Scientia Iranica (2024) 31(17), 1504–1516

Sharif University of Technology
Scientia Iranica
Transactions D: Computer Science & Engineering and Electrical Engineering
https://scientiairanica.sharif.edu

A joint encryption-encoding scheme using QC-LDPC codes based on finite geometry

Hossein Khayami [a], Taraneh Eghlidos[b,*], and Mohammad Reza Aref[a]

a. *Information Systems and Security Laboratory, Department of Electrical Engineering, Sharif University of Technology, Tehran 11155-11365, Iran.*
b. *Electronics Research Institute, Sharif University of Technology, Tehran 11155-11365, Iran.*

Received 11 May 2021; received in revised form 19 June 2022; accepted 1 August 2022

KEYWORDS
Joint encryption-encoding;
Secure channel coding;
QC-LDPC code;
Code-based cryptography;
Finite geometry.

Abstract. Joint encryption-encoding schemes have been released to fulfill both reliability and security desires in a single step. Using Low Density Parity-Check (LDPC) codes in joint encryption-encoding schemes, as an alternative to classical linear codes, would shorten the key size as well as improving error correction capability. In this article, a joint encryption-encoding scheme using Quasi-Cyclic Low Density Parity-Check (QC-LDPC) codes based on finite geometry is presented. It is observed that our proposed scheme not only outperforms its predecessors in key size and transmission rate, but also remains secure against all known cryptanalyses of code-based secret key cryptosystems. In this paper, we have proposed an idea to make QC-LDPC based cryptosystems secure against reaction attacks. It is subsequently shown that our scheme benefits from low computational complexity. By taking the advantage of QC-LDPC codes based on finite geometry, the key size of our scheme is very close to its target security level. In addition, using the proposed scheme, a wide range of desirable transmission rates are achievable. This variety of codes makes our cryptosystem suitable for a number of different communication and cryptographic standards such as Wireless Personal Area Networks (WPAN) and Digital Video Broadcasting (DVB).

1. Introduction

The first code-based cryptosystem has been introduced by McEliece [1]. The security of this cryptosystem is based on the general decoding problem, which is known to be an NP-complete problem [2]. Although at the time of writing this paper, no algorithm running on quantum computers has been published to break the code-based cryptosystems, its large key size and low transmission rate in comparison with the prevalent cryptosystems such as RSA and ElGamal made these cryptosystems unusable from implementation perspective.

After McEliece published his public key code-based cryptosystem [2], Rao proposed a symmetric key cryptosystem inspired by the McEliece public key cryptosystem [3]. In 1986, Rao and Nam made a security modification on their proposed scheme [4]. In

*. *Corresponding author.*
E-mail addresses: h.khayami@alum.sharif.edu (H. Khayami); teghlidos@sharif.edu (T. Eghlidos); aref@sharif.edu (M.R. Aref)

To cite this article:
H. Khayami, T. Eghlidos, and M.R. Aref "A joint encryption-encoding scheme using QC-LDPC codes based on finite geometry", *Scientia Iranica* (2024) **31**(17), pp. 1504-1516
https://doi.org/10.24200/sci.2022.58300.5658

1987, Struik and Tilburg pointed out some weaknesses of the Rao-Nam cryptosystem and proposed an improved version of it [5]. In 2000, a secret key code-based cryptosystem with much shorter key size was introduced by Barbero and Ytrehus [6].

In conventional communication systems the encryption and encoding is being performed separately and in series. On the other hand, joint encryption-encoding schemes perform encryption and encoding as well as decryption and decoding, each in a single step [3,4] with lower complexity than classical encryption-then-encoding schemes. This scheme, using quasi-cyclic structure succeeded in shortening the key size. Moreover, it gains benefits from the fast decoding algorithms and superior error performance of the LDPC codes. In 2012, another scheme using QC-LDPC codes based on Extended Difference Families (EDF) was proposed [7], which could not achieve further improvement on the key size. In 2014, Esmaeili et al. introduced a joint encryption-encoding scheme with the novel idea of puncturing, instead of adding a perturbation vector [8]. Then, in 2015, they added random insertions with the idea of improving the security of their cryptosystem [9]. In [10], they added an agreed random error vector to their encryption process. In [11], they used random interleaving instead of random insertions and deletions. The cryptosystem in [10,11] is an encoding then encryption system rather than a joint encryption-encoding scheme. Besides, it is shown that the use of two pairs of Linear Feedback Shift Registers (LFSRs) has made Esmaeili-Gulliver cryptosystem vulnerable against ciphertext-only attack [12]. Another approach for joint encryption-encoding, which uses polar codes as generator matrix, has been proposed [13,14]. In [15], a nonlinear cryptosystem based on QC-LDPC codes was introduced and claimed to be secure against differential attacks and have a relatively low hardware complexity. In [16], Guan and Liang used LDPC codes based on quadratic permutation polynomials for the Gaussian wiretap channel. For the first time, performing encryption, encoding and modulation simultaneously using QC-LDPC lattice-codes has been proposed in [17] with relatively small key size.

Although the key sizes of recent schemes reduced considerably in comparison to the trailblazing code-based studies, the proportion of their target security level to their key size are still smaller than that of conventional AES. Due to this fact, attaining a more compact secret key, which is close to its target security level, is one of our motivations in this article. Besides shortening the secret key, increasing the transmission rate, decreasing the computational complexity of algorithm, and efficiently correcting channel errors, as well as keeping the cryptosystem secure are the most challenging issues in joint encryption-encoding researches. Resolving these issues needs a proper family of codes to be utilized. This code should possess the following characteristics:

- Efficiently decodable;
- A large family of equivalent codes;
- Achievable high transmission rate;
- Sparse parity-check matrices.

In this paper, we propose a joint encryption-encoding scheme utilizing QC-LDPC codes based on finite geometry (FG-QC-LDPC) in order to obtain a practical solution for the above mentioned issues. We can construct circulant matrices whose first rows are derived from incident vectors of a line in this geometry. In finite geometry, every line is identified through a pair its points. We show that this property enables to achieve a shorter key size. The wide acceptable range in the size of parameters in our proposed scheme makes it suitable for various applications and different levels of security. Furthermore, we show that the FG-QC-LDPC joint scheme is secure against all known cryptanalyses of such schemes including recent statistical attacks.

The rest of this paper is organized as follows. Section 2 introduces some basic definitions about finite geometry and QC-LDPC codes based on them that are used in this article. Next, the description of our new joint encryption-encoding scheme using FG-QC-LDPC codes is given in Section 3. The security and performance including key size, error performance, and complexity of our scheme are discussed in Section 4. Finally, Section 5 summarizes and concludes the paper.

2. Preliminaries

We took the advantages of FG-QC-LDPC codes to achieve the designated goals, namely improving the performance in comparison to the best known systems in the literature and also keeping the system secure against all known cryptanalyses. The basic definitions of QC-LDPC codes based on finite geometry is summarized in this section.

2.1. QC-LDPC

In cryptographic applications, quasi-cyclic LDPC codes allow one to reduce the key size as well as the complexity in comparison with the general LDPC codes [18]. The parity-check matrix of a QC-LDPC code is represented as follows:

$$H = \begin{bmatrix} H_{0,0} & \cdots & H_{0,n_0-1} \\ \vdots & \ddots & \vdots \\ H_{r_0-1,0} & \cdots & H_{r_0-1,n_0-1} \end{bmatrix}, \quad (1)$$

where each H_i is a circulant block of size $p \times p$.

