Chapter

The Security of Cryptosystems Based on Error-Correcting Codes

Ahmed Drissi

Abstract

Quantum computers are distinguished by their enormous storage capacity and relatively high computing speed. Among the cryptosystems of the future, the best known and most studied which will resist when using this kind of computer are cryptosystems based on error-correcting codes. The use of problems inspired by the theory of error-correcting codes in the design of cryptographic systems adds an alternative to cryptosystems based on number theory, as well as solutions to their vulnerabilities. Their security is based on the problem of decoding a random code that is NP-complete. In this chapter, we will discuss the cryptographic properties of error-correcting codes, as well as the security of cryptosystems based on code theory.

Keywords: McEliece cipher, hash function, syndrome decoding, correcting codes, random code

1. Introduction

Like all asymmetric cryptographic systems, the idea is to base security on the difficulty of reversing a one-way function with a trap door. The theory of error-correcting codes contains well-structured and difficult problems to solve, more or less suitable for use in cryptography. The first who had the idea of using error-correcting codes for cryptographic purposes was McEliece in 1978 and he proposed an asymmetric encryption algorithm. In 1986, Niederreiter proposed another cryptographic system equivalent to that of McEliece [1]. The two systems of McEliece and Niederreiter are of equivalent security against a passive attack; however, they are not against an active attack [2]. In the following paragraph, we give an overview of the theory of error-correcting codes. In the third paragraph, we will only deal with the basic systems based on this theory. The last paragraph is devoted to the discussion of security settings and the most well-known attacks. In what follows we note.

F_{2^m}: a finite field of 2^m elements.
$K[x]$: the ring of polynomials with an indeterminate.
$K[x]/(P)$: the quotient ring $K[x]$ de modulo P.
K^*: a private set of the element 0.
$dQ(x)$: the degree of the polynomial $Q(x)$.
F_2^m: the set of length vectors m and components 0 and 1.
F^n: the scalar product n times of the set F.
$[x]$: the integer part of x.

A^t: the transpose of the matrix A.
I_k: the identity matrix of order k.
gcd: greatest common divisor.
C_n^t: the combination of t elements among n elements.

2. Error-correcting codes

2.1 Finite fields

Finite fields are the basis of many error-correcting codes and cryptographic systems, it is therefore essential to recall the theory of finite fields in order to understand the functioning of linear codes. In this paragraph we present some properties of finite fields and a method of representing them for later use. We are interested in constructing finite fields F_{2^m} and the calculations on these fields. Finite fields are generally constructed from primitive polynomials [3].

Definitions

The minimal polynomial of an element β on a finite field F is the unit polynomial with coefficients in F smaller degree and its value in β is zero.

Proposition

1. The ring $K[x]/(P)$ is a field if and only if the polynomial $P(x)$ is irreducible on the field K.

2. If $P(x)$ is irreducible of degree m and K a finite field of q elements then $K[x]/(P)$ is field of q^m elements.

This proposition gives us a way to build a finite field: Take a polynomial P irreducible over a field K et former le quotient $K[x]/(P)$.

Theorem (the primitive element)

If K is a finite field of order q, then the multiplicative group K^* is cyclic generated by an element α called primitive element of K and we write $K^* = \{\alpha^i, i = 1...q-\}$. Any generator of this group is called a primitive element of K.

Definition (primitive polynomial)

We say that a polynomial $P \in F_2[x]$ of degree m is primitive if it is the minimal polynomial of a generator of $F_{2^m}^*$.

Lemma

Let $F_2[x]^{(m)} = \{Q(x) \in F_2[x], dQ(x) \leq m-1\}$, $P(x) \in F_2[x]^{(m)}$ primitive and α a root of $P(x)$, so we have: $F_2^m \approx F_2[x]^{(m)} \approx F_2[x]/(P(x)) \approx F_{2^m} \approx \{0\} \cup \{1, \alpha, ...\alpha^{2^m-1}\}$.

It follows from this lemma that we can represent the nonzero elements of a finite field F_{2^m} by nonzero vectors of F_2^m and that the α^i have representatives of $x^i \mathrm{mod} P(x)$ and consequently $\alpha^i = x^i \mathrm{mod} P(x)$. In what follows we denote by α a primitive element of F_{2^m}.

2.2 Principle of error-correcting codes

In order to transmit a message, it must be coded, it consists in temporarily giving it a certain form, the coding mode depends on the means of transmission, it can be disturbed by noise, hence the need for coding which allows the receiver to find the initial message even if it has been altered. Such coding is called channel coding.

