Secure Modified QC- LDPC Code Based McEliece Public key Encryption Scheme

Renuka Sahu[1], B.P. Tripathi[2]
[1,2]Dept. of Mathematics, Govt. N. P.G College of Science, Raipur (C.G), India

ABSTRACT
In this paper, a modified method of QC-LDPC McEliece cryptosystem is presented. Authors of [3] suggested that the recovery of Q is possible by an adversary using power trace method. To overcome with this problem, we present a modification in the existing scheme so that QC-LDPC McEliece cryptosystem by using a random linear non-singular matrix. And also we have tried to hide the structure of the generator matrix. The modified scheme has the ability to detect all the errors and correct nearly up to 30% of the errors that occurs. Thus, it has better error correcting capacity than the existing schemes.

I INTRODUCTION

With the rapid development of technologies, our society is concerned completely upon the security of current public key infrastructures. The fundamental components for current public key infrastructure are based on public cryptographic strategies like RSA and DSA, etc. However, which was proved that these cryptographic strategies would be simply broken by the super powerful quantum computers. Thus, it becomes very important to develop some new public key cryptographic strategies in such a way that the new PKC method would be secure against quantum attack.

In 1978, Robert. J. McEliece presents a public key cryptosystem primarily based t-error correcting Goppa codes [10], which is known as McEliece cryptosystem. The general decoding problem of the linear block codes is NP-Complete, which was hard to handle. McEliece Cryptosystem has been considered as one of the candidate for the post-quantum cryptography. The originalversion of McEliece cryptographic scheme uses Goppa codes. As compared with the other cryptographic schemes like RSA, McEliece cryptographic schemes have high-speed encryption/ decryption algorithms. However, because of its large public key size and low code rate aren't in demand these days. To overcome these drawbacks of McEliece Cryptosystem, a number of variants are introduced by replacing the Goppa code with the other significant codes. For example, H. Niederreiter et al. [12] presented "GRS Codes" primarily based scheme. Then sub codes of H. Niederreiter were suggested by T. Berger and Loidreau [16]. V. M. Sidelnikov et al. [17] used "R. M. codes", H. Janwa and Morena [5] used "Algebraic Geometric codes", M. Baldi et al. [1] used "Low-Density parity check (LDPC) codes, and Misoczki et al. [11] used "Moderate Density Parity Check (MDPC) codes, and Londahl et al. [7] used "Convolutional Codes". Most of these cryptographic schemes have been broken through Moderate density parity check codes (MDPC) / Low density parity check codes (LDPC) based on McEliece cryptographic encryption schemes. Recently in [18] RLCE Scheme is presented using Hexi code was presented .The original McEliece Cryptographic encryption scheme was considered to be secure.

In [1], Baldi and Chiaralue introduced "quasi-cyclic low density parity check code (QC- LDPC codes)" in the McEliececryptosystem which reduces its public key size. The Cryptosystem is now called as the QC-LDPC McEliece cryptosystem. In[13], Otmani et al. showed that the proposed system had several vulnerabilities. An amended version of the cryptographic techniques was introduced by Baldi et al. in [2], which was secure against the Otmani's et al. [13] attack. In 2016 [3], Fabsic et al. demonstrate that a threat is present in the QC- LDPC variant of the McEliece cryptosystem. In this paper, we present a modified method for constructing and encoding QC- LDPC Codes.

This paper is organized as follows: Section II gives a brief introduction of QC- LDPC McEliece cryptosystem. In sectionIII, we present the modified method of the QC-LDPC McEliece cryptosystem. In Section IV, we have shown that our new modified scheme would resists against attacks given by [3] by adopting a different form for its constituent matrices, without altering other parameters. In section V, the performances of the modified scheme are compared and finally conclude the paper.

II PRELIMINARIES

In this section, we recall the keywords concerning with the modified Encryption scheme.

(a) QC- LDPC Codes

QC-LDPC codes are called as "reputable structured" type Low density parity check (LDPC) codes. Quasi- Cyclic codes was first studied by Townsend and Welson, where a QC-codes is defined as linear block code with dimension "$k = p.k_0$" and length "$n = p.n_0$ "having the following properties:

(i) A series of "p" blocks of "n_0" symbols will form each code word, each codeword is formed by k_0 information symbols defined by $r_0 = n_0 - k_0$ rebundancy symbols and

(ii) Another valid codeword is formed by each cyclic shift of codeword by n_0 symbols.

$$\mathbf{G} = \begin{bmatrix} G_0 & G_1 & \cdots & G_{p-1} \\ G_{p-1} & G_0 & \cdots & G_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ G_1 & G_2 & \cdots & G_0 \end{bmatrix} \quad \textbf{(1)}$$