There are different families of QC-LDPC codes used in code-based cryptography, namely, the Ex-

tended Difference Family (EDF) [7,18], and the Random Difference Family (RDF) [19,20]. In the current scheme the using of finite geometry to construct circulant blocks of the parity-check matrix is proposed. This helps us attain a shorter secret key than those available in the literature for joint encryption-encoding schemes.

2.2. Finite geometry

A finite geometry is composed of finite number of points. In this paper we focus on two types of finite geometry, namely Projective Geometry (PG) and Euclidean Geometry (EG). The definitions of finite geometry are generally provided from [21,22] and explained in Appendix A.

2.3. FG-QC-LDPC codes

In our scheme we exploit a QC-LDPC code with one block row of the form:

$$H_{qc} = [H_0 H_1 \dots H_{n_0-1}]. \tag{2}$$

In FG-QC-LDPC codes, as a subset of QC-LDPC codes, the first rows of the circulant blocks are derived from incident vectors of a line in that geometry. Thanks to the geometric construction, each line, and therefore its incident vector, can be identified by only two points lying on that line. This property helps us to shorten the key size. Other details regarding the key size are mentioned in Section 4.

The number of circulant blocks in the parity-check matrix, n_0, is limited to the number of cyclic classes in that particular geometry, i.e., $n_0 \leq \mathcal{N}_c$. The parity-check matrix derived from finite geometry has the following characteristics, which correspond to the parameters given in Appendix :

- The Hamming weight of each row in each circulant block is equal to the number of points lying on each line in that finite geometry;
- The size of each circulant block is $p \times p$, where p is the total number of points in that geometry;
- No two columns have more than one common locations of '1's. This is due to the fact that two distinct lines in finite geometry are either disjoint or intersect at only one point;
- The Tanner graph contains no length 4 cycles;
- The codeword length is $n = n_0 \times p$;
- The length of message vectors or equally the dimension of the code is $k = (n_0 - 1) \times p = k_0 \times p$.

3. FG-QC-LDPC joint encryption-encoding scheme

Here is the description of the proposed joint encryption-encoding scheme based on FG-QC-LDPC codes in three different steps, that is, key generation, encryption-encoding, and decryption-decoding. Then, we discuss the range of suitable parameters for our proposed scheme.

3.1. Key generation

The secret key of the joint encryption-encoding scheme is composed of a parity-check matrix, H, a permutation matrix, P, and the seed of the Pseudo Random Number Generator (PRNG).

3.1.1. Parity-check matrix

The parity-check matrix of the FG-QC-LDPC code in Eq. (2) can be constructed based on either Euclidean geometry or projective geometry. The construction procedure first starts with choosing between these two types of geometries and their parameters. According to Section 2, a finite geometry is defined in terms of two parameters, that is, its dimension, m, and the corresponding field, $GF(q)$.

As discussed in Section 2, in both cases of Euclidean and projective geometries all lines are partitioned into different cyclic classes. Each cyclic class in a finite geometry forms a set of rows of a circulant block. Thus, for generating a circulant block H_i one needs to simply specify a cyclic class and then assign only its first row.

In the case of EG, the number of cyclic classes, according to Appendix A.2 is $\mathcal{N}_{c,EG^*} = \frac{J_o}{n} = \frac{q^{m-1}-1}{q-1}$ and the number of lines in each cyclic class is $p = q^m - 1$ which is equal to the length of each row vector of circulant blocks.

In the case of PG, the number of cyclic classes is $\mathcal{N}_{c,even} = \frac{q^m-1}{q^2-1}$ or $\mathcal{N}_{c,odd} = \frac{q(q^{m-1}-1)}{q^2-1}$, when the dimension of the geometry is even or odd, respectively. Here, the number of lines in each cyclic class is $p = \frac{q^{m+1}-1}{q-1}$.

To sum up with the generation of the parity-check matrix, we should choose public parameters, that is, the type of geometry, its dimension m, its corresponding field $GF(q)$, and the number of circulant blocks of the matrix, n_0. Then each circulant block must be generated in the above fashion.

3.1.2. Permutation matrix

In the current scheme, the permutation matrix is a block diagonal matrix in the form of:

$$P = \begin{pmatrix} \pi & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \pi \end{pmatrix}_{xl \times xl}, \tag{3}$$

where each π block is an $l \times l$ permutation matrix and $xl = n$. To prevent reaction attack [23], the block size l should be chosen in a way that $l \nmid p$. The reason behind this condition is discussed in Section 4.

3.1.3. The PRNG seed

In order to generate a sequence of perturbation vectors

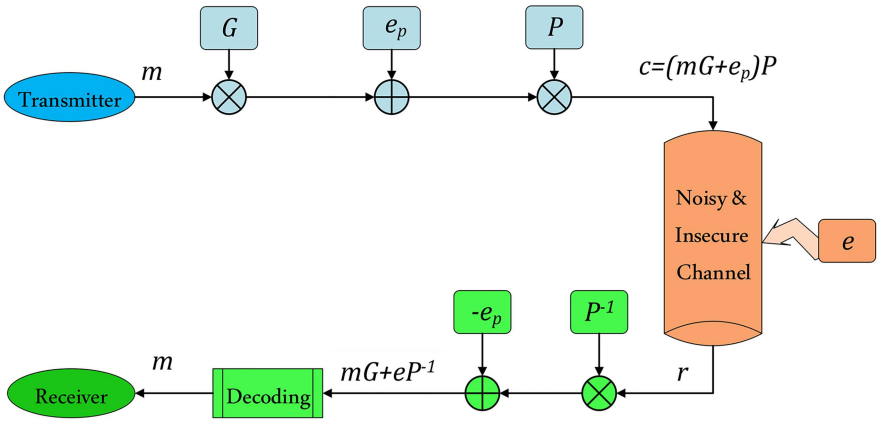

Figure 1. Block diagram of the proposed encryption-encoding/decryption-decoding scheme.

e_P we should utilize a PRNG. Thus, in order to use the same sequence as perturbation vectors by the transmitter and the receiver, it suffices they agree on the same seed for the PRNG. The sequence generated by the PRNG is then divided into $(n-k)$-bit vectors, z. The perturbation vectors are computed by $e_P = H^{-1}z$, where H^{-1} is the right inverse of H. Therefore, the perturbation vector e_P is of length n. Different PRNGs can be employed depending on the hardware/software resources and applications of the joint encryption-encoding scheme.

3.2. Encryption-encoding

For doing joint encryption-encoding, the transmitter needs to compute the generator matrix G from the parity-check matrix H. In QC-LDPC codes with a parity-check matrix in the form of one block row (see Eq. (2)), the generator matrix can be constructed as given below:

$$G = \left(I_k \middle| \begin{matrix} (H_{n_0-1}^{-1}H_0)^T \\ \vdots \\ (H_{n_0-1}^{-1}H_{n_0-2})^T \end{matrix} \right). \tag{4}$$

Note that for G being used as the generator matrix, it is sufficient for at least one circulant block, H_i, to be non-singular. Without loss of generality, one could assume that the circulant block H_{n_0-1} is a non-singular matrix.

Next, the transmitter generates a perturbation vector e_P as given below:

$$e_P = H^{-1}z, \tag{5}$$

where z is an $(n-k)$-bit vector produced by the PRNG, and the right inverse of the parity-check matrix is computed through a public algorithm such as that given in [24]. Finally, the ciphertext is obtained as follows:

$$c = (mG + e_P)P. \tag{6}$$

3.3. Decryption-decoding

It is assumed that, the error vector e is added to the ciphertext through a noisy channel between the transmitter and the receiver. Thus, we denote the received vector by:

$$r = c + e = (mG + e_P)P + e. \tag{7}$$

This algorithm works as follows:

1. Find the inverse permutation, P^{-1}.
2. Multiply both sides of Eq. (7) by P^{-1}:

$$r' = rP^{-1} = mG + e_P + eP^{-1}. \tag{8}$$

3. Subtract the perturbation vector e_P from r':

$$c' = r' - e_P = mG + eP^{-1}. \tag{9}$$

4. Decode c' using a belief propagation algorithm to find m.

Note that the $e' = eP^{-1}$ has the same Hamming weight as e.

