McEliece Cryptosystem and its Signature Scheme: A Survey

***Renuka Sahu*[1] and *B. P. Tripathi*[2]**
***Research scholar* [1] and *Assistant Professor*[2]**
***Department of Mathematics*[1]**
[1]*Govt.N.P.G.College of Science , Raipur, Chhattisgarh, India.*

Abstract : In this paper, McEliece cryptosystem and its digital signature schemes using various significant codes are reviewed. McEliece cryptographic algorithm is very fast using Goppa codes which was considered to be secure against several quantum attacks but, the major drawback is its large public key size. Therefore, to reduce the size of public key many improvements are made and is still in process without compromising with its security. The paper provides several modifications and developments done in the field of McEliece cryptosystem. Also focus on the digital signature schemes in the code-based cryptography.

Index terms: *Code-based cryptography, McEliece cryptosystem, Algebraic codes, Goppa code.*

I. INTRODUCTION

In the field of information or data security, the word “cryptography", “cryptanalysis", and “cryptology" have different meanings. Cryptology is a mathematical encoding and decoding techniques for ensuring the secrecy and authenticity of information or data. It has two main branches, one is cryptography and other is cryptanalysis. A technique is required to design a kind of system which produces unique information or data that cannot be understood by any person, except the intended recipient. This technique is called “cryptography" and the method of doing this process is called “cryptosystem". Cryptanalysis is an investigation process for unintended recipient of disguised information or data that attempting to remove the disguise and understand the information. The successful cryptanalysis is sometimes called “breaking" or “cipher cracking". The term “Cryptology" includes cryptography, cryptanalysis and interaction between them.

When system is used by two parties to exchange information, the undisguised information is called Plaintext, and the disguised information is called cipher-text. The process of converting plaintext to cipher-text is called Encryption. After receiving a cipher-text, the recipient must removes the disguise information. The conversion of cipher-text to plaintext is called Decryption. For effective encryption and decryption of the message, two parties must have to share knowledge of secret key. Encryption schemes are divided into two parts “Symmetric" and “Asymmetric". Symmetric encryption scheme permits two parties to communicate information securely but they need to agree beforehand. In this scheme, identical key is used for encryption and decryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys. It is important to note that with a secret key anyone can decrypt the message and this is why asymmetrical encryption uses two different keys to boosting security. A public key is made freely available to anyone who might want to send a message. The second private key is kept secret so that receiver can only know. A message which is encrypted by using a public key can only be decrypted by using a private key. While a message encrypted by using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the Internet. Asymmetric key has better power in ensuring the security of information transmitted during communication. Asymmetrical encryption scheme is also known as public key cryptography, which is a new method, as compared to symmetric encryption scheme. The first modern Asymmetric cryptographic scheme became introduced within the groundbreaking work of Diffie and Hellman [19]. They vaticinated the desires of a global-huge spanning network which is known as the Internet, a place where communication between strangers occurs continuously. They suggested DH cryptosystem, based on a mathematical problem referred as the discrete logarithm problem. Merkle-Hellman cryptosystem [43] is a public key cryptosystem obtained from knapsack problem. However it is broken and is not current in use. At the same time Rivest, Shamir, and Adleman created the RSA cryptosystem [43], is still remain unbroken and is one of the mostly used cryptosystem nowadays. The RSA cryptosystem is based on multiplication and factoring; multiplying number is simple - even large one, however factorization of a number is extremely hard. After that, Shor [53] developed an algorithm that includes exceptional trait, which efficiently works with integers. There is only one drawback: to run it, one wants a quantum computer. The Concept of quantum computers, initiated by Manin [39] and Feynman [23] in 1980's. It takes advantage of quantum mechanics, which allows the quantum computer to function simultaneous computation over a massive scale. Quantum computer efficiently performs issues of number theory and different logarithmic problems. The series of overwhelming discoveries lead researches between a modern direction i.e. Post-quantum cryptography. Code-based cryptography is one among the candidates of post quantum cryptography. It is related to the coding theory and based on linear codes.

The theoretical and practical aspects of code based cryptography are briefly explained in this review paper. As it was claimed that the quantum algorithms would break all of the public key cryptosystems. Thus, some alternative public key cryptosystems are introduced, which have been proven to be safe against the various quantum attacks. Code-based cryptography is related to coding theory and is based on Linear codes. In 1978, first code-based cryptosystem is presented by McEliece [40], which totally depends on the error correcting code. This cryptosystem uses irreducible Goppa Code as a private key and random generator matrix which is randomly permuted form of that code. The block diagram for a coding system is shown in fig. 1.

