Secure Channel Coding Schemes based on Polar Codes

Behnam Mafakheri, Taraneh Eghlidos, and Hossein Pilaram

Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran
mafakheri/h_pilaram@ee.sharif.edu,teghlidos@sharif.edu

Abstract. In this paper, we propose two new frameworks for joint encryption encoding schemes based on polar codes, namely efficient and secure joint secret/public key encryption channel coding schemes. The issue of using new coding structure, i.e. polar codes in McEliece-like and RN-like schemes is addressed. Cryptanalysis methods show that the proposed schemes have an acceptable level of security with a relatively smaller key size in comparison with the previous works. The results indicate that both schemes provide an efficient error performance and benefit from the higher code rate which can approach to the channel capacity for large enough polar codes. The resulted characteristics of the proposed schemes make them suitable for high-speed communications, such as deep space communication systems.

Keywords: Joint encryption encoding scheme, McEliece cryptosystem, Polar Code.

1 Introduction

The main challenges of satellite communications are in short security, error performance, energy efficiency and implementation costs. A solution to the shortcomings rised 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 low code rate, this cryptosystem is not used widely. For removing these two imperfections in McEliece cryptosystem, several modifications [6, 7], and [8–10] were presented.

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 Density Parity Chack (LDPC) codes in the McEliece-cryptosystem [10, 17, 23, 24].

Polar codes 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, first we slightly modify the secure channel coding scheme proposed in [17] using polar codes. This scheme is designed so that it is 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. The proposed scheme avoids the weaknesses of Rao-Nam (RN) scheme. Furthermore, we introduce a new public-key cryptosystem based on polar codes. This scheme uses the properties of polar codes, which is more efficient than the previously used LDPC codes. We discuss about the security and efficiency of this scheme and observe that the proposed scheme meets our expectations. The main problem of the previously proposed public-key schemes is the large public-key size, which makes them impractical. The proposed scheme solves this problem by adding randomly an additional row vector to the square generator matrix of the code, which results in a block diagonal matrix as the public key and consequently needs less memory space to store it. Moreover, we show that for any choice of the public key, there is a nonsingular scrambler matrix as a part of the private key of this scheme. On the other hand, the code rate of the proposed public key scheme is close to the channel capacity, and still we have a reliable communication.

The rest of this paper is organized as follows: In Section 2 we recall the basic polar code construction. The new symmetric and public-key cryptosystems based on polar codes are addressed in Section 3. Section 4 deals with the security and efficiency of the proposed schemes. Finally, Section 5 concludes the paper.

2 Introduction to Polar Codes

In [18] 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 that 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 large, for all but a vanishing subset of indices i the symmetric capacity terms $I(W_N^{(i)})$ tend towards 0 or 1 [19]. 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 $W_N : X^N \rightarrow Y^N$, where $N = 2^n$. Figure 1 shows how to construct the channel W_2 with the probability of

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

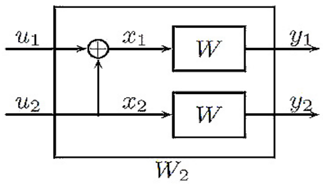

Fig. 1. The Channel W_2

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 reverse shuffle operation, which converts its inputs s_1^N to $v_1^N = (s_1, s_3, ..., s_{N-1}, s_2, s_4, ..., s_N)$. Actually, polar code is similar to Reed-Muller (RM) code which is a class of linear codes [20, 21].

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

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

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 $i \in 1, 2, ..., N$ 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 $A_N \subset 1, ..., N$, $N \in 1, 2, ..., 2^n, ...,$ 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 $W_N^{(i)}$.