Figure 1 shows block diagram of the joint encryption-encoding/decryption-decoding algorithms.

3.4. The code parameters

To deploy a fitting EG-QC-LDPC or PG-QC-LDPC code, length, rate, and density of the parity-check matrix should be chosen properly. Our search results reflect the parameter values for different codes and we have summarized some suitable codes in Tables 1 and 2. Although parameters of any particular future usage may need a value out of this range, we selected only those within the range of existing standards as samples.

3.4.1. Code rate

The code rate of QC-LDPC codes with one block row is:

Table 1. Parameters of EG-QC-LDPC codes designed for the proposed scheme.

n_0	q	m	p	$\mathcal{N}_c$	n	R	r	$log_2(N_{EG})$
6	2	8	255	127	1530	0.833	0.0078	81.7
6	3	6	728	121	4368	0.833	0.0041	88.9
7	7	4	2400	57	16800	0.857	0.0029	107.7
8	2	9	511	255	4088	0.875	0.0039	126.8
9	2	10	1023	511	9207	0.889	0.0020	160.9
15	2	10	1023	511	15345	0.933	0.0020	274.6

Table 2. Parameters of PG-QC-LDPC codes designed for the proposed scheme.

n_0	q	m	p	$\mathcal{N}_c$	n	R	r	$log_2(N_{EG})$
6	2	8	511	85	3066	0.833	0.0059	83.2
6	2	9	1023	170	6138	0.833	0.0029	94.3
8	3	6	1093	91	8744	0.875	0.0037	122.3
11	2	8	511	85	5621	0.909	0.0059	159.5
13	5	5	3906	130	50778	0.923	0.0015	233.6
15	3	7	3280	273	49200	0.933	0.0012	284.3

$$R = \frac{k}{n} = \frac{k_0 p}{n_0 p} = \frac{n_0 - 1}{n_0}. \tag{10}$$

In different communication standards, code rates vary from 1/5 in DVB-S2 [25] to 14/15 in IEEE 802.15.3c [26].

3.4.2. Code length

The code lengths of EG-QC-LDPC and PG-QC-LDPC are as follows using the parameters given in Appendix A:

$$n_{EG} = n_0 p_{EG} = n_0(q^m - 1), \tag{11}$$

$$n_{PG} = n_0 p_{PG} = n_0 \left(\frac{q^{m+1} - 1}{q - 1} \right). \tag{12}$$

Similarly, code lengths in different standards bound our search for suitable parameters from 336 bits in ITU-T G9960 [27] to 64800 bits in DVB-S2 [25].

3.4.3. Parity-check matrix density

A parity-check matrix of density 0.01 or lower is categorized as a low density parity-check matrix. LDPC codes of density about 0.001 have better error performance [28]. The density of the parity-check matrices of EG-QC-LDPC and PG-QC-LDPC codes are given below, respectively:

$$r_{EG} = \frac{\rho}{p} = \frac{q}{q^m - 1}, \tag{13}$$

$$r_{PG} = \frac{\rho}{p} = \frac{q+1}{\frac{q^{m+1}-1}{q-1}} = \frac{q^2 - 1}{q^{m+1} - 1}, \tag{14}$$

where ρ is the Hamming weight of the incident vector of each line in the geometry and p is its length.

4. Security and performance

In order to evaluate a joint encryption-encoding scheme, also known as a secure channel coding scheme, we investigate the scheme from security and efficiency perspectives, namely, key size, error performance, and complexity of the scheme. Our goal in design of the FG-QC-LDPC joint encryption-encoding scheme is to decrease the key size as well as complexity of the scheme while improving error performance in comparison with the so far best previous schemes in the literature. In addition, keeping it secure against all known cryptanalytic attacks.

4.1. Security

Provable security for symmetric key cryptography is an open problem. There exists no natural hard problem to which the security of symmetric schemes can be reduced. To assess the security of symmetric key cryptosystems, there is a method to reduce the security of that scheme to the problem of distinguishing between the output of an oracle which encrypts a message with a random key and an oracle which outputs a random ciphertext [29]. This reduction in oracle model is given [30], for chosen-plaintext attack on symmetric key cryptosystems which is applicable to analyze the security of modes of operations using a secure block cipher. Besides, provable security is a "tool" and old-fashioned cryptanalysis is more reasonable in practical point of view [31].

Based on the level of a priori knowledge, which is available to the cryptanalyst, there are different kinds of cryptanalyses. We have examined our scheme against brute-force, ciphertext-only, message resend, chosen-plaintext attacks, and statistical attack.

4.1.1. Brute-force attack

The secret key consists of the parity-check matrix, H, the permutation matrix, P, and the seed of the $PRNG$, S. These parameters must be chosen large enough in order to keep our scheme secure against brute-force attack.

The number of parity-check matrices of FG-QC-LDPC codes is:

$$N_{FG} = p^{n_0 - 1} \times \frac{\mathcal{N}_c!}{(\mathcal{N}_c - n_0)!}, \tag{15}$$

where $\mathcal{N}_c$ is the number of cyclic classes on that geometry. Let s denote the required security parameter of our scheme, then in Eq. (15) we can simply assign the number of blocks, n_0, and the block size, p, such that $N_{FG} \times N_P \times N_{PRNG} = N_{FG} \times l! \times 2^L > 2^s$, where L is the length of PRNG.

According to this condition and those described in Section 3.4, our search for parameters of the suitable codes has been resulted in various examples summarized in Tables 1 and 2.

4.1.2. Ciphertext-only attack

The goal of this attack is to recover the plaintext from its ciphertext without any knowledge of the key. In code-based cryptosystems, this is interpreted as decoding an encoded message without access to its parity-check or generator matrix. To achieve this goal, the adversary needs to solve the general decoding problem, which is known to be NP-hard problem [2]. This attack was applied on the McEliece-like public-key code-based cryptosystems [32–34], whose public key is algebraically equivalent to their generator matrix. Since in our symmetric key code-based scheme the parity-check matrix is kept secret, the adversary deals with the general decoding problem.

4.1.3. Message resend attack

The aim of the message resend attack is to find the perturbation vector, e_P, used by the transmitter and then recover the message in the following manner. Suppose that the transmitter sends $c_1 = (mG + e_{P1})P$ to the receiver. The attacker, as the man in the middle, alter some bits of c_1 such that the receiver receives a false or undecodable vector. Therefore, the receiver has to make a request to the transmitter for resending the message, m. This time, the transmitter encrypts the same message using a different perturbation vector e_{P2}, as $c_2 = (mG + e_{P2})P$. This scenario is called message resend [35]. In this situation, the attacker has access to two different ciphertexts c_1 and c_2 of the same message m. So the attacker can obtain the following equation and thereby guessing the positions of non-zero entries of e_{P1} and e_{P2}:

$$c_1 - c_2 = (e_{P1} - e_{P2})P. \tag{16}$$

This attack is only feasible when the perturbation vectors have low Hamming weight. Since the used perturbation vectors in the proposed scheme are generated uniformly at random, it is not feasible to find each of e_{P1} and e_{P2} from $c_1 - c_2$. Moreover, the secret permutation matrix, P, changes the location of '1's and '0's.