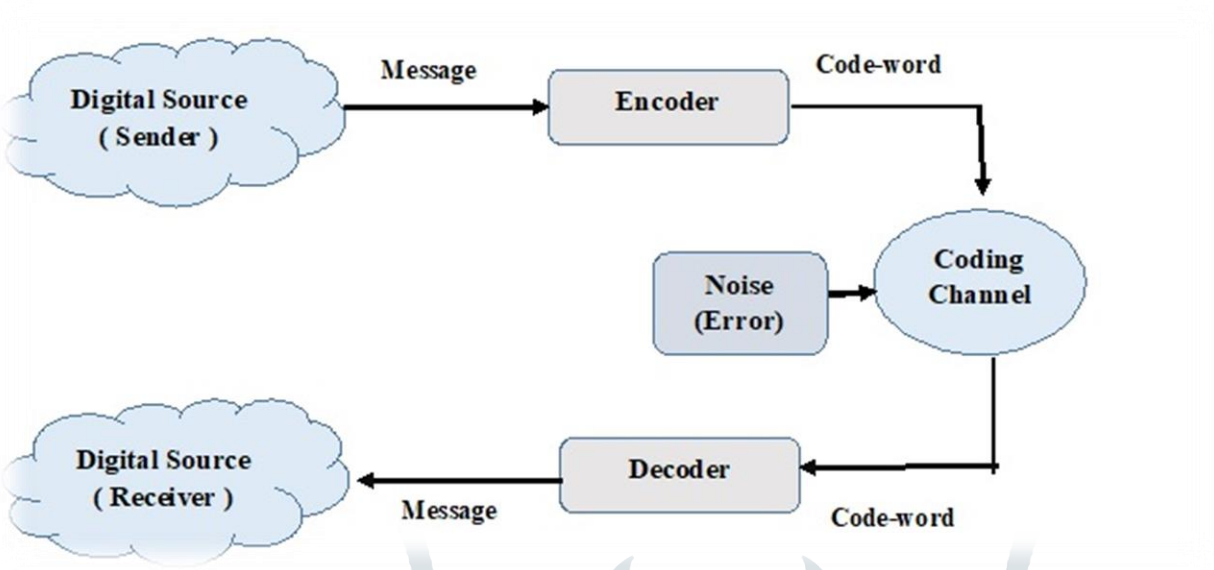


Figure 1. Block Diagram of coding system

Sender encrypts the information or message and transmit it through a coding channel. Cipher-text is a code word obtained by adding some errors to the plain-text so that only receiver having the private key will decrypt it by removing the added errors. This process of error-detection and error-correction is done using codes which have the capability of correcting errors. The McEliece cryptosystem is still considered to be secured based on some parameters against quantum attacks. In this chapter we will first recall the facts on Algebraic Coding theory to introduce linear codes, Hamming codes, generator matrix, parity check matrix and their properties. Next we discuss the McEliece Encryption algorithm with its advantages and disadvantages.

II. ALGEBRAIC CODING THEORY

Error-Correcting Code

In coding theory, the mathematical strategy used for protecting data/ information over noisy communication channel is Error Correcting code. The fundamental idea behind this concept is used by the sender to encrypt the plain-text by adding some error/redundancy to it. The receiver will then correct the errors if it was altered by anyone other than sender during transmission and recover the original message. Error-correcting codes is categorized into Block code and convolutional code which is explained in fig 2.

Linear Code

Linear codes is one of the most important families of error-correcting codes. A *(n, k)* code, where *n* and *k* are length and dimension of a linear subspace *C* respectively over the vector space F_q^n, where F_q^n is the finite field with *q* elements is called Linear Code.

Examples of linear block codes are Cyclic codes, Perfect codes and Low Density Parity Check (LDPC) Codes.

Hamming Distance

The hamming distance is known as the number of different bit locations. Consider two vectors $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in *n* dimensional vector space over the field $a = (a_1, \ldots, a_n)$, the Hamming distance *d (a, b)* is defined as:

$$d(a, b) = |\{ a_i : a_i \neq b_i; a_i \in a, b_i \in b \}| \qquad (1)$$

Let us consider two code-words *a* and *b* of length 4 each. Therefore, Hamming Distance denoted by *d (a, b)* is the amount of bits that vary in both the code word. Example: *a* = 1100 and *b* = 0101; here two bits in its location are different, so *d (a, b)* =2. The minimum hamming distance is known as the smallest hamming distance between any two different code-word combinations.

Hamming Code

Hamming codes are *(n, k)* codes having the following properties:

- $n = 2^q - 1$, q = number of parity bits *(n - k).*
- $k = 2^q - q - 1$, k = number of information bits.
- $q \geq 3$, i.e minimum number of parity bit is 3.

Hamming Weight

The number of elements in code word which are non-zero is called Hamming weight. Consider two vectors $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in *n* dimensional vector space over the field $a = (a_1, \ldots, a_n)$, the Hamming distance *d (a, b)* is defined as:

$$w(a) = |\{ a_i : a_i \neq 0; a_i \in a,\}| \quad (2)$$

Generator Matrix

A generator matrix in coding theory is a matrix whose rows forms the basis for a linear code. The code-words are all arranged linearly in the rows of this matrix.

The general form of the generator matrix is defined as

$G = [I_k \mid P]$;

where, I_k denotes the $k \times k$ identity matrix and P denotes the $k \times (n - k)$ matrix.

The code word is given by matrix multiplication modulo 2 of row matrix corresponding to message M and G i.e. code word = M.G.

Cyclic Codes

An *(n, k)* block code is defined as cyclic code is it obeys the cyclic shift properties. For a code word $c = (c_1, \ldots, c_n)$ from C, the word $(c_m, c_1, \ldots, c_{n-1})$ is obtained by a cyclic right shift of components is again a code word.

III. Literature Review

There are many works pertaining to the secure information and that have been carried out. Some of the important works have been surveyed and cited here. Our study is based on the codes used in McEliece cryptosystem and a brief review of the related work is being presented.

The classical McEliece Encryption scheme was proposed by R. J. McEliece [40] in 1978, using Binary Goppa code which seems quite secure while at the same time permitting extremely rapid information rates. This type of cryptosystem is perfect for the use in a multi-user communication network, such as those predicted by Nasa for the distribution of space acquired data. After that in 1986, Niederreter [45] presented a cryptosystem which involves public key with fewer bits and yields a higher information rate than Chor-Rivest cryptosystem. The design of this cryptosystem was based on Algebraic coding theory. An algorithm for computing the minimum weight of large error-correcting codes was given by Leon in 1988. Then in the next year stern proposed a method for finding code-words of small weight and an observation was focused on the security of McEliece public key cryptosystem by Lee. In 1992, Sidelnilkov et al. [54] presented an attack against [40], [45] and suggested a method of finding the unknown matrices H and A which determines the matrix B in O(s4 + sN) arithmetical operations in F_q. By this method, the insecurity of such public-key cryptosystems is demonstrated. Again in 1994, Sidelnikov et al. [55] proposed an improvement of [40] and [45] cryptosystem and provided some evidence that this improvement enhanced the cryptosystem security. Also they studied the complexity of cracking the original as well as the improved encryption scheme and conclude that considering code-based cryptosystem, especially the improved one, possesses for N greater equal to 1024 a high security. After two years in 1996, Janwa et al. [31] looked at significant variants of McEliece encryption scheme with use of new and larger class of q-ary Algebraic Geometric i.e. A-G goppa codes. In 1998, Sendrier [53] focused on the problem of finding

