The ISC Int'l Journal of Information Security

January 2012, Volume 4, Number 1 (pp. 1–12)

http://www.isecure-journal.org

Improving the Rao-Nam Secret Key Cryptosystem Using Regular EDF-QC-LDPC Codes

Reza Hooshmand [1,2,*], Taraneh Eghlidos [3], and Mohammad Reza Aref [2]

[1] *Faculty of Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran*

[2] *Information System and Security Lab, Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran*

[3] *Electronics Research Institute, Sharif University of Technology, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 3 December 2011
Revised: 25 February 2012
Accepted: 26 January 2012
Published Online: 30 May 2012

Keywords:
Rao-Nam Secret Key Cryptosystem, Low-Density Parity-Check Codes, Difference Families.

ABSTRACT

This paper proposes an efficient joint secret key encryption-channel coding cryptosystem, based on regular Extended Difference Family Quasi-Cyclic Low-Density Parity-Check codes.

The key length of the proposed cryptosystem decreases up to 85 percent using a new efficient compression algorithm. Cryptanalytic methods show that the improved cryptosystem has a significant security advantage over Rao-Nam cryptosystem against chosen plaintext attacks, benefiting from an improvement on the structure of the Rao-Nam cryptosystem and proper choices of code parameters. Moreover, the proposed cryptosystem benefits from the highest code rate and a proper error performance.

1 Introduction

Security, error performance, speed, energy efficiency and implementation costs are the main challenges, facing present secure wireless communications in noisy environments. These challenges can be reduced to some extent using joint secret key encryption-channel coding scheme appropriately [1], which forms the basis of our approach. These cryptosystems provide security and reliability in one process to guarantee the confidentiality and the integrity of transmitted data. Establishing a suitable trade-off between security and efficiency is an important point in designing such cryptosystems.

In 1984, Rao proposed the first Private-key Algebraic-coded Cryptosystem (PRAC) based on (1024,524) Goppa code [2]. The idea behind this cryptosystem was based on the fact that the decoding of an arbitrary linear code is an NP-complete problem. In 1986, Rao-Nam (RN) modified Rao's cryptosystem to enable the use of simpler code and decrease the key length by a significant increase in code rate [3]. However, this cryptosystem is insecure against chosen plaintext attacks.

Some proposed modifications on RN cryptosystem are based on adopting nonlinear or linear codes or modifying the set of allowed perturbation vectors [4]. However, almost all of the proposed modification cryptosystems are either insecure or inefficient.

In recent years, *Low-Density Parity-Check* (LDPC) [5] codes gained considerable attention from researchers because of their powerful channel coding technique and proper error performance. So, it is reasonable to consider a variant of RN secret key cryptosystem based on a class of LDPC codes, namely *Extended Difference Family Quasi-Cyclic Low-Density Parity-Check* (EDF-QC-LDPC) [6] codes.

The remainder of the paper is structured as follows: section 2 recalls the construction of the RN secret key cryptosystem. Section 3 describes QC-LDPC codes

* Corresponding author.
Email addresses: r.hooshmand@srbiau.ac.ir (R. Hooshmand), teghlidos@sharif.edu (T. Eghlidos), aref@sharif.edu (M. R. Aref).

ISSN: 2008-2045

based on Extended Difference Families. The modified RN secret key cryptosystem based on regular EDF-QC-LDPC codes is presented in section 4. Section 5 deals with cryptanalysis of the proposed cryptosystem and provides insights into overcoming some of the weaknesses found in the original RN cryptosystem. Section 6 presents the key length, computational complexity and error performance of the proposed cryptosystem. Finally, section 7 concludes the paper.

2 The RN secret key cryptosystem

In the subsequent sections, we give a brief description of the RN cryptosystem [3].

2.1 Secret Key

Let $\mathcal{S}$ be a $k \times k$ nonsingular matrix, named scrambling matrix, G be a $k \times n$ generator matrix of Hamming code and $\mathcal{P}$ be an $n \times n$ permutation matrix. Construct a predetermined set of perturbation vectors (syndrome error table) that are used by the authorized sender and receiver.

2.2 Encryption

The sender encrypts plaintexts as follows,

$$\begin{aligned} c &= M\mathcal{S}G\mathcal{P} + e\,(s)\,\mathcal{P} \\ &= (M'G + e\,(s))\,\mathcal{P}, \end{aligned}$$

where M is a plaintext of length k; c is the ciphertext of length n and $e(s)$ is an error vector that is selected randomly from a syndrome error table, and has the average Hamming weight equal approximately to $n/2$. The goal of using $e(s)$ is to prevent a chosen plaintext attack by majority voting for each position of a row of the encryption matrix $G' = \mathcal{S}G\mathcal{P}$.

2.3 Decryption

The authorized receiver decrypts ciphertext c as follows:

(1) Obtains,

$$c' = c\mathcal{P}^T = M\mathcal{S}G + e(s).$$

(2) Finds the perturbation vector using the syndrome error table, and computes:

$$c'\mathcal{H}^T = M\mathcal{S}G\mathcal{H}^T + e\,(s)\,\mathcal{H}^T = e\,(s)\,\mathcal{H}^T.$$

Then recovers $M' = M\mathcal{S}$ by correcting for perturbation vectors.

(3) Finally recovers the plaintext $M = M'\mathcal{S}^{-1}$.

In this work, we consider two problems associated with RN cryptosystem; the first is how to reduce the key length. The second is how to increase the security. We solve the first problem using the new compression/decompression algorithm. Also, we deal with the second problem by applying regular EDF-QC-LDPC codes and improving the encryption/decryption algorithm.

The security of the RN cryptosystem against chosen plaintext attacks depends on the Hamming weight and the number of perturbation vectors [3]. It also appears that this approach requires long keys ($\mathcal{S}$, $\mathcal{P}$, G, and the syndrome error table).

3 QC-LDPC codes based on Extended Difference Families

QC-LDPC codes based on Extended Difference Families are an important class of structured LDPC codes that are able to join low complexity encoding of QC codes, good error performance of LDPC codes and proper characteristics of Extended Difference Families.

3.1 LDPC Codes

The LDPC codes was first discovered by Gallager in 1963 [5] and then rediscovered by Mackay and Neal in 1995 [7]. The (n, k) LDPC codes are a class of linear block code defined by a sparse parity check matrix $\mathcal{H}_{m\times n}$, where $n > m$ and $m = n - k$. The parity check matrix has ρ '1's in each row (row weight) and γ '1's in each column (column weight) such that the number of '1's in common between any two rows or columns is at most one.

The parameters ρ and γ are small compared to n and m respectively, therefore the parity check matrix has a small number of '1's compared to the dimension of the matrix, so called Low-Density Parity-Check matrix. The code specified by $\mathcal{H}$ is called an LDPC code. LDPC codes can be either *regular* or *irregular*. A regular LDPC code is one in which both ρ and γ are constant, otherwise it is called irregular.

LDPC codes are represented effectively using a bipartite graph that is also known as *Tanner* graph [8]. The nodes in a bipartite graph can be separated into two sets such that each node is connected to a node in the other set by an edge. The two sets of nodes in a Tanner graph are called *variable (bit)* nodes and *check* nodes.