Apart from these issues while applying this attack, error correction capability of capacity approaching FG-QC-LDPC codes could obviate the need for resending the message. Because the alterations made by the attacker can be recovered by the error correction code. Thus, the message resend attack can be thwarted.

4.1.4. Chosen-plaintext attack

There are two major chosen-plaintext attacks against secret key code-based cryptosystems, namely Struik-Tilburg [5] and Rao-Nam [36] attacks.

Struik and Tilburg [5] proposed chosen-plaintext attacks against secret-key code-based cryptosystems. In this attack two plaintexts m_1 and m_2 are chosen such that they are only different on their ith position, i.e., $m_1 - m_2 = u_i$. As a result, the corresponding ciphertext difference is:

$$\begin{aligned} c_1 - c_2 =& u_i GP + (e_{P1} - e_{P2})P \\ =& g'_i + (e_{P1} - e_{P2})P, \end{aligned} \tag{17}$$

where g'_i is the ith row of the generator matrix $G' = GP$. The attacker repeats the procedure for the same u_i and different perturbation vectors e_P until a set of all possible ciphertexts differing on ith position, namely u_i, for $i = 1, \ldots, n$ are collected. The cardinality of this set is equal to the number of total perturbation vectors, N_e. Doing a brute-force over all perturbation vectors, g'_i is obtained. Repeating the above scenario for all i reveals the whole matrix G'.

The work factor of this attack is of $O(knN_e^2 log_2(N_e))$ [36]. Therefore, this attack will be successful only if the set of all perturbation vectors, N_e, is of small cardinality. In FG-QC-LDPC joint encryption-encoding scheme $N_e = 2^{(n-k)} = 2^p$ and according to Tables 1 and 2, $p \geq 255$. Therefore the work factor of this attack is at least $1275 \times 1530 \times 2^{510} \times 255$, which is dramatically large and therefore the Struik-Tilburg attack is not applicable to the FG-QC-LDPC joint encryption-encoding scheme in polynomial time.

Rao and Nam [36] proposed their attack based on the previously mentioned Struik-Tilburg [5] attack. They similarly used chosen-plaintexts m_1 and m_2 differing only in one position. They noticed that when the perturbation vectors has low Hamming distance the attacker can use majority voting to estimate g'_i and thereby revealing the whole matrix G'. The work factor of this attack, obtained by Rao and Nam [36], is $O(N_e^k)$. Based on Tables 1 and 2, The work factor of this attack on our proposed scheme is at least $(2^{255})^{1275}$. Therefore, the FG-QC-LDPC joint scheme is far more secure to be threatened by this attack.

4.1.5. Statistical attack

This type of attack include reaction attacks and timing attacks. In the following we investigate our proposed cryptosystem against both kinds of attacks.

Reaction attacks have been proposed against McEliece-like public key cryptosystems. We show that these attacks are not feasible on symmetric cryptosystems including our proposed scheme.

A reaction attack has been proposed on MDPC codes based on a statistical fact that if the parity-check matrix has distance d in one of their circulant blocks, the probability of failed decoding of error vectors having two 1s with the same distance is relatively low [37]. In [23], they extended this attack to QC-LDPC based cryptosystems. They argued that in such systems even multiplying error vector e by a

matrix Q, instead of permutation matrix with greater row and column Hamming weight than that of P, would not prevent the reaction attack because eQ also contains 1 entries with distance d with high probability. According to [23], the attacker can learn the distances between '1's in eQ when Q is composed of circulant blocks of size $p \times p$. However, in our proposed scheme the secret permutation matrix P, instead of a quasi-cyclic matrix Q, changes the distances between '1's in the error vector eP^{-1}, hence the attacker could not learn information about the distances in eP^{-1} and consequently in H.

QC-LDPC codes with higher Decoding Failure Rates (DFR) are known to be vulnerable to reaction attacks. Using monomial codes has been proposed to achieve a lower DFR [38]. Several studies proposed theoretical models and bounds for the DFR under different decoding algorithms [39–41]. However, instead of lowering the DFR, our proposed scheme uses the secret permutation matrix to mask the information which is used to apply the reaction attack introduced in [23].

An adversary may want to recover an equivalent version of the secret parity-check matrix $\tilde{H} = HP$. In this case $\tilde{H}$ is the parity-check matrix of $\tilde{G} = GP$ because $\tilde{G}\tilde{H}^T = GPP^TH^T = GH^T = 0$. The adversary needs to reconstruct both $\tilde{H}$ and e_PP to decode the received vector:

$$r = (mG + e_P)P + e = mGP + e_PP + e$$

$$\Rightarrow r - e_PP = mGP + e. \tag{18}$$

In our proposed scheme the size of permutation blocks in P, l, is chosen such that $l \nmid p$. Therefore, $\tilde{H} = HP$ is not quasi-cyclic and the attack in [23] is not feasible. Moreover, e_PP is secret and the adversary cannot even reach to the $r - e_PP$ in Eq. (18). For McEliece-like public key cryptosystems, using the condition $l \nmid p$ is worth considering whether it would thwart reaction attacks.

Timing attack is a kind of side-channel attacks exploiting the duration of decoding process to gain information about the private key. By performing constant-time decoding algorithm the proposed scheme is remained secure against timing attacks [42]. Generally, we can protect the cryptosystem against statistical attacks by refreshing keys every while.

4.2. Key size

The secret key of the FG-QC-LDPC joint encryption-encoding scheme as mentioned in Section 3.1 consists of the seed vector for a PRNG (S), the parity-check matrix (H), and the permutation matrix (P):

$$|K_s| = |S| + |K_P| + |K_H| \tag{19}$$

First, choosing a suitable PRNG for each application, keeps the size of the seed at a desirable extent. Comparing PRNGs is not in the scope of this paper. However, as pointed in Section 1, it is not recommended to use simple LFSRs based on the reasons mentioned in [12]. In our example, we use Sosemanuk-128 stream cipher as an example of PRNG [43]. The size of the seed vector of this PRNG is only 128 bits.

Owing to quasi-cyclic structure of the parity-check matrix, storing only the first row of each circulant block of this matrix suffices to create the parity-check matrix. Furthermore, thanks to the finite geometry construction of these blocks, the whole first row of each block can be produced by only knowing the location of two "1"s on each. Since each row is an incident vector of a line on finite geometry, the two "1"s indicate the two points where a line go through them. Thus, these two location numbers can regenerate the line and its incident vector.

We introduce a practical method to achieve the information theoretic lower bound for storing the first row of each circulant block. In this regard, we need to identify two things, the representative of cyclic class and the number of cyclic right shift to obtain the first row. The following constraints must be considered to assign a unique line as a representative for each cyclic class:

(i) The first element of its incident vector must be "1";

(ii) The next "1" in the incident vector must be located at the nearest possible locations among all lines of the class.