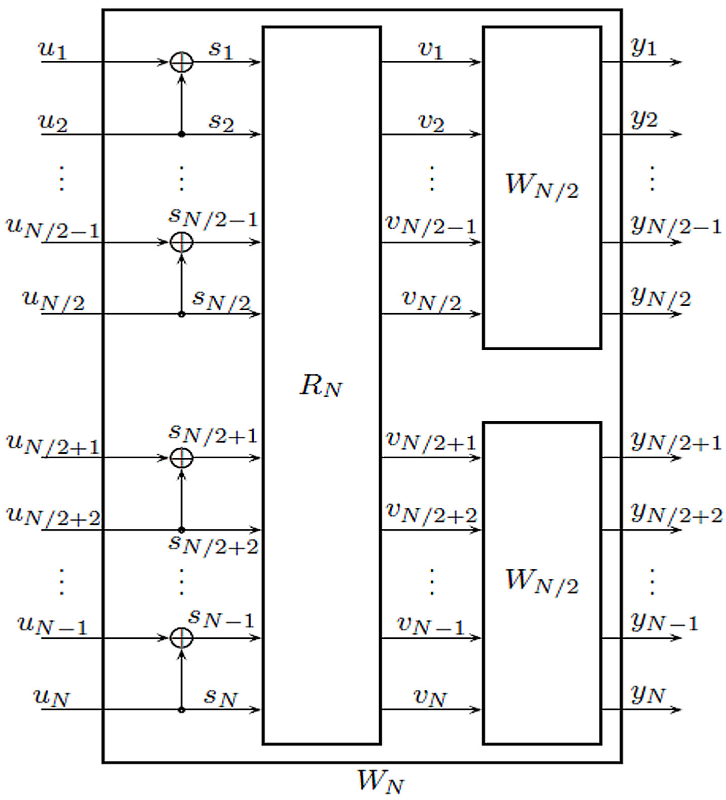

Fig. 2. Recursive construction of W_N from two copies of $W_{N/2}$

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 near 0 or equivalently $I(W_N^{(i)})$ is near 1.

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

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

where G_N is the generator matrix and A is a K-element subset of $\{1, 2, ..., N\}$. By fixing the index set A, pointing the information set, and u_{A^c}(frozen bits), 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.

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 [22, 25]. The SC decoder generates $\hat{u}_1^N$ by computing

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

where

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

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:

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

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 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 $O(NlogN)$. So, 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 New Schemes Based on Polar Codes

In this section, we first introduce our proposed secure channel coding scheme and then, we modify the design to obtain the proposed public key scheme.

3.1 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 binary symmetric channel. For this purpose we construct the generator matrix of length N for encoding purpose. Then we select the indices of bad channels and choose the frozen bits randomly. 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, according to the coding rate and keep them secret. Even though by this construction we distance from the channel capacity to some extent, we obtain a more reliable communication as it will be discussed in section 4.1.

Encryption-Encoding For our secure channel coding scheme, 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 polar code.

Decryption-Decoding The legal receiver receives the following vector

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

Using secret key P, e_s, u_{A^c}, v_s he can decrypt it 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 (11) and obtain $mG + e_{ch}P^{-1}$.

3. Decode using u_{A^c} and v_s to recover m.

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 introduce a public key scheme based on polar codes using a similar framework.

3.2 Public key Scheme

In satellite communication, there is a ground station that chooses public and private keys for secure communication. In our scheme, the ground station chooses a random matrix $K_{(N+1)\times N}$ as its public key, constructed by a random submatrix $\kappa_{l\times l}$ and a random row vector $\kappa'_{1\times N}$ as below

$$\begin{pmatrix} \kappa_{l\times l} & 0 & \dots & 0 \\ 0 & \kappa_{l\times l} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \kappa_{l\times l} \\ & \kappa'_{1\times N} & & \end{pmatrix} \tag{12}$$

where l is a divisor of N. The other components of the proposed scheme consist of a random permutation matrix P similar to the previous scheme and a random nonsingular matrix $S_{(N+1)\times(N+1)}$. Thus, the ground station chooses private and public keys according to the following algorithm:

1. Randomly select submatrices $\kappa_{l_2\times l_2}$ and $\pi_{l_2\times l_2}$.
2. Add a random row vector g_s to the generator matrix of the polar code $G'_{N\times N}$ and construct $G_{(N+1)\times N}$ as follows:

$$G = \begin{pmatrix} G' \\ g_s \end{pmatrix} \tag{13}$$

3. Select one of the solutions of the equation

$$K_{(N+1)\times N} = S_{(N+1)\times(N+1)} G_{(N+1)\times N} P_{N\times N} \tag{14}$$

and compute a nonsingular matrix S which is described subsequently. Now, the ground station releases $K_{(N+1)\times N}$ as its public key and keeps S, P and g_s as its private keys. In the following we give a method to compute S.