The principle of error-correcting codes is to add to a message to be transmitted additional information called redundant or control information, so that transmission errors can be detected and corrected. This operation is called coding and its result is a code word, each message is associated, therefore a code word of length greater than that of the message.

The code is the set of code words thus obtained. We assume that all messages are words of the same length >0, written using an alphabet F of q elements. Each message $(x_0, x_1, ...x_{k-1},)$ is an element of the set of F^k (message space). We then have q^k possible messages. We assume that all the code words are of the same length $n > k$. Encode m messages of length k, $(m \leq q^k)$ consists in choosing an integer $n > k$, and associate with each message from F^k a word from F^n (injectively). The coding introduces a redundancy equal to $n - k$. Decoding consists of receiving a word x of F^n to determine if x is a code word and if not correct it thanks to the redundancy. This is done using the Hamming distance.

Definition (hamming distance)

let $x = (x_0, x_1, ...x_{n-1}) := x_0x_1...x_{n-1}$ and $y = (y_0, y_1, ...y_{n-1}) := y_0y_1...y_{n-1}$ of F^n. We call the Hamming distance between words x and y, and we note $d_H(x, y) = d(x, y)$ the number of index $i \in \{0, 1, 2...n-1\}$ such as $x_i \neq y_i$, we call Hamming's weight of a word x the number of nonzero components of x, we note $w(x) = d(x, 0)$.

Definitions

We call the minimum distance of a code C an integer d such as $d = \min\{d(m, m'), m \in C, m' \in C, m \neq m'\}$. We call the weight of a word x of code C on integer $w(x) = d(x, 0)$.

Proposal (correction capacity)

Let C a minimum distance code d, and $x \in F^n$ a received message assigned to r errors, with $r \geq 1$.

1. If $2r < d$ that is to say that $r \leq \left[\frac{d-1}{2}\right]$, the code C correct r errors.

2. If $\left[\frac{d-1}{2}\right] < r = \left[\frac{d}{2}\right]$, the C code detects the existence of r errors but cannot always correct them.

3. If $\left[\frac{d}{2}\right] < r \leq d - 1$, the C code detects the existence d' errors but risk of making an erroneous correction.

The integer $t = \left[\frac{d-1}{2}\right]$ is called code correction capability, we also say that C is a t-corrector code.

Proof

Let m the code word transmitted and x the message received and assigned from r errors then $d(m, x) = r$.

1. We show that the code word m is the only code word such as $d(m, x) \leq r$.

Otherwise it exists m' of C such as $d(m', x) \leq r$, we are $d(m, m') \leq d(m, x) + d(x, m') \leq 2r < d$, then $m = m'$.

2. There is no code word m' of C such as $d(x, m') < d(m, x) = r$, but the code word m is not necessarily the only one to check $d(m, x) = r$. Indeed be $m = m_1m_2...m_n$ and $m' = m'_1m'_2...m'_n$ two code words and if we receive the message $x = m_1m_2...m_rm'_1...m'_r$, we'll have $d(x, m) = d(x, m') = r$.

3. We know there is an error because $x \notin C$, but there may be a code word $m' \notin C$ such as $d(m', x) < d(m, x) = r$.

The most used codes are the linear codes which we discuss in the next part.

2.3 Linear codes

Definitions

A linear code C of size n and dimension k on the finite field F_q is a vector subspace of F_q^n. We note it $[n, k, d]_q$ with d its minimum distance.

Linear codes are codes in which each code word y is obtained by linear transformation of the components of the initial word (information) x.

A linear code is characterized by its generator matrix G, we have $C = \left\{ y = xG / x \in F_q^k \right\}$.

let H $(n - k) \times n$ matrix with coefficients in F_q. H is called the parity control matrix of C if "$x \in C \Leftrightarrow Hx^t$".

F_q^k: the message space.

The systematic code

The matrix G defines a bijective function $F_q^k \rightarrow C$ by $x \rightarrow xG$ which we represent q^k messages, its length k by code words, of length n.

The generator matrix G of a C code is not unique; G can be transformed into $G' = (I_k|A)$ with I_k the identity matrix with k order and A the matrix of k lines and $n - k$ columns.

G and G′ generate the same C subspace; G′ is called canonical generator matrix and if the generator matrix of a code is of the form $G = (I_k|A)$, this code is said systematic.

Theorem

Let C a $[n, k]_q$ linear code.

1. If G is a generator matrix of C and H a parity control matrix of C then $GH^t = 0$.

2. If G is a $k \times n$ matrix of rank k and H is a $(n - k) \times n$ matrix of rank $n - k$ such as $GH^t = 0$ then we have:

H is a parity control matrix of C if and only if G is a generator matrix of C.

