme is secure against the brute force, RN and Struik-Tilburg attacks, and it is more efficient than the previous schemes from the view of the key size (1.6Kbits), the implementation complexity ($O(NlogN)$), the code rate (0.87) and the error performance ($<10^{-6}$) for the codes with comparable parameters.

The new scheme employs polar codes based on the following four reasons: (1) Polar codes can achieve the channel capacity, (2) the performance of the code improves in large block lengths which is desirable for satellite communications, (3) the total complexity of encoding and decoding of the codes is lower than the previously used codes and (4) the specific structure of the generator matrix of polar codes makes it possible to have a small key size (1.6Kbits) to be exchanged which is less than the smallest key size of the previously proposed schemes to the best of our knowledge.

References

[1] C. N. Mathur. *A Mathematical Framework for Combining Error Correction and Encryption*. Stevens Institute of Technology, 2007.

[2] Robert J. Mceliece. A public-key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Lab Deep Space Network Progress report, 1978.

[3] E. Berlekamp, R. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems (Corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, May 1978.

[4] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. 1986.

[5] S. Goldwasser and S. Micali. Probabilistic Encryption and How To Play Mental Poker Keeping Secret All Partial Information. pages 270–299. ACM, 1982.

[6] C. S. Park. Improving code rate of McElieces public-key cryptosystem. *Electronics Letters*, 25(21):1466–1467, 1989.

[7] M. C. Lin and H. L. Fu. Information rate of McElieces public-key cryptosystem. *Electronics Letters*, 26(1):1618–, 1990.

[8] Grigory Kabatiansky, S. Semenov, and E. Krouk. *Error correcting coding and security for data networks : analysis of the superchannel concept*. J. Wiley and sons, Chichester, Hoboken, NJ, Weinheim, 2005.

[9] Philippe Gaborit. Shorter keys for code based cryptography. In *WCC 2005, Oyvind Ytrehus, Springer, Lecture Notes Computer Science, volume 3969*, pages 81–90, 2005.

[10] Marco Baldi and Franco Chiaraluce. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. pages 2591–2595, 2007.

[11] T. R. N. Rao. Joint encryption and error correction schemes. In *ISCA*, pages 240–241. ACM, 1984.

[12] T. R. N. Rao and K. H. Nam. Private-key algebraic-coded cryptosystems. In *Proceedings on Advances in cryptology—CRYPTO '86*, pages 35–48, London, UK, UK, 1987. Springer-Verlag.

[13] P. J. M. Hin. *Channel-error-correcting privacy cryptosystems*. Delft University of Technology, 1986.

[14] E. F. Brickell and A. M. Odlyzko. *Cryptanalysis: A Survey of Recent Results*. IEEE Proceedings. IEEE, 1988.

[15] A. Payandeh. Adaptive secure channel coding based on punctured turbo codes. *IEE Proceedings - Communications*, 153(2):313–316, April 2006.

[16] S. A. Barbulescu. Secure satellite communications and turbo-like codes. In *Proc. 3rd Int. Symp. Turbo Codes, ISTC 2003, Brest, France*, pages 227–230, 2003.

[17] A. A. Sobhi Afshar, T. Eghlidos, and M. R. Aref. Efficient secure channel coding based on quasi-cyclic low-density parity-check codes. *Communications, IET*, 3(2):279–292, 2009.

[18] C. Monico, J. Rosenthal, and A. Shokrollahi. Using low density parity check codes in the mceliece cryptosystem. In *Information Theory, 2000. Proceedings. IEEE International Symposium on*, pages 215–, 2000.

[19] M. Baldi, F. Chiaraluce, R. Garello, and F. Mininni. Quasi-cyclic low-density parity-check codes in the mceliece cryptosystem. In *Communications, 2007. ICC '07. IEEE International Conference on*, pages 951–956, 2007.

[20] Marco Baldi, Marco Bianchi, and Franco Chiaraluce. Optimization of the parity-check matrix density in qc-ldpc code-based mceliece cryptosystems. In *Communications Workshops (ICC), 2013 IEEE International Conference on*, pages 707–711. IEEE, 2013.

[21] K. Bagheri, M. R. Sadeghi, T. Eghlidos, and D. Panario. A secret key encryption scheme based on 1-level qc-ldpc lattices. In *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, pages 20–25, Sept 2016.

[22] Morteza Esmaeili, Mohammad Dakhilalian, and T. Aaron Gulliver. New secure channel coding scheme based on randomly punctured quasi-cyclic-low density parity check codes. *IET Communications*, 8(14):2556–2562, 2014.

[23] Morteza Esmaeili and T. Aaron Gulliver. Joint channel coding-cryptography based on random insertions and deletions in quasi-cyclic-low-density parity check codes. *IET Communications*, 9(12):1555–1560, 2015.