Computation of Scrambler matrix Here, we propose a method based on linear algebra for computing the nonsingular matrix S. The problem is to find $(N+1)\times(N+1)$ unknown elements of the matrix S in the $(N+1)\times N$ equations obtained from the Equation (14). We have:

$$KP^{-1} = SG \Longleftrightarrow (KP^{-1})^T = G^T S^T. \tag{15}$$

In this relation, the number of unknown variables is more than the number of equations and knowing G is full rank. From linear algebra, this equation is always consistent, however, Equation (15) has not unique solution, so we choose matrix S as follows,

$$S = \left(S' | e_{N+1}^T\right) \tag{16}$$

where $e_{N+1} = (0, ..., 0, 1)_{1\times N+1}$ and from Equation (15) we obtain

$$\left(G'^T | \;\; g_s^T\right) \begin{pmatrix} S'^T \\ e_{N+1} \end{pmatrix} = (KP^{-1})^T \triangleq K'^T \tag{17}$$

Equation 17 implies

$$G'^T S'^T + g_s^T e_{N+1} = K'^T, \tag{18}$$

then

$$S'^T = (G'^T)^{-1}(K'^T - g_s^T e_{N+1}) \tag{19}$$

The matrix S has to be nonsingular. The following statement gives the nonsingularity condition for S.

Proposition 1: The matrix S is nonsingular if and only if the submatrix $\kappa_{l_2 \times l_2}$ is nonsingular.

Proof: Let S be defined as follows:

$$S = \begin{pmatrix} S''_{N\times N} & 0_{N\times 1} \\ s_{1\times N} & 1 \end{pmatrix} \tag{20}$$

Form this and Equation (18) we have:

$$G'^T \left(S''^T | \ \ s^T \right) = K'^T - g_s^T e_{N+1} \tag{21}$$

Where $g_s^T e_{N+1}$ is a matrix whose (N+1)th column is equal to g_s^T and the remaining entries are zero. By taking a look at the first N columns of both sides of Equation (21), we have

$$G'^T S'^T = (K'^T)_1^N \Longleftrightarrow S''^T = (G'^T)^{-1}(K'^T)_1^N, \tag{22}$$

where $(K'^T)_1^N$ denotes the first N columns of K'^T. Consequently, for nonsingularity of S'', both matrices $(G'^T)^{-1}$ and $(K'^T)_1^N$ should be nonsingular. Nonsingularity of G' is obvious due to the definition of the polar code. In order $(K'^T)_1^N$ to be nonsingular, the first N rows of K' are to be linearly independent. In addition, we have

$$K' = KP^{-1} = KP^T \tag{23}$$

From Equation 23 it is obvious that the first N rows of matrix K should be nonsingular, for P is a permutation matrix. from Equation 12, we conclude that the submatrix $\kappa_{l_2 \times l_2}$ ought to be nonsingular.

Thus far, we have obtained K' as the public key and $\{S, P, g_s\}$ as the private keys. Below, we explain the encryption and decryption method of our proposed scheme.

Encryption For data encryption, the sender first pads the message m by one bit as follows,

$$m' = (m_1, m_2, ..., m_N) = (m, 1) \tag{24}$$

So the length of the code is $N + 1$. Note that, in the encoding phase, the sender sets all frozen bits to be zero and computes

$$c = m'K + z \tag{25}$$

where K is the public key and z is an error vector with Hamming weight less than the error correction capability of polar codes for this channel. then he sends c through the channel.

