ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Random Hexi Code Based Public Key Encryption (RHCE) Scheme for Code-Based Cryptography

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

***Abstract* - Nowadays security on network is major challenge. For securing the information on network various public key Encryption schemes are used. In this paper, we introduced a new scheme called Random Hexi Code Encryption Scheme. In this encryption scheme, Binary Goppa Code is changed via Hexi Code which is more secure against attacks executed on the present variations of McEliece PKC and RLCE scheme. This new scheme has better error correcting ability and lesser time complexity making it more feasible to apply.**

***Keywords:* McEliece Encryption scheme, Hexi codes, Hexi polynomial Codes, Hexi McEliece public key cryptosystem, RLCE scheme. (AMS) Mathematics Subject Classification No: 94A60**

INTRODUCTION

In 1978, [8] McEliece presented a cryptosystem named McEliece Public Key Cryptosystem, which might have been at present unbroken by Cryptologists. The original McEliece Public Key Cryptosystem is based on Binary Goppa Codes. A few variants have been introduced to replace Goppa codes in the McEliece Encryption scheme. For example, Niederreiter [6] proposed the use of generalized Reed-Solomon codes and later, Berger and Loidreau [5] proposed the use of sub-codes of generalized Reed-Solomon codes. Sidelnikov [4] proposed the use of Reed-Muller codes, Janwa and Moreno [6] proposed the use of algebraic geometry codes, Baldi et al [1] proposed the use of LDPC codes, Misoczki et al [11] proposed the use of MDPC codes, Londahl and Johansson [7] proposed the use of convolutional codes, and Berger et al [2] and Misoczki-Barreto [10] proposed quasi-cyclic and quasi-dyadic structure based compact variants of McEliece encryption schemes. Most of them have been broken though MDPC/LDPC code based McEliece encryption scheme [1], [11] and the original binary Goppa code based McEliece encryption scheme are still considered secure. In the quite a while 2015, [16] Y.Wang suggested Quantum Resistant RLCE which offers Numerous qualities for those random linear code. In 2013,[4] AES created hexi code for error correction. Further On 2014, K.Ilanthenral gives improvement for these codes in paper [5]. They demonstrated that these codes are used to create variants of McEliece Public Key Cryptosystem known as Hexi McEliece Public Key Cryptosystem and its variants.

This paper introduced Random Hexi code Encryption scheme (RHCE) was prepared into five sections. Section 1 is introductory in nature. Section 2 recalls the definition of Hexi codes and other related codes and their decoding and error correcting ability are discussed. Section 3 introduces the proposed scheme i.e Random hexi code encryption (RHCE) scheme. In section 4 the security and some feasible attacks are discussed and ultimately, last but not the least section 5 offers the conclusion.

II. PRELIMINARIES

2.1 *Hexi field*

Let $S=Z_2^4$ be a field of 16 elements which is isomorphic to $\frac{Z_2[x]}{<x^4+x+1>}$ where $<x^4+x+1>$ is the ideal generated by the irreducible polynomial $<x^4+x+1>$ in $Z_2[x]$. Now the elements are given hexadecimal notation, where 0 = 0000, 1 = 0001, 2 = 0010, 3 = 0011, 4 = 0100, 5 = 0101, 6 = 0110, 7 = 0111, 8 = 1000, 9 = 1001, A = 1010, B = 1011, C = 1100, D = 1101, E = 1110 and F = 1111. In short S=0,1,2,...,9,A,...,F. Clearly $(S,\oplus,\otimes)$ is a field of order 16. The operator '$\oplus$' denotes XOR modulo 2, is given in Table 1 and each element is inverse of itself with respect to $\oplus$. The operator '$\otimes$' denotes multiplication modulo $<x^4+x+1>$ is given in Table 2. This operator '$\otimes$' multiplication modulo $<x^4+x+1>$ was used in Mini AES in [27] and also described in [14]. This field is called as hexi field. Let $V^n=(x_1,\ldots,x_n)|x_i\in S;1\le i\le n$ be a n-dimensional vector space defined over S [5] .

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

2.2 *Hexi Codes*

A block code of length n with $(2^4)^k$ code words is called a hexi (n,k) block code, denoted by $C_{HC}(n,k)$, if and only if its $(2^4)^k$ code words form a k-dimensional subspace of the vector space V^n of all n tuples over the hexi field S [5].

