Transactions on Engineering and Computing Sciences - Vol. 11, No. 5
Publication Date: October 25, 2023
DOI:10.14738/tecs.115.15567.
Farota, A. K., Adoum, Y. M., & Diop, B. (2023). Implementation of McEliece Encryption Scheme Based on Quasi- Cyclics Goppa Codes (QC-GOPPA). Transactions on Engineering and Computing Sciences, 11(5). 59-68.

SERVICES FOR SCIENCE AND EDUCATION

Implementation of McEliece Encryption Scheme Based on Quasi-Cyclics Goppa Codes (QC-GOPPA)

Abdou Karim Farota
Laboratoire des Sciences de l'Atmosphère et de l'Océan : Matériaux, Energie et Dispositifs (LSAO-MED), Université Gaston Berger de Saint-Louis, Sénégal

Yacoub Mahamat Adoum
Laboratoire des Sciences de l'Atmosphère et de l'Océan : Matériaux, Energie et Dispositifs (LSAO-MED), Université Gaston Berger de Saint-Louis, Sénégal

Bouya Diop
Laboratoire des Sciences de l'Atmosphère et de l'Océan : Matériaux, Energie et Dispositifs (LSAO-MED), Université Gaston Berger de Saint-Louis, Sénégal

ABSTRACT

The McEliece cryptosystem is one of the oldest public key cryptosystems. It is also the first public key cryptosystem based on error correcting codes. Its main advantages are its speed of encryption and decryption, and high security (promised to resist the quantum computer). But it suffers from a major drawback. Indeed, it requires a very large size of the public key, which makes it very difficult to use in practice. The use of codes having compact generator matrices can significantly reduce the size of the public key. However, with such matrices, security must be strengthened by making a good choiceof parameters of the code, if not an opponent will use this change to attack the system. In article we will propose an implementation of the schema of encryption, introducing at the same time the decryption for a bettrer explanation of the global system. Here, we use the quasi-cyclic version of Goppa codes instead of the classical Goppa codes of theoriginal system for encryption. For the McEliece system is considered safe, we need a security of at least 2^{80}bits. What we propose here is an implementation that offers us a 6502bits public key size for a security in the [2^{85}bits, 2^{90}bits] interval. We simulate our scheme with Xilinx ISE 14.7. The VHDL is the langage used to describe the scheme.

Keywords: Linear codes, quasi-cyclic codes, Goppa codes, McEliece cryptosystem.

INTRODUCTION

Today, the most used public key cryptosystems are RSA, Diffie-Hellman, El Gamal and the elliptic curve cryptography. Experiences have shown that once quantum computers are operational, all these systems will be vulnerable. The main explanation is that the seminal Shor algorithm solves very quickly and efficiently the factoring problem for RSA and discrete logarithm problem of El Gamal using the quantum computer [1].

However, there are alternatives including the McEliece system [2,3,4] which is supposed resistantbecause it's not yet broken by the quantum computer.

The original McEliece system uses conventional binary Goppa [5. Here, we propose a McEliece scheme using codes QC- Goppa [6]. The generator matrix elements of such a code are obtained from a single row or a single column. We present theoretical arguments and practical tools (simulation results) to estimate a compromise between security and encryption -related complexity [7].

LINEAR ERROR CORRECTING CODES

The construction of a code word having n –bit is performed from k bits of the message source binary $k\text{-}tuple$ = (u_1, u_2, u_3, ..., u_k), usually called information message, and r $bits$ of redundancy. The simplest coding method is to leave unchanged the k information bits and to postpone such in the code word by adding r (= nk) redundancy bits {a_1, a_2, . . ., a_r}, which are generally called bit controls. The V^T vector line called code word:

$$V^T = [\, v_1\, v_2\, \ldots\, v_n] = [\, u_1, u_2, u_3, \ldots . u_k\, a_1, a_2, \ldots, a_r]$$

- When control bits are calculated only from the block of information bits to which theybelong, the code C (n, k) is called code block;
- When control bits are calculated from the bits of information belonging to several blocks,the code is said recurrent.

Linear codes have the property that all the code words form a vector space.