a concatenated structure in linear code C given by its generating matrix and also they had shown that it is possible to recover codes. In 2000, Loidreau et al. [39] presented a modification of the McEliece cryptographic scheme which strengthens the security of cryptosystem without increasing the public key size by using some properties of the automorphism groups of the codes to build decodable patterns of large weight errors. Again in 2000, Canteaut et al. [3] presented an attack against [40] which actually consists of a new probabilistic algorithm for finding minimum-weight words in any large linear code. In 2005 Berger et al. [8] showed how to strengthen public key cryptography against known attacks, together with reduction of the public key with using some properties of sub codes to mask the structure of codes and proposed some new parameters with public key size of less than 4000 bits. Moreover in 2007, Minder et al. [43] presented a structural attack against the Sidelnikov cryptosystem. The attack creates private key from public key. Its running time is sub-exponential and is effective if the parameters of the Reed Muller code allow for efficient sampling of minimum weight code word. Its main application is an attack of the McEliece cryptographic scheme based on A-G codes defined on curves of small genus.

In the year 2008, Baldi et al. [5] adopted a class of quasi-cyclic low-density parity check codes that allow to overcome the main limitations of the original McEliece cryptosystem based on Goppa codes, that have large key size and low transmission rate. The codes are designed by using a new algorithm based on Random Difference Families that permits to construct very large sets of equivalent codes. An extensive cryptanalysis was developed to verify the security level achievable through a selected choice of the system parameters. They extended an implementation of the McEliece cryptographic scheme based on QC-LDPC codes to deal with the main drawbacks of its original version that had been discovered to be dangerous attacks. Few modifications was done by Baldi et al. in the next year. In 2009, a method was discussed to reduce the size of public key by constructing Quasi-cyclic codes over F_2^8. Cryptanalysis of variants of McEliece cryptosystem based on Quasi Cyclic codes was given in 2010. In the same year, Wieschebrink et al. [64] presented a new structural attack on the McEliece / Niederreiter public key cryptosystem based on sub codes of generalized Reed Solomon codes proposed by Berger and Loidreau. It allows the reconstruction of the private key for almost all practical parameter choices in polynomial time with high probability. Then in 2012, Sendrier et al. [43] proposed two McEliece cryptosystem variants: one from Moderate Density Parity-Check (MDPC) codes and another from quasi-cyclic MDPC codes. These variant reduces all processes (key-generation, encryption and decryption) to very low-complexity operations. That same year a new version of McElece public key encryption scheme based on convolutional codes are introduced. This construction uses a large part of randomly generated parity checks which makes structural attack more complex. After two year Coureur et al. [19] presented a polynomial time attack on the McEliece public key encryption scheme based on A-G codes. As compared to previous attacks, they allow to recover a decoding algorithm for the public key even for codes from high genus curves. After that in 2014, Illantheral et al. [29] introduced a new class of hexi codes namely "hexi polynomial codes", "hexi Rank Distance codes", "hexi Maximum Rank Distance codes", "hexi Goppa codes" and "hexi wild Goppa codes". With the help of these codes, a variant of McEliece cryptosystem known as hexi McEliece public key cryptosystem was created. This newly created cryptosystem has lesser time complexity and better error correcting capacity which make it more feasible to use. In the same year, Ilantheral et al. [37] also proposed the chained hexi codes (CHC) signature scheme. The major advantage of the proposed scheme is the decrease in the size of public key and also a good decrease in the signature size. Due to the small size of the public key, the decoding, signing and verification can be done faster.

In the year 2014, Shrestha et al. [20] studied a candidate of post-quantum cryptography, a new version of McEliece cryptosystem based on polar codes. Again in the same year Hooshmand et al. [8] introduced a public key scheme based on polar codes to improve the performance of McEliece cryptosystem. Their proposed scheme had a number of advantages such as a higher transmission rate (R = 0.85) and a smaller private as well as public key size (MPB = 65.19 kbytes, MPR = 2.75 kbytes) compared with the original McEliece cryptosystem.

In 2015, Bardet et al. [15] presented a key-recovery attack given by Shrestha et al. [20] that makes it possible to recover a description of the structure of the polar code which provides all the information/data required for decrypting any message. Again in 2015, Wang et al. [65] presented some techniques for designing general random linear code based public encryption schemes using linear codes. They had shown that their schemes are secure against existing attacks on linear codes based encryption schemes. Recently in 2016, Moufek et al. [15] introduced a new variant of the McEliece cryptographic scheme based on QC-LDPC and QC-MDPC codes. A modified self-shrinking generator was used to obtain random bits to construct the generator matrix. Their system was shown to be secure against known structural and decoding attacks. Dragoi et al. [23] presented an attack on the modified McEliece cryptographic scheme which was recently proposed by Moufek, Guenda and Aaro Gulliver in 2017. The attack is entirely based on finding the structure of the LDPC code, regardless of the nature of the second code. As a consequence, their result can be applied even if the MDPC code is replaced by another code.

IV. McEliece Public Key Encryption Algorithm

One of the essential code-based cryptography cryptosystem is McEliece Public Key Cryptosystem [40]. Professor Robert J. McEliece proposed it in 1978 with very dedicated work on Code-based cryptography. It was the first system to use the randomization method in its encryption. The methodology is totally based on the difficulty of a linear code decoding, which implies it is NP-hard (Non-Polynomial Deterministic Time Hard) problem. The McEliece public key cryptosystem's private key is a binary Goppa code in the original algorithm, and the private key can also be drawn in any class of alternative code variants. However, such a choice might not search the desired security as Goppa codes.

Key Setup

Generally, McEliece cryptosystem consists of the following algorithms:

1. *A Probabilistic Key Generation Algorithm*

   A Probabilistic Key Generation Algorithm designed to produce a public and private key for further operation. The Public Key is a dynamically chosen Generator matrix. The private key is binary irreducible Goppa code. The code word gained by inserting any error to the initial plain-text message via a noisy channel is called Cipher-text. The only one who has private key's knowledge can eliminate all of the errors from the cipher text and release the original message.