Decryption The legal receiver receives $c = m'K + z = m'SGP + z$ and compute m in the following steps:

1. Multiply both sides of Equation (25) by P^{-1} and obtain $c' = cP^{-1} = m'SG + zP^{-1}$

2. Add g_s from c' and compute c'' as follows:

$$c'' = c' + g_s \tag{26}$$

3. Decode c'' using frozen bits and the fixed bits and recover $\tilde{m} = mS'' + s$.

4. Add s to $\tilde{m}$ and obtain mS'' .

5. Multiply mS'' by $(S'')^{-1}$ to obtain m.

Corectness: In the following, we show that the decryption algorithm works. In step 1, we have

$$\begin{aligned} c' = cP^{-1} = m'SG + zP^{-1} &= (m_{N\times 1}, 1) \begin{pmatrix} S''_{N\times N} & 0_{N\times 1} \\ s_{1\times N} & 1 \end{pmatrix} \begin{pmatrix} G'_{N\times N} \\ g_s \end{pmatrix} + zP^{-1} \\ &= (mS'' + s, 1) \begin{pmatrix} G'_{N\times N} \\ g_s \end{pmatrix} + zP^{-1} = (mS'' + s)G' + g_s + zP^{-1} \end{aligned} \tag{27}$$

In step 2, we have

$$c'' = c' + g_s = (mS'' + s)G' + g_s + zP^{-1} + g_s = (mS'' + s)G' + zP^{-1} \tag{28}$$

In step 3 it is obvious that by decoding c'' we can recover $\tilde{m} = mS'' + s$. From step 4 we have

$$\tilde{m} + s = mS'' + s + s = mS'' \tag{29}$$

In step 5 we have

$$mS''(S'')^{-1} = m \tag{30}$$

4 Efficiency and Security

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

4.1 Efficiency

The efficiency of the proposed schemes is discussed from the viewpoints of complexity, bit error rate, code rate and key size.

complexity Here, we discuss the implementation complexity of the two proposed schemes. Since for satellite communication we use codes with large block lengths [32], we should give evidence for applicability of our schemes in low complexity.

Symmetric scheme: In the symmetric case, there is no precomputation phase, and 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 complexity have the same order $O(NlogN)$. We observe that the complexity of the proposed scheme is low, which is indeed more desirable for satellite communications.

Asymmetric scheme: In the case of public key scheme, the precomputation phase includes three parts: Construction of generator matrix, computation of nonsingular matrix S and computing the inverse of matrix S''. As it was stated, constructing the generator matrix for polar codes has the complexity order of $O(NlogN)$, where N is the block length. The computational load of obtaining matrix S from Equation (19) is inefficient, because of imposing the computation of G'^{-1}, where G' is the generator matrix of polar codes. Note that the computation of matrix S is done offline in the ground station and it is not changed as long as the secret key (K) is not changed. Also, nonsingularity of matrix S should be confirmed. However from Proposition (1), the nonsingularity of the submatrix $\kappa_{l_2 \times l_2}$ implies that of the matrix S. So, the matrix $\kappa_{l_2 \times l_2}$ should be chosen in such a way to make sure that it is nonsingular. For example, it can be chosen as an upper or lower triangular matrix, then it is not necessary to check the nonsingularity of matrix S. Finally, computing the inverse of nonsingular matrix S'' is also done offline in the ground station.

In the computation phase, the complexity consists of two parts: Encryption and decryption. As it is mentioned before, the order of Complexity for both parts is $O(NlogN)$. Notice that, in the decryption phase of section (3.2), the fifth step is just a matrix multiplication and does not contain the complexity of computing the matrix inversion, because the inverse of S'' is computed just once and stored.

Error Performance As it is mentioned in section 2, polar codes provably achieve the capacity of the channel. In [33] 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 N large enough. Another problem is to determine the trade-off between the rate and block length for a given error probability when we use successive cancellation decoder. In our schemes, because of the finite length of 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 [34], Thus, from [25] we know that the number of frozen bits is approximately equal to 21 bits, but in this rate, we have not reliable communications. So, the rate should be reduced to obtain reliability. In [35,36] authors showed that for any BEC, W, with capacity $I(W)$, reliable communication requires the rates that satisfy the following inequality:

$$R < I(W) - N^{-\frac{1}{\mu}} \tag{31}$$

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

$$N > (\frac{1}{I(W) - R})^{\mu} \tag{32}$$

In the proposed schemes, to make a comparison with the results obtained in other publications, the block length is considered to be 2048. Therefore from Equation (31), if the coding rate is lower than 0.87, a reliable communication is achieved. Figure 3 shows the rate vs. reliability trade off for W using polar codes with $N = 2048$. It should be noted that, from this we can conclude that the number of fixed bits is approximately equal to $((I(W) - R) \times N) \approx 245$.