If the non-zero elements of the incident vector of the representative are $\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_\rho}$, (i) forces that $j_1 = 0$ and (ii) forces $j_2 - j_1 < \min(j_{i+1} - j_i), (j_1 - j_\rho)(modp)$. By using this method we only store j_2 to indicate the cyclic class. This needs only $\lceil \log_2(\frac{p}{\rho}) \rceil$ bits. Another $\lceil \log_2(p) \rceil$ bits is needed to indicate the amount of cyclic shift for the first row of each block. As a result, the amount of memory to store each circulant block of FG-QC-LDPC parity-check matrix is:

$$\lceil \log_2(\frac{p}{\rho}) \rceil + \lceil \log_2(p) \rceil \quad bits. \tag{20}$$

While a permutation in the rows of the parity-check matrix makes no difference in the code, we can suppose that the first circulant block (or one of the others) made by the representative without being cyclically shifted. As a result, the whole parity-check matrix with one block row and n_0 blocks needs the following amount of memory to be stored:

$$|K_H| = n_0 \times \lceil \log_2(\frac{p}{\rho}) \rceil + (n_0 - 1) \times \lceil \log_2(p) \rceil \ bits. \tag{21}$$

The block diagonal permutation matrix, P, in this

scheme will be stored in similar way as in [6]. The size of the permutation matrix of the key is as follows. Where l is the length of each block and $l' = 2^{\lfloor \log_2(l) \rfloor}$:

$$|K_P| = l(\log_2 l' + 1) - 2l' + 1. \quad (22)$$

Tables 3 and 4 show examples of codes and their key sizes for 220 bits and 270 bits security parameters, respectively.

The key size of the proposed scheme, taking the advantages of FG-QC-LDPC codes, is only 235 bits. Table 5 compares the key size of the proposed cryptosystem with those known similar ones. However, one needs to perform $N_{FG} \times N_P \times N_{PRNG} \cong 2^{220}$ computations to recover the key that means our effective key size is 220 bits. In Table 6, we compare the key sizes of the recent cryptosystems along with their effective key sizes (target security levels).

4.3. Error performance

At the receiver the FG-QC-LDPC code used in our system is decoded by a logarithmic Sum-Product decoder. We took the following considerations to simulate encoding, channel, and decoding processes. In our simulation codewords transmitted via a Binary Phase Shift Keying (BPSK) channel with additive white Gaussian noise. The receiver has access to soft information of channel. We compared decoders of 10 and 100 iterations with a Reed-Solomon code in Figure 2. This figure shows that there is no remarkable improvement in 100 iterations decoding in compare to 10 iterations.

Figure 2 shows the error performance using simple logarithmic Sum-Product decoder. In cryptography, there is typically a trade-off between security and performance. To reach a better error performance with a lower error floor extensive analysis is required which is beyond the scope of this work. We will consider some modifications in the decoding algorithm for LDPC codes, such as those in [45–47], and examine the feasibility of having reduced error floor in our future work.

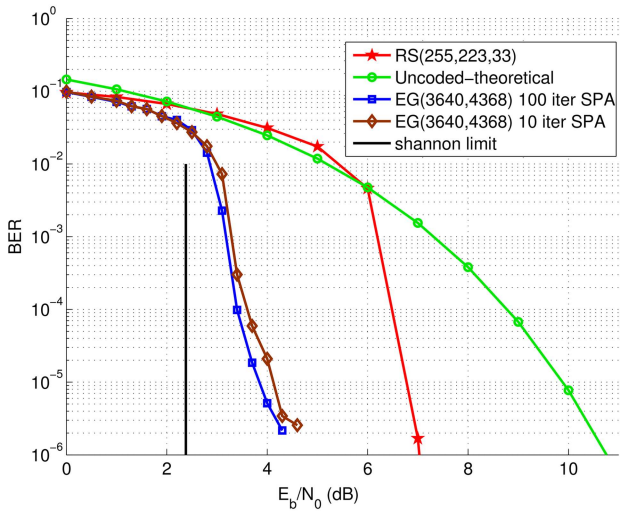

Figure 2. Performance comparison of log-SPA decoder of 10 and 100 iterations with Reed-Solomon code.

4.4. Complexity

There are two separate process which their computational complexity needs to be assessed, encryption-encoding and decryption-decoding processes.

4.4.1. Encryption-encoding

The complexity of this process can be calculated as follows:

$$\mathcal{C}_{Enc} = \mathcal{C}_{mul}(mG) + \mathcal{C}_{add}(mG + e_P) + \mathcal{C}_{mul}(H^{-1}.s) + \mathcal{C}_{mul}(P). \quad (23)$$

In this equation $\mathcal{C}_{add}(mG + e_P)$ stands for adding two n-bit vectors which consume n binary operations.

Table 3. The key size of the proposed system with more than 220 bits security parameter.

Secret key parts	Proposed parameters	Computational complexity to find key	Key size
H	$q = 2, m = 8, n_0 = 6$	$2^{81.7}$	82 bits
P	$l = 10$	$2^{21.8}$	25 bits
S	Sosemanuk-128	$> 2^{120}$	128 bits
	Total	$> 2^{220}$	**235 bits**

Table 4. The key size of the proposed system with more than 270 bits security parameter.

Secret key parts	Proposed parameters	Computational complexity to find key	Key size
H	$q = 3, m = 6, n_0 = 6$	$2^{88.87}$	98 bits
P	$l = 21$	$2^{65.46}$	74 bits
S	Sosemanuk-128	$> 2^{120}$	128 bits
	Total	$> 2^{270}$	**300 bits**

Table 5. Comparison of the key size of the proposed scheme with the preceding schemes.

Cryptosystem	Code	Key size
Rao [3]	C(1024,524)	2 Mbits
Rao-Nam [36]	C(72,64)	18 Kbits
Struik-Tilburg [5]	C(72,64)	18 Kbits
Barbero-Ytrehus [6]	C(30,20) over $GF(2^8)$	4.9 Kbits
Sobhi Afshar et al. [44]	C(2044,1024)	2.5 Kbits
Hooshmand et al. [7]	C(2470,2223)	3.55 Kbits
Esmaeili et al. [8]	C(2048,1536)	2191 bits
Esmaeili Gulliver [9]	C(2048,1536)	2272 bits
Mafakheri et al. [13]	C(2048,1781)	1611 bits
Guan-Liang [16]	C(2040,1020)	864 bits
Han et al. [14]	C(1024,620)	686 bits
Bagheri et al. [17]	C(258,215)	252 bits
Stuart-Deepthi [15]	C(248,124)	182 bits
The proposed Scheme I	C(1530,1275)	235 bits
The proposed Scheme II	C(4368,3640)	300 bits

Table 6. Comparison of the key size and security level of the proposed scheme with the recent schemes.

Cryptosystem	Target security level	Code	Key size
Han et al. [14]	597 bits	C(1024,620)	686 bits
Bagheri et al. [17]	178 bits	C(258,215)	252 bits
Stuart-Deepthi [15]	129 bits	C(248,124)	182 bits
The proposed Scheme I	220 bits	C(1530,1275)	235 bits
The proposed Scheme II	270 bits	C(4368,3640)	300 bits

Multiplying a vector by a sparse matrix a_{1n}, B_{nn}, needs nw binary operations [48], where w is the Hamming weight of rows of the sparse matrix. Here permutation matrix, P, has $w = 1$ so $\mathcal{C}_{mul}(P) = n$.

The generator matrix, G, and the inverse of parity-check matrix, H^{-1}, are dense matrices and need kn and $(n-k)n$ binary operations respectively. By the way, their quasi-cyclic property leads to a 92% lower computational complexity in multiplying operations [48]. Therefor, one could conclude that:

$$\mathcal{C}_{Enc} = 0.08 \times k.n + n + 0.08 \times (n-k).n + n = \frac{0.08n + 2}{R}, \quad (24)$$

where $R = \frac{k}{n}$.

