ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPLEMENTATION OF MC ELIECE ENCRYPTION SCHEME BASED ON QUASI-CYCLICS GOPPA CODES (QC-GOPPA).

[1]IDY DIOP, [2]IBRA DIOUM, [3]SAMBA DIAW , [4]MADIOP DIOUF, [5]SIDI MOHAMED FARSSI, [6]YACOUB MAHAMAT ADOUM

[1,2,3] LECTURER, [5]Professor,[4,6]Student at IT Department, Polytechnic Institute (ESP)/Cheikh Anta DIOP University (UCAD), Dakar, Senegal

E-mail: idy.diop@esp.sn, samba.diaw@esp.sn,ibra.dioum@esp.sn, madiop.diouf@esp.sn

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 choice of parameters of the code, if not an opponent will use this change to attack the system.

the objective of this paper is to see and propose solutions on hardware difficulty encryption algorithms and deciphering based on Key size and transmission rate.

This work is an electronic contribution on the using of Goppa codes in McEliece cryptosystems. We propose in this paper implementation on FPGA cart of the schema of encryption based on these codes inspired by the mathematical approach. We evaluated the performance by of our method by study Key size and transmission rate .

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

1. INTRODUCTION

Today, the most used public key cryptosystems are RSA, Diffie- Hellman, ElGamal 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 [4].

However there are alternatives including the McEliece system which is supposed resistant because it's not yet broken by the quantum computer.

The original McEliece system uses conventional binary Goppa. Here, we propose a McEliece scheme using codes QC- Goppa[1]. The generator matrix elements of such a code is 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.

The rest of the paper is organized as follows. The section II presents the linear error correcting code linear error correcting codes. Section III is dedicated to McEliece cryptosystem The proposed scheme based on the quasi- cyclic codes of Goppa is presented in the section IV. Simulation results and the performance of electronic implementation are shown in this section.

2. LINEAR ERROR CORRECTING CODES

The construction of a code word having n –bit is performed from k bits of the message source binary $k - tuple = (u_1, u_2, u_3, \ldots, u_k)$, 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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

code word by adding $r\ (= nk)$ redundancy bits $\{a_1, a_2, \dots, a_r\}$, which are generally called bit controls. The V^T vector line called code word:

$$VT = [v1\ v2\ \dots\ vn] = [u1, u2, u3, \dots, uk\ a1, a2, \dots, ar]. \quad (1)$$

When control bits are calculated only from the block of information bits to which they belong, 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^k code 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 are also a 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 $R = \frac{1}{n} log_2 |C|$ where C is an abusive notation of the number of codewords [5].

2.1 Generator and parity check matrices

2.1.1 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. To form a codeword, we calculate the product of a row vector $(u_1, \dots, u_k)$ and the generator matrix

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

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 operations on the row and a permutation on the columns.

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

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.

2.1.2 Parity check matrix

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

$$x \in C \Leftrightarrow H.x^T = 0 \quad (4)$$

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 to the lines of the matrix H.

2.2 Cyclic and quasi-cyclic codes

2.2.1 Cyclic code

Let F_q^n be any subspace and T defined by:

$$T: \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$
$$(x_1, x_2, \dots, x_n) \mapsto (x_n, x_1, \dots, x_{n-1}) \quad (6)$$

The circular shift application called as 'shift'.
Let C be a code of length n on F_q^n.
By definition:

$$C\ is\ cyclic \Leftrightarrow \forall\ c \in C, T(c) \in C \quad (7)$$

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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:

$$c = (c_0, c_1, \dots, c_{n-1}) \leftrightarrow c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \quad (8)$$

2.2.2 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 $l \in \mathbb{N}^*$. By definition:

C is l-quasi-cyclic $\leftrightarrow \forall c \in C, T^l(c) \in C$

The T^l permutation is called quasi-shift.