Rows and columns in $\mathcal{H}$ are represented by check and variable nodes, respectively. A *cycle* in a Tanner graph is defined as a sequence of associated non-iterative edges which begins from a node and ends at the same node. The number of edges in a cycle is called the length of the cycle. The minimum cycle length of the

graph is called the *girth*. All cycles in Tanner graph have even lengths and their minimum is 4-length cycle. It is required for any LDPC code to be free of 4-length cycle in the parity check matrix or Tanner graph for having efficient decoding [9].

Based on the methods of construction, LDPC codes can be classified into two general categories: *random* and *structured* codes. Random codes are constructed by computer search based on certain design guidelines and do not have any predefined row-column parity check matrix interconnection. On the other hand, structured codes are constructed based on algebraic and combinatorial methods and have a known row-column interconnection pattern [10].

3.2 QC codes

Cyclic codes are a type of linear block codes, where shifting a codeword any number of symbol positions, either to the right or to the left, results in another codeword. *Quasi Cyclic* (QC) codes are another type of linear block codes that have partial cyclic structure, where shifting a codeword a fixed number $n_0 \neq 1$ (or a multiple of n_0) of symbol positions either to right or to the left results in another codeword. It is clear that for $n_0 = 1$, a QC code is a cyclic code [11].

A $C(mn_0, mk_0)$ QC code can be described by a parity check matrix $\mathcal{H}_{r_0 m \times n_0 m}$ that is formed by $r_0 \times n_0$ array of circulant submatrices $H_{m\times m}$, as follows,

$$\mathcal{H} = \begin{bmatrix} H_{1,1} & H_{1,2} & \dots & H_{1,n_0} \\ H_{2,1} & H_{2,2} & \dots & H_{2,n_0} \\ \vdots & \vdots & \ddots & \vdots \\ H_{r_0,1} & H_{r_0,2} & \dots & H_{r_0,n_0} \end{bmatrix}, \quad (1)$$

where, $r_0 = n_0 - k_0$ and each $H_{i,j},\ i = 1, \dots, r_0,\ j = 1, \dots, n_0$ is an $m \times m$ binary circulant submatrix over $GF(2)$ as below,

$$H_{i,j} = \begin{bmatrix} h_1 & h_2 & \cdots & h_m \\ h_m & h_1 & \cdots & h_{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_2 & h_3 & \cdots & h_1 \end{bmatrix}. \quad (2)$$

A circulant submatrix has the feature that its l^{th}, $l = 1, \cdots, m$ row is obtained through a cyclic shift by l positions of the elements of its first row. A circulant submatrix $H_{i,j}$ is completely described by the generator polynomial (3) with coefficients from its first row [12]. A code C of the form (1) is completely characterized by the generator polynomials $h_{i,j}(x), i = 1, \dots, r_0,\ j = 1, \dots, n_0$.

$$h_{i,j}(x) = h_1 + h_2 x + h_3 x^2 + \cdots + h_m x^{m-1}. \quad (3)$$

The simplest QC code is a row circulant $C(mn_0,\ m(n_0 - 1))$ code that is shown as follows,

$$\mathcal{H} = [H_1\ \ H_2\ \cdots\ H_{n_0}]. \quad (4)$$

In this case, each $H_i,\ i = 1, \dots, n_0$ is an $m \times m$ binary circulant submatrix. If H_{n_0} is nonsingular, the generator matrix G for such code can be constructed in systematic form as below,

$$G = \begin{bmatrix} & & (H_{n_0}^{-1}H_1)^T \\ I_{m(n_0-1)} & \vdots & (H_{n_0}^{-1}H_2)^T \\ & & \vdots \\ & & (H_{n_0}^{-1}H_{n_0-1})^T \end{bmatrix}. \quad (5)$$

Encoding can be achieved with linear complexity using an $(n_0 - 1)m$-stage shift register in much the same way as for cyclic codes [13].

3.3 QC-LDPC Codes

A $C(mn_0, mk_0)$ QC code is a QC-LDPC code if each $m \times m$ circulant $H_{i,j},\ i = 1, \cdots, r_0,\ j = 1, \cdots, n_0$ submatrix of its parity check matrix is sparse. For a QC-LDPC code, the property to have a Tanner graph free of 4-length cycles can be ensured through algebraic considerations, when the parity check matrix is row circulant [13].

In this paper, QC-LDPC codes with row circulant parity check matrices are used. However, applying row circulant matrices yields lack of flexibility on the code length [6]. Thus, to prevent such constraint, we use regular QC-LDPC codes based on Extended Difference Families.

3.3.1 DF-QC-LDPC codes

Definition 1. Let $F = \{D_1,\ D_2, \dots, D_{n_0}\}$ be a family of μ-subsets in an additive group of Z_m. We say that F with $D_i = \{d_{i,1}, d_{i,2}, \cdots, d_{i,\mu}\}$ is an (m, μ, λ) Difference Family, or (m, μ, λ)-DF in short, if all intraset distances shown in (6) give each nonzero element of Z_m exactly λ times, where $m \equiv 1 \pmod{\mu(\mu-1)}$ must be a prime power [14].

$$d_{i,x} - d_{i,y},\ i = 1, \dots, n_0;\ x, y = 1, \dots, \mu;\ x \neq y. \quad (6)$$

The members of a difference family are called *base blocks*. Difference families can be used to construct QC-LDPC codes. The generator polynomial of each circulant submatrix, H_i, shown in (4), is produced as equation (7), if we consider the n_0 subsets D_i being in $(m,\ \mu,\ 1)$ difference family F.

$$h_i(x) = \sum_{j=1}^{\mu} x^{d_{i,j}} = x^{d_{i,1}} + \cdots + x^{d_{i,\mu}},\ i = 1, \dots, n_0, \quad (7)$$

where $d_{i,j}$ is the j^{th} element of D_i whose dimension is μ. With this choice, the parity check matrix is regular with column Hamming weight μ and row Hamming weight $n_0\mu$ [13].

Using difference families with $\lambda = 1$, all the elements are used once, so the parity check matrix is row circulant and the resulting code has a Tanner graph free of 4-length cycles. Lower code rate DF-QC-LDPC codes are constructed, if we select fewer blocks of H_i in (4). It is always possible to design $(n_0 m, (n_0 - 1)\, m)$ regular DF-QC codes, where m is prime power as below.

$$m = n_0.\mu\,(\mu - 1) + 1.$$

The codes based on DFs have low encoding complexity and easy construction, but these codes are rather inefficient due to the restriction on the number of check equation $(m = n - k)$ in (3). For example consider a design with $\mu = 5$, Then it is required that $m = 20n_0 + 1$ be a prime power. The only integers within [100, 200] that satisfy this condition are 101, 121 and 181. So, it is not possible to design DF-QC-LDPC codes with a different number of check equations than these integers [6].

3.3.2 EDF-QC-LDPC Codes

Definition 2. Let $F = \{D_1, D_2, \ldots, D_{n_0}\}$ be a family of sets of μ nonnegative integers. F is a $(\mu,\ n_0)$ Extended Difference Family or $(\mu,\ n_0)$-EDF in short, for $\mu = 3,\ 4,\ 5$, if all intraset distances, shown in (6), are distinct. The largest of all distances is denoted by d_{max} [6].

The restrictions on the distances between nonnegative integers used in extended difference families are less compared with difference families. Here we express two lemmas that are proved in [6] to exhibit the characteristics of EDF-QC-LDPC codes.