2.3 *Hexi Polynomial Codes*

There are two types of Polynomial codes, x^n+1 and x^n+z ($z \in S\backslash\{0\}$ and $z \neq 1$). When x^n+1 is used, it forms a usual cyclic code, $g(x)$ is a polynomial which divides x^n+1 and its coefficients are from S. To generate a $C_{HC}(n,k)$ cyclic hexi code, consider only the polynomial of the form x^n+1. Instead of x^n+1, consider x^n+z ($z \in S\backslash\{0,1\}$), then $x^n+z = g(x)\times h(x)$, $g(x)$ and $h(x)$ are polynomials belonging to S[x]. Let G_H be the generator matrix associated with generator polynomial $g(x)$. Let H be the parity check matrix associated with the parity check polynomial $h(x)$. The $C_{HC}(n,k)$ hexi code is not cyclic. Clearly $GH^T = (0)$. If $(x_1,\ldots,x_n) \in C_{HC}(n,k)$, then in general $(x_n,x_1,\ldots,x_{(n-1)})$ not belongs $C_{HC}(n,k)$ [5].

$C_{HC}(n,k)$, The hexi polynomial code produced by the polynomial $g(x)$ may be characterized as takes after.

Let x^n+z, ($z \in S\backslash\{0,1\}$), be a hexi polynomial in S[x]. If $x^n+z = g(x)h(x)$ where $g(x)$ is the hexi generator polynomial associated with the generator matrix G_H and $h(x)$ is the hexi parity check polynomial associated with the parity check matrix H. If $g(x)$ generates a code $C_{HC}(n,k)$, then $C_{HC}(n,k)$ is defined as the hexi polynomial code associated with the hexi generator polynomial $g(x)$.

Let $g(x) = g_0+g_1x+\ldots+g_mx^m$ be the hexi generator polynomial, then the generator matrix G of the hexi polynomial code $C_{HC}(n,k)$ is as follows:

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_m & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{m-1} & g_m & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & g_0 & g_1 & \vdots & g_m \end{pmatrix}$$

3 Random Hexi Code Based Public Key Encryption (RHCE) Scheme

The Random hexi code Encryption scheme is primarily based on hexi polynomial code which isn't cyclic in nature. Hexi polynomial code is used rather than binary Goppa code. Hexi GPT cryptosystem and hexi wild McEliece cryptosystem are also discussed [5]. The Random hexi code Encryption scheme has better error correcting ability and less time complexity. The important parameters of the Random hexi code Encryption scheme based totally on hexi polynomial codes are as follows:

let G be the generator matrix for a $C_{HC}(n,k)$ hexi polynomial code based on the generator polynomial $g(x) = g_0+g_1x+\ldots+g_{(n-k)}x^{(n-k)}$ where $x^n+z \in S[x]$, $z \in S\backslash\{0,1\}$, and S_H be the $k\times k$ invertible matrix over the hexi field S.

let P be the $n\times n$ permutation matrix. Let A be the $n\times n$ random nonsingular diagonal matrix.

The decoding of the message can be performed in time complexity of $(n-k)lg(n-k)$, if $n=\Theta(n-k)$.

The public key for the cryptosystem may be given by means of G'

$$G' = S_H \times G_H \times A \times P \qquad (1)$$

in which G' is a $k\times n$ matrix. The error correcting capacity of hexi polynomial code $C_{HC}(n,k)$ with generator matrix G_H is $n-k$. 2^{n-k} error patterns are generated, depending on the permutation matrix P. Error is added only to the parity elements within the resultant vector. Any of the error pattern e_p is chosen and random error e_r of length n is taken. If i^{th} element of the error pattern is 1, then the i^{th} element of error e is the i^{th} element of error e_r, else it is set as 0.

Algorithm 1. Encryption Algorithm for encryption in RHCE scheme.

Input: m - Message, G' - Public key, e_p - Error Pattern, e_r - Random error, e - Final error.

Output: y- Ciphertext

begin

Compute $m\times G'$

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Select error pattern e_p, Random error e_r of length n
For i = 1 to n do
If $e_{pi} \neq 0$ then $e_{ri}=e_i$
else $e_i = 0$
end
Return $y = m \times G' + e$
end

Algorithm 2. Decryption Algorithm for Decryption in RHCE scheme.

Input: G_H, S_H, P, A - Private key, y_1 - Ciphertext, C_{HC} (n,k) -Hexi Code,

Output: m – Message

begin
Compute $y_1 \times P^{-1} \times A^{-1}$
Use decoding algorithm to remove error and obtain code word $m=S_H G_H AP$
Compute m_0 such that $m_0=mG_H$
Calculate $m=m_0 S_H^{-1}$
Return Original message m
end

3.1 Example

Let us consider a hexi polynomial $x^7+F \in S[x]$. Also let $x^7+F=g(x) \times h(x)$ where $g(x)=x^4+cx^3+Fx^2+A$ and $h(x)=x^3+cx^2+8$ be the hexi polynomial and parity check hexi polynomial respectively in the hexi field $S[x]$

Addition Table

⊕	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Table 1

Multiplication table

⊗	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

Table 2

The Generator matrix of the hexi polynomial code $C_{HC}(7,3)$ is represented by G_H

$$G_H = \begin{pmatrix} A & 0 & F & C & 1 & 0 & 0 \\ 0 & A & 0 & F & C & 1 & 0 \\ 0 & 0 & A & 0 & F & C & 1 \end{pmatrix}$$