   - *System Parameters:*

     Select a binary *(n, k)* linear code C which is capable of correcting *t* errors, *where* $t \leq n$.

   - *Key Generation*

     The above linear code has an effective decoding method and can produce the following matrices:

     G: $k \times n$ generator matrix of code C having minimum distance $d \geq 2t + 1$.
     S: $k \times k$ randomly chosen binary non-singular matrix.
     P: $n \times n$ randomly chosen permutation matrix.

After generating all the matrices compute $k \times n$ matrix denoted by G_{pub} by algebraic multiplication of generator matrix G, non-singular matrix S and permutation matrix P as

$$G_{pub} = S\ G\ P$$

- Public Key: (G_{pub}, t)
- Private Key: (S, G, P).

2. *A Probabilistic Encryption Algorithm*

If the sender wants to transmit a message $M \in k$ to any user with a public key (G_{pub}, t). Then, in the initial step, the sender must encode the message M as a binary string of *k* length. The sender must produce $z \in F_n$ vector of length *n* and weight *t* randomly and then compute cipher-text C_t as follows:

$$C_t = M\ G_{pub} + z$$

3. *A Probabilistic Encryption Algorithm*

After receiving cipher-text C_t, the receiver will perform the following steps to decode the message.

- First compute the inverse of *P* i.e. P^{-1}.

Then compute

$$Code_t = C_t$$
$$= (M\ G_{pub} + z)\ P^{-1}$$
$$= M\ G_{pub} P^{-1} + z P^{-1}$$
$$= MSGP P^{-1} + z P^{-1}$$
$$= MSG + z P^{-1}$$

Then applying the decoding algorithm for G which can correct upto *t* errors. Also the word MSG is at a hamming distance of *t* from GP^{-1}.

Thus the correct code word is obtained as Message = MS

Now on multiplying the inverse of S i.e. S^{-1}, we get

Message S^{-1} = MSS^{-1}

Message S^{-1} = M

which is the plain-text (original message).

Security Parameter

The parameter for McEliece cryptosystem is *[n; k; d]*, where *n* is code length, *k* is dimension and *d* is the hamming distance of weight *t*.

$$k = n - mt$$

Robert J. McEliece suggested the use of binary (p=2) Goppa codes with $m = 10$, $n = 1024$ and $t = 50$.

After McEliece cryptosystem, Niederreiter cryptosystem [45] based on algebraic coding theory was introduced by Niederreiter in 1986. Many researchers have tried to reduce the size of public key by using other significant codes.

V. Decoding Problem

In this section, we will discuss about the assumptions on which the security of code-based cryptography depends.

Assumption I: Decoding a random linear code is a difficult problem.

Assumption II: The Generator matrix of a Goppa code looks random**.**

1. ***General Decoding Problem***:

Given an *[n; k]* code C over F_q, an integer t_0 and a vector c ∈ F_q^n, find a code word $x \in$ C with $d(x ; c) \leq t_0$.

2. The Syndrome Decoding (SD) Problem

Given a $(n - k) \times n$ binary matrix *H*, a *(n-k)* syndrome S over the field F_2 and a non-negative integer $w \in Z$ as the weight. The issue with the decision, faces the following question; Does there exists an error pattern e ∈ F_2 of weight w_H(e) at most *w* such that eH^T = S ? and is considered to be NP-complete. While the computational problem is to find vector F_2which is considered to be NP-Hard.
The syndrome decoding problem was proven to be NP-Complete by Berlekamp, McEliece and Tilbarg [9] in the year 1978 and in 1997 by Barg [6] for codes over all finite fields.

3. The Bounded-Distance decoding (BDD) problem

Given a $(n - k) \times n$ binary matrix *H*, a *(n-k)* syndrome S over the field F_2 and a non-negative integer $w \in Z$ as the weight. Here the computational problem is to find vector e ∈ $F_2$of weight w_H(e) at most $\frac{d-1}{2}$ such that eH^T = S. This problem is not NP- Complete problem, however it is conjectured to be NP- Hard by Barg [6].

4. The Goppa Parameterized Syndrome Decoding

Given a binary matrix H of size $(n - k) \times n$ with $k = n - mt$ and $n = 2m$ where *t* is the correction capability, a syndrome S over the field F_2. In this case the computational problem is to find vector e of n-dimension over F_2 having weight $w_H(e) \leq \frac{n-k}{2}$ such that eH^T = S.

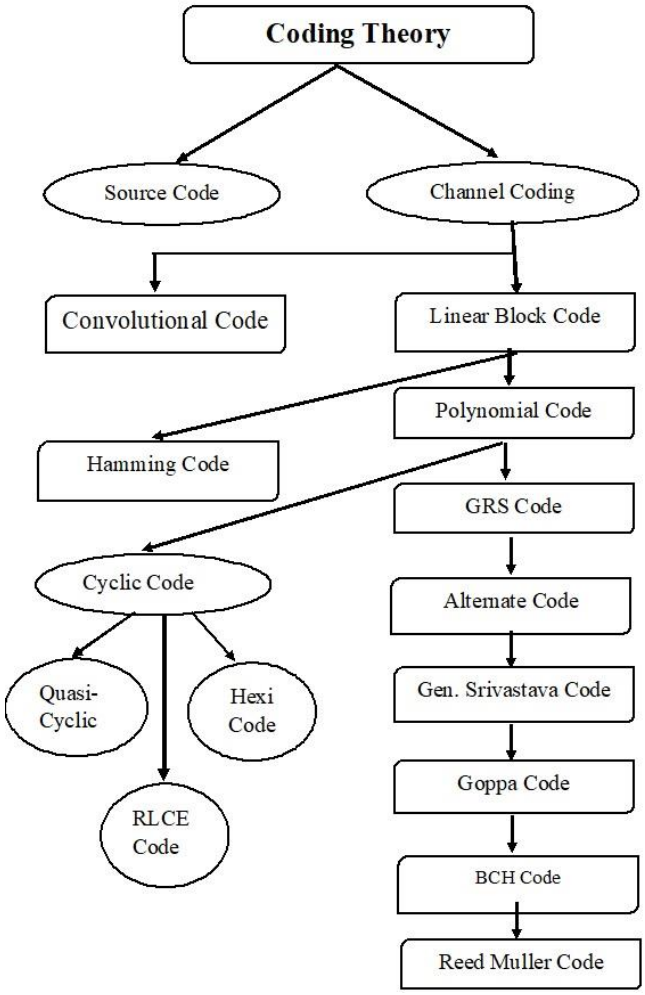
5. Goppa Code Distinguishing (GCD) problem