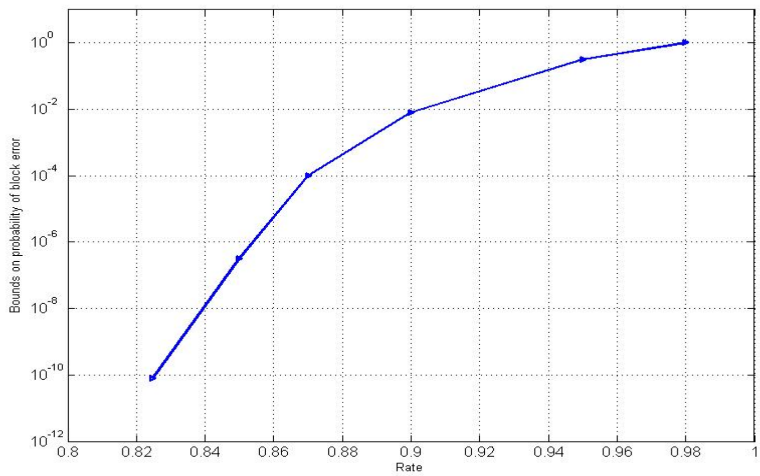

Fig. 3. Rate vs. reliability for polar coding and SC decoding at block-lengths $N = 2^{11}$

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 [37]	C(72,64)	0.89
Barbero-Ytrehus [38]	C(30,20) over GF(2^8)	0.66
SobliAfshar-Eghlidos [17]	C(2044,1024)	0.5
Baldi-Chiarluce [24]	C(8000, 6000, 40)	0.75
Proposed Scheme	C(2048, 1781)	0.87

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

Symmetric Scheme In the proposed symmetric scheme, 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 sections 2 and 4.1, the number of frozen bits depends on the channel capacity which in our scheme $(|u_{A^c}|+|v_s|) = 21+245 =$ 266bits, 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 [38]. 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 380 bits [38].

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 should be at least 1024 bits. These yield the total secret key size of $1670bits \approx 1.6Kbits$ to be exchanged. 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 [37]	C(72,64)	18Kbits
Barbero-Ytrehus [38]	C(30,20) over GF(2^8)	4.9Kbits
SobliAfshar-Eghlidos [17]	C(2044,1024)	2.5Kbits
Proposed Scheme	C(2048, 1781)	1.6Kbits

Public Key Scheme In the proposed public key scheme, as it was mentioned in Section 3.2 the public key $K_{(N+1)\times N}$ is constructed by the submatrix $\kappa_{l_2\times l_2}$ and a random row vector $\kappa'_{1\times N}$. So, it is enough to store these two arrays as the public key. For example, if we choose $l_2 = 128$, we need $128 \times 128 + 2048 =$ $18432bits = 2304bytes$ to store the public key of the proposed scheme. Note that we could choose $l_2 = 64$ or $l_2 = 32$ to have shorter keys and still have secure scheme. The security of the scheme is discussed in Section 4.2. It is known that the main weakness of the McEliece public-key scheme is the large size of the public-key. A comparison between the key sizes of the proposed scheme and the previous McEliece-like cryptosystems is given in Table 3. The results show that the key sizes of the proposed schemes are reduced to a more reasonable value.

Table 3. Key size of the new scheme compared with other McEliece-like schemes

Scheme	Code	Key Size (Bytes)
McEliece [2]	C(1024,524)	67072
Niederreiter [4]	C(1024, 524)	32750
Baldi (1) [39]	C(16384, 12288)	6144
Baldi (2) [39]	C(24576, 16384)	6144
Baldi (3) [39]	C(49152, 32768)	12288
Propose Scheme (1)	C(2048, 1781), $l_2 = 128$	2304
Propose Scheme (2)	C(2048, 1781), $l_2 = 64$	768
Propose Scheme (1)	C(2048, 1781), $l_2 = 32$	384

It is noteworthy by increasing the code length N, not only the key size of the proposed schemes remains constant, but also the security of the scheme increases. So, from Equation 31 one concludes that by increasing the code length, the code rate can be increased without any change in the key size. As it was stated previously, this property is much more interested in satellite communications.