(c) Parity-Check Matrix of a Quasi-Cyclic Code

Similarly to the generator matrix G, the following form holds for the parity check matrix H of a quasi-cyclic code.

$$\mathbf{H} = \begin{bmatrix} H_0 & H_1 & \cdots & H_{p-1} \\ H_{p-1} & H_0 & \cdots & H_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ H_1 & H_2 & \cdots & H_0 \end{bmatrix} \quad \textbf{(2)}$$

(d) Alternative "Circulants Block" form

Lemma 3 [1]. Given a matrix in the "blocks circulant" form (1) or (2), it can be put in an alternative "circulants block" form that, for the matrix H in (2), is:

$$H^c = \begin{bmatrix} H^c_{00} & H^c_{01} & \cdots & H^c_{0(n_0-1)} \\ H^c_{10} & H^c_{11} & \cdots & H^c_{1(n_0-1)} \\ \vdots & \vdots & \ddots & \vdots \\ H^c_{(r_0-1)0} & H^c_{(r_0-1)1} & \cdots & H^c_{(r_0-1)(n_0-1)} \end{bmatrix} \quad (3)$$

where each matrix H^c_{ij} is a "p × p" circulant matrix:

$$\mathbf{H^c_{ij}} = \begin{bmatrix} h^{ij}_0 & h^{ij}_1 & h^{ij}_2 & \cdots & h^{ij}_{(p-1)} \\ h^{ij}_{(p-1)} & h^{ij}_0 & h^{ij}_1 & \cdots & h^{ij}_{(p-2)} \\ h^{ij}_{(p-2)} & h^{ij}_{(p-1)} & h^{ij}_0 & \cdots & h^{ij}_{(p-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h^{ij}_1 & h^{ij}_2 & h^{ij}_3 & \cdots & h^{ij}_0 \end{bmatrix} \quad \textbf{(4)}$$

III MCELIECE CRYPTOSYSTEM WITH QC-LDPC CODES

The use of LDPC codes in the McEliece cryptosystem should allow reducing the public key length, at least in principle, since such codes are defined by sparse parity-check matrices, whose storage size increases linearly in the code length**.**

(a) Key Setup

(i) "$(n-k) \times n$" parity check matrix **H** of an LDPC code correct less than "t " errors.

(ii) "$k \times k$ " invertible matrix **S** blocks of " $p \times p$ " circulants.

(iii) "$n \times n$ " a sparse invertible matrix **Q** blocks of " $p \times p$ " circulants.

(b) Generator Matrix of a Quasi-Cyclic Code

A first form for the generator matrix of a quasi-cyclic code directly follows from the code definition, as shown by the following

Lemma 1.[1] The generator matrix G of a quasi-cyclic code has the form of a "blocks circulant" matrix, where each block $G_i$has size $k_0 \times n_0$.

Lemma 2[1]. The parity-check matrix H of a quasi-cyclic code has the form of a "blocks circulant" matrix, where each block H_i has size $r_0 \times n_0$

S and **Q** are formed by blocks of "$p \times p$" circulant matrices.

Public Key: $\mathbf{G'} = \mathbf{S^{-1}} \times \mathbf{G} \times \mathbf{Q^{-1}}$ **(4)**

Private Key: (**H, S, Q**)

(b) Encryption

For a row vector message$u \in GF(q)^k$, Choose a random row vector error having length "n" and weight "t ".

Sender computes the ciphertext as

$$\mathbf{x} = \mathbf{u} \times \mathbf{G'} + \mathbf{e}$$
$$= \mathbf{c} + \mathbf{e}$$

(c) Decryption

For a received ciphertext "x", receiver computes

$$x' = x \times Q$$
$$= (u \times S^{-1} \times G) + (e \times Q) \quad (5)$$

x' → Codeword vector of the QC-LDPC code choosen by receiver corresponds to the information vector $u' = u \times S^{-1}$.

$e \times Q$ → error vector ,

$t = t' m$ → maximum weight.

Receiver is able to correct all the errors with high probability, by means of LDPC decoding. Thus recovering u' and then u through a post-multiplication by S.

IV MODIFIED QC- LDPC CODE BASED MCELIECE CRYPTOSYSTEM

In this section, we have proposed a modified QC-LDPC code in order to hide the structure of the private key. To receive the message, the receiver randomly chooses a code in a family of (n_0, d_v, p) QC-LDPC code based on Random Difference Families [ ].