The linear binary codes with the following generator matrix

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \quad (9)$$

Is 2-quasi-cyclic

2.2.3 Binary Goppa Codes

Goppa binary codes are from the generalized Reed-Solomon codes and enable to obtain a good minimal distance. These codes are used in cryptography[4] (cryptosystem McEliece).

The Goppa code $\Gamma\,(L;\, g\,(x)\,)$ 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 $GF(\,q^m)$.

$$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_t x^t \quad (10)$$

$$L = \{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq GF(q^m) \quad (11)$$

such as $g(\alpha_i) \neq 0, \forall\, i \in \{1, \dots, n\}$

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

$$R_c(x) = \sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} \quad (12)$$

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

$$R_c(x) = 0\big(mod\; g(x)\big) \quad (13)$$

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

Goppa code $\Gamma\,(L\; g\,(x))$ of size n is a linear code over $GF(q)$ with the following properties in [6]:

- The size of the code satisfies the following relationship $k \geq n\; - mt$
- The minimum distance of the code satisfies $d \geq t\, +\, 1$.

3. McEliece Cryptosystem

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

3.1 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 the recipient 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 $x_0\; = xG_p\; + e$

Where e is 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

$$x_0\,P^{-1} = xSG + eP^{-1} \quad (14)$$

Using an efficient algorithm for decoding the code, he finds xS . Since S is invertible, then recovered x.

Encryption algorithm:

Input: $x, Kpub\; = (G_p;, t)$

Output: cipher x_0;

1. Encode the message x into a sequence of binary characters with length n
2. $c' \leftarrow x \cdot G_p$;
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:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

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

4. Proposal of the scheme based on the quasi-cyclic codes of Goppa

4.1 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 $n = n_0 \cdot k$, with size $p = k_0 \times k$ and having redundancy $r = k$ is adopted, where n_0 is the index of quasi- cyclicality $(n_0 = 2,3,4,\dots)$, $k_0 = (n_0 - 1)$ 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:

$$H = [H_0|H_1|\dots|H_{n_0} - 1] \quad (15)$$

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 H_{n_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.

$$Q = \begin{bmatrix} (H_{n_0-1}^{-1} \cdot H_0)^T \\ (H_{n_0-1}^{-1} \cdot H_1)^T \\ \vdots \\ (H_{n_0-1}^{-1} \cdot H_{n_0-2})^T \end{bmatrix} \quad (16)$$

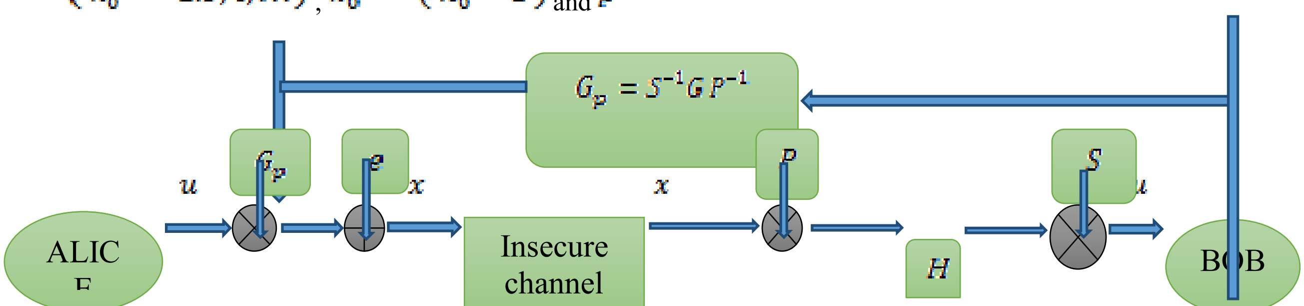

Figure 1 : Le Cryptosystème De Mceliece Basé Sur Les Codes QC-Goppa [7]

4.2 Encryption and its complexity

4.2.1 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 matrix, 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 the execution of n binary operations for the random error vector. [7]

$$N = (n_0 - 1) \cdot n_0 \cdot k\ b \quad (17)$$

4.2.2 Encryption complexity

Encryption is performed by calculating the product u*G_p and adding to it the random error vector.