Lemma 1. *For a $(\mu,\ n_0)$-EDF, the following assertion holds,*

$$d_{max} \geq n_0\mu(\mu - 1)/2.$$

Lemma 2. *An $(m,\ \mu,\ n_0)$-EDF-QC code has no 4-length cycle, if $m \geq 2d_{max} + 1 = n_0\mu\,(\mu - 1) + 1$, where m is the number of row/column of each circulant submatrix in the parity check matrix.*

Parity check matrices of EDF-QC-LDPC codes may also be constructed from EDFs in the form of (4) as following algorithm [6], where the circulant submatrices H_i are generated from the sets D_i. In this case, the number of check equations need not to be a certain prime power as the case for DF-QC-LDPC codes.

The resulted code is an $(mn_0, m\,(n_0 - 1))$ regular EDF-QC-LDPC code with characteristic vector $chr = (m, \mu, n_0)$ which has Tanner graph free of 4-length cycle. Assuming that one of the H_is in parity check matrix $\mathcal{H}$ (i.e. H_{n_0}) is invertible, the generator matrix can be constructed in a systematic form as (5). EDF-QC-LDPC codes are one of the most efficient linear block codes that can be applied in code based cryptosystems with the following reasons,

Algorithm 1

Input:

- Nonnegative integers m, μ, n_0.

Output:

- Row circulant parity check matrix $\mathcal{H}_{m\times mn_0}$ of $(mn_0,\ m\,(n_0 - 1))$ regular EDF-QC-LDPC code.

Algorithm:

1: Select nonnegative integers m, μ, n_0 such that $\mu = 3, 4, 5,\ \mu \ll m$, and Lemma 2 is satisfied.
2: Generate (μ, n_0)-EDFs as large as needed.
3: Generate a full zero $\mathcal{H}_{m\times mn_0}$ matrix which consists of n_0 submatrices $H_{m\times m}$.
4: Randomly select non-iterative base blocks $D_i,\ i = 1, 2, \ldots, n_0$ from EDFs.
5: Construct generator polynomials $h_i\,(x)$ as equation (7), by using elements of the selected base blocks D_i.
6: Insert the coefficients of the polynomial $h_i\,(x)$ into the first row of each $m \times m$ submatrix H_i.
7: **for** $l = 1$ to $m - 1$ **do**
8: Shift the first row of H_i, l positions to the right.
9: Insert the l^{th} shift of the first row in the $(l+1)^{\text{th}}$ row of H_i.
10: **end for**
11: **return** $\mathcal{H}$, shown in(4).

(1) These codes can be designed to have a very large class of equivalent codes with the same code rate and length. If an attacker chooses a code from this class at random, he can neither recover the secret key, nor should be able to obtain it through an exhaustive search attack. The number of equivalent regular EDF-QC-LDPC codes with $chr = (m, \mu, n_0)$ is given below [12],

$$N_{EDF}(m, \mu, n_0) = \binom{m}{\mu}^{n_0}. \qquad (8)$$

It should be noted that $N_{EDF}\,(m, \mu, n_0)$ grows exponentially with n_0. So, the cardinality of a family of equivalent $(mn_0, m\,(n_0 - 1))$ regular EDF-QC-LDPC codes increases with their code rate, $R = (n_0 - 1)/n_0$.

Table 1 compares the characteristic vector, chr, density, r, and the number of the shortest equivalent $(n_0 m, (n_0 - 1)\, m)$ regular EDF-QC-LDPC codes [6] with $\mu = 3, 4, 5$, $n_0 = 10$ and $R = 0.9$. It is clear that the code $C_1(2470, 2223)$ has the lowest density, the largest N_{EDF} and

Table 1. Comparing the shortest EDF-QC-LDPC codes with $n_0 = 10$, $\mu = 3,\ 4,\ 5$..

chr	$C\,(n,k)$	r $=\mu/m$	N_{EDF}
$(247,\ 5,\ 10)$	$C_1\,(2470,\ 2223)$	$\cong 0.02$	$\cong 2^{327}$
$(139,\ 4,\ 10)$	$C_2(1390,\ 1251)$	$\cong 0.029$	$\cong 2^{238}$
$(63,\ 3,\ 10)$	$C_3(630,\ 567)$	$\cong 0.047$	$\cong 2^{153}$

the largest code length among them.

(2) As stated before, the security of the RN cryptosystem against chosen plaintext attacks depends on the number of perturbation vectors. Using regular DF-QC-LDPC codes in the RN cryptosystem leads in a vulnerable system, because of their restriction on the number of check equation, m, and the number of perturbation vectors, $N_e = 2^m$. Instead, we apply regular EDF-QC-LDPC codes in the proposed cryptosystem to utilize the advantages of such codes and improve the security of the RN cryptosystem. In these codes the restrictions on m and N_e are rather loose compared with DF-QC-LDPC codes.

(3) Short/medium code lengths of high code rate ($R \geq 0.9$), low encoding/decoding complexity, good error performance and easy construction are the other properties of EDF-QC-LDPC codes [6].

4 Modified RN cryptosystem based on regular EDF-QC-LDPC codes

To achieve high security and reliability in the RN secret key cryptosystem, we use the regular EDF-QC-LDPC equivalent codes with characteristic vector $chr = (247, 5, 10)$ and dimension $(n, k) = (2470, 2223)$ in the proposed cryptosystem. These parameters yield the shortest code length, the highest code rate and the largest N_{EDF} among regular EDF-QC-LDPC codes with $\mu = 3, 4, 5$ and $n_0 = 10$. Secret key and encryption/decryption algorithms of the modified cryptosystem are described in the next sections.

4.1 Secret Key

Secret key composed of the set $\{\mathcal{H}, \mathcal{S}, \mathcal{P}, \mathcal{I}\}$ which is explained as follows.

(1) Let $\mathcal{H}_{m\times mn_0}$ be a parity check matrix of regular EDF-QC-LDPC codes with $chr = (m, \mu, n_0)$ that is formed by n_0 binary circulant $H_{m\times m}$ submatrices as (2), the Hamming weight of each row/column of circulant submatrices is $\mu = 5$. Also, the density of the parity check matrix $\mathcal{H}$ is $r = \mu/m \cong 0.02 \ll 1$ which points its sparsity.

(2) Let $\mathcal{S}_{k\times k}$ be a regular sparse nonsingular scrambling matrix formed by $(n_0 - 1) \times (n_0 - 1)$ binary circulant $m \times m$ submatrices $S_{j,k}$, $j = 1, \ldots, n_0-1$, $k = 1, \ldots, n_0-1$ with row/column Hamming weight $\mu_S = 2$ as follow,

$$\mathcal{S} = \begin{bmatrix} S_{1,1} & S_{1,2} & \cdots & S_{1,n_0-1} \\ S_{2,1} & S_{2,2} & \cdots & S_{2,n_0-1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n_0-1,1} & S_{n_0-1,2} & \cdots & S_{n_0-1,n_0-1} \end{bmatrix}.$$

(3) Let $\mathcal{P}_{n\times n}$ be an $n\times n$ block diagonal permutation matrix formed by $n_0 \times n_0$ submatrices $P_{m\times m}$ over $GF(2)$ as below,

$$\mathcal{P} = \begin{bmatrix} P_{1,1} & 0 & \cdots & 0 \\ 0 & P_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P_{n_0,n_0} \end{bmatrix}.$$

The diagonal elements are permutation submatrices and the other elements are zero submatrices. The number of these matrices satisfies the following equation,

$$N_{\mathcal{P}} = (m!)^{n_0}. \tag{9}$$

(4) Let $\mathcal{I}$ be an initial state of a Linear Feedback Shift Register, LFSR, to generate $N_e = 2^{n-k}$ pseudorandom syndromes synchronously. The required memory for using the syndrome error table in joint secret key cryptosystem is of $\mathcal{O}\left(2^{n-k}.n\right)$ [3]. This method is not applicable for long length codes, therefore in the proposed cryptosystem we use LFSRs instead of the syndrome error table. In this way, the size of the secret key reduces, since the value of memory required to save the initial state is considerably less than the syndrome error table.

