A Code-Based Digital Signature Scheme using Modified Quasi-Cyclic Low-Density Parity-Check Codes (QC-LDPC)

Renuka Sahu, B. P. Tripathi

Abstract: ***Nowadays, all our information are kept in electronic form using the internet and trust that it cannot be accessed by anyone except the intended recipient. For the sake of this purpose, digital signature schemes play a significant role in providing authenticity and record management efficiency. A digital signature is an encoded record that moves with the electronically available document which needs to be signed and returns after the transaction has been completed. In code-based cryptography many digital signature scheme were given among them is CFS code-based digital signature scheme introduced in 2001. It is still considered to be the most popular electronically based signature scheme. The major drawback of this algorithm is its large publickey size. Due to this problem of CFS algorithm, new scheme is presented in this paper using the modified Quasi Cyclic LDPC code and LLR-BP decoding algorithm by replacing the Goppa code and the Patternson decoding scheme for the signing process. This scheme provides a fast and secure signature with public key size smaller than the previously existing schemes and it also strengthens the signature without being compromised with its security.***

Keywords: CFS digital signature, LLR-BP decoding algorithm, QC-LDPC code, code-based cryptography, McEliece cryptosystem

I. INTRODUCTION

Since several attempts has been made by researchers to make secure cryptographical schemes depending on "Error-Correcting Codes". The cryptosystem introduced by McEliece [11] in the year 1978 was still not broken by cryptologists. However, as a result of its large public key size and low performance rate, this cryptosystem isn't being currently in use. Recently, LDPC codes is an error-correcting code proposed by Gallager [8] in 1962. Thus, it seems attention-grabbing to analyze the McEliece scheme towards its variant. In 2007, Baladi [1] introduces a new application for the McEliece cryptosystem using QC-LDPC Codes. The digital signature is a scientific mathematical strategy for demonstrating the credibility of an electronic computerized message or record. A portion of the generally utilized digital signature algorithms, like DSA signature scheme, RSA signature scheme, and Elgamal signature scheme depends on Mathematical issues. However, Shor [14] and Grover [9] introduces a quantum attack algorithm which may easily break these troublesome Mathematical issues. The Digital Signature scheme was first practically revealed in 2001 by Courtois et al. [3] referred to as the "CFS code". CFS digital signature scheme is the primary secure signature algorithm which thoroughly relies upon binary Goppa codes [19] and is built on the premise of the Niederrieter encoding algorithm.

Various far-reaching discussions about the authenticity of the CFS has been made in a previous couple of years [4, 6]. Variations of CFS signature scheme has been introduced by many researchers like parallel CFS [5], mCFS [4], etc. In [12] Zen et al. presented a variation of CFS Code-based signature algorithm in reference with Quasi Cyclic LDPC. During the last thirty years, various kinds of Code-based signature schemes were presented; the primarily attempt was done by Wang [17] which was pursued by Harn et al. [10]. Then after many signature schemes were proposed but unfortunately, these schemes were proven to be insecure. In 2018, RCHC signature scheme [12] for code-based cryptography was presented using Hexi codes which are based on BCHS2 and McEliece cryptosystem.

In this paper, a concept for the CFS signature scheme using modified Quasi-Cyclic LDPC code based McEliece scheme is presented for the first time. Rather than utilizing Goppa code, Quasi-Cyclic LDPC code utilizes the parity-check matrix of LDPC code which is inadequate. Parity-check matrix effectively reduces the size of the general public key and its storage space. Also, in addition with the CFS signature scheme, the BP decoding scheme will be implemented to increase the decoding speed. The BP decoding algorithm will greatly improve the efficiency of CFS signature scheme for modified Quasi-Cyclic LDPC code. This paper is utilized as follows: Section 2 discussed about CFS signature scheme and also, we recall some definitions. Modified Quasi-Cyclic LDPC Code was briefly discussed. In section 4 our proposed signature scheme was presented. Security analysis was discussed for the proposed scheme in section 5. And finally, in section 6 conclusion is discussed.