4.2 Security

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

Symmetric Key Scheme Here, we discuss the security of the proposed symmetric key scheme against brute force attack, RN attack and Struik-Tilburg attack.

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. So, the attacker should 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. So, 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 are a large number of non-zero vectors (i.e. $2^N - 1$), 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. So, choosing each of the values for l makes the computation impractical. Therefore, one can choose $l = 32$, to reduce the key size.

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 that showed the RN scheme is insecure [37]. 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, so that such an attack is not practical.

Public Key Scheme Now, we discuss the security of the proposed public key scheme. Because of the special features of this scheme, any of the previously known attacks cannot directly be applied to it. In the following, we are going to apply some modified versions of these attacks to the proposed scheme and evaluate its security.

Brute Force Attack: The private key of the proposed scheme consists of three parts: A row vector , a permutation matrix and a scrambler matrix $S_{(N+1)\times(N+1)}$. To compute each part, the attacker faces the following computational complexities:

1. The row vector g_s has N entries. So, there are 2^N such vectors. Because of the large code length, this indicates an impractical preliminary work for an attacker.

2. The number of block diagonal permutation matrices $P_{N\times N}$ for $l_2 = 128$, $l_2 = 64$, and $l_2 = 32$ is factorially large which makes the computation of such matrix infeasible.

3. The number of nonsingular scrambling matrices $S_{(N+1)\times(N+1)}$, N_S, as Equation 20, is given below [12]

$$\begin{aligned} N_S = \prod_{i=0}^{N-1} (2^N - 2^i) + 2^N &> (2^N - 1)(2^N - 2)...(2^N - 2^{N-1}) \\ &> (2^{N-1}).(2^{N-1})....(2^{N-1}) = 2^{(N-1)N} = 2^{N^2-N} \end{aligned} \tag{33}$$

In our scheme, the number of nonsingular scrambling matrices with $N = 2048$ is huge, which indicates that finding the scrambling matrix is infeasible in practice.

Information Set Decoding Attack: This attack was proposed by McEliece in his original work [2]. Lee and Brickell in [40] systemized and generalized it. We begin with presenting the idea of this attack. Assume we are given a generator matrix G of a linear (N, k)-code and a ciphertext $c = mG + e$. Let

$J \subset \{1, 2, ..., N\}$ with $|J| = k = dimG$. We denote k columns of G, c and e by G_J, c_J and e_J, respectively. So, the following relationship holds:

$$c_J = mG_J + e_J \tag{34}$$

If G_J is nonsingular and e_J, then

$$m = c_J(G_J)^{-1} \tag{35}$$

Because of the special form of the generator matrix of our scheme, it can easily be seen that this attack cannot be applied to it. However, Let $I \subset \{1, 2, ..., N\}$ with $|I| = k = NR$, where R denotes the code rate and I is the set of indices of good channels. We assume that the attacker knows the channel and hence he knows the set J. Now, we can apply the attack to our scheme. We estimate the work factor of this attack. The number of sets such that there are no errors in vector is at least:

$$\binom{N-t}{k} = \binom{N-t}{NR} \approxeq \binom{2020}{1781} \gg 2^{1000}, \tag{36}$$

where t is the Hamming weight of the error vector. This denotes an impractical work factor.

5 Conclusions

In this paper, we have proposed two new schemes based on polar codes: A symmetric-key secure channel coding scheme and a public-key scheme. The symmetric case 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 and it is concluded that the proposed scheme is secure and more efficient than the previous schemes. The proposed public-key scheme is a McEliece-like scheme and make use of polar codes by adding randomly an additional row vector to the generator matrix of polar code as the new generator matrix, and choosing a private permutation (P) and a public key (K) matrices in block diagonal form, we obtain the nonsingular scrambler matrix as a part of the private key. Because of the specific structure of this scheme, we could reduce the size of the public key which is the lowest value published so far.