4.4.2. Decryption-decoding

The complexity of this process is obtained as follow:

$$\mathcal{C}_{Dec} = \mathcal{C}_{mul}(r \times P^{-1}) + \mathcal{C}_{add}(r' + e_P), \mathcal{C}_{mul}(H^{-1}s) + \mathcal{C}_{mul}(c' \times H^T) + \mathcal{C}_{SPA}. \quad (25)$$

The complexity of the Sum-Product Algorithm, as mentioned in [48], is:

$$\mathcal{C}_{SPA} = I_{avg}.n[d(8\rho + 12R - 11) + \rho]. \quad (26)$$

In this equation I_{avg} is the average number of decoding iterations and d is the number of quantization bits in analog-to-digital converter. Finally letting $I_{avg} = 10$ and $d = 6$, the number of binary operations for each information bit to be decrypted-decoded is:

$$\mathcal{C}_{Dec/k} = \frac{1}{R}(2 + n - k + n_0\rho + 490\rho + 720R - 110). \quad (27)$$

In this equation it could be seen that the complexity of decryption-decoding algorithm is linearly proportional to the redundancy $(n-k)$.

5. Conclusion

This paper introduces a joint encryption-encoding scheme, also known as secure channel coding, using QC-LDPC codes based on finite geometry. We have taken advantage of FG-QC-LDPC codes to shorten the secret key to 235 bits for 220 bits security level.

Thanks to the LDPC codes and their fast iterative decoding, the error performance of the proposed scheme is among the best of the literature. The FG-QC-LDPC joint encryption-encoding scheme is secure against cryptanalyses of code-based cryptosystems. We

have also proposed an idea that makes symmetric key QC-LDPC cryptosystems secure against reaction attacks. It is worth considering if this idea makes McEliece-like public key cryptosystems secure against reaction attacks.

The joint algorithm leads to lower complexity than conventional encryption-then-encoding methods. We have shown that our system can provide reliability and security simultaneously with the lower cost of one joint system rather than two disjoint systems.

References

1. McEliece, R.J. "A public-key cryptosystem based on algebraic coding theory", *DSN Progress Report*, **42**(44), pp. 114–116 (1978). NASA Code 310-10-67-11
2. Berlekamp, E., McEliece, R., and van Tilborg, H. "On the inherent intractability of certain coding problems (corresp.)", *IEEE Transactions on Information Theory*, **24**(3), pp. 384–386 (1978). DOI: 10.1109/TIT.1978.1055873
3. Rao, T.R.N. "Joint encryption and error correction schemes", *ACM SIGARCH Computer Architecture News*, **12**(3), pp. 240–241 (1984). DOI: 10.1145/773453.808188
4. Rao, T. and Nam, K.H. "Private-key algebraic-coded cryptosystems", in *Advances in Cryptology - CRYPTO' 86*, **263**, (Santa Barbara, California, USA), pp. 35–48, Springer, August (1986). DOI: 10.1007/3-540-47721-7_3
5. Struik, R. and van Tilburg, J. "The Rao-Nam scheme is insecure against a chosen-plaintext attack", in *Advances in Cryptology - CRYPTO '87*, **293**, (Santa Barbara, California, USA), pp. 445–457, Springer, August (1987). DOI: 10.1007/3-540-48184-2_40
6. Barbero, Á.I. and Ytrehus, Ø. "Modifications of the rao-nam cryptosystem", in *Coding Theory, Cryptography and Related Areas*, (Berlin, Heidelberg), pp. 1–12, Springer (2000). DOI: 10.1007/978-3-642-57189-3_1
7. Hooshmand, R., Eghlidos, T., and Aref, M.R. "Improving the Rao-Nam secret key cryptosystem using regular EDF-QC-LDPC codes", *The ISC International Journal of Information Security*, **4**(1), pp. 3–14 (2012). DOI: 10.22042/isecure.2015.4.1.2
8. Esmaeili, M., Dakhilalian, M., and Gulliver, T.A. "New secure channel coding scheme based on randomly punctured quasi-cyclic-low density parity check codes", *IET Communications*, **8**(14), pp. 2556–2562 (2014). DOI: 10.1049/iet-com.2014.0101
9. Esmaeili, M. and Gulliver, T.A. "Joint channel coding-cryptography based on random insertions and deletions in quasi-cyclic-low-density parity check codes", *IET Communications*, **9**(12), pp. 1555–1560 (2015). DOI: 10.1049/iet-com.2015.0026
10. Esmaeili, M. and Gulliver, T.A. "A secure code based cryptosystem via random insertions, deletions, and errors", *IEEE Communications Letters*, **20**(5), pp. 870–873 (2016). DOI: 10.1109/LCOMM.2016.2540625
11. Esmaeili, M. and Gulliver, T.A. "Code-based security with random interleaving", *IET Communications*, **11**(8), pp. 1195–1198 (2017). DOI: 10.1049/iet-com.2016.0303
12. Lee, Y., Kim, Y.-S., and No, J.-S. "Ciphertext-only attack on linear feedback shift register-based Esmaeili-Gulliver cryptosystem", *IEEE Communications Letters*, **21**(5), pp. 971–974 (2017). DOI: 10.1109/LCOMM.2017.2654238
13. Mafakheri, B., Eghlidos, T., and Pilaram, H. "An efficient secure channel coding scheme based on polar codes", *The ISC International Journal of Information Security*, **9**(2), pp. 13–20 (2017). DOI: 10.22042/isecure.2017.84609.380
14. Han, X., Chen, D., Zhang, C., et al. "Joint encryption and channel coding scheme based on balancing indices and polar codes", in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, pp. 276–282, October (2019). DOI: 10.1109/ICCT46805.2019.8947156
15. Stuart, C.M. and Deepthi, P. "Nonlinear cryptosystem based on qc-ldpc codes for enhanced security and reliability with low hardware complexity and reduced key size", *Wireless Personal Communications*, **96**(3), pp. 4177–4197 (2017). DOI: 10.1007/s11277-017-4376-z
16. Guan, W. and Liang, L. "Efficient secure channel coding based on qpp-block-ldpc codes", *Wireless Personal Communications*, **98**(1), pp. 1001–1014 (2018). DOI: 10.1007/s11277-017-4905-9
17. Bagheri, K., Eghlidos, T., Sadeghi, M.R., et al. "A joint encryption, channel coding and modulation scheme using QC-LDPC lattice-codes", *IEEE Transactions on Communications*, **68**(8), pp. 4673–4693 (2020). DOI: 10.1109/TCOMM.2020.2996781
18. Baldi, M., Chiaraluce, F., Garello, R., et al. "Quasi-cyclic low-density parity-check codes in the mceliece cryptosystem", in *Proc. 2007 IEEE International Conference on Communications*, (Glasgow, UK), pp. 951–956, June (2007). DOI: 10.1109/ICC.2007.161
19. Baldi, M. and Chiaraluce, F. "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes", in *Proc. 2007 IEEE International Symposium on Information Theory*, (Nice, France), pp. 2591–2595, June (2007). DOI: 10.1109/ISIT.2007.4557609
20. Baldi, M., Bianchi, M., Maturo, N., et al. "Improving the efficiency of the LDPC code-based McEliece cryptosystem through irregular codes", in *Proc. 2013 IEEE Symposium on Computers and Communications (ISCC)*, (Split, Croatia), pp. 197–202, July (2013). DOI: 10.1109/ISCC.2013.6754945
21. Lin, S. and Costello, D.J., *Error Control Coding: Fundamentals and Applications.*, Pearson-Prentice Hall (2004). ISBN: 0130426725
22. Ryan, W. and Lin, S., *Channel Codes: Classical and Modern.* Cambridge University Press (2009). ISBN 1139483013, 9781139483018

23. Fabšič, T., Hromada, V., Stankovski, P., et al. "A reaction attack on the QC-LDPC McEliece cryptosystem", in *Post-Quantum Cryptography*, (Cham), pp. 51–68, Springer, June (2017). DOI: 10.1007/978-3-319-59879-6_4

24. Ben-Israel, A. and Greville, T.N., *Generalized Inverses: Theory and Applications*, **15**. Springer Science & Business Media (2003). DOI: 10.1007/b97366

25. ETSI, "Digital video broadcasting (dvb); implementation guidelines for the second generation system for broadcasting, interactive services, news gathering and other broadband satellite applications; part 1: Dvb-s2" (2015).