4.2 Encryption

(1) To encrypt a massage, first choose a $C(mn_0,\ m(n_0 - 1))$ regular EDF-QC-LDPC code with characteristic vector $chr = (m, \mu, n_0)$ randomly by selecting its parity-check matrix $\mathcal{H}$ and produce a generator matrix G in reduced echelon form shown in (5). Then select a block diagonal permutation matrix $\mathcal{P}$ randomly.

(2) Generate $(n - k)$-bit pseudorandom syndrome $s \in F_2^{n-k}$ for each plaintext and compute an n-bit perturbation vector $e\,(s) = s.(\mathcal{H}^{-1})^T$, where $\mathcal{H}^{-1}$ is a right inverse matrix of $\mathcal{H}$. The number of $e(s)$ is given below,

$$N_e = 2^{n-k}. \tag{10}$$

(3) At last, divide the plaintext to k-bit blocks M and encrypt them as follows,

$$\begin{aligned} c &= ((M+e')\,\mathcal{S}G + e'')\,P \\ &= M\mathcal{S}G\mathcal{P} + (e'\mathcal{S}G + e'')\,\mathcal{P} \\ &= MG' + e'\,(s)\,\mathcal{P}, \end{aligned} \tag{11}$$

where e' is a k-bit vector that is obtained by selecting k Least Significant Bits (LSBs) of the perturbation vector $e(s)$. The parameter e'' is an n-bit vector that is adaptively chosen according to the n-bit vector $e'\mathcal{S}G$ such that $w_H(e'(s)) \approx n/2$, where $w_H(e'(s))$ denote the Hamming weight of the vector $e'(s)$. The value $e'(s) = (e'\mathcal{S}G + e'')\mathcal{P}$ is an n-bit combined perturbation vector that is used instead of $e(s)$ to withstand the cryptosystem against chosen plaintext attack, namely Rao-Nam attack.

4.3 Decryption

The authorized receiver decrypts the received vector r, influenced by channel error e_{ch},

$$r = c + e_{ch} = M\mathcal{S}G\mathcal{P} + (e'\mathcal{S}G + e'')\,\mathcal{P} + e_{ch}.$$

The decryption process is performed as below.

(1) Apply $\mathcal{P}^T$ to vector r and compute r',

$$r' = r\mathcal{P}^T = (M+e')\,\mathcal{S}G + e'' + e_{ch}\mathcal{P}^T.$$

In this case, matrix $\mathcal{P}$ is a permutation matrix. So, $e_{ch}\mathcal{P}^T$ is a vector having the same Hamming weight as e_{ch}. Then, eliminate $e_{ch}\mathcal{P}^T$ using iterative decoding algorithm of LDPC codes based on *Belief Propagation* [11] and obtain n-bit vector r'',

$$r'' = (M+e')\,\mathcal{S}G + e''.$$

(2) Use the syndrome s generated by sender and compute $e\,(s) = s.(\mathcal{H}^{-1})^T$, then obtain n-bit vector r''',

$$r''' = r'' - e'' = (M+e')\,\mathcal{S}G.$$

(3) Obtain $M'' = (M+e')\,\mathcal{S}$ by choosing the k left most bits of the vector r''', due to systematic form of generator matrix G, also obtain k-bit vector M',

$$M' = M + e' = M''\mathcal{S}^{-1}.$$

(4) Obtain e' by choosing the k right most bits of $e(s)$; subtract it from M' and obtain M as below,

$$M = M' - e'.$$

5 Security

In this section, we consider two types of attacks. The first type was developed for the original RN-like cryptosystems such as Rao-Nam, Brute force and Struik-Tilburg attacks. The second type, such as OTD attacks, was proposed to threaten cryptosystems based on QC-LDPC codes.

5.1 Brute force Attack

This attack would be possible, only if the size of key space is not large enough, that is the key can be found in polynomial time. The key, consisting the parameters set $\{\mathcal{H},\ \mathcal{S},\ \mathcal{P},\ \mathcal{I}\}$, of the proposed cryptosystem is computed as follows.

(1) The number of equivalent regular EDF-QC-LDPC codes with $chr = (m, \mu, n_0)$ is given in (8). In the proposed cryptosystem, we use $chr = (247, 5, 10)$, So the involved parameters produce a family of $(2470, 2223)$ equivalent regular EDF-QC-LDPC codes, the number of which is $\approx 2^{327}$. Nowadays, complexity of order 2^{80} is considered as the lower bound of security; hence, there are large enough equivalent EDF-QC-LDPC codes for the proposed cryptosystem to resist against brute force attack.

(2) The number of perturbation vectors is equal to 2^{247} (see (10)), therefore finding the perturbation vector is infeasible.

(3) The number of nonsingular scrambling matrices $\mathcal{S}_{k\times k}$ over $GF(2)$, $N_{\mathcal{S}}$, is given below [3],

$$N_{\mathcal{S}} = \prod_{i=0}^{k-1} (2^k - 2^i) > 2^{k^2-k}.$$

In our scheme, the number of nonsingular scrambling matrices with $k = 2223$ is huge, namely $N_{\mathcal{S}} > 2^{500}$ which indicates an impractical preliminary work for an attacker.

(4) The number of block diagonal permutation $\mathcal{P}_{n\times n}$ matrices for $m = 247$, is $N_{\mathcal{P}} = (247!)^{10} \gg 2^{80}$ (see (9)). So, finding the permutation matrix is infeasible in polynomial time.

5.2 Majority Voting Attack

The goal of Majority Voting (MV) attack [15] against RN-like secret key cryptosystem is obtaining the secret matrix $G' = \mathcal{S}G\mathcal{P}$ in an efficient way. Let $\mathcal{M}(\mathcal{E})$ be a matrix representation of a set $\mathcal{E} = \left\{e'_1(s), e'_2(s), \ldots, e'_{2^{n-k}}(s)\right\}$ of distinct n-bit combined perturbation vectors,

$$\mathcal{M}(\mathcal{E}) = \left(e'_{ij}(s)\right), 1 \le i \le 2^{n-k}, 1 \le j \le n.$$

where $e'_{ij}(s)$ is j^{th} bit of the i^{th} vector in $\mathcal{M}(\mathcal{E})$. The following two steps recover the secret matrix $G' = \mathcal{S}G\mathcal{P}$ [15].