The new schemes employ polar codes based on the following four reasons: (1) Polar codes can achieve the channel capacity, (2) the performance of the codes become better in large block lengths which is desirable for satellite communications, (3) the total complexity of encoding and decoding of the codes is low in comparison to the previously used codes, (4) the specific structure of the generator matrix of polar codes makes it possible to have a small key size to be exchanged.

References

1. C. N. MATHUR, "A mathematical framework for combining error correction and encryption" PhD thesis, Department of Electrical and Computer Engineering, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ, USA, 2007.
2. R. J. MCELIECE, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report, pp. 114116, 1978.
3. E. BERLEKAMP, R. MCELIECE, and H. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Trans. Inform. Theory, vol. 24, pp. 384386, May 1978.
4. H. NIEDERREITER, "Knapsack-type cryptosystems and algebraic coding theory," Probl. Contr. and Inform. Theory, vol. 15, pp. 159166, 1986.
5. GOLDWASSER S., MICALI S, "Probabilistic encryption and how to play mental poker keeping secret all partial information," Proc. 14th ACM Symp. Theory of Computing, 1982, pp. 270299
6. PARK C.S, "Improving code rate of McElieces public-key cryptosystem, " Electron. Lett, 1989, 25, (21), pp. 14661467
7. LIN M.C., FU H.L., "Information rate of McElieces public-key cryptosystem," Electron. Lett, 1990, 26, (1), pp. 1618
8. KABATIANSKY G., KROUK E., SEMENOV .S, "Error correcting coding and security for data networks," (John Wiley Sons Ltd., 2005)
9. GABORIT P., "Shorter keys for code based cryptography," Proc. CLC2006, Technische Universitat Darmstadt, September 2006
10. BALDI M., CHIARALUCE F., "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes," Proc. IEEE Int. Symp. Information Theory 2007, Nice, France, June 2007, pp. 25912595
11. RAO T.N.R., "Joint encryption and error correction schemes, " Proc. 11th annual Int. symposium on Computer architecture, Ann Arbor, Mich., pp. 240241
12. RAO T.N.R., NAM K.H., "A private-key algebraic-coded cryptosystem," Proc. Crypto86, 1986, pp. 3548
13. HIN P.J.M., "Channel-error-correcting privacy cryptosystems," PhD, dissertation (in Dutch), Delft University of Technology, 1986
14. BRICKELL E.F., ODLYZKO A., "Cryptanalysis: a survey of recent results, " Proc. IEEE, 1988, 76, (5), pp. 153165
15. PAYANDEH A., AHMADIAN M., AREF M.R., "Adaptive secure channel coding based on punctured turbo codes," IEE Proc. Commun., 2006, 153, (2), pp. 313316
16. BARBULESCU S.A., "Secure satellite communications and turbo-like codes," In JAGO, C., AMIS, K., BERROU, C. (EDS.), Proc. 3rd Int. Symp. Turbo Codes, ISTC 2003, Brest, France, 2003, pp. 227230,
17. A. A. SOBHI AFSHAR, T. EGHLIDOS, and M. R. AREF, "Efficient secure channel coding based on quasi-cyclic low-density parity-check codes," Journal of IET-Communications, 3(2):279-292, 2009.
18. SHANON, C.E., "A mathematical theory of communication," Bell System Tech. J. 27(2), 379 423, 623656 (1948)
19. E. ARIKAN, "Channel Combining and Splitting for Cutoff Rate Improvement," IEEE Trans. Inform. Theory, Vol.52, No.2, February 2006.
20. REED, I. ,"A class of multiple-error-correcting codes and the decoding scheme," IRE Trans. Inform. Theory 4(4), 3944 (1954)
21. MULLER, D.E.,"Application of boolean algebra to switching circuit design and to error correction," IRE Trans. Electronic Computers EC-3, 612 (1954)