(a) Key Setup

(i) Select"$(n-k) \times n$" parity check matrix H and produces a "$k_0 \times n_0$" generator matrix G in reduced echelon form. The matrix H is formed by a row $\{H_0, \ldots, H_{n_0-1}\}$ of $n_0 = \frac{n}{n-k}$ binary circulant blocks with size "$p \times p$", where $p = n - k$. Generator marix G is formed by a "$k \times k$" identity matrix I with $k = k_0 . p$ and $k_0 = n_0 - 1$, followed by a column of k_0 binary circulant blocks with size p. If $H_{n_0-1}$is non-singular , then Generator matrix can be obtained as follows:

$$G = \begin{bmatrix} & (H_{n_0-1}^{-1}.H_0)^T \\ I & (H_{n_0-1}^{-1}.H_1)^T \\ & \vdots \\ & (H_{n_0-1}^{-1}.H_{n_0-2})^T \end{bmatrix}$$

(ii) Let $C_0, C_1, \ldots, C_{n-1} \in GF(q)^{k_0 \times r}$ be "$k \times r$" matrices drawn at random and let $G_\emptyset = [G_0, C_0, G_1, C_1, \ldots, G_{n-1}, C_{n-1}]$ be the $k_0 \times n_0(r+1)$ matrices obtained by inserting the random matrices C_i into G.

(iii) Let us choose uniformly random dense invertible $(r+1) \times (r+1)$ matrices $A_0, \ldots, A_{n-1} \in GF(q)^{((r+1)\times(r+1))}$.

$$A = \begin{pmatrix} A_0 & & & \\ & A_0 & & \\ & & \ddots & \\ & & & A_{n-1} \end{pmatrix}$$

be an $n_0(r+1) \times n_0(r+1)$ invertible matrix.

(iv) Let "S" be a randomly selected dense "$k \times k$" binary non-singular matrix.

(v) Let "Q" be a "$n \times n$" sparse invertible matrix having fixed "m". ["S" and "Q"are formed by block of "$p \times p$" circulant matrices].

(vi) Public key is the $k_0 \times n_0 (r+1)$ matrix. $G^\emptyset = S^{-1} \times G_\emptyset \times A \times Q^{-1}$.

(vii) Private key ($S, G_\emptyset, A, Q$).

(b) Encryption

Sender, who wants to send he encrypted message to recviver extracts $G^\emptyset$ from the public key and divides the message into k- bit blocks.If "Ψ" is one of these bocks, sender computes the encrypted, message as follows.

$$E_c = (\Psi \times G^\emptyset) + e$$

(c) Decryption

When receiver receives the encrypted message E_c, then receiver compute

$$\begin{aligned} E_c^\emptyset &= E_c Q A^{-1} \\ &= (\Psi G^\emptyset + e) Q A^{-1} \\ &= \Psi G^\emptyset Q A^{-1} + e Q A^{-1} \\ &= \Psi S^{-1} G_\emptyset A Q^{-1} Q A^{-1} + e Q A^{-1} \\ &= \Psi S^{-1} G_\emptyset + e Q A^{-1} \end{aligned}$$

Where

$$A^{-1} = \begin{pmatrix} A_0^{-1} & & & \\ & A_1^{-1} & & \\ & & \ddots & \\ & & & A_{n-1}^{-1} \end{pmatrix}$$

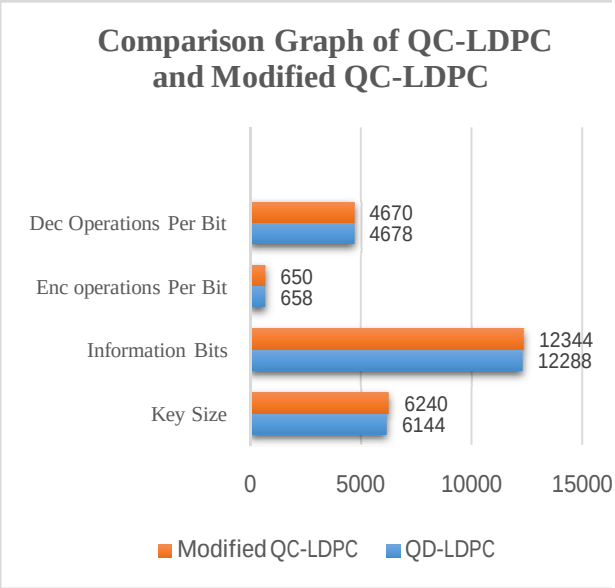
Vector $E_c^\emptyset$ is a codeword of the LDPC code choosen by receiver corresponding to the information vector $\Psi^\tau = \Psi . S^{-1}$ affected by an error vector e. Q, whose maximum weight is $t = t' m$.

By using efficient LDPC decoding algorithm, receiver is able to correct all the errors, thus recovering Ψ and the obtaining Ψ^τthrough multiplication by S.