26. IEEE, "Wireless medium access control (mac) and physical layer (phy) specifications for high rate wireless personal area networks (wpans) amendment 2: Millimeter-wave-based alternative physical layer extension" (2009).

27. ITU-T, "Unified high-speed wireline-based home networking transceivers - system architecture and physical layer specification" (2015).

28. Baldi, M., Bianchi, M., and Chiaraluce, F. "Optimization of the parity-check matrix density in qc-ldpc code-based mceliece cryptosystems", in *Proc. 2013 IEEE International Conference on Communications Workshops (ICC)*, (Budapest, Hungary), pp. 707–711, June (2013). DOI: 10.1109/ICCW.2013.6649325

29. Dent, A.W. "Fundamental problems in provable security and cryptography", *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, **364**(1849), pp. 3215–3230 (2006). DOI: 10.1098/rsta.2006.1895

30. Bellare, M., Desai, A., Jokipii, E., et al. "A concrete security treatment of symmetric encryption", in *Proc. 38th Annual Symposium on Foundations of Computer Science*, (Miami Beach, FL, USA), pp. 394–403, IEEE, October (1997). DOI: 10.1109/SFCS.1997.646128

31. Menezes, A. "Another look at provable security", in *Advances in Cryptology - EUROCRYPT 2012*, **7237**, (Cambridge, UK), p. 8, Springer, April (2012). DOI: 10.1007/978-3-642-29011-4_2

32. Lee, P.J. and Brickell, E.F. "An observation on the security of McEliece's public-key cryptosystem", in *Advances in Cryptology - EUROCRYPT '88*, **330**, (Davos, Switzerland), pp. 275–280, Springer, May (1988). DOI: 10.1007/3-540-45961-8_25

33. Becker, A., Joux, A., May, A., et al. "Decoding random binary linear codes in 2 n/20: how 1 + 1 = 0 improves information set decoding", in *Advances in Cryptology - EUROCRYPT 2012*, **7237**, (Cambridge, UK), pp. 520–536, Springer, April (2012). DOI: 10.1007/978-3-642-29011-4_31

34. May, A. and Ozerov, I. "On computing nearest neighbors with applications to decoding of binary linear codes", in *Advances in Cryptology-EUROCRYPT 2015*, **9056**, (Sofia, Bulgaria), pp. 203–228, April (2015). DOI: 10.1007/978-3-662-46800-5_9

35. Berson, T.A. "Failure of the McEliece public-Key cryptosystem under message-resend and related-message attack", in *Advances in Cryptology - CRYPTO '97*, **1294**, (Santa Barbara, California, USA), pp. 213–220, Springer, August (1997). DOI: 10.1007/BFb0052237

36. Rao, T. and Nam, K.H. "Private-key algebraic-code encryptions", *IEEE Transactions on Information Theory*, **35**(4), pp. 829–833 (1989). DOI: 10.1109/18.32159

37. Guo, Q., Johansson, T., and Stankovski, P. "A key recovery attack on mdpc with cca security using decoding errors", in *Advances in Cryptology - ASIACRYPT 2016*, **10031**, (Berlin, Heidelberg), pp. 789–815, Springer, November (2016). DOI: 10.1007/978-3-662-53887-6_29

38. Santini, P., Baldi, M., Cancellieri, G., et al. "Hindering reaction attacks by using monomial codes in the mceliece cryptosystem", in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 951–955 (2018). DOI: 10.1109/ISIT.2018.8437553

39. Tillich, J.-P. "The decoding failure probability of mdpc codes", in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 941–945 (2018). DOI: 10.1109/ISIT.2018.8437843

40. Santini, P., Battaglioni, M., Baldi, M., et al. "Analysis of the error correction capability of ldpc and mdpc codes under parallel bit-flipping decoding and application to cryptography", *IEEE Transactions on Communications*, **68**(8), pp. 4648–4660 (2020). DOI: 10.1109/TCOMM.2020.2987898

41. Santini, P., Battaglioni, M., Baldi, M., et al. "Hard-decision iterative decoding of ldpc codes with bounded error rate", in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6 (2019). DOI: 10.1109/ICC.2019.8761536

42. Santini, P., Battaglioni, M., Chiaraluce, F., et al. "Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes", in *Code-Based Cryptography*, (Cham), pp. 115–136, Springer, July (2019). DOI: 10.1007/978-3-030-25922-8_7

43. Berbain, C., Billet, O., Canteaut, A., et al. "Sosemanuk, a fast software-oriented stream cipher", *Lecture Notes in Computer Science*, **4986**, pp. 98–118 (2008). DOI: 10.1007/978-3-540-68351-3_9

44. Sobhi Afshar, A., Eghlidos, T., and Aref, M.R. "Efficient secure channel coding based on quasi-cyclic low-density parity-check codes", *IET Communications*, **3**(2), pp. 279–292 (2009). DOI: 10.1049/iet-com:20080050

45. Zhang, Z., Dolecek, L., Nikolic, B., et al. "Lowering ldpc error floors by postprocessing", in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, pp. 1–6 (2008). DOI: 10.1109/GLOCOM.2008.ECP.590

46. Zhang, S. and Schlegel, C. "Controlling the error floor in ldpc decoding", *IEEE Transactions on Communications*, **61**(9), pp. 3566–3575 (2013). DOI: 10.1109/TCOMM.2013.071813.120659

47. Angarita, F., Valls, J., Almenar, V., et al. "Reduced-complexity min-sum algorithm for decoding ldpc codes with low error-floor", *IEEE Transactions on Circuits and Systems I: Regular Papers*, **61**(7), pp. 2150–2158 (2014). DOI: 10.1109/TCSI.2014.2304660

48. Baldi, M., Bodrato, M., and Chiaraluce, F. "A new analysis of the mceliece cryptosystem based on qc-ldpc codes", *Security and Cryptography for Networks*, **5229**, pp. 246–262 (2008). DOI: 10.1007/978-3-540-85855-3_17

Appendix A

Finite geometry definitions

The definitions of finite geometry in this Appendix are generally provided from [21] and [22].

Euclidean geometry

Definition 1 (Euclidean geometry). All m-tuples $(a_0, a_1, \ldots, a_{m-1})$ with a_i from $GF(q = p^s)$ where p is prime and s is a natural number form a vector space. This vector space is also known as the finite Euclidean geometry of dimension m over $GF(q)$, denoted by $EG(m, q)$. Vector additions and scalar multiplications of these m-tuples are conducted in $GF(q)$.

Definition 2 (Point). Each m-tuple $\mathbf{a} = (a_0, a_1, \ldots, a_{m-1})$ represents a point in $EG(m, q)$.

Definition 3 (Origin). The all-zero m-tuple $\mathbf{0} = (0, 0, \ldots, 0)$ is called the origin.

Definiton 4 (Line). The set of $\{\mathbf{a_0} + \beta\mathbf{a} | \beta \in GF(q), \mathbf{a} \neq \mathbf{0}\}$ is a line, which is composed of q points.