The GCD problem depends on our second assumption that there exist no efficient distinguisher for Goppa code that it is Pseudo-random. Given an $r \times n$ matrix G, decide whether G $\in K_{Goppa}$, where K_{Goppa}= all generator matrices of a $[n; k]$-binary Goppa code. In 2013, Faugre - Gauthier - Umaa - Otmani - Perret - Tillich [22] showed that high rate binary Goppa codes can be distinguished from random linear codes. However it does not work at

- 8 errors for n = 1024 (where McEliece used 50 errors)
- 20 errors for n = 8192 (a variant of classic McEliece)

shown by Loidreau and Sendrier in [36] known to be best attack depends on support splitting algorithm which have exponential times. Therefore, one should be careful while choosing the parameters in code-based cryptography; it is possible to use codes that do not have high code.

VI. Various Family of Codes



1. Goppa Code

The Binary Goppa Code is the best known code in the field of mathematics and computer science. It is a code which corrects errors which belongs to the general Goppa code class. Valerii Denisovich Goppa initially introduced the concept of Goppa code. Its binary form was ideal for using the benefit of Goppa code in computers and telecommunications. In McEliece's public key cryptography and related cryptosystems, Binary Goppa codes play an important part. Goppa is also known as Algebraic Geometric Code AG codes.

A Binary Goppa code is defined by a polynomial *g(x)* of degree *t* over a finite field GF(2^m) and a sequence *L* of *n* distinct elements from GF(2^m).

$$\Gamma(g,L)=\left\{c\ \epsilon\ \{0,1\}^n|\sum_{i=0}^{n-1}\equiv 0\ mod\ g(x)\right\}$$

code defined by tuple (g, L) has minimum distance *2t + 1* errors, thus it can correct t = $\frac{(2t+1)}{2}$ errors in a word of size *n - mt* using code words of size *n*.

The parity check matrix H can be of the form

H = V D

$$=\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ L_0^1 & L_1^1 & L_2^1 & \dots & L_{n-1}^1 \\ L_0^2 & L_0^2 & L_0^2 & \dots & L_{n-1}^2 \\ \vdots & \vdots & \vdots & \ddots & L_{n-1}^{t-1} \\ L_{n-1}^{t-1} & L_{n-1}^{t-1} & L_{n-1}^{t-1} & \dots & L_{n-1}^{t-1} \end{pmatrix}\begin{pmatrix} \frac{1}{g(L_0)} & & & & \\ & \frac{1}{g(L_1)} & & & \\ & & \frac{1}{g(L_2)} & & \\ & & & \ddots & \\ & & & & \frac{1}{g(L_{n-1})} \end{pmatrix}$$

where, V is the Vandremonde matrix and D is the diagonal matrix. Decoding of binary Goppa code is generally done by Patterson decoding algorithm.

2. *GRS Code*

GRS code is an important class of code which are strongly related to the class of Goppa codes used by McEliece to define his cryptosystem. In the year 1992, Sidelnikov and Shestakov [54] and Niederretier cryptosystem [45]. The author suggested a method of finding the unknown matrices which reveals the private key in polynomial run time. Even though, the result doesn't affect the security of the original McEliece cryptosystem.

A GRS code of length *n* is defined by two vectors a, z ∈ F_q^n, where $a_i \neq a_j$ for i ≠ j and all z_i = 0. The canonical check matrix of the GRS code is of the form

$$H^T=\begin{pmatrix} z_1a_1^0 & z_1a_1^1 & \dots & z_1a_1^{t-1} \\ z_2a_2^0 & z_2a_2^1 & \dots & z_2a_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ z_na_n^0 & z_na_n^1 & \dots & z_na_n^{t-1} \end{pmatrix}$$

This subfield F subcode of a generalized reed-solomon codes is called an Alternate Code, having dimension $k \geq n - mt$. In [8] Berger and Loidreau presented an article to mask the structure of codes for a cryptographic use. This was attacked by Weischebrink [64].

3. *Reed-Muller codes*

In 1954, Reed-Muller codes are found by Muller and provided by Reed with a decoding algorithm. In the area of cryptography Sidelnikov [55] introduced the Reed-Muller code. His key idea is to use a Reed-Muller method to reduce the Goppa code from the McEliece Cryptographic Algorithm. The modifications of [40] and [45] were made in [5].In 2007, Minder [43] presented a structural attack against the Sidelnikov. Then in 2013, Chizlove et al. presents the failure of McEliece public key scheme based on Reed-Muller codes.

4. Quasi Cyclic- Low Density Parity Check Codes (QC-LDPC)

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 $k = pl_0$ having the following properties:

i. A series of *p* blocks of l_0 symbols will formed by k_0 information symbols defined by $r_0 = l_0 - k_0$ rebundancy symbols and

ii. Another valid code word is formed by cyclic shift of each code word by l_0 symbols.

VII. Security of the McEliece Cryptosystem

The security of the McEliece cryptosystem generally based on the two types of attack; one is Structural Attack and another one is Decoding Attack. Let us discuss about them in short.

1. Structural Attack

The attack where Oscar aims to have the secret key G from the public key Gpub and then decipher the message is called Structural Attack. In other words, the structural attack exploits the structure of the underlying code. If such an attempt by an Oscar is successful, then the private key, the generator matrix is revealed in polynomial time and the cryptosystem would be broken. In the past, most of the structural attacks against code-based cryptosystem have targeted specific classes of codes. Shestakov and Sidelnikov [54] presented a successful attack using generalized Reed-solomon codes. Overbeck presented an attack against rank-metric code [49].