[24] Reza Hooshmand, Mohammad Reza Aref, and Taraneh Eghlidos. Secret key cryptosystem based on non-systematic polar codes. *Wireless Personal Communications*, 84(2):1345–1373, 2015.

[25] E. Arikan. Channel polarization: A method for constructing capacity-achieving codes. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 1173–1177, 2008.

[26] E. Sasoglu, I. E. Telatar, and E. Arikan. Polarization for arbitrary discrete memoryless channels. In *Information Theory Workshop, 2009. ITW 2009. IEEE*, pages 144–148, 2009.

[27] A. G. Sahebi and S. S. Pradhan. Multilevel polarization of polar codes over arbitrary discrete memoryless channels. *CoRR*, abs/1107.1535, 2011.

[28] R. Mori and T. Tanaka. Channel polarization

on q-ary discrete memoryless channels by arbitrary kernels. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 894–898, 2010.

[29] E. Arikan. Source polarization. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 899–903, 2010.

[30] Satish Babu Korada. *Polar codes for channel and source coding*. PhD thesis, IC, Lausanne, 2009.

[31] S. B. Korada and R. L. Urbanke. Polar codes are optimal for lossy source coding. *Information Theory, IEEE Transactions on*, 56(4):1751–1768, 2010.

[32] C. E. Shannon. A mathematical theory of communication. *Bell system technical journal*, 27, 1948.

[33] Erdal Arikan. Channel combining and splitting for cutoff rate improvement. *CoRR*, abs/cs/0508034, 2005.

[34] I. Reed. A class of multiple-error-correcting codes and the decoding scheme. *IRE Transactions on Information Theory*, 4(4):38–49, September 1954.

[35] D. E Muller. Application of boolean algebra to switching circuit design and to error correction. *IRE Transactions on Electronic Computers*, 3(3):6–12, 1954.

[36] E. Arikan, H. Kim, U. Markarian, Ozgur, and E. Poyraz. Performance of short polar codes under ml decoding. In *Proceeding of ICT-MobileSummit Conference, Santander, Spain, 2009*, 2009.

[37] CCSDS. TM synchronization and channel coding, Recommendation for Space Data System-Standards. Technical report, Washington, DC, Blue Book, 2003.

[38] E. Arikan and I. E. Telatar. On the rate of channel polarization. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 1493–1495, 2009.

[39] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory 2nd Edition (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, July 2006.

[40] S. B. Korada, A. Montanari, I. E. Telatar, and R. Urbanke. An empirical scaling law for polar codes. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 884–888, 2010.

[41] S. H. Hassani, K. Alishahi, and R. Urbanke. On the scaling of polar codes: Ii. the behavior of un-polarized channels. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 879–883, 2010.

[42] René Struik and Johan van Tilburg. The rao-nam scheme is insecure against a chosen-plaintext attack. In *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, CRYPTO '87, pages 445–457, London, UK, UK, 1988. Springer-Verlag.

[43] I. Barbero and O. Ytrehus. Modifications of the rao-nam cryptosystem. In *Coding Theory, Cryptography and Related Areas*, pages 1–12. Springer Berlin Heidelberg, 2000.

Behnam Mafakheri received the B.S. and M.S. (First-Class Hons.) degrees from the Department of Electrical Engineering, Sharif University of Technology, in 2011 and 2013, respectively. Since 2014, he is a Ph.D. student at Sharif University of Technology. Prior to his Ph.D. study, he was with Kurdistan University as a lecturer. His research interest lies in post quantum cryptography including code based and lattice based cryptography, information theory and wireless energy harvesting.

Taraneh Eghlidos received her B.S. degree in Mathematics in 1986, from the University of Shahid Beheshti, Tehran, Iran, and the M.S. degree in Industrial Mathematics in 1991 from the University of Kaiserslautern, Germany. She received her Ph.D. degree in Mathematics in 2000, from the University of Giessen, Germany. She joined the Sharif University of Technology in 2002 and she is currently an associate professor in the Electronics Research Institute of Sharif University of Technology. Her research interests include interdisciplinary research areas such as symmetric and asymmetric cryptography, application of coding theory in cryptography, and mathematical modelling for representing and solving real world problems. Her current research interests include lattice based cryptography and code based cryptography.

Hossein Pilaram received his B.S. degree in Electrical Engineering and the M.S. degree in Communication Systems from the Sharif University of Technology, Tehran, Iran, in 2010 and 2012, respectively. He is currently working on his Ph.D. dissertation at the Department of Electrical Engineering of Sharif University of Technology. His research interests are cryptography, coding theory, and mobile networks.