Thus, the complexity of encryption lies in the multiplication of the matrixes of huge sizes and. Table 1 provides information on the number of needed binary operations for each encrypted bit to a circular matrix of size $k \times k$, and with indices of cyclicality $n_0 = 3\ et\ n_0 = 4$.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

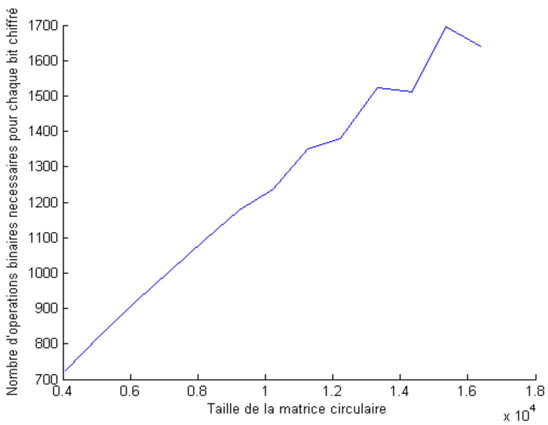

Figure 2: Change In Number Of Binary Operations For Each Encrypted Bit For N_0=3.

We note that with a very large (13k bits and 17kbits), growth in the number of binary operations is not stable

5. Selection of parameters

In [5], the authors proposed a variant of McEliece scheme based on codes of 2^{80} Goppa. With this variant, they can get a security of for a public key of 6000 bits and a security of 2107 for a public key of 11.

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: the size of the Galois field used $L = F_2^n = \{0,1\}^n$: Code support n_0=2: index of quasi-cyclic code n=6502Length of the code word..K=3251 length of the message $S(3251 * 3251)$: No 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 $C[n_0,\ k,\ n]_{F_2^n}$.

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_o=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 (17) 6502 bits.

6. IMPLEMENTING STEPS

The Galois field in which we work is the GF (2^{13}), we have for our implementation encryption circuit [8], regrouping the generation of code words and the encryption.

The choice of t=251 satisfies the relationship $k \geq n - mt$ for code Goppa.

6.1 Encryption

The encryption algorithm is described in Section 3.1. Here VHDL encryption module is processed. Encryption is designed using the architectural model [9].

Figure 2 shows the encryption block and the figure 3, the simulation result of the encryption using the simulation tool ISIM of XILINX 14.7 development software.

Journal of Theoretical and Applied Information Technology
31st December 2016. Vol.94. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

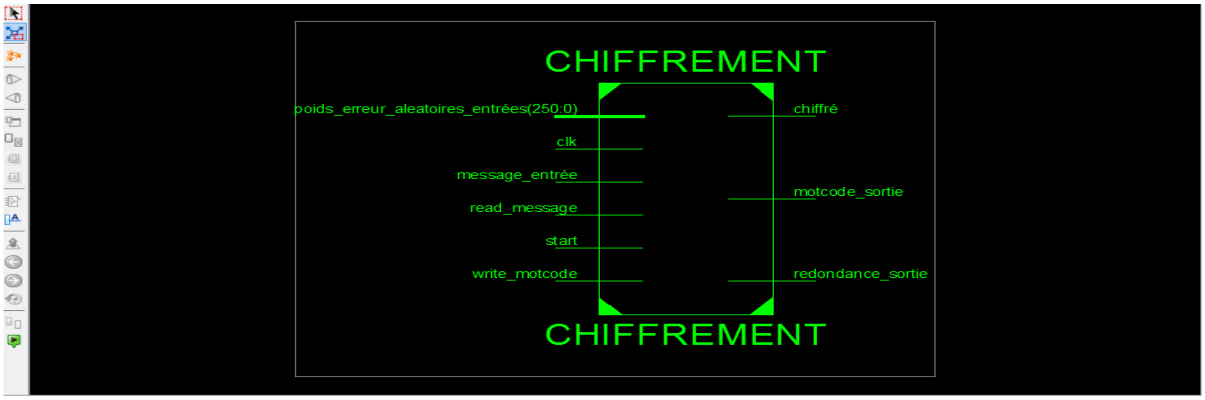

Figure2 Encryption Block Of Mceliece

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 and redundancy.