2. Decoding Attack

Decoding attack involves an attempt to decipher the message that is encrypted. In other terms the Oscar may try to decipher the encrypted message in the form of cipher-text, without understanding the meaning of the Goppa code. This form of attack is often referred to as Direct attack.

Information Set Decoding

Lee and Brickel [33] were the first to use it for analyzing McEliece Public key cryptography protection. After that Leon and Stern [35] proposed some further changes. The fig.3 represents the appropriate weight profile for progress.

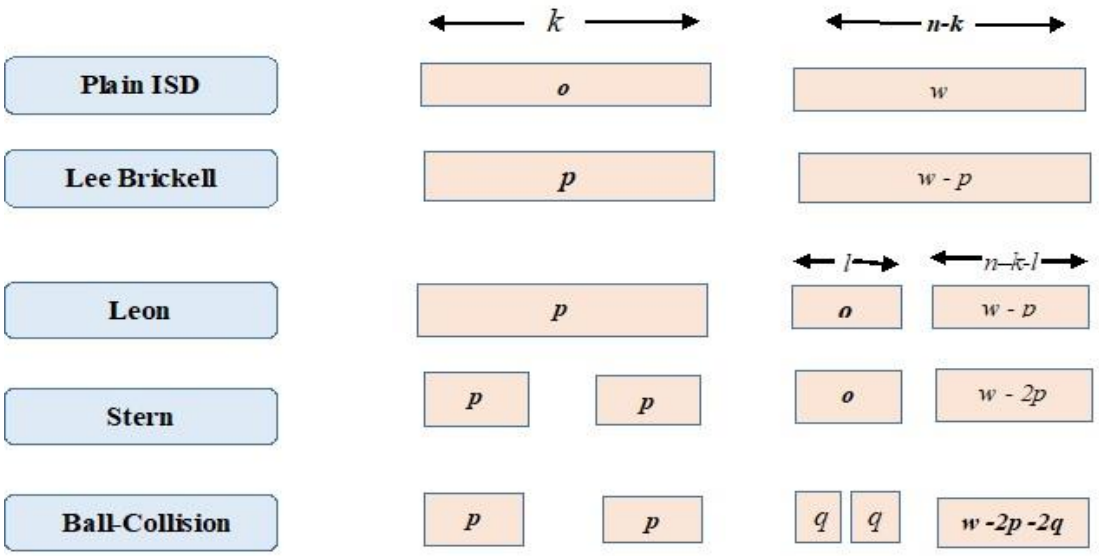


Figure. 3 Decoding

The latest evolution of Information set decoding was presented in 2011 by Berstein, Lange and peters with the name Ball Collision Decoding [11].

The Canteaut-Chabaud Decoding Algorithm

Another well-known decoding algorithm was developed by Canteaut and Chabaud [13] and is a Stern algorithm with a further enhancement as Van Tiburg [61] consists of changing only one aspect of the information set at each iteration.

Generalized Birthday Problem

One of the fastest attack on the FSB hash function and the [17] CFS scheme relies on the [62] approach from Wagner. The approach requires very wide collections. The original McEliece cryptosystem based on Goppa codes of length 1024 are resistant against several decoding attacks [33], [61], [15], etc.

VIII. Code-Based Digital Signature Scheme

Within this section the digital signature systems are explored with brief explanation on code-based cryptography. from [1] it is obvious that it is not possible to hash a text through decodable syndrome. However, it is possible to hash onto the space of all syndromes: the document hash is not always decodable. In the last twenty years several code-based signature systems have been suggested. The first approach was attributed to the Wang [65] in 1990 that relies on the complexity of factoring broad matrices and the properties of error-correction codes. This approach was cryptanalysed in 1992 by Harn and Wang [26] and a version of Wang [65] was also introduced. In 1993 a signature scheme was implemented by Alabbadi and Wicker [1] focused on linear error correction of block codes. Yet unfortunately that was cryptanalyzed in the same year by Stern [58]. Subsequently, many signature systems were planned to solve these issue

1. *Kabatianskii et al. Scheme*

The KKS Signature scheme named after Kabatianskii, Krouk and Smeets [30] proposed a digital signature scheme based on arbitrary linear error-correcting codes. They introduce four KKS-Signature Scheme variants: KKS-1, KKS- 2, KKS-3, KKS-4. In 2007, however, Cayrel et al. [14] proposed that, by utilizing few signatures, an intruder would easily identify the private key. Otmani and Tillich [47] now carried out a successful attack on all practical KKS ideas in 2011 and destroyed the scheme.

2. *Stern's Identification Scheme*

In 1993, the identification scheme [57] of Stern was introduced which was related to the cryptosystem of the Niederreiter. In this scheme, Hpub will be a publicly known matrix of $(n\text{-}k) \times n$ for all users. Therefore, a user's private key would be word e of low-weight term w, which sums up the public key to $eH = S$ syndrome.

3. *CFS Signature Scheme*

One of the most famous signature scheme which was still considered to be secure is CFS Signature scheme. The scheme was introduced by Courtois, Finiaz and Sendrier [17]. The CFS signature scheme uses the concept of Goppa code. For a given integer n and t, binary Goppa code with length $n = 2m$, dimension $k = n\text{-}mt$, and capacity for error correction t. The basic principle of using the signature scheme for CFS is to hash the message, randomize it to bit length r, until the result is decryptable cipher-text. The signer then uses his private key to compute the associated error-vector along with the current value, this error vector will act as a signature.

Such other signature scheme with additional properties on code-based cryptography are Ring Signature Scheme [66], Threshold Ring Signature Scheme [41], Blind Signature scheme [16] and Identity-based Signature scheme [27].

IX. CONFERENCE

The main contribution of this review paper is find the merit and demerits of McEliece cryptosystem. The paper also concludes the relative comparison of several modification or improvements and developments of algorithms for reducing the size of public key. Encryption algorithm for McEliece Encryption scheme are reviewed. Study of various significant codes for McEliece cryptosystem are done. The security and attacks are also discussed regarding different codes. Small devices like USB tokens, PDAs and mobile phones are nowadays able to even use McEliece PKC for an increased storage space. We hope McEliece PKC might be used over the next few decades, even though there is no quantum machine. Code-based encryption provides a better encryption and decryption, which helps raising the loss of batteries on mobile systems from cryptographic applications. The fact that a full network can be constructed from it is another fascinating property of code-based encryption.