II. DEFINATIONS

A. Linear Codes

Recalling definition of linear code from [18]. A "linear code" is a linear subspace $\mathbb{C}$ having length 'l' and rank 'r' with dimension 'k' over $\mathcal{F}_q^l$ where $\mathcal{F}_q$ is the finite field with 'q' elements and is called a q-ary code. For binary code q = 2, and for ternary code q = 3. The vectors in $\mathbb{C}$ are called *codewords*. The code size is the number of codewords which equals q^k. A linear code having length 'l ', dimension 'k ', and distance 'd ' is represented as [l, k, d] code. The generator matrix G is of the form [I_k|P] where, I_k denotes the '$k \times k$' identity matrix and P denotes the '$k \times (l - k)$' matrix, then we can say G is in its standard form. If $\mathbb{C}$ is a code with a generator matrix G = [I_k|P], then H = $[-P^T \mid I_{l-k}]$ is a

Parity-check matrix for $\mathbb{C}$. The code generated by H is termed as the dual code of $\mathbb{C}$. It can be verified that G is a '$k \times l$' matrix, while H is a '$(l-k)\times l$'matrix.

B. CFS Signature Scheme

The primary code-based digital signature scheme which is still considered to be secure is the CFS digitalsignature scheme. The evolution of the CFS scheme depends on the Niederreiter PKC.

Algorithm 1. The CFS Signature scheme

Key Generation:

- Let us select randomly '*(l, k)*' Goppa code C over the field $\mathcal{F}_q$.
- Construct an '$(l-k) \times l$' Parity-check matrix H of C.
- Randomly choose an '$(l-k) \times (l-k)$'invertible matrix Q over F_q.
- Randomly choose an '$(l \times l)$'permutation matrix P overF_q.

Let 'ζ' denotes the syndrome decoding algorithm for Goppa Code.

The Public-Key is computed as : H_p = Q × H × P

The Private-Key for decoding is : (H, Q, P, ζ)

Signature:

- To sign a message M, compute z = $\zeta(Q^{-1}h(h(M)||i)$, i ϵ N.
- The signature of message M is Ψ= [z||i].

Verification:

- Compute s'= $H_p z^T$ and s = h[h(M)||i].
- The signature is valid if s' and s is equal; otherwise Ψ is invalid.

C. Quasi-Cyclic LDPC Code [2]

Quasi-Cyclic LDPC codes are called as "reputable structured" type LDPC codes. This code was first studied by Townsend and Welson, and it is defined as linear block code with dimension "$k = p.k_0$" and length "$l = p.l_0$" having the following properties:

(i) A series of "p" blocks of "l_0" symbols will form each code word, each codeword is formed by k_0 information symbols defined by "$r_0 = l_0 - k_0$" rebundancy symbols and

(ii) Another valid codeword is formed by cyclic shift of each codeword by "l_0" symbols.

III. MODIFIED QUASI-CYCLIC LDPC CODE BASED MCELIECE CRYPTOSYSTEM

In this section, modified Quasi-Cyclic LDPC code [14] was discussed in short.

(a) Key Setup

(i) Select "$(l-k)\times l$" parity-check matrix H and produces a "$k_0 \times l_0$" generator matrix G in its reduced echelon form. The matrix H is formed by a row $\{H_0, \dots, H_{n_0-1}\}$ of $l_0 = \frac{l}{l-k}$ binary circulant blocks with size "$p \times p$", where $p = l-k$. Generator marix $\mathbb{G}$ is formed by a "$k \times k$" identity matrix I with $k = k_0.p$ and$k_0 = l_0 - 1$, followed by a column of k_0 binary circulant blocks with size p. If $H_{n_0-1}$is invertible, then Generator matrix can be obtained as follows:

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

(iii) Let $C_0, C_1, \dots, C_{n-1} \in GF(q)^{k_0 \times r}$ be "$k \times r$" matrices drawn at random,

and let $G_\emptyset = [G_0, C_0, G_1, C_1, \dots, G_{n-1}, C_{n-1}]$ be the "$k_0 \times l_0(r+1)$" matrices obtained by inserting the random matrices C_i into G.

(iv) Let us choose uniformly random dense invertible "$(r+1)\times(r+1)$" matrices $A = A_0, \dots, A_{n-1} \in GF(q)^{((r+1)\times(r+1))}$be an "$l_0(r+1) \times l_0(r+1)$" invertible matrix.

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

(vi) Let "Q" be a "$l \times l$" sparse invertible matrix having fixed "m".