A block code of length n and 2^kcode words is called linear code (n, k) if and only if its 2^k code words form a k -subspace of the Galois field GF (2).

In fact, a binary block code is linear if and only if the sum $modulo$-2 of 2 code words is alsoa codeword.

If C is our linear block code parameters (n, k) and if in addition its minimal distance is d then C be called (n, k, d) - linear code.

The information rate of C code with length n is $R = k / n$. It is also given by R =1/n $log_2|\, C|$ where C is an abusive notation of the number of codewords [2]

Generator and Parity Check Matrices

Generator Matrix:

To know the code as a subspace, it is enough to have a basis. This one is usually represented as a $k \times n$ matrix over K, the code generator matrix, whose rows are the vectors of this base. Toform a codeword, we calculate the product of a row vector ($u_1, \ldots, u_k$) and the generator matrix

$$[u_1, \ldots, u_k] \begin{bmatrix} g_1^1 & g_1^2 & \ldots & g_1^n \\ \vdots & \vdots & . & \vdots \\ g_k^1 & g_k^2 & \ldots & g_k^n \end{bmatrix} = [x_1, \ldots, x_n] \quad (2)$$

Let C be a linear code (n, k, d). The encoding is done by multiplying the source word by the generator matrix code. The source word must be of length k. Redundancy is $n - k$ symbols. Any generator matrix of a linear code C (n, k, d) can be reduced in a systematic form by operatios on the row and a permutation on the columns.

$$G = (I_k|P) = \begin{pmatrix} 1 & 0 & \ldots & 0 & P_{00} & \ldots & p_{0l} & \cdots & p_{0,n-k-1} \\ 0 & 1 & \ldots & 0 & P_{1,0} & \ldots & p_{1,l} & \cdots & p_{1,n-k-1} \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & 1 & P_{k-1,0} & \ldots & p_{k-1,l} & \cdots & p_{k-1,n-k-1} \end{pmatrix} \quad (3)$$

I_k is the identity matrix $(k \times k)$, P matrix $(k \times (n - k))$.

A generator matrix of a systematic form generates a linear code in which the k information bits explicitly appear in the code words and the $(n - k)$ remaining are linear combinations of the information bits.

Parity Check Matrix:
A parity check matrix of a code C is a matrix H of size $n \times (n - k)$ such as:

$$x \text{ G } C \text{ - } Hx^T = 0 \quad (4)$$

With $x^T$the transposed vector of x.

To each code C (n, k) of generator matrix G correspond a code (called the dual code) C $(n, n - k)$ of generator matrix H such as

$$GH^T = 0 \quad (5)$$

Where $H^T$is the transposed matrix of H. Each code word of C generated by G is orthogonal tothe lines of the matrix H.

Cyclic and Quasi-Cyclic Codes
Cyclic Code:
Let F_q^n be any subspace and T defined by:

$$T: Æ_q^n \rightarrow Æ_q^n$$

$$(x_1, x_2, \ldots, x_n) \rightarrow (x_n, x_1, \ldots, x_{n-1})$$

the circular shift application called as 'shift'.

Let C be a code of length n on F_q^n. By definition:

$$C \text{ is } cyclic \text{ - } \bigstar\ c \in C, T(c) \in C$$

In other words, C is stable by the action of the permutation on T columns.

For the sake of ease of writing and to study the algebraic properties of these codes, it is more convenient to write the words of a cyclic code in polynomial form due to the following identification:

$$c = (c_0, c_1, \ldots, c_{n-1}) \text{ ① } c(\mathrm{X}) = c_0 + c_1\mathrm{X} + \cdots + c_{n-1}\mathrm{X}^{n-1} \quad (7)$$

Quasi-Cyclic Codes:
The quasi- cyclic codes are a generalization of cyclic codes. Consider the shift function T and C code defined above. Now, let us chose $l \in^*$. By definition:

$$C \text{ is } l - quasi - cyclic \text{ - } \bigstar\ c \in C;\ T^l(c) \in C$$

The T^l permutation is called quasi-shift.