Reference

1. Mohssen Alabbadi and Stephen B Wicker, Digital signature schemes based on error-correcting codes, Proceedings. IEEE International Symposium on Information Theory, IEEE, 1993, pp. 199.
2. Anne Canteaut and Nicolas Sendrier. Cryptanalysis of the original mceliece cryptosystem. In International Conference on the Theory and Application of Cryptology and Information Security, pages 187-199. Springer, 1998.
3. Marco Baldi, Qc-ldpc code-based cryptography, Springer Science & Business, 2014.
4. Marco Baldi, Marco Bodrato, and Franco Chiaraluce, A new analysis of the mceliece cryptosystem based on qc-ldpc codes, International Conference on Security and Cryptography for Networks, Springer, 2008, pp. 246.
5. Marco Baldi and Franco Chiaraluce, Cryptanalysis of a new instance of mceliece cryptosystem based on qc-ldpc codes, 2007 IEEE International Symposium on Information Theory, IEEE, 2007, pp. 2591.
6. Alexander Barg, Complexity issues in coding theory, Algebraic Coding (1998).
7. R Hooshmand, M Koochak Shooshtari, T Eghlidos, and MR Aref. Reducing the key length of mceliece cryptosystem using polar codes. In 2014 11th International ISC Conference on Information Security and Cryptology, pages 104{108. IEEE, 2014.
8. Thierry P Berger and Pierre Loidreau, How to mask the structure of codes for a cryptographic use, Designs, Codes and Cryptography 35 (2005), no. 1, 63-79.
9. Elwyn Berlekamp, Robert McEliece, and Henk Van Tilborg, On the inherent intractability of certain coding problems (corresp.), IEEE Transactions on Information Theory 24 (1978), no. 3, 384-386.
10. Daniel J Bernstein, Daira Hopwood, Andreas Hulsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O Hearn, Sphincs: practical stateless hash- based signatures, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2015, pp. 368-397.
11. Daniel J Bernstein, Tanja Lange, and Christiane Peters, Smaller decoding exponents: ball-collision decoding, Annual Cryptology Conference, Springer, 2011, pp. 743-760.
12. Johannes Buchmann, Erik Dahmen, and Andreas Hulsing, Xmss-a practical forward secure signature scheme based on minimal security assumptions, InternationalWorkshop on Post-Quantum Cryptography, Springer, 2011, pp. 117-129.
13. Anne Canteaut and Florent Chabaud, A new algorithm for finding minimum-weight words in a linear code: application to mceliece's cryptosystem and to narrow-sense bch codes of length 511, IEEE Transactions on Information Theory 44 (1998), no. 1, 367-378.
14. Pierre-Louis Cayrel, Ayoub Otmani, and Damien Vergnaud, On Kabatianskii-Krouk-Smeets signatures, International Workshop on the Arithmetic of Finite Fields, Springer, 2007, pp. 237-251.
15. Florent Chabaud, On the security of some cryptosystems based on error-correcting codes, Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1994, pp. 131-139.
16. Hamza Moufek, Kenza Guenda, and T Aaron Gulliver. A new variant of the mceliece cryptosystem based on qc-ldpc and qc-mdpc codes. IEEE Communications Letters, 21(4):714{717, 2017
17. Nicolas T Courtois, Matthieu Finiasz, and Nicolas Sendrier, How to achieve a Mceliece-based digital signature scheme, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2001, pp. 157-174.
18. Nicolas Sendrier. On the concatenated structure of a linear code. Applicable Algebra in Engineering, Communication and Computing, 9(3):221-242, 1998.
19. W Diffiee and ME Hellman, \new directions in cryptography" IEEE transactions on information theory, v. it-22, n. 6, (1976).
20. Sujan Raj Shrestha and Young-Sik Kim. New mceliece cryptosystem based on polar codes as a candidate for post-quantum cryptography. In 2014 14th International Symposium on Communications and Information Technologies (ISCIT), pages 368{ 372. IEEE, 2014.
21. Tomas Fabsic, Ondrej Gallo, and Viliam Hromada, Simple power analysis attack on the qc-ldpc mceliece cryptosystem, Tatra Mountains Mathematical Publications 67 (2016), no. 1, 85-92.
22. Jean-Charles Faugere, Valerie Gauthier-Umana, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich, A distinguisher for high-rate mceliece cryptosystems, IEEE Transactions on Information Theory 59 (2013), no. 10, 6830-6844.
23. Richard P Feynman, Simulating physics with computers, International journal of theoretical physics 21 (1982), no. 6, 467-488.
24. Matthieu Finiasz and Nicolas Sendrier, Security bounds for the design of code-based cryptosystems, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2009, pp. 88-105.
25. Lov K Grover, A fast quantum mechanical algorithm for database search, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212-219.
26. L Harn and DC Wang, Cryptanalysis and modification of digital signature scheme based on error-correcting code, Electronics Letters 28 (1992), no. 2, 157-159.
27. Florian Hess, Efficient identity based signature schemes based on pairings, International Workshop on Selected Areas in Cryptography, Springer, 2002, pp. 310-324.
28. K Ilanthenral and KS Easwarakumar, Hexi Mceliece public key cryptosystem, Applied Mathematics & Information Sciences 8 (2014), no. 5, 2595.
29. Heeralal Janwa and Oscar Moreno, Mceliece public key cryptosystems using algebraic-geometric codes, Designs, Codes and Cryptography 8(1996), no. 3, 293-307.