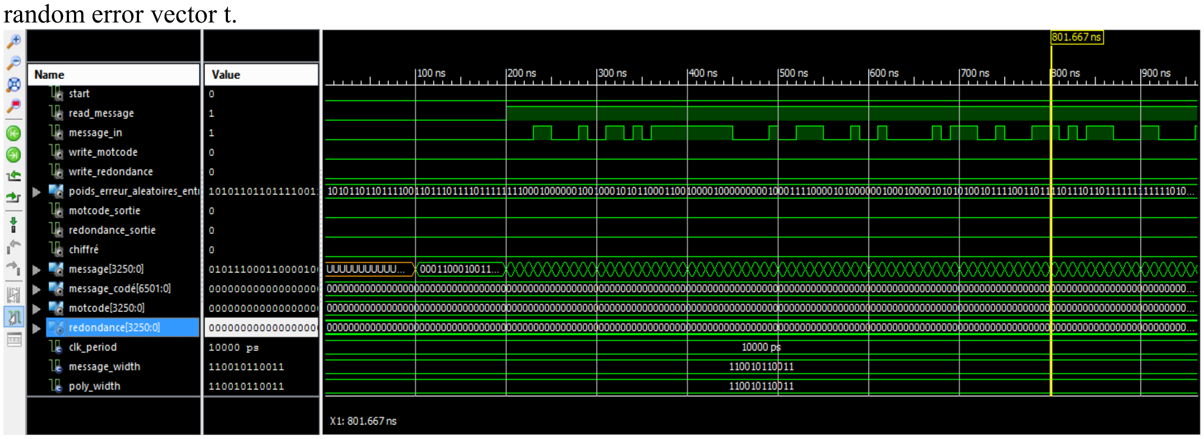

Figure3: Simulation Of Mceliece Encryption Scheme With The Xilinx ISE 14.7 Software
We Note That Although This Figure 100 Ns, We Get A Code Word, So That Encryption Is Relatively Fast