The linear binary codes with the following generator matrix

$$\begin{matrix} 01\ 1\ 0\ 1\ 1 \\ (01\ 1\ 0\ 1\ 1) \\ 11\ 0\ 1\ 1\ 0 \end{matrix} \text{ is } 2 - quasi - cyclic.$$

Binary Goppa Codes:
Goppa binary codes are from the generalized Reed- Solomon codes and enable to obtain a goodminimal distance. These codes are used in cryptography (cryptosystem McEliece).

The Goppa code $(L;\ g\ (x))$ is defined by the polynomial $g\ (x)$, which is one of degree t polynomial on $GF\ (q^m)$ with q a prime number and L a $support\ of\ GF(q^m)$.

$$g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_tx^t \quad (8)$$

$$L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \leq GF(q^m),$$

such as

$$g(\alpha_i)\ \mathrm{G}\ 0, \bigstar\ \mathrm{i}\ \mathrm{G}\ \{1, \ldots., n\}$$

With a vector $c = \{c_0, \ldots.,\ c_n\}$ of $GF(q)$, associating the function:

$$R_c(x) = \sum_{i=1}^{n} \frac{c_i}{X - a_i} \quad (9)$$

The Goppa code is constitued of all vectors c such as:

$$R_c(x) = 0(mod\ g(x))$$

The parameters of Goppa code are $[n, k, d]$. The parameter n is the length of the code words andis determined by L.

Goppa code ($L\ g\ (x)$) of size n is a linear code over $GF(q)$ with the following properties:

- The size of the code satisfies the relationship $k \geq n - mt$ [6]
- The minimum distance of the code satisfies $d \geq t + 1$.

MCELIECE CRYPTOSYSTEM

The McEliece cryptosystem incorporates a linear error correcting code (Goppa code) that isdisguised as a simple linear code.

Schema Description

The McEliece cryptosystem is an asymmetric system. Which implies the presence of a private key and a public key. The private key is a family of Goppa codes. It is chosen as follows:

- Select an invertible matrix S $(k \times k)$ and a permutation matrix P $(n \times n)$. Only therecipient knows the private key.

The public key is $G_p = SGP$, where G is the generator matrix of the used Goppa code.Let x be the message having $k\ bits$ of information to be encrypted. The sender sending $x_0 = xG_p + e$, with e a random error vector of $n\ bits$ with a weight t which is also the degree of Goppa code generator polynomial. On receiving x_0, to decipher the message, the recipient calculates $x_0\ P^{-1} = xSG + eP^{-1}$. Usingan efficient algorithm for decoding the code, he finds xS. Since S is invertible, then recovered x.

Encryption Algorithm:

Input: $x, Kpub^1 = (G_p; t)$
Output: cipher x_0;

1. Encode the message x into a sequence of binary characters with length n;
2. $c' \rightarrow xG_p$;
3. Generate a random error vector e of length n able to correct t errors;
4. $x_0 = c' + e$;
5. return x_0;

Decryption Algorithm:

Input: $x, K_{sec}^2 = (P^{-1}, G, S^{-1})$;
Output: plaintext message x;

1. $c^\circ \rightarrow xP^{-1}$;
2. Use the decoding algorithm to decode the Goppa code c° and get $x^\circ = xS$;
3. $x \rightarrow x^\circ S^{-1}$;
4. return x;

PROPOSAL OF THE SCHEME BASED ON THE QUASI- CYCLIC CODES OF GOPPA

Mceliece Cryptosystem Based on Qc-Goppa Code

The main functions of the cryptographic system based on codes QC-Goppa are presented in Figure 1. Here for QC-Goppa, a code word of length $n = n_0 \times k$, with size $p = k_0 \times k$ and having redundancy $r = k$ is adopted, where n_0 is the index of quasi- cyclicality ($n_0 = 2.3, 4, \ldots$), $k_0 = (n_0 - 1)$ and p is the size of the message (of the order of several thousand). The private key is formed by the check matrix H randomly selected with the following elements:

$$H = [H_0|H_1|\ldots|H_{n_0} - 1] \tag{10}$$

H is a row of n_0 circulating h_i blocks, each with rows and columns with the same weight w. It is assumed that Hn_{0-1} is not singular. Thus, a systematic generator matrix of the code is $G = [I \mid Q]$, where I is the identity matrix of size $k \times k$ and where the exponent T denotes the transposition of a matrix.