(1) Choose an arbitrary k-bit vector x, and obtain $N_e = 2^{n-k}$ distinct encryptions of x (i.e.,

$c_i = xG' + e'_i(s)$ with $1 \leq i \leq N_e$). Let $\mathcal{C} = \{c_1, c_2, c_3, \ldots, c_{2^{n-k}}\}$be a set of ciphertexts, such that,

$$\mathcal{M}(\mathcal{C}) = \mathcal{M}(xG') + \mathcal{M}(\mathcal{E}),$$

where $\mathcal{M}(xG')$ denotes a $2^{n-k} \times n$ matrix in which the n-bit vector xG' iterates 2^{n-k} times in its rows.Then, majority voting on each column of $\mathcal{M}(\mathcal{C})$ leads to an estimate xG' of $x\mathcal{SGP}$, that is when the number of '1's in each column is greater than the number of its '0's, set the corresponding bit to '1', otherwise to '0'.

(2) Repeat step 1 for k linearly independent vectors x. Let the rows of a matrix $X_{k\times k}$ consist of these k vectors and let the rows of $(XG')_{k\times n}$consist of the corresponding k estimates. Then, an estimate G' for the matrix $\mathcal{SGP}$ follows from,

$$G' = X^{-1}(XG').$$

These steps require $k \times 2^{n-k}$ majority votes over n columns of $\mathcal{M}(\mathcal{C})$, so that, the computational complexity of this attack is of $\mathcal{O}(kn2^{n-k})$ bit operations. Therefore, the work factor of this attack is approximately of $\mathcal{O}(2^{269.4})$ for the proposed cryptosystem. Also, an MV attack is not successful when the average Hamming weight of each perturbation vector equals to $n/2$. In this case, an attacker can obtain a bit on an arbitrary coordinate of xG' with probability 1/2. In other words, the n-bit vector xG' is guessed randomly. Therefore, we propose using a set $\mathcal{E}$ of predefined perturbation vectors with Hamming weight $\approx n/2$ to resist against MV attack.

5.3 Rao-Nam Attack

RN attack [3] is a chosen plaintext attack. Let M_1 and M_2 be two plaintext vectors differing only in the i^{th} position $i = 1, 2, \ldots, k$; c_1 and c_2 be the corresponding ciphertext vectors as follows,

$$c_1 = M_1\mathcal{SGP} + (e'_1\mathcal{SG} + e''_1)\mathcal{P} = M_1G' + e'_1(s)\mathcal{P}$$
$$c_2 = M_2\mathcal{SGP} + (e'_2\mathcal{SG} + e''_2)\mathcal{P} = M_2G' + e'_2(s)\mathcal{P},$$

whose difference is given below,

$$\begin{aligned} c_1 - c_2 &= (M_1 - M_2)G' + (e'_1(s) - e'_2(s))\mathcal{P} \\ &= g'_i + (e'_1(s) - e'_2(s))\mathcal{P}, \end{aligned}$$

where g'_i is the i^{th} row vector of the matrix G'. If $w_H(e'(s))$ is much smaller than n, the majority voting of the vector $c_1 - c_2$ corresponds directly to g'_i. By repeating this step several times, a number of estimates of g'_i can be obtained. Repeating this step for all $i = 1, 2, \ldots, k$ will give us G', which can be used to break the cryptosystem.

A work factor of chosen plaintext attack will be small if $w_H(e'(s))/n$ is small and it will not if $w_H(e'(s)) \approx n/2$. In the proposed cryptosystem, the Hamming weight of the difference between combined perturbation vectors, $(e'_1(s) - e'_2(s))\mathcal{P}$, is the same as $e'_1(s) - e'_2(s)$, since $\mathcal{P}$ is a permutation matrix. Also, the Hamming weight of $w_H(e'_1(s) - e'_2(s))$ is approximately equal to $n/2$. Therefore $c_1 - c_2$ is not an estimate of g'_i and this attack is failed.

5.4 Struik-Tilburg Attack

The RN secret key cryptosystem is not optimally secure for practical code lengths against a chosen plaintext attack which was proposed by Struik and Tilburg [16]. One of the weaknesses of the RN cryptosystem they showed is as follows. The total number of perturbation vectors based on the syndrome error table for the RN recommended code parameters is restricted in cardinality to 2^{n-k} over $GF(2)$. If the number of different perturbation vectors is equal to $N_e = 2^{n-k}$ for a binary code $C(n, k)$, then an attacker has to encrypt $\mathcal{O}(N_e log N_e)$ times the chosen plaintexts on average to obtain all proper perturbation vectors.

$$N_e \sum_{i=0}^{N_e-1} 1/(N_e - i) = \mathcal{O}(N_e \log N_e)$$

The work factor of this attack on the proposed cryptosystem based on the (2470, 2223) regular EDF-QC-LDPC code is given below.

$$\text{WF} = \mathcal{O}\left(2^{247}\log_2^{2^{247}}\right) = \mathcal{O}(2^{255})$$

Therefore, this attack is infeasible for the used code parameters of the proposed cryptosystem. Note that, the number of perturbation vectors in the RN cryptosystem using the shortened (72, 64) Hamming code is of $\left(2^8\, log_2^{2^8}\right) = \mathcal{O}\left(2^{11}\right)$. Thus, the proposed cryptosystem is far more secure than RN cryptosystem by the factor of $\mathcal{O}(2^{244})$.

5.5 OTD Attack

The cryptosystems based on QC-LDPC codes can be vulnerable to some attacks because of sparse matrices used in the structure of secret key.

Otmani, Tillich and Dallot (OTD) in 2008 developed an attack [17] against Baldi's public key cryptosystem [18] based on QC-LDPC codes. They proved that using QC (but not LDPC) codes for shortening the public key of the McEliece cryptosystem is not secure, if the block diagonal permutation matrix $\mathcal{P}$ is used to hide the generator matrix G. In this attack, an eavesdropper can obtain the generator matrix G, that is part of the secret key, first by selecting the k left most columns of the matrix $G' = \mathcal{SGP}$, because of systematic form of the generator matrix G.

In the secret key code based cryptosystems, the encryption matrix G' is secret. If the attacker can

obtain the matrix G', the OTD attack is applicable. A lower bound for work factor of chosen plaintext attack on secret key code based cryptosystems to determine the matrix G' is obtained as follows [3],

$$\text{WF} \geq 1/2(N_e^2/2),$$

Considering $N_e = 2^{247}$, the work factor for determining G' is really dominant and the OTD attack is failed.

6 Efficiency

We consider the efficiency of the proposed cryptosystem from three viewpoints: key length, computational complexity and error performance.

6.1 Key length

In this section, we compute the key length of the proposed cryptosystem before and after executing key compression/decompression algorithms. These algorithms are based on circulant block of submatrices in the structure of $\mathcal{S}$ and $\mathcal{H}$ matrices.