V SECURITY ANALYSIS

The security of the modified encryption scheme is based on the fact that the adversary needs decoding in the code G, while G is not only different to the code G as in McEliece cryptosystem. But, after inserting C in G, it becomes more complicated to decode for an adversary. In [3], it is shown that the attacker can recover the matrix "Q" in the QC-LDPC McEliece Cryptosystem by used power trace method. However, only knowing the pattern of "Q" doesn't completely reveal the secret key. Since there is one another matrix "S" whose weight is approximately equal to "p/2". Also, in this paper we have suggested a random non-singular matrix "A" which will multiply with "Q" to make it more complex for an adversary to decode easily. If an adversary try to recover the matrix "Q" from the positive pattern in the power trace, then get the matrix multiplication of "QA^{-1}". Then decomposing the matrix "QA^{-1}" in Q and A^{-1}

is not feasible for an adversary. Thus, our modified QC-LDPC McEliece Cryptosystem will resist against the attack given in [3] without compromising with its performance with the existing scheme.



VI CONCLUSION

In this paper, a Modified version of QC-LDPC McEliece cryptosystem is proposed. This system belongs to the class of cryptosystems based on complete decoding task. We have shown that our modified scheme is more secure without compromising with the performance of the existing QC-LDPC McEliece Cryptographic scheme.

REFERENCES

[1] Baldi M., Chiaraluce F., (2007): Cryptanalysis of a new instance of McEliece cryptosystembased on QC-LDPC codes, in: Proceedings IEEE ISIT ’07, Nice, France,,pp. 2591–2595.

[2] Baldi M., Bodrato M., Chiaraluce, F.(2008,): A new analysis of the McEliece cryptosystem based on QC-LDPC codes,in: 6th Internat. Conf. on Security and Cryptographyfor Networks—SCN ’08 (R. Ostrovsky et al., eds.), Lecture Notes in Math., Vol. 5229, Springer-Verlag, Berlin, pp. 246–262.

[3] Fabsic T., Gallo O., Hromada V., (2016). Simple Power analysis attack on the QC-LDPC McEliece Cryptosystem, Slovak Academy of Sciences, Tatra Mt. Math. Publ. 67, pp-85-92.

[4] Heyse S., Moradi A., Paar C .(2010): Practical power analysis attacks on software implementationsof McEliece, in: Post-Quantum Cryptography (N. Sendrier, ed.), LectureNotes in Math., Vol. 6061, Springer-Verlag, Berlin, pp. 108–125.

[5] Janwa H,. and Moreno O.(1996), "McEliece public cryptosystem using algebraic-geometric codes." Des. Codes Cryptography, 8 pp. 293-307, (1996).

[6] Koochak Shooshtari M., Ahmadian-Attari M., Johansson T., Reza Aref M., (2016): Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes, IET Information Security **10, pp**-194–202.

[7] Londahl C., Johansson T., Shooshtari M. K., Ahmadian Attari M,. Aref M. R., (2016): Squaring attacks on McEliece public-key cryptosystems using quasi-cycliccodes of even dimension, Des. Codes Cryptogr. **80** pp. 359–377.

[8] Loidreau P.,(2000) "Strengthening McEliece Cryptosystem", International conference on the theory and application of cryptology and information security, Asiacrypt 2000, pp. 585-598.

[9] Mceliece R. J.,(1978): A public-key cryptosystem based on algebraic coding theory, Deep Space Network Progress Report **44, PP**-114–116.

[10] Misoczki R., Tillich J. P., Sendrier N., Barreto P. S. L. M,.: MDPC--McEliece: new McEliece variants from moderate density parity-check codes, in: IEEEInternat. Symp. on Information Theory—ISIT ’13), Istanbul, pp. 2069–2073.

[11] Niederreiter H., (1986), Knapsack-type cryptosystems and algebraic coding theory. ProblemsControl Inform. Theory, 15(2):159–166

[12] Otmani A., Tillich J. P., Dallot L., (2010): Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes, in: The 1st Internat. Conf. on Symbolic Computationand Cryptography—SCC ’08, Beijing, China, 2008, Math. Comput. Sci., **3** no. 2,pp-129–140.

[13] Repka M., Zajac P., (2014): Overview of the McEliece cryptosystem and its security, Tatra Mt. Math. Publ. **60** pp. 57–83.

[14] Wang Y.(2016), " Quantum Resistant Random Linear Code Based Public Key Encryption Scheme RLCE", IEEE International Symposium on Information Theory (ISIT) .

[15] Berger T., and Loidreau P. (2005)., "How to mask the structure of codes for a cryptographic use". Des. Codes Cryptography, 35 pp. 63-79.

[16] Sidelnikov V M.,(1994) "A public-key cryptosytem based on Reed-Muller codes." Discrete Math. Appl., 4(3), pp. 191-207.

[17] Sahu R., and Tripathi B. P., (2018)., "Random Hexi Code Based Public Key Encryption (RHCE) Scheme for Code-Based Cryptography" International conference on Advances in Computing applications (ICACA-18) held at NIT, (Uttarakhand).