$$Q = \begin{matrix} (H_{n0-1}^{-1}. & H_0)^T \\ (H_{n0-1}^{-1}. & H_1)^T \\ (H_{n0-1}^{-1} & H_0^{n-2})^T \end{matrix} \tag{11}$$

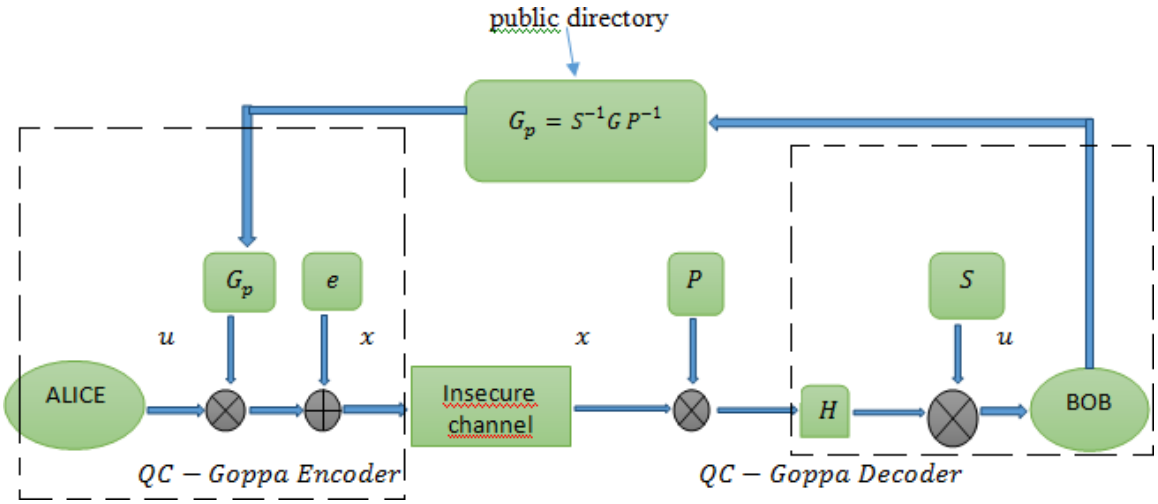


Figure 1: The McEliece cryptosystem based on QC-Goppa [4]

Encryption and Its Complexity

Key Size and Transmission Rate:

In the encryption system based on the code QC-Goppa, due to the particular shape of the matrix H, the code rate $(n_0 - 1) / n_0$. We chose $n_0 = 2$ above, which gives us a transmission rate equal to 1/2. Regarding the size of the key, we observe that, in the given system, the public key is a binary matrix formed by $k_0 \times n_0 = (n_0 - 1) \times n_0$ circular matrixes, each with a $k \times k$ size. Given that each circular block is completely described by an only row (or column), having k *bits*, the size of the public key is:

$$N = (n_0 - 1)\, n_0\, k \;\; bits\; [7] \tag{12}$$

Encryption Complexity:

Encryption is performed by calculating the product $u \times G_p$ and adding to it the random error vector e.

Thus, the complexity of encryption lies in the multiplication of the matrixes of huge sizes and the execution of n binary operations for the random error vector.

Table 1 provides information on the number of needed binary operations for each encrypted bitto a circular matrix of size $k \times k$, and with indices of cyclicality $n_0 = 3$ *et* $n_0 = 4$.

Table 1: Number of needed binary operations for each encrypted bit

$k[bits]$	4096	5120	6144	7168	8192	9216	10240	11264	12288	13312	14336	15360	16384
$n_{0=}3$	726	823	919	1005	1092	1178	1236	1351	1380	1524	1510	1697	1639
$n_0 = 4$	956	1081	1206	1321	1437	1552	1624	1783	1811	2013	1984	2244	2157