22. E. ARIKAN, H. KIM, G. Markarian, U. Ozgur, E. Poyraz, Performance of Short Polar Codes Under ML Decoding, Proceeding of ICT-MobileSummit Conference, Santander, Spain, June 2009.
23. MONICO C., ROSENTHAL J., SHOKROLLAHI A., "Using low density parity check codes in the McEliece cryptosystem," Proc. IEEE Int. Symp. Information Theory, Italy, June 2000, p. 215
24. BALDI M., CHIARALUCE F., GARELLO R., MININNI F., "Quasi-cyclic LDPC codes in the McEliece cryptosystem," Proc. IEEE Int. Conf. Communications 2007, Glasgow, UK, June 2007, pp. 951956
25. E. ARIKAN, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," IEEE Trans. Inf. Theory, vol. 55, no. 7, pp. 30513073, Jul. 2009.
26. E. SASOGLU, E. TELATAR, and E. ARIKAN, "Polarization for arbitrary discrete memoryless channels," in Proc. 2009 IEEE Information Theory Workshop, Taormina, Italy, 1116 Oct. 2009, pp. 144148.
27. AREA G. SAHEBI and S. SANDEEP PARDHAN, "Multilevel polarization of polar codes over arbitrary discrete memoryless channels," 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton) , 17181725 (2011).
28. R. MORI and T. TANAKA, "Channel Polarization on q-ary Discrete Memoryless Channels by Arbitrary Kernels," Proc. IEEE Int. Symp. Information Theory, 2010, Austin, TX.
29. E. ARIKAN, "Source polarization," Proc. IEEE Int. Symp. Inform. Theory, Austin, 2010.
30. S. B. KORADA, "Polar codes for channel and source coding," Ph.D. dissertation, Ecole Polytechnique Federale de Lausanne, July 2009.
31. S. B. KORADA and R. L. URBANKE, "Polar codes are optimal for lossy source coding," IEEE Transactions on Information Theory, vol. 56, pp. 17511768, April 2010.
32. CCSDS 131.0-B-1, "TM synchronization and channel coding, Recommendation for Space Data SystemStandards," CCSDS, Washington, DC, 2003, Blue Book, Issue 1
33. E. ARIKAN and E. TELATAR, "On the rate of channel polarization," in Proc. of the IEEE Int. Symposium on Inform. Theory, Seoul, South Korea, July 2009, pp. 14931495.
34. T. M. COVER and J. A. THOMAS, "Elements of Information Theory," New York: Wiley, 1991.
35. S. B. KORADA, A. MONTANARI, E. TELATAR and R. URBANKE , "An emprical scaling law for polar codes," in Proc. ISIT (2010), pp.884-888.
36. S. H. HASSANI, K. ALISHAHI and R. URBANKE, "On the scaling of Polar codes: II. The behavior of un-polarized channels," in Proc. ISIT (2010), pp.879-883
37. STRUIK R., TILBURG J., "The RaoNam scheme is insecure against a chosen-plaintext attack," Advances in Cryptology, Crypto87, 1988, (LNCS), pp. 445457
38. BARBERO A.I., YTREHUS O., "Modifications of the RaoNam cryptosystem," Proc. Int. Conf. Coding Theory Cryptography and Related Areas, Guanajuato, Mexico, 1998, pp. 113
39. M. BALDI, "LDPC codes in the McEliece cryptosystem: attacks and countermeasures," ser. NATO Science for Peace and Security Series - D: Information and Communication Security. IOS Press, 2009, vol. 23, pp. 160174.
40. P. J. LEE, E. F. BRICKELL, "An observation on the security of McEliece's public key cryptosystem," In Advances in Cryptology-EUROCRYPT'88, volume 330 of LNCS, pp 275-280. Springer Verlag, 1989.

41. BALDI M., CHIARALUCE F., GARELLO R., MININNI F., "Quasi-cyclic LDPC codes in the McEliece cryptosystem," Proc. IEEE Int. Conf. Communications 2007, Glasgow, UK, June 2007, pp. 951956

Appendix: Springer-Author Discount

LNCS authors are entitled to a 33.3% discount off all Springer publications. Before placing an order, the author should send an email, giving full details of his or her Springer publication, to `orders-HD-individuals@springer.com` to obtain a so-called token. This token is a number, which must be entered when placing an order via the Internet, in order to obtain the discount.

6 Checklist of Items to be Sent to Volume Editors

Here is a checklist of everything the volume editor requires from you:

- [ ] The final LaTeX source files
- [ ] A final PDF file
- [ ] A copyright form, signed by one author on behalf of all of the authors of the paper.
- [ ] A readme giving the name and email address of the corresponding author.