The number of points in $EG(m, q)$ is equal to the number of all m-tuples i.e., $n = q^m$. For every two distinct points there exists exactly one line connecting them. The number of lines intersecting at each point can be obtained by dividing the number of possible second points of that line by the number of other points in each line:

$$\gamma = \frac{q^m - 1}{q - 1}. \tag{A.1}$$

Therefore, the number of lines in the $EG(m, q)$ is as follows:

$$J = q^{m-1}\frac{q^m - 1}{q - 1}. \tag{A.2}$$

Euclidean geometry without origin

By omitting the origin and all lines intersecting at the origin, a new geometry appears which is denoted by $EG^*(m, q)$.

If α is primitive in $GF(q^m)$, then α^i for $0 \leq i \leq q^m - 2$ represents the elements of $GF(q^m)$. So the incident vector of line F is as given below:

$$V_F = (v_0, v_1, \ldots, v_{q^m-2}), \tag{A.3}$$

where, $v_i = 1$ if the line F intersects at point α^i, otherwise $v_i = 0$.

In this geometry, a circularly shifted incident vector of a line is an incident vector for another line [22]. This property partitions the set of all lines, J_o, into $\mathcal{N}_{c,EG^*}$ cyclic classes:

$$\mathcal{N}_{c,EG^*} = \frac{J_o}{n} = \frac{q^{m-1} - 1}{q - 1}. \tag{A.4}$$

These cyclic classes enable us to generate circulant blocks for parity-check matrices of QC-LDPC codes. All the necessary information of Euclidean geometry is summarized in Table A.1.

Projective geometry

Consider the Galois field $GF(q^{m+1})$ and α, a primitive element in this field. So $\alpha^0, \alpha^1, \ldots, \alpha^{q^{m+1}-2}$ constitute all non-zero elements of $GF(q^{m+1})$. Let $n = \frac{q^{m+1}-1}{q-1}$ and $\beta = \alpha^n$. Therefore the order of α is $q - 1$. Now, $0, \beta^0, \beta^1, ..., \beta^{q-2}$ form the elements of $GF(q)$. Considering the definition of α and β, all non-zero elements of $GF(q^{m+1})$ could be partitioned into n disjoint subsets as shown below:

$$\begin{aligned}
&(\alpha^0) \triangleq \{\alpha^0, \beta\alpha^0, \beta^2\alpha^0, \ldots, \beta^{q-2}\alpha^0\}\\
&(\alpha^1) \triangleq \{\alpha^1, \beta\alpha^1, \beta^2\alpha^1, \ldots, \beta^{q-2}\alpha^1\}\\
&\vdots\\
&(\alpha^{n-1}) \triangleq \{\alpha^{n-1}, \beta\alpha^{n-1}, \beta^2\alpha^{n-1}, \ldots, \beta^{q-2}\alpha^{n-1}\}
\end{aligned} \tag{A.5}$$

Table A.1. Parameters of the euclidean geometry.

Parameters	$EG(m, q)$	$EG^*(m, q)$
Field	$GF(q)$	$GF(q)$
Dimension	m	m
No. of points	$n = q^m$	$n = q^m - 1$
No. of lines	$J = q^{m-1}\frac{q^m-1}{q-1}$	$J_o = \frac{(q^{m-1}-1)(q^m-1)}{q-1}$
No. of points in each line	$\rho = q$	$\rho = q$
No. of lines intersecting at each point	$\gamma = \frac{q^m-1}{q-1}$	$\gamma = \frac{q^m-1}{q-1} - 1$
No. of cyclic classes	–	$\mathcal{N}_{c,EG^*} = \frac{J_o}{n} = \frac{q^{m-1}-1}{q-1}$

Table A.2. Parameters of the projective geometry.

Parameters	Value
Field	$GF(q)$
Dimension	m
No. of field's elements that consist each point	$q-1$
No. of points	$n=\frac{q^{m+1}-1}{q-1}$
No. of lines	$J=\frac{n\gamma}{\rho}=\frac{(q^{m+1}-1)(q^m-1)}{(q-1)(q-1)(q+1)}$
No. of points in each line	$\rho=q+1$
No. of lines intersecting at each point	$\gamma=\frac{q^m-1}{q-1}$
No. of cyclic classes (even m)	$\mathcal{N}_{c,even}=\frac{q^m-1}{q^2-1}$
No. of cyclic classes (odd m)	$\mathcal{N}_{c,odd}=\frac{q(q^{m-1}-1)}{q^2-1}$

Each of the above subsets represents a distinct point in projective geometry, denoted by $PG(m,q)$. In this geometry, each line consists of $q+1$ points, formed by linear combination of two distinct α^{j_1} and α^{j_2} points:

$$(\eta_1\alpha^{j_1}+\eta_2\alpha^{j_2});\quad \eta_i\in GF(q). \tag{A.6}$$

The number of lines intersecting at every particular point is $\gamma=\frac{n-1}{q}=\frac{q^m-1}{q-1}$, which is obtained by dividing the remaining number of points chosen as the second point of line $(=n-1)$ by the number of other points in each line $(=q)$.

Let $F=(\eta_1\alpha^{j_1}+\eta_2\alpha^{j_2});\eta_i\in GF(q)$ be a line in $PG(m,q)$, then for all $0\leq i<n$, α^iF is also a line in $PG(m,q)$. The α^iF is called the ith circular shift of line F.

If m is even, all lines in $PG(m,q)$ have primitive incident vector and partitioned into $\mathcal{N}_{c,even}=\frac{q^m-1}{q^2-1}$ cyclic classes, where each cyclic class consists of n lines. If m is odd, only J_0 lines of $PG(m,q)$ have primitive incident vector [22]:

$$J_o=\frac{q(q^{m+1}-1)(q^{m-1}-1)}{(q^2-1)(q-1)}. \tag{A.7}$$

These incident vectors are partitioned into $\mathcal{N}_{c,odd}$ cyclic classes:

$$\mathcal{N}_{c,odd}=\frac{q(q^{m-1}-1)}{(q^2-1)}. \tag{A.8}$$

Table A.2 summarizes necessary information of the projective geometry.

In finite geometry, since there is exactly one line connecting two distinct points, no two incident vectors have more than one non-zero elements in the same location. As a result of this property, the girth of QC-LDPC codes based on finite geometry is at least 6.

Biographies

Hossein Khayami received his BSc degree in Electrical Engineering - Telecommunications from University of Tehran, in 2013, and the MSc degree in Electrical Engineering-Communications from Sharif University of Technology, in 2015. His research interests include wireless communications, Internet of Things, coding theory and its application in distributed computing.

Taraneh Eghlidos received her BSc degree in mathematics from the University of Shahid Beheshti, Tehran, Iran, in 1986, and the MSc degree in industrial mathematics from the University of Kaiserslautern, Germany, in 1991. She received her PhD degree in mathematics from the University of Giessen, Germany, in 2000. She joined the Sharif University of Technology (SUT) in 2002, as the faculty member, and is currently an Associate Professor with the Electronics Research Institute at SUT. Her research interests include interdisciplinary research areas, such as symmetric and asymmetric cryptography, applications of coding theory in cryptography, and mathematical modeling for representing and solving real world problems. Her current fields of research include lattice-based and code-based cryptography.

Mohammad Reza Aref received the BSc degree from School of Electrical and Computer Engineering, University of Tehran, in 1975. The MSc and PhD degrees from Stanford University, Stanford, CA, USA, in 1976 and 1980, respectively. He was the Faculty member of Isfahan University of Technology from 1982 to 1997. Since 1997, he is the Professor of Electrical Engineering at Sharif University of Technology. He has published 470 technical papers in the field of Communication and Information Theory and Cryptography in international journals and conferences proceedings.