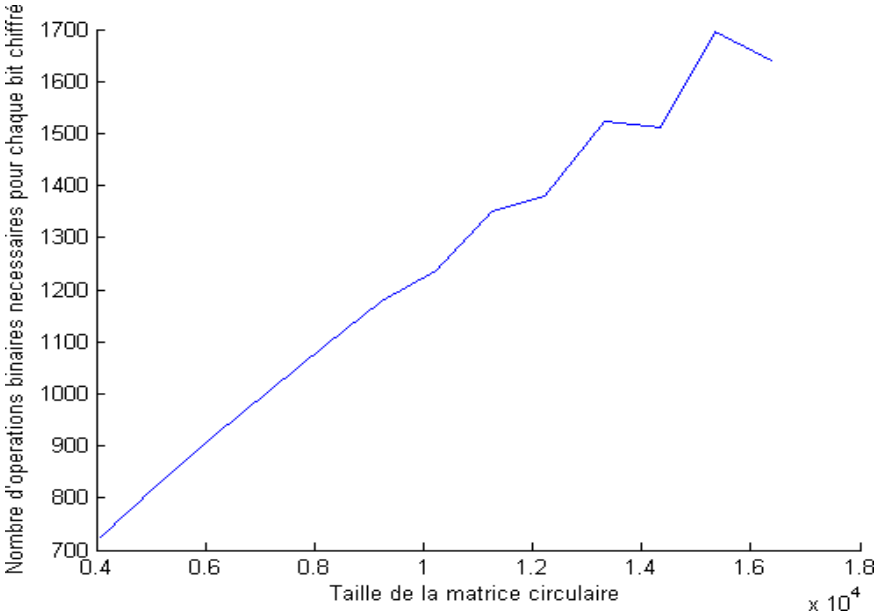


Figure 2: Change in number of binary operations for each encrypted bit for $n_0 = 3$

SELECTION OF PARAMETERS

In [2], the authors proposed a variant of McEliece scheme based on codes of Goppa. With this variant, they can get a security of 2^{80} for a public key of $6000 bits$ *and a security of* 2^{107} for a *public key of* 11,160 *bits*. Given that for McEliece system, a security level *of* 2^{80} is considered safe, we systematically chose the parameters so as to be within a range of *security* [2^{85} *bits*, 2^{90} *bits*] but also avoiding very large sizes of the public keys. Thus, we avoid having memories of very large sizes and slow encryption.

The Cryptosystem Parameters

$$m = 13: \textit{the size of the Galois field used}$$

$$L = F_2^n = \{0,1\}^n : \text{Code support}$$

$n_0 = 2$: $index\ of\ quasi - cyclic\ code$

$n = 6502$: $length\ of\ the\ code\ word.$

$k = 3251$: $length\ of\ the\ messsage.$

S (3251 * 3251): $non\ singular\ random\ circular\ matrix.$

P (6502 * 6502): $random\ permutation\ matrix$

$t = 251$: $weight\ of\ the\ random\ error$

With these parameters we build the QC-Goppa $C\ [n_0,\ k,\ n]F_2^n$.

$$C[n_0,\ k,\ n]_{F_2^n} = C[2,6502,3251]\ _{F_2^n} \quad (13)$$

By using the security level diagram provided in [6], we observe although with a choice of = 3251 $bits$, we get a security level between $2^{85}$and 2^{90}. Which makes our model an unbreakable scheme. In addition, with this choice and $n_0 = 2$, we can get a minimum number of binary operations required to encrypt each bit (See Figure 2). Finally, the most important is that with these parameters, we obtain a public key of the same size as the length code words. Thus, the size of the public key is, according to the relation (12)6502 $bits$.

Implementing Steps

The Galois field in which we work is the GF (2^{13}). we have for our implementation encryption circuit, regrouping the generation of code words and the encryption. The choice of $t = 251$ satisfies the relationship $k \geq n - mt$ for code Goppa.

Encryption

The encryption algorithm is described in Section 3.1. Here VHDL encryption module is processed. Encryption is designed using the architectural model.

Figure 3 shows the encryption block and the figure 4, the simulation result of the encryption using the simulation tool ISIM of XILINX 14.7 development software.