6.1.1 Actual key length

Without executing compression algorithms, we require only the first rows of $m \times m$ submatrices $H_i, i = 1, 2, \ldots, n_0$ to store the parity check matrix $\mathcal{H}$.Therefore, the required memory is given below,

$$M_{\mathcal{H}} = n_0 m.$$

Furthermore, we require only the first rows of $m \times m$ submatrices $S_{j,k}, j = 1, \ldots, n_0 - 1, k = 1, \ldots, n_0 - 1$ to store the sparse nonsingular scrambling matrix $\mathcal{S}_{n\times n}$. So, the required memory is given below,

$$M_{\mathcal{S}} = (n_0 - 1)^2 m.$$

The number of permutation matrices $\mathcal{P}_{k\times k}$ which consists of $P_{m\times m}$ submatrices is $(m!)^n$, so the lower bound of the required memory, $M_{\mathcal{P}}$, for storing the matrix $\mathcal{P}_{k\times k}$ is $M_{\mathcal{P}} = n\log_2^{(m!)}$ bits. Storing the initial vector, $\mathcal{I}$, requires $M_{IV} = n - k = m$ bits of memory. So, the actual key length of the proposed cryptosystem is computed as follow,

$$\begin{aligned} M_{\mathcal{K}_{actual}} &= M_{\mathcal{H}} + M_{\mathcal{S}} + M_{\mathcal{P}} + M_{\mathcal{IV}} \\ &= n_0 m + (n_0 - 1)^2 m + n_0 m \log_2^{(m!)} + m. \end{aligned}$$

6.1.2 Key compression algorithms

In this section, we present two compression algorithms 2 and 3 for the sparse parity check matrix $\mathcal{H}$ and the nonsingular matrix $\mathcal{S}$ respectively. Below we introduce two compressed vectors $\mathcal{H}_c$ and $\mathcal{S}_c$.

In the proposed cryptosystem, the Hamming weight of each row/column of the submatrix H_i is μ. So,

Algorithm 2

Input:

- Parity check matrix $\mathcal{H}_{m\times mn_0}$.

Output:

- Compressed vector $\mathcal{H}_c$.

Algorithm:

1: Generate a full zero vector $\mathcal{H}_c$ consisting of μn_0 coordinates.
2: **for** $i = 1$ to n_0 **do**
3: Select nonzero positions in the first row of the submatrix H_i from matrix $\mathcal{H}$.
4: Insert the selected positions from left to right in the vector $\mathcal{H}_c$
5: **end for**
6: **return** $\mathcal{H}_c$.

the compressed vector $\mathcal{H}_c$ consists of μn_0 nonzero positions which involves at most $8\mu n_0$ bits of memory.

Algorithm 3

Input:

- Sparse scrambling nonsingular matrix $\mathcal{S}$.

Output:

- Compressed vector $\mathcal{S}_c$.

Algorithm:

1: Consider a full zero vector $\mathcal{S}_c$ consisting of $\mu_S(n_0 - 1)^2$ coordinates.
2: **for** $j = 1$ to $n_0 - 1$ **do**
3: **for** $k = 1$ to $n_0 - 1$ **do**
4: Select nonzero positions in the first row of the submatrix $S_{j,k}$ from the matrix $\mathcal{S}$.
5: Insert the selected positions from left to right in the vector $\mathcal{S}_c$.
6: **end for**
7: **end for**
8: **return** $\mathcal{S}_c$.

In the proposed cryptosystem, the Hamming weight of each row/column of $S_{j,k}$ submatrices is μ_S. So, the compressed vector $\mathcal{S}_c$ consists of $\mu_S(n_0 - 1)^2$ nonzero positions which involves at most $8\mu_S(n_0 - 1)^2$ bits of memory. Using the compression algorithms, the maximum required memory for storing secret key is computed as follow,

$$\begin{aligned} M_{\mathcal{K}_{comp.}} &= M_{\mathcal{H}_c} + M_{\mathcal{S}_c} + M_{\mathcal{P}} + M_{\mathcal{I}} \\ &\leq 8\mu n_0 + 8\mu_S(n_0 - 1)^2 + n_0 m \log_2^{(m!)} + m. \end{aligned}$$

The key lengths of various RN-like secret key cryptosystems, using $\mathcal{S}$ and $\mathcal{P}$ in their structure, are compared in Table 2. It is clear that the key length of the proposed cryptosystem is decreased with a factor of $2^{-2.78}$ (85%) after applying the corresponding compression algorithms to $\mathcal{H}$ and $\mathcal{S}$.

Table 2. Comparing the key lengths of RN-like secret key cryptosystems.

Cryptosystems	$(n,\ k)$	Key length
Rao [2]	(1024, 524)	2Mbit
Rao-Nam [3]	(72, 64)	18kbit
Struik-Tilburg [16]	(72, 64)	18kbit
Barbero-Ytrehus [19]	(30, 20) over $GF(2^8)$	4.9kbit
Proposed cryptosystem	(2470, 2223)	Before Comp. = 24.4kbit After Comp.= 3.55kbit

6.1.3 Key decompression algorithms

After compressing $\mathcal{S}$ and $\mathcal{H}$, the sender should send a new characteristic vector $CHR = (m, \mu, n_0, \mu_S)$ to the authorized receiver, where μ and μ_S are the Hamming weights of each row/column of submatrices in $\mathcal{H}$ and $\mathcal{S}$, respectively.

The intended receiver can decompress the vectors $\mathcal{H}_c$ and $\mathcal{S}_c$ to the matrices $\mathcal{H}$ and $\mathcal{S}$, using the following algorithms 4 and 5, respectively.

Algorithm 4

Input:

- $\mathcal{H}_c$, $CHR = (m, \mu, n_0, \mu_S)$.

Output:

- $\mathcal{H}$.

Algorithm:

1: Construct a full zero $\mathcal{H}_{m\times mn_0}$ matrix consisting of $1\times n_0$ submatrices $H_{m\times m}$.
2: **for** $i = 1$ to n_0 **do**
3: Select, the i^{th} μ coordinates of $\mathcal{H}_c$, from left to right.
4: Insert '1's in the μ positions of the first row of the H_i (the i^{th} submatrix of $\mathcal{H}$) corresponding to the values of the selected μ coordinates.
5: **for** $l = 1$ to $m - 1$ **do**
6: Shift the first row of H_i, l positions to the right.
7: Insert the l^{th} shift of the first row in the $(l + 1)^{th}$ row of H_i.
8: **end for**
9: **end for**
10: **return** $\mathcal{H}$.

6.2 Computational Complexity

Computational complexity of the proposed cryptosystem can divide into two parts:

(1) Encryption/Encoding complexity,
(2) Decoding/Decryption complexity.

Algorithm 5

Input:

- $\mathcal{S}_c$, $CHR = (m,\ \mu, n_0, \mu_S)$.

Output:

- $\mathcal{S}$.

Algorithm:

1: Construct a full zero $\mathcal{S}_{m(n_0-1)\times m(n_0-1)}$ matrix consisting of $(n_0-1)\times(n_0-1)$ submatrices $S_{m\times m}$.
2: **let** $g \leftarrow 1$.
3: **for** $j = 1$ to $n_0 - 1$ **do**
4: **for** $k = 1$ to $n_0 - 1$ **do**
5: Select, the g^{th} μ_S coordinates of $\mathcal{S}_c$, from left to right.
6: Insert '1's in the μ_S positions of the first row of the $S_{j,k}$ (the $(j, k)^{th}$ submatrix of $\mathcal{S}$) corresponding to the values of the selected g^{th} μ_S coordinates.
7: **for** $l = 1$ to $m - 1$ **do**
8: Shift the first row of $S_{j,k}$, l positions to the right.
9: Insert l^{th} shift of the first row in $(l + 1)^{th}$ row of $S_{j,k}$.
10: **end for**
11: **end for**
12: **let** $g \leftarrow g+1$.
13: **end for**
14: **return** $\mathcal{S}$.