Proof

1. We know that $H^t = 0$, $\forall x \in C$, in particular we have $G_i H^t = 0$ for all $i = 1...k$ with G_i is line of G. It follows that $GH^t = 0$.

2. $\Rightarrow$) Since $GH^t = 0$, then we have $G_i H^t = 0$. For all $i = 1...k$. And since H is a parity control matrix of C, we have the G_i belong to C. $rg(G) = k$, then $\{G_i, i = 1...k\}$ constitute a basis of C. It follows that G is a generator matrix of C.

$\Leftarrow$) we have $y \in C$ if and only if it exists $x \in F_q^k$ such as $y = xG$. Then $y \in C$ if and only if $yH^t = xGH^t = 0$. Then H is a parity control matrix of C.

In the case of systematic code, we have the following corollary.

Corollary

Let C a $[n, k]_q$ linear code

1. If $G = (I_k|A)$ a canonical generator matrix of C then $H = (-A^t|I_{n-k})$ is a parity control matrix ofC.

2. If $H = (B|I_{n-k})$ is a parity control matrix of C then, $G = (I_k|-B^t)$ is a generator matrix of C.

Proof
By applying the preceding theorem

1. we have $GH^t = (I_k|A)(-A^t|I_{n-k})^t = -A + A = 0$, if G is a generator matrix of C then, H is a parity control matrix of C.

2. we have $GH^t = (I_k|-B^t)(B|I_{n-k})^t = B^t - B^t = 0$ then if H is a parity control matrix of C we will have G is a generator matrix of C.

Encoding and decoding
The coding is obtained by applying the generator matrix. Decoding consists in applying the control matrix to the message; if the result is 0 then the message is valid otherwise look for errors and correct them. Hx^t is called syndrome. Suppose the word x is sent through a noisy channel and the word received is y so the error vector is $e = y - x$.

Given y, the decoder must decide which word of the code x has been transmitted (which error vector?). For a vector u and a code C we call coset class of C, the set $u + C = \{u + c, c \in C\}$. A representative of a class of C of minimum weight is called a leader of this class.

Theorem
Let C a $[n, k, d]_q$ linear code then,

1. u and v are of the same coset class of C if and only if $u - v \in C$.

2. Any vector of F_q^n is in a coset of C.

3. Given two coset classes, they are either disjoint or identical.

Proof

1. If $u, v \in x + C$ then, it exists $y, z \in C$ such as $u = x + y$ and $v = x + z$, then $u - v = y - z \in C$, because C is a vector subspace of F_q^n.

If $u - v \in C$ it exists $x \in C$ such as $u - v = x$ then $u = v + x \in v + C$ and we have $v = v + 0 \in v + C$.

2. Let $a \in F_q^n$, on a $0 \in C$ then$a = a + 0 \in a + C$.

3. Suppose that $(a + C) \cap (b + C) \neq \emptyset$, the nit exists $v \in F_q^n$ such as $(a + C) \cap (b + C)$ contains the element v, the nit exists $x, y \in C$ such as $v = a + x = b + y$ hence $b = a + (x - y)$ and $a = b + (y - x)$. $\forall b + c \in b + C$ we have $b + c = a + (x - y) + c \in a + C$ (then $b + C \subset a + C$). $\forall a + c \in a + C$ We have $a + c = b + (y - x) + c \in b + C$ (then $a + C \subset b + C$), hence $b + C = a + C$.

Principle

We construct the standard array of C which is a matrix of q^{n-k} lines and q^k columns. It contains all the vectors of F_q^n; its first line corresponds to the words of C with vector 0 on the left. The other lines represent the cosets $u_i + C$ with the class leader u_i to the left. The procedure is as follows:

1. We list the words of C starting with 0 on the first line.

2. We choose a vector u_1 of minimum weight that does not belong to the first line and we list in the second line the elements $u_1 + C$, by entering below 0 the class leader u_1 and below each element $x \in C$ the element $u_1 + x$.

3. We choose u_2 in the same way and we repeat the same operation.

4. We iterate this process until all the side classes are listed and all the vectors of F_q^n appear only once.

When the word y is received, we look for its position in the standard table. The decoder then decides that the error vector e corresponds to the class leader who is located in the first column of the same row of y and decode y like $x = y - e$, by choosing the code word of the first line on the same column ofy.

Remark

The standard table provides nearest neighbor decoding. Note that this process is too slow and too expensive in memory for large codes. In practice each code has by its structure a decoding algorithm.