30. Gregory Kabatianskii, Evgenii Krouk, and Ben Smeets, A digital signature scheme based on random error-correcting codes, IMA International Conference on Cryptography and Coding, Springer, 1997, pp. 161-167.
31. Ilanthenral Kandasamy and KS Easwarakumar, Chained hexi codes signature scheme, International Journal of Computer Science and Network Security (IJCSNS) 14 (2014), no. 12, 20.
32. Kazukuni Kobara and Hideki Imai, New chosen-plaintext attacks on the one-wayness of the modified Mceliece pkc proposed at asiacrypt 2000, International Workshop on Public Key Cryptography, Springer, 2002, pp. 237-251.
33. Pil Joong Lee and Ernest F Brickell, An observation on the security of McElieces public-key cryptosystem, Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1988, pp. 275-280.
34. Hendrik Willem Lenstra, Arjen K Lenstra, L Lovasz, et al., Factoring polynomials with rational coefficients, (1982).
35. Jeffrey S Leon, A probabilistic algorithm for computing minimum weights of large error-correcting codes, IEEE Transactions on Information Theory 34 (1988), no. 5, 1354-1359.
36. P Loidrean and Nicolas Sendrier, Some weak keys in mceliece public key cryptosystem, Proceedings. 1998 IEEE International Symposium on Information Theory (Cat. No. 98CH36252), IEEE, 1998, p. 382.
37. Pierre Loidreau, Strengthening mceliece cryptosystem, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2000, pp. 585-598.
38. Carl Londahl, Thomas Johansson, Masoumeh Koochak Shooshtari, Mahmoud Ahmadian-Attari, and Mohammad Reza Aref, Squaring attacks on Mceliece public-key cryptosystems using quasi-cyclic codes of even dimension, Designs, Codes and Cryptography 80 (2016), no. 2, 359-377.
39. Yuri Manin, Computable and uncomputable, Sovetskoye Radio, Moscow 128 (1980).
40. Robert J McEliece, A public-key cryptosystem based on algebraic, Coding Thv 4244 (1978), 114-116.
41. Carlos Aguilar Melchor, Pierre-Louis Cayrel, Philippe Gaborit, and Fabien Laguillaumie, A new efficient threshold ring signature scheme based on coding theory, IEEE Transactions on Information Theory 57 (2011), no. 7, 4833-4842.
42. Ralph Merkle and Martin Hellman, Hiding information and signatures in trapdoor knapsacks, IEEE transactions on Information Theory 24 (1978), no. 5, 525-530.
43. Lorenz Minder and Amin Shokrollahi, Cryptanalysis of the sidelnikov cryptosystem, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2007, pp. 347-360.
44. Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo SLM Barreto, Mdpc-mceliece: New mceliece variants from moderate density parity-check codes, 2013 IEEE international symposium on information theory, IEEE, 2013, pp. 2069-2073.
45. Harald Niederreiter, Knapsack-type cryptosystems and algebraic coding theory, Prob. Control and Inf. Theory 15 (1986), no. 2, 159-166.
46. Michael A Nielsen and Isaac Chuang, Quantum computation and quantum information, 2002.
47. Ayoub Otmani and Jean-Pierre Tillich, An efficient attack on all concrete kks proposals, International Workshop on Post-Quantum Cryptography, Springer, 2011, pp. 98-116.
48. Ayoub Otmani, Jean-Pierre Tillich, and Leonard Dallot, Cryptanalysis of two mceliece cryptosystems based on quasi cyclic codes, Mathematicsin Computer Science 3 (2010), no. 2, 129-140.
49. R Overbeck, A new brute-force attack for gpt and variants, Proc. of Mycrypt, vol. 3517, 2005, pp. 5-63.
50. Fang Ren, Xuefei Yang, and Dong Zheng, A qc-ldpc code based digital signature algorithm, 2018 International Conference on Networking and Network Applications (NaNA), IEEE, 2018, pp. 257-262.
51. Ronald L Rivest, Adi Shamir, and Leonard Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (1978), no. 2, 120-126.
52. Renuka Sahu and BP Tripathi, Random chained hexi code (RCHC) signature scheme, Journal of Computer and Mathematical Sciences 9 (2018), no. 12, 2096-2106.
53. Peter W Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM review 41 (1999), no. 2, 303-332.
54. Vladimir M Sidelnikov and Sergey O Shestakov, On insecurity of cryptosystems based on generalized reed-solomon codes, Discrete Mathematics and Applications 2 (1992), no. 4, 439-444.
55. Vladimir Michilovich Sidelnikov, A public-key cryptosystem based on binary reed-muller codes, Discrete Mathematics and Applications 4 (1994), no. 3, 191-208.
56. Jacques Stern, A method for finding codewords of small weight, International Colloquium on Coding Theory and Applications, Springer, 1988, pp. 106-113.
57. A new identification scheme based on syndrome decoding, Annual International Cryptology Conference, Springer, 1993, pp. 13-21.
58. Can one design a signature scheme based on error-correcting codes?, International Conference on the Theory and Application of Cryptology, Springer, 1994, pp. 424-426.
59. Richard Townsend and E Weldon, Self-orthogonal quasi-cyclic codes, IEEE Transactions on Information Theory 13 (1967), no. 2, 183-195.
60. BP Tripathi and Renuka Sahu, Modified random linear code scheme (rlce) with using properties of automorphism group of goppa code, Journal of Theoritical Physics and Cryptography (2016), 5-12.
61. Johan van Tilburg, On the mceliece public-key cryptosystem, Proceedings on Advances in cryptology, Springer-Verlag, 1990, pp. 119-131.

62. David Wagner, A generalized birthday problem, Annual International Cryptology Conference, Springer, 2002, pp. 288-304.
63. Yongge Wang, Quantum resistant random linear code based public key encryption scheme rlce, 2016 IEEE International Symposium on Information Theory (ISIT), IEEE, 2016, pp. 2519-2523.
64. Christian Wieschebrink, Cryptanalysis of the niederreiter public key scheme based on grs subcodes, International Workshop on Post-Quantum Cryptography, Springer, 2010, pp. 61-72.
65. Wang Xinmei, Digital signature scheme based on error-correcting codes, Electronics Letters 26 (1990), no. 13, 898-899.
66. Dong Zheng, Xiangxue Li, and Kefei Chen, Code-based ring signature scheme., IJ Network Security 5 (2007), no. 2, 154-157.