6.2.1 Encryption/Encoding complexity

Consider the ciphertext vector c of the proposed cryptosystem as follow,

$$c = ((M + e')\,\mathcal{S}G + e'')\,P = M'G' + e''\mathcal{P}.$$

The Encryption/Encoding complexity, $\mathcal{C}_{Enc}$, is computed as given below,

$$\mathcal{C}_{Enc} = \mathcal{C}_{add}\,(M + e') + \mathcal{C}_{mul}\,(M'G') + \mathcal{C}_{mul}\,(e''\mathcal{P})\,.$$

(1) $\mathcal{C}_{add}\,(M + e')$ is the number of required binary operations for adding k-bit vectors M and e' as follow,

$$\mathcal{C}_{add}\,(M + e') = k.$$

(2) $\mathcal{C}_{mul}\,(M'G')$ is the number of required binary operations for multiplying k-bit vector M' to matrix $G' = \mathcal{S}G\mathcal{P}$, consisting of $k_0 \times n_0$ circulant submatrices $\mathcal{G}'_{m\times m}$. A lower bound for $\mathcal{C}_{mul}\,(M'G')$ is given below,

$$\mathcal{C}_{mul}\,(M'G') \geq k\mu_S m(n_0 - 1)^2\,[k + mk/2]\,n$$
$$= \mu_S k^4(n_0 + n/2).$$

(3) $\mathcal{C}_{mul}\,(e''.\mathcal{P})$ is the number of required binary operations for multiplying n-bit vector e'' to permutation matrix $\mathcal{P}$ which is computed as follow,

$$\mathcal{C}_{mul}\,(e''.\mathcal{P}) = n.$$

Hence,

$$\mathcal{C}_{Enc} \geq k + \mu_S k^4 (n_0 + n/2) + n.$$

6.2.2 Decoding/Decryption complexity

The complexity of Decoding/Decryption algorithm is obtained as follow,

$$\mathcal{C}_{Dec} = \mathcal{C}_{mul}\left(r.\mathcal{P}^T\right) + \mathcal{C}_{SPA} + \mathcal{C}_{sub}\left(r'' - e''\right) + \mathcal{C}_{inv}\left(S\right) + \mathcal{C}_{mul}\left(M''\mathcal{S}^{-1}\right) + \mathcal{C}_{sub}\left(M' - e'\right).$$

(1) $\mathcal{C}_{mul}\left(r.\mathcal{P}^T\right)$ is the number of required binary operations for multiplying n-bit received vector r to the transposed permutation matrix $\mathcal{P}$ as given below,

$$\mathcal{C}_{mul}\left(r.\mathcal{P}^T\right) = n.$$

(2) $\mathcal{C}_{SPA}$ is the complexity of Sum Product decoding Algorithm [20] which is given as follow,

$$\mathcal{C}_{SPA} = I_{ave}.n\left[q\left(8\mu + 12R - 11\right) + \mu\right].$$

where, I_{ave} is the average number of decoding iterations, q is the number of used quantization bits in the decoder and R is the code rate.

(3) $\mathcal{C}_{sub}\left(r'' - e''\right)$ is the number of required binary operations for subtracting n-bit vector e'' from n- bit vector r'' as given below,

$$\mathcal{C}_{sub}\left(r'' - e''\right) = n.$$

(4) $\mathcal{C}_{inv}\left(\mathcal{S}\right)$ is the number of required binary operations for inverting the nonsingular matrix $\mathcal{S}$ which is as given below,

$$C_{inv}\left(\mathcal{S}\right) \leq k^3.$$

(5) $\mathcal{C}_{mul}(M''\mathcal{S}^{-1})$ is the number of required binary operations for multiplying the k-bit vector $M'' = (M + e')\mathcal{S}$ to the inverse matrix $\mathcal{S}^{-1}$ which is obtained as follows,

$$C_{mul}\left(M''\mathcal{S}^{-1}\right) \leq k^2.$$

(6) $C_{sub}\left(M' - e'\right)$ is the number of required binary operations for subtracting k-bit vector e' from the vector M'which is computed as follows,

$$C_{sub}\left(M' - e'\right) = k.$$

Hence,

$$\mathcal{C}_{Dec} \leq 2n + I_{ave}.n\left[q\left(8\mu + 12R - 11\right) + \mu\right] + k^3 + k^2 + k.$$

6.3 Error performance

The highest code rate for an $(mn_0, m(n_0 - 1))$ regular LDPC code based on $(m, \mu, 1)$-DF is $(n_0 - 1)/n_0$ [21]. According to Lemma 2 [6], this code rate is also achievable for regular (m, μ, n_0)-EDF-QC code if the number of rows, m, in the parity check matrix $\mathcal{H}$, as shown in (4), is greater than twice d_{max} of the (μ, n_0)-EDF.

In this work, the used regular $(247, 5, 10)$-EDF-QC-LDPC code satisfies Lemma 2, so the highest code rate $R = 0.9$ can be achieved. As we have shown in Section 5, achieving this code rate doesn't weaken the security of the proposed cryptosystem. A comparison in terms of code rates of RN-like secret key cryptosystems with their originally recommended code parameters is given in Table 3. We observe that the code rate of the proposed cryptosystem is higher than the others.

Table 3. Comparing the code rates of RN-like secret key cryptosystems.

Cryptosystem	Code	Code Rate
Rao [2]	$C(1024,\ 524)$	≈ 0.51
Rao-Nam [3]	$C(72,\ 64)$	≈ 0.89
Struik-Tilburg [16]	$C(72,\ 64)$	≈ 0.89
Barbero-Ytrehus [19]	$C(30,\ 20)$ over $GF(2^8)$	≈ 0.67
Cryptosystem based on EG-QC-LDPC [4]	$C(2044,\ 1024)$	≈ 0.51
Proposed cryptosystem	$C(2470,\ 2223)$	0.9

The upper bound of the minimum distance, d_{min}, for $(m,\ \mu,\ n_0)$-QC code based on EDFs is determined by the following Lemma [6].

Lemma 3. *The minimum distance of a (m, μ, n_0)-QC code with column weight μ is upper bounded by 2μ.*

On the other hand, the d_{min} of a regular (m, μ, n_0)-EDF-QC code free of 4-length cycle is lower bounded by $\mu + 1$. Therefore, d_{min} of EDF-QC-LDPC code with $chr = (m, \mu, n_0)$ is bounded by the inequality $\mu + 1 \leq d_{min} \leq 2\mu$. We require an exhaustive search to determine the exact value of d_{min} [6]. In the proposed cryptosystem, as we use regular EDF-QC-LDPC code with $chr = (m, \mu, n_0)$, the minimum distance is bounded by $6 \leq d_{min} \leq 10$.

The minimum distances of the shortest regular EDF-QC-LDPC codes with $\mu = 3, 4, 5$, $n_0 = 10$ and shortened Hamming code used in RN cryptosystem are compared in Table 4. It is observed that $(247, 5, 10)$-EDF-QC-LDPC code, used in the proposed cryptosystem, has the highest minimum distance among the others.