2.4 The hamming code

A Hamming code with $r \leq 2$ redundancy is a linear code $[2^r - 1, 2^r - 1 - r]_2$ its parity control matrix H, with H is a matrix of r lines and $2^r - 1$ columns that correspond to the set of all nonzero vectors of F_2^r.

Theorem

The minimum distance of the Hamming $[2^r - 1, 2^r - 1 - r]_2$ code is $d = 3$ (it therefore corrects a single error).

Proof

This code does not contain any element of weight 1 and 2 otherwise we would have a column of H which would be zero or two columns of H would be identical.

It exists $x \in C$ such as $w(x) = 3$, indeed by definition of the parity control matrix H, the first 3 columns are $\begin{pmatrix} 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & \dots \\ 1 & 0 & 1 & \dots \end{pmatrix}$ then the vector $x = (1\ 1\ 1\ 0 \cdots\ 0)$ its weight $w(x) = 3$ and belongs to C because $Hx^t = 0$.

Decoding

The vector syndrome x of which only the jth component is nonzero is none other than the transpose of the jth column of H. If the columns of H are ordered in increasing order of binary numbers, the jth column corresponds to the binary writing of j, hence the following decoding algorithm:

Let y a message received, we calculate Hy^t. If $Hy^t = 0$ then, y corresponds to the message transmitted. If $Hy^t \neq 0$ and assuming there is only one error, Hy^t directly

gives the position of the error written in binary in the form $\cdots b_3 b_2 b_1 b_0$. We can then correct $y = y_1 \cdots y_n$ like $x + e_j$ for $j = \sum_{i=1}^{n} b_i 2^i$ and e_j the vector of which only the jth coordinate is nonzero.

2.5 The Reed-Solomon codes

Let $n = q - 1$ with $q = 2^m$ et $F_q[x]^{(k)}$ The set of polynomials of degree strictly less than k on F_{2^m}. Let us build a length code n and dimension k. Let $L = (\alpha_1, \alpha_2, \cdots \alpha_n,)$ a vector formed of distinct elements of $F_{2^m}^* = \{\alpha^i, i = 1 \ldots n\}$, with α primitive of F_{2^m}. Each word of the code is the evaluation of a function f of $F_q[x]^{(k)}$ on L then, we have a length code n and dimension k and generator matrix

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ .. & .. & \ldots & .. \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix}.$$

By its structure, this code has a minimum distance of at least $n - k + 1$, because two polynomials of degrees less than k distinct cannot be equal in addition to $k - 1$ positions. This distance is exactly equal to $n - k + 1$, since the evaluation of a polynomial of the form $\prod_{i=1}^{k-1}(x - \alpha_i)$ his weight is $n - k + 1$. So we have a code on F_{2^m} of the form $[n, k, n - k + 1]_q$ which can have both good transmission rate and good correction ability.

Remark

Reed-Solomon codes represent a special case of a slightly more general class called generalized Reed-Solomon codes GRS whose definition is as follows.

Definition

Let $(v_1, v_2, \ldots v_n)$ a vector of length n in $F_{2^m}^*$ et $(\alpha_1, \alpha_2, \cdots \alpha_n,)$ a vector of length n in $F_{2^m}^*$, with the α_i are distinct two by two.

The set of codes with the generator matrix G of the form

$$G = \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \ldots & v_n\alpha_n \\ \ldots & .. & \ldots & \ldots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \ldots & v_n\alpha_n^{k-1} \end{pmatrix}$$ is called the family of generalized Reed-Solomon codes.

2.6 The classical Goppa codes

Definition

Let $L = (\alpha_1, \alpha_2, \ldots \alpha_n)$ a suite of n distinct elements of F_{2^m} and $g(z) \in F_{2^m}[z]$ a unit polynomial of degree r irreducible in $F_{2^m}[z]$. The irreducible binary Goppa code, its support L (generator vector) and its generator polynomial g noted $\Gamma(L, g)$ is the set of words $a = (a_1, \ldots a_n) \in F_2^n$ such that one of the following equivalent characterizations is verified:

1. $R_a(z) = \sum_{i=1}^{n} \frac{a_i}{z - \alpha_i} = 0 \bmod g(z)$.

2. $Ha^t = 0$ with $H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ .. & .... & \ldots & \ldots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \ldots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} g(\alpha_1)^{-1} & & & \\ & .. & & \\ & & .. & \\ & & & g(\alpha_n)^{-1} \end{pmatrix}$

parity check matrix.

3. $g(z)$ divided $\frac{d\sigma_a(z)}{dz}$ with c $\sigma_a(z) = \prod_{i=1}^{n}(z - \alpha_i)^{a