Public key is the $k_0 \times l_0 (r+1)$ matrix.

$$G^\emptyset = S^{-1} \times G_\emptyset \times A \times Q^{-1} .$$

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

Encryption

Sender, who needs to send the scrambled message to the receiver will extracts $G^\emptyset$ by using the public key and then divides the message into k-bit blocks. If "Ψ" is one of these blocks, the sender computes the encoded message as $E_c = (\Psi \times G^\emptyset) + e$

Decryption

When receiver receives the encrypted message E_c, then receiver compute

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

Vector $E_c^\emptyset$ is a codeword of the LDPC code chosen by beneficiary relating to the data vector $\Psi^\tau = \Psi.S^{-1}$ influenced by an error vector 'e. Q', most extreme weight is $t = t'm$.

IV. A MODIFIED QUASI-CYCLIC LDPC BASED DIGITAL SIGNATURE SCHEME

CFS algorithm was proposed in 2001 by Courtois-Finiasz-Sendreir [3] one of the secure Code-based signature scheme [12]. Since the classical CFS digital signature scheme utilizes the well-known code for example Goppa code. In this section, a CFS digital signature scheme dependent on the modified Quasi Cyclic LDPC code is exhibited. It means to say that the Goppa codes are replaced by modified Quasi-Cyclic LDPC Codes, whereas the decoding technique of Goppa Code is replaced by BP decoding algorithm.

The CFS digital signature scheme comprises of three algorithms:

Key Generation Algorithm–

Key generation comprises of two parts. In the first part selection of algorithmic parameters is done and share it between various clients of the framework, and in the second part, the calculation of the public, and the private keys for a single user has been done.

Signing Algorithm–

In this part, the message was given with its private key then it computes a signature.

Signature Verification Algorithm –

For the verification, message, public key, and signature are compared based on the comparison result, verifiers decides whether the digital signature is valid or invalid.

In the traditional CFS digital signature scheme, the message digest is of length "r" (r<n) but in the BP decoding algorithm of LDPC codes the input sequence is of length "n". Thus to convert the message digest "s" into an arrangement of length "n" some improvements were given in this paper.

For the complete process, follow the Algorithm 1.

Algorithm 1.

Input :- Parity check matrix "H" and message digest "s" of length "r".

Transforming H into row simplest "G" using row transformation,

i.e $M.H = G$,

where "M" is an invertible matrix will get $H = M^{-1}.G$;

From $H = M^{-1}.G$ (1)

and $H.v^T = s$ (2)

from eqn. (1) and (2), we get

$M^{-1}.G.v^T = s$

Multiplying M on both the side of the above eqn. , we get

$M.M^{-1}.G.v^T = M.s$

$G.v^T = M.s$

"v" can be satisfied by using the known matrix G, M and message digest 's'.

Output:- sequence of v

Modified Quasi-Cyclic LDPC based CFS digital scheme.

Algorithm 2.

Key Generation:-

Let us select randomly a modified Quasi-Cyclic LDPC code C (l, k) whose error-correcting ability is 't'. Select '(l – k) × l' parity check matrix and produce '$k_0 \times l_0$' generator matrix.

Let us consider $C_0, C_1, \dots, C_{n-1} \epsilon\, GF(q)^{k_0 \times l_0}$ be 'k × r' matrices drawn at random and let $G = [G_0, C_0, G_1, C_1, \dots, G_{n-1}, C_{n-1}]$ be the '$k_0 \times l_0(r+1)$' matrices obtained by inserting the random matrices C_i into G.

Let us choose '(r+1) × (r+1)' uniformly random dense invertible matrices $A_0, \dots, A_{n-1} \epsilon\, GF(q)^{((r+1)\times(r+1))}$. Randomly select 'k × k' binary invertible matrix S and 'l × l' dense non-singular matrix.

Computing $G^{\emptyset} = S^{-1} \times G \times A \times Q^{-1}$, BP decoding algorithm is represented by α. We denoted algorithm 1 by β which converts a message digest 's' of length 'r' into a sequence of length 'n'.

Let us select the hash function as h: $\{0,1\}^* \rightarrow F_2^{n-k}$

The matrix $G^{\emptyset}$ is the public key and (S, $G^{\emptyset}$, A, Q, α) are the private keys.

Signature Algorithm:-

Input m- message

→ Compute $s = h$ (m),

→ Calculate $s_i = h(s|i)$ using hash function where i = 0, 1, …….

→ Converting s_i to v_i having length 'n' by using the algorithm 1.