Let S_H be 3×3 be random invertible matrix given below

$$S_H = \begin{pmatrix} 1 & 2 & 0 \\ C & F & 0 \\ 0 & 4 & A \end{pmatrix}$$

Let A=(7,A,F,2,C,1,D) be an 7×7 non-singular diagonal matrix.
Let P be 7×7 permutation matrix given by

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

The public key is 3×7 matrix G obtained by

$$G' = S_H G_H AP = \begin{bmatrix} 3 & 3 & A & 2 & 1 & 2 & 0 \\ 0 & 1 & 0 & 7 & A & F & 0 \\ 0 & 6 & 1 & 1 & 6 & 5 & B \end{bmatrix}$$

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Encryption:-
Let us assume that m_H = (2 0 B) be the original message which needs to be encrypted for this, compute $m^{'}$ obtained by follows:

$$m^{'}=m_H \times G^{'} = (6\ 5\ 9\ 9\ F\ D\ C)$$

where $m^{'}$ is the encrypted message.
Possible error patterns for the encrypted message will be:

e_p=(0 0 0 0 0 0 0),
e_p=(0 0 0 0 0 0 1),
e_p=(0 0 0 0 0 1 0),
e_p=(0 0 0 0 0 1 1),
e_p=(0 0 0 0 1 0 0),
e_p=(0 0 0 0 1 0 1),
e_p=(0 0 0 0 1 1 0),
e_p=(0 0 0 0 1 1 1).

Let e_r= (A B 0 4 7 1 0) be the random error and selected error pattern be (0 0 0 0 1 1 1).
Then error e can be written as e = (0 0 0 0 7 1 0).

The cipher text is
$y=m^{'}G^{'}+e$
y = (6 5 9 9 F D C) + (0 0 0 0 7 1 0)
= (6 5 9 9 8 C C)
y is the final encrypted message.

Decryption:-
For the received cipher text
y=(6 5 9 9 8 C C),
compute $yP^{-1}A^{-1}$ where,

$w=y_1P^{-1}A^{-1}$ = (7 6 A 4 1 5 2)
which can be expressed as a hexipolynomial as
$w(x)=2x^6+5x^5+x^4+4x^3+Ax^2+6x+7$
Now by using the decoding algorithm [5], the error correcting and the decoding of the intermediate message is calculated and produce message as a quotient
$m_0=2x^2+Ex+8$
and the remainder as the error
$e=Bx^3+Ax^2+6x+8$

The message m_0=(2 E 8) and the error e=(0 0 0 B A 6 8) are obtained.

The inverse of the invertible matrix S_H is S_H^{-1} which is given below:

$$S_H^{-1} = \begin{pmatrix} 1 & 9 & 0 \\ 0 & 8 & 0 \\ 0 & E & 3 \end{pmatrix}$$

Now for obtaining original message we compute
$m= m_0 \times S_H^{-1}$ = (2 0 B)
Here m is the original message which is computed after decryption.

IV. ATTACKS ON THE RHCE SCHEME

In any code-based cryptosystem, there are two major attacks named structural attack and decoding attack.

4.1 *Structural attack*

4.1.1. Chosen Ciphertext attack(CCA)

This step is used to defeat chosen cipher text attacks (CCA). In a CCA attack, an adversary gives a random vector y to the decryption oracle to research a decrypted value. This decrypted value will be used to gain sure information about the non-public generator matrix G_H. As a substitute, one may also use the correct padding scheme to pad a message before encryption. Then it's far enough for the decryption technique to verify whether or not the decrypted message has the precise padding strings to defeat the CCA attacks.
So as for the attacks within the previous paragraphs to work, the adversary needs to have the know-how of the permutation matrix P. Since the number of candidate permutation matrices P is big, this kind of attacks are still infeasible in practice.

4.1.2 Niederreiter's scheme and Sidelnikov-Shestakov's attack

Sidelnikov and Shestakov's cryptanalysis approach [15] turned into used to research Niederreiter's scheme which is based totally on GRS codes.

The crucial step in Sidelnikov and Shestakov assault is to use the echelon shape $E(G)=[I|G^{'}]$ of the general public key to getting minimum weight codewords which are co-related to every other helps. In the encryption scheme RHCE, each column of the general public key G consists of combined randomness. For that reason the echelon shape $E(G)=[I|G^{'}]$ obtained from the public key G couldn't be used to build any beneficial equation system. In different phrases, it is expected that Sidelnikov and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Shestakov attack does not work towards the RHCE scheme.

Here to break the cryptosystem, one should locate the generator $g(x)$ of degree m, given the message, one ought to attempt at least m! guesses. That is also not possible for large m. When m is as small as ten, nearly 362900 guesses must be attempted.