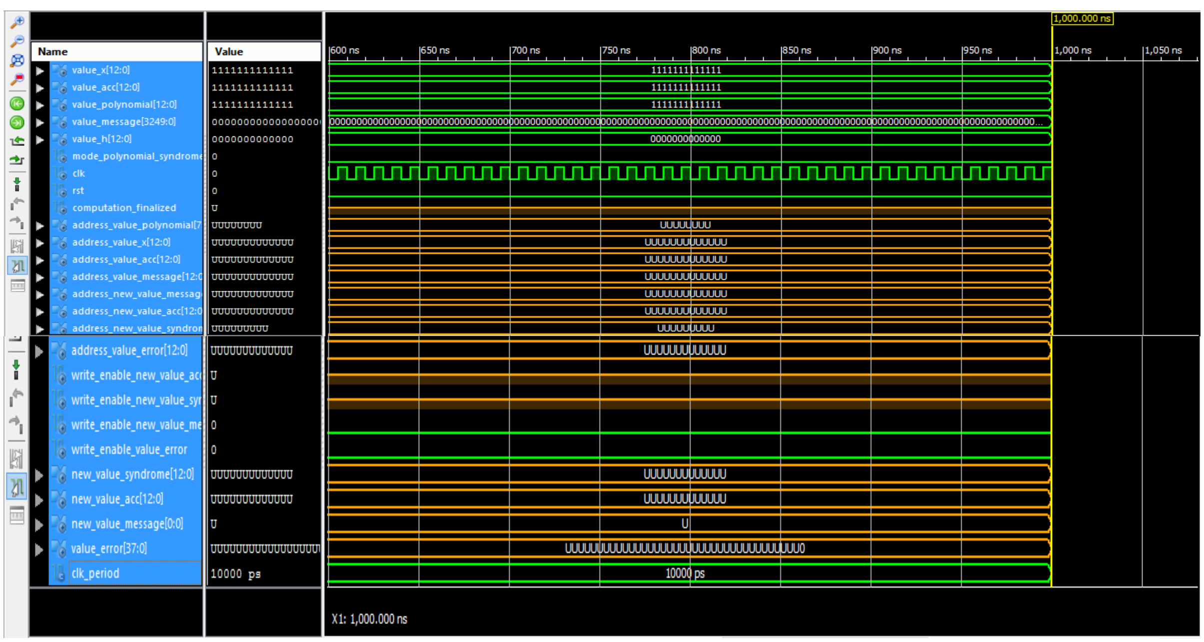

Figure4: Simulation Of Syndrome Décoding

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

6.2 Decryption

Decryption process has three (3) main stages. VHDL program circuit is divided into three (3) stages: calculation of the syndrome, the key equation solving and research roots. Two sub-circuits can perform these three functions. All circuits have some common inputs and outputs.
The first circuit, Calcul_du_syndrome, calculates the syndrome from the encrypted message received, private keys, and the support L of the polynomial g (x) (See Chapter 1, paragraph 2.8).
The second circuit, Resolution_equation_clef, calculates the error locator polynomial sigma through the syndrome calculated by the first circuit.
Finally, it uses the first circuit to find the roots of the polynomial sigma and correct errors in the encrypted message and finally obtain the plaintext message.

- Syndrome decoding.

Compared to the speed of encryption, decryption is slow. We note here that the calculation of the syndrome take up to 1000ns.
This slowness is due to the fact that the decryption is performed sequentially and contains several circuits that are related. To treat a circuit, it takes the availability of other circuit elements.
And to retrieve the error in the next circuit, we need the system of calculating the syndrome because it is the latter who compiled the error introduced encryption

In this section, we proposed a McEliece scheme using quasi-cyclic codes Goppa instead of traditional Goppa codes. Such an amendment is to overcome the main drawbacks of the original system McEliece as it will achieve a satisfactory level of safety.
The results confirm that the use of quasi-cyclic codes allows significantly reduce the size of the keys McEliece scheme.
Compared with conventional Goppa codes that provide for a securié 2 ^ 90 with a key 2.5Mbits, we conclude that the quasi-cyclic codes are ideal versions for research in the area . The use of these codes also has limitations; including reducing the encryption speed is explained by the circular structure of the matrices used

7. 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 the McEliece 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 2.5 Mbits , 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.

REFRENCES:

[1] Quasi-cyclic codes as codes over rings of matrices.Pierre Louis Cayrel, Christophe Chabot, Abdelkhader Nacer.
[2] Reducing key lengh of the McEliece cryptosystem. Thierry Berger, Pierre Louis Cayrel.
[3] Code-based cryptography: Implementing the McEliece Scheme on Reconfigurable Hardware. Stefan Heyse (May 2009).
[4] Biswas and Sendrier. McEliece Cryptosystem Implementation: Theory and Practice. PQCrypto2008.
[5] Reducing key lengh of the McEliece cryptosystem. Thierry Berger, Pierre Louis Cayrel
[6] Goppa codes and the McEliece cryptosystem.Vrije University of Amsterdam.
[7] Security and complexity of the McEliece cryptosystem based son QC-LDPC codes Marco Baldi, Marco Bianchi and Franco Chiaraluce. Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche. Ancona, Italy.
[8] https://github.com/pmassolino/hw-goppa-mceliece. Hardware implementation of the cryptosystem McEliece in VHDL for binary (QD-) Goppa codes. Consulté pour la dernière fois le 06 Avril 2016.
[9] A Software implementation of the McEliece public-key cryptosystem. Bart Preneel, Antoon Bosselaers, René Govaerts1 and Joos Vandewalle