→ Now, try to decrypt v_i with the help of BP decoding algorithm and compute the smallest possible 'i' which makes $\alpha(v_i)$ exist, $i \rightarrow i_0$ and $s_i \rightarrow s_{i_0}$.

'z' is the translated word, satisfies $G^{\emptyset} z^T = s_{i_0}$, $w(z) = l$.

The Signature of Message m is $\Psi = [z|i]$.

(m,Ψ) is represented as the signature.

Verification:-

After receiving the encoded message m and the signature (m,Ψ).

→ With the help of public key H and translated message z, calculate $s_i = G^{\emptyset} z^T$;

→ According to i_0 calculate $s_2 = h[h(m)|i_0]$;

The signature Ψ is valid if and only if s_1 equals to s_2; otherwise the signature is invalid.

V. SECURITY ANALYSIS

With the help of the security analysis discussed in [2], we have shown more security against several attacks. The hash function 'h' of the proposed algorithm depends on the syndrome decoding problem i.e. SD problem. For decoding, the relationship between 'z' and the translatable code s_{i_0} can be taken as the error vector and the syndrome. From the translatable code s_{i_0} and the public key $G^{\emptyset}$, one may directly compute the equation $G^{\emptyset}z^T = s_{i_0}$, where w(z) ≤ t. . Thus according to the concept of error-correction code, this is a non-deterministic polynomial complexity problem i.e. NPC problem which can resists against all the existing known attacks of quantum cryptographic algorithm for eg. Grover's algorithm and the Shor's algorithm. In [16] Stern suggested that the message can be directly obtained by the attackers. The probability if a codeword of weight w of (n, k) LDPC code is found in one iteration by

$$\sigma = \frac{\binom{n-k-w-2f}{l}\binom{n-w}{\frac{k}{2}-f}\binom{w}{p}\binom{w-f}{f}\binom{n-w-\frac{k}{2}+f}{\frac{k}{2}-f}}{\binom{n-k}{l}\binom{n-k/2}{k/2}\binom{n}{k/2}} \quad (5)$$

where 'f' and 'l' are two parameters..

The average no. of iteration required for calculating a low-weight code word is given as b = σ_w^(-1) .

For finding the minimum distance, Stern's algorithm is used and continue the process until, the error-probability will be ≤ ε. For each iteration the codewords obtained is independent. Thus after r^th iteration the probability of finding the codeword with weight w is 1 - ⟦(1- σ_w^(-1))⟧ ^r.

Cost of each iteration:

$$C \approx \frac{2f(n-k)\binom{\frac{k}{2}}{f}^2 + k(n-k)^2 + \frac{(n-k)^3}{2} + 2pl\binom{\frac{k}{2}}{f}}{2^l} \quad (6)$$

binary operations.

Table1. Comparison between the proposed and the existing schemes [2].

Codes	Parameter	Key size	Information Rate	Codes	Parameter
Goppa	(1024,524)	32750	0.51	Goppa	(1024,524)
Goppa	(1024,1036)	131054	0.51	Goppa	(1024,1036)
Goppa	(16384,12296)	6283256	0.75	Goppa	(16384,12296)
LDPC	(16384,12288)	20481	0.75	LDPC	(16384,12288)
QC-LDPC	(16384,12288)	6144	0.75	QC-LDPC	(16384,12288)
Modified QC-LDPC	(16384,12344)	6140	0.77	Modified QC-LDPC	(16384,12344)

The total work-factor W for calculating the low-weight code is W= b C. By taking the classical parameters (4096, 2048), d = 82, l = 36 and p = 3, the computed minimum work-factor W is approx 2^98.39, so the proposed scheme will resist against stern's attack. Table 1 shows the comparison of the proposed scheme with the existing scheme. Also from [12], we can conclude that the proposed signature scheme is secure against OTD attack also.

VI. CONCLUSION

A Code-based signature scheme with using the modified Quasi-Cyclic LDPC code is presented in this paper. The proposed scheme depends on the well-known NP complete problem. CFS signature scheme is one of the important scheme based on error correction code. The major drawback of this algorithm is its large public key size. To overcome with the problems, the proposed scheme takes advantages of the circularity and sparseness of the Quasi-Cyclic LDPC code check matrix. Our proposed scheme has smaller key and signature size which makes it faster and more secure when compared with CFS signature scheme. Also the use of LLR-BP decoding algorithm in our proposed scheme improves the efficiency and security of the signature.