Error performance curves for codes C_1, C_2 and C_3 on Additive White Gaussian Noise (AWGN) channel with 100 iterations of Massage-Passing decoding algorithm are depicted in [6]. The Signal to Noise Ratio (SNR) of these codes with error probability of bits, $P_b = 10^{-7}$, are equal to 4.8, 5.25 and 6 dBs, respectively. Also, The Shannon limit of AWGN channel for $R = 0.9$ and $R = 0.5$ are equal to 3.1 and 0.223 dBs, respectively. Table 5 compares the distances of SNRs from Shannon

Table 4. Comparing the minimum distances of three types of EDF-QC-LDPC codes and shortened Hamming code.

Code	$(n,\ k)$	d_{min}
EDF-QC-LDPC	C_1 (2470, 2223) proposed cryptosystem	$6 \leq d_{min} \leq 10$
EDF-QC-LDPC	C_2(1390, 1251)	$5 \leq d_{min} \leq 8$
EDF-QC-LDPC	C_3(630, 567)	$4 \leq d_{min} \leq 6$
Shortened Hamming code	C_4(72, 64) RN cryptosystem [3]	$d_{min} = 4$

limit for three EDF-QC-LDPC codes C_1, C_2 and C_3 and EG-QC-LDPC code C_4 with $P_b = 10^{-7}$ [4].

Table 5. Comparing the error performances of three types of EDF-QC-LDPC codes and EG-QC-LDPC code.

$C(n,\ k)$	SNR in $P_b = 10^{-7}$	R	Distance from Shannon limit
EDF-QC-LDPC C_1 (2470, 2223) Used in proposed cryptosystem	4.8 dB	0.9	1.7 dB
EDF-QC-LDPC C_2(1390, 1251)	5.25 dB	0.9	2.15 dB
EDF-QC-LDPC C_3(630, 567)	6 dB	0.9	2.9 dB
EG-QC-LDPC C_4(2044, 1024) Used in code based cryptosystem [4]	2.65 dB	0.51	2.327 dB

It is clear that the code C_3 has the closest SNR to Shannon limit, having the best error performance among them.

7 Conclusion

This paper presents an RN-like cryptosystem, using the regular EDF-QC-LDPC codes for combining security with efficiency and gives comments on the original RN and the previous RN-like cryptosystems. Applying EDF-QC-LDPC codes together with an improvement of the structure of encryption/decryption algorithms and developing compression/decompression algorithms resulted in advantages in terms of security and efficiency (i.e. the transmitted compressed key up to 85%, computational complexity of encryption/decryption algorithms and error performance), compared to the previous secret key code based cryptosystems. Besides, using the proposed cryptosystem implies that there is no trade-off between efficiency and security.

Acknowledgements

This work was partially supported by Iran NFS-Cryptography chair.

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] T. R. N. Rao. Joint encryption and error correction schemes. In *Proceedings of the 11th annual international symposium on computer architecture*, pages 240–241, 1984.

[3] T. R. N. Rao and K. H. Nam. Private-key algebraic-code encryption. *IEEE Transactions on Information Theory*, IT-35(4):829–833, 1987.

[4] 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.

[5] R. Gallager. *Low density parity check codes*. PhD thesis, Cambridge, MA: MIT Press, 1963.

[6] T. Xia and B. Xia. Quasi-cyclic codes from extended difference families. In *Proceedings of IEEE Wireless Communications and Networking Conference*, volume 2, pages 1036–1040, 2005.

[7] D. J. C. Mackay and R.M. Neal. Near shannon limit performance of low-density parity check codes. *Electronics Letters*, 32(18):1645–1646, 1996.

[8] M. Tanner. A recursive approach to low complexity codes. *IEEE Transactions on Information Theory*, IT-27(5):533–547, 1981.

[9] G. A.Malema. *Low-density parity-check codes: construction and implementation*. PhD thesis, The University of Adelide, Australia, 2007.

[10] Z. Li, L. Chen, L. Zeng, S. Lin, and W. H. Fong. Efficient encoding of quasi-cyclic low-density parity-check codes. *IEEE Transactions on Communications*, 54(1):71–81, 2006.

[11] S. Lin and D. J. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, NJ, USA, 2nd edition edition, 2004.

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

[13] S. J. Johnson and S. R. Weller. A family of irregular ldpc codes with low encoding complexity. *IEEE Communications Letters*, 7(2):79–81, 2003.

[14] M. Buratti. Constructions of (q,k,1) difference

families with q a prime power and k=4,5. *Discrete Mathematics*, 138(1-3):169–175, 1995.

[15] J. V. Tilburg. *Security-analysis of a class of cryptosystems based on linear error-correcting codes*. PhD thesis, Technische Universiteit Eindhoven, 1994.

[16] R. Struik and J. Tilburg. The Rao-Nam scheme is insecure against a chosen-plaintext attack. In *Advances in Cryptology-CRYPTO'87*, Lecture Notes in Computer Science, pages 445–457. Springer, 1988.

[17] A. Otmani, J.P. Tillich, and L. Dallot. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*, 3(2):129–140, 2010.

[18] M. Baldi and F. Chiaraluce. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In *IEEE International Symposium on Information Theory*, volume 2, pages 2591–2595, Nice, France, 2007.

[19] A. I. Barbero and O. Ytrehus. Modifications of the Rao-Nam Cryptosystem. In *Proceedings of International Conference on Coding Theory, Cryptography and Related Areas (ICCC98)*, pages 1–13, Guanajuato, Mexico, 1998.

[20] Marco Baldi, Marco Bodrato, and Franco Chiaraluce. A new analysis of the McEliece cryptosystem based on QC-LDPC codes. In *Proceedings of the 6th International Conference on Security and Cryptography for Networks*, Lecture Notes in Computer Science, pages 246–262. Springer, 2008.

[21] D. J. C. Mackay. Good error correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory*, IT-45(2):399–341, 1999.

Reza Hooshmand received the B.S. and M.S. degrees in electrical engineering from Shahid Sattari University of Aeronautical Science and Technology, Tehran, Iran. Since October 2011, He has been a Ph.D. student in Science and Research Branch of the Islamic Azad University (SRBIAU),Tehran, Iran. His research interests include coding, cryptography and code based cryptosystems.

Taraneh Eghlidos received her B.Sc. degree in Mathematics in 1986, from the University of Shahid Beheshti, Tehran, Iran, and the M.Sc. 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 (SUT) in 2002 and is currently an associate professor in the Electronics Research Institute of SUT. Her research interests include interdisciplinary research areas in subjects such as cryptology, code based cryptosystems and mathematical modeling for representing and solving real world problems.

Mohammad Reza Aref received the B.S. degree in 1975 from the University of Tehran, Iran, and the M.Sc. and Ph.D. degrees in 1976 and 1980, respectively from Stanford University, Stanford, CA, all in electrical engineering. He returned to Iran in 1980 and was actively engaged in academic and political affairs. He was a Faculty member of Isfahan University of Technology from 1982 to 1995. He has been a professor of electrical engineering at Sharif University of Technology, Tehran, since 1995, and has published more than 260 technical papers in communications, information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory and cryptography with special emphasis on network information theory and security for multiuser wireless communications. At the same time, during his academic activities, he has been involved in different political positions: First Vice President of I. R. Iran, Vice President of I. R. Iran and Head of Management and planning Organization are the most recent ones. He is currently the president of Iranian Society of Cryptology (ISC).