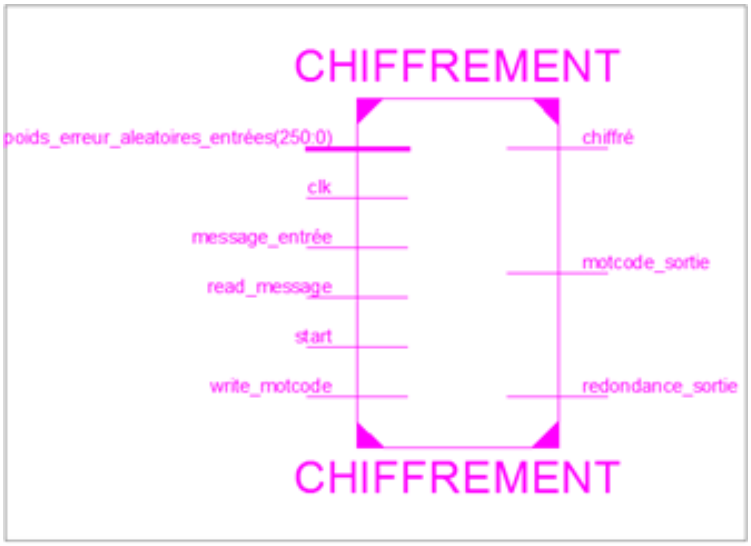


Figure3: Encryption block of McEliece

This block ENCRYPTION performs both encoding and encryption. In input it receives messages from the sender and the weight of the random error vector t. In output, it provides us the encrypted message for the recipient as well as the code words andredundancy.



Figure4: Simulation of McEliece encryption scheme with the Xilinx ISE 14.7 software

We well notice in this figure for 100ns, we obtain an encryption codeword, that is to say, a bit is encrypted to 0.15 ps. So, encryption is still relatively rapid.

CONCLUSION

In this paper, we have proposed a McEliece scheme by using quasi- cyclic Goppa codes instead of classical Goppa codes. Such a modification is to overcome the main drawbacks of theMcEliece original system as it will achieve a satisfactory level of safety. The results confirm that the use of quasi- cyclic codes allows to significantly reduce the size of the keys of McEliece scheme.

Compared with conventional Goppa codes that provide for a security 2^{90} an almost key of $2.5Mbits$, we think that the codes of compact structures are ideal versions for research in the field.

The use of these codes has also limitations, including reducing the speed encryption affected by the circular nature of the matrix. However, it stays relatively fast.

ACKNOWLEDGMENTS

This work was financially supported in part by the CEA-MITIC /UFR SAT/UGB

References

[1] Biswas and Sendrier. "McEliece Cryptosystem Implementation: Theory and Practice", PQCrypto2008. Proceedings of the 2nd International Workshop on Post-Quantum Cryptography. Pages 47-62, Cincinnati, OH — October 17 - 19, 2008

[2] Thierry Berger, Pierre Louis Cayrel, "Reducing key lengh of the McEliece cryptosystem", Chapter Progress in Cryptology – AFRICACRYPT 2009. Volume 5580 of the series Lecture Notes in Computer Science pp 77-97

[3] Stefan Heyse, "Code-based cryptography: Implementing the McEliece Scheme on Reconfigurable Hardware", (May 2009), Diploma Thesis Ruhr-University Bochum

[4] Marco Baldi, Marco Bianchi and Franco Chiaraluce, "Security and complexity of the McEliece cryptosystem based on QC-LDPC codes", Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche. Ancona, Italy.

[5] Valentijn, Ashley, "Goppa Codes and Their Use in the McEliece Cryptosystems" (2015). Syracuse University Honors Program CapstoneProjects. Paper 845

[6] https://github.com/pmassolino/hw-goppa-mceliece. Hardware implementation of the cryptosystem McEliece in VHDL for binary (QD-) Goppa codes. (Consulté pour la dernière foisle 06 Avril 2016).

[7] Bart Preneel, Antoon Bosselaers, René Govaerts1 and Joos Vandewalle, "A Software implementation of the McEliece public-key cryptosystem", Proceedings of the 13th Symposium on information Theory in the Benelux, Werkgemeenschap voor Informatieen Communicatietheorie, pp. 119{126, 1992.

[8] Pierre Louis Cayrel, Christophe Chabot, Abdelkhader Nacer, "Quasi-cyclic codes as codes over rings of matrices", In Finite Fields and Their Applications Vol. 16, 2010, pp 100-115