4.1.3 Algebraic attack

Because a big public key length is one of the drawbacks of code-based cryptography, there have been many proposals attempting to reduce the key length. Frequently, the authors used highly structured codes which can be stored extra successfully. Examples of highly structured codes consist of Quasi-cyclic and Quasi-dyadic codes, as well as Low-Density Parity check (LDPC) codes. Currently, there were numerous attempts using structural attacks against such highly structured codes. Algebraic attacks cannot be performed on this public key cryptosystem because the hexi polynomial codes that are used are not cyclic or Quasi-cyclic or Quasi-dyadic and those codes do not have low degree algebraic equation for code support.

4.2. *Decoding Attack*

4.2.1 Information set Decoding

A deciphering attack includes decoding the intercepted ciphertext. Information Set decoding (ISD) and the Generalized Birthday algorithm (GBA) are the two maximum essential kinds of regularly occurring attacks towards code-based cryptosystems. The information set decoding attack is a top risk to the original McEliece cryptosystem, in a usual deciphering technique. Information set decoding relies upon on syndrome decoding and systematic form of the generator matrix G to break the cryptosystem.

But this newly delivered hexi McEliece cryptosystem does no longer rely on syndrome deciphering. The generator matrix G of the hexi polynomial code this is used on this cryptosystem is no longer given in its systematic form, hence information set deciphering attack can't be effortlessly executed on the cryptosystem.

4.2.2 Generalized birthday algorithm

The generalized birthday algorithm isn't as efficient as the information set decoding attack on code-based cryptosystems. The CFS signature scheme [13] was attacked the use of this technique. The method uses a very large list. For a sufficiently huge n, this cryptosystem is secure.

V. CONCLUSION

This paper introduced a method for designing Random hexi code based public key Encryption Scheme. This scheme have better errors correcting capacity as compared with Goppa codes. The time complexity of decoding hexi polynomial code is O(m lg m) lesser as compared with the polynomial time for decoding Goppa code. Totally Based on Hexi polynomial code, Random Hexi code primarily based Encryption scheme is created. The viable attacks on this RHCE system have also analyzed. Conclusion that the RHCE scheme is not susceptible to several structural and decoding attacks.

REFERENCES

[1] M. Baldi, M. Bodrato, and F. Chiaraluce. A new analysis of the mceliece cryptosystem based on qc-ldpc codes. In Security and Cryptography for Networks, pages 246–262. Springer, 2008.

[2] T.P. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing key length of the mceliece cryptosys- ˜ tem. In Progress in Cryptology–AFRICACRYPT 2009, pages 77–97. Springer, 2009.

[3] T.P Berger and P. Loidreau. How to mask the structure of codes for a cryptographic use. Designs, Codes and Cryptography, 35(1):63–79, 2005.

[4] K. Ilanthenral and K.S. Easwarakumar, Design of Hexi cipher for error correction–using Quasi Cyclic Partial hexi codes, Journal of Applied Mathematics and Information Sciences, 7, 2063-2071 (2013).

[5] K. Ilanthenral and K.S. Easwarakumar, Hexi McEliece Public key cryprosystem, Journal of Applied Mathematics and Information Sciences, 5, 2595-2603 (2014)

[6] H. Janwa and O. Moreno. Mceliece public key cryptosystems using algebraic-geometric codes. Designs, Codes and Cryptography, 8(3):293–307, 1996.

[7] C. Londahl and T. Johansson. A new version of mceliece pkc based on convolutional codes. In ¨ Information and Communications Security, pages 461–470. Springer, 2012

[8] R.J. McEliece, A public-key cryptosystem based on algebraic coding theory, Jet Propulsion Laboratory DSN Progress Report, 4244, 114-116 (1978).

[9] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In

Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, pages 2069–2073. IEEE, 2013.

[10] R. Misoczki and P. Barreto. Compact mceliece keys from goppa codes. In Selected Areas in Cryptography, pages 376–392. Springer, 2009.

[11] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. Barreto. MDPC- McEliece: New McEliece variants from moderate density parity-check codes. In Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, pages 2069–2073. IEEE, 2013.

[12] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. Prob. Control and Information Theory, 15(2):159–166, 1986.

[13] N. Courtois, M.Finiaz and N.Sendrier, How to achieve a McEliece based digital signature scheme, Advances in cryptology - ASIACRYPT 2001, Springer Verlag, 2248, 157-174 (2001).

[14] V.M. Sidelnikov. A public-key cryptosystem based on binary reed-muller codes. Discrete Mathematics and Applications, 4(3):191–208, 1994.

[15] V. M. Sidelnikov and S. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete mathematics and Applications,2(4):439-444, 1992.

[16] Y. Wang. Random linear code based public key encryption implementation http://webpages.uncc. edu/yonwang/rlce.html, 2015