REFERENCES

1. Baldi, M., Chiaraluce, F., Garello, R.: Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem. IEEE International Conference on Communications, 951- 956 (2007).
2. Baldi, M.:QC-LDPC Code Based Cryptography, Springer Brief in Electrical and Computer Engineering, Springer international publishing, ISSN-9783319025568 (online), 21- 60 (2014).
3. Courtois, N., Finiasz, M., Sendrier, N.: How to Achieve a McEliece Based Digital Signature Scheme. International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 157-174 (2001).
4. Dallot, L.: Towards a Concrete Security Proof of Courtois, Finiasz and Sendrier Signature Scheme, in Research in Cryptology, 65–77, Berlin Heidelberg: Springer (2008).
5. Finiasz, M.: Parallel-cfs, in Selected Areas in Cryptography, 159–170 (2011).
6. Finiasz, M., Sendrier, N.: Security Bounds for the Design of Code-Based Cryptosystems, in Advances in Cryptology (ASIACRYPT'09), 88–105, Berlin Heidelberg: Springer (2009).
7. Harn, L., Wang, D.C.: Cryptanalysis and Modification of Digital Signature Scheme Based on Error-Correcting Codes, Electronics Letters, vol. 28(00), 157–159 (1992).
8. Gallager, R.G.: Low-density Parity Check Codes, IRE Transactions on information Theory, vol. 8, 21-28 (1960).
9. Grover, L.K.: A Fast Quantum Mechanical Algorithm for Database Search, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of computing. ACM, 212-219 (1996).
10. Harn, L., Wang, D.C.: Cryptanalysis and Modification of Digital Signature Scheme Based on Error-Correcting Codes, Electronics Letters, vol. 28(00), 157–159 (1992).
11. McEliece, R.J.: A Public-key Cryptosystem Based on Algebraic Coding Theory, Jet Propulsion Laboratory DSN Progress Report, 114–116 (1978).
12. Ren, F., Yang, X., Zheng, D.: A QC-LDPC Code Based Digital Signature Algorithm, International Conference on Networking and Network Applications, 217-262 (2018).
13. Sahu, R., Tripathi, B.P.: Random Hexi Code Based Public Key Encryption Scheme (RHCE) Scheme for Code Based Cryptography, International journal of Engineering Research in Computer Science and Engineering, vol. 5(2), 591-596 (2018).
14. Sahu, R., Tripathi, B.P.: Secure Modified QC-LDPC Code Based McEliece Public Key Encryption Scheme, National Conference on Advances in Computer Science and Information Technology (NCACSIT) at Dr. C. V. Raman University, Kota, Bilaspur, Chhattisgarh, India (2019).
15. Shor, P.W: Algorithms for Quantum Computation: Discrete logarithms and factoring. Foundations of Computer Science, 1994 Proceedings. 35th Annual Symposium on. IEEE, 124-134 (1994).
16. Stern, J.: A Method for Finding Codewords of Small Weight, International Colloquium on Coding Theory and Applications. Springer,

Berlin, Heidelberg, 106-113 (1988).
17. Wang, X.: Digital Signature Scheme Based on Error-Correcting Codes, Electronics Letters, vol. 26(00), 898–899 (1990).
18. http://en.wikipedia.org/wiki/Linear_code.
19. https://en.wikipedia.org/wiki/Goppa_code.

AUTHORS PROFILE

Renuka Sahu received the B. Sc, M.Sc. and M. Phil degrees in Mathematics from Pt. Ravishankar Shukla University, Raipur, Chattisgarh (India) in 2010, 2012 and 2013 respectively. She is currently a research scholar at the Department of Mathematics in Govt. N. P. G College of Science. This institute is affliated from Pt. Ravishankar Shukla University, Raipur, Chattisgarh (India). Her main research interest include Post Quantum Cryptography, especially in Code-Based Cryptography.

Dr. B. P. Tripathi, is Assistant Professor, in the Deptt. of Mathematics, Govt. N. PG. College of Science, Raipur. The institute is affiliated to Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India. His field of interest are Non-linear Analysis, Fixed point theory and Public Key Cryptography. He has teaching experience of 24 years of undergraduate and postgraduate classes. He has written 2 books and published 35 research papers in various National and International Journals. His one scholar has awarded Ph.D. degree, one has submitted their thesis and four scholars are pursuing his research work under the supervision of Dr. B. P. Tripathi. Two scholars are working on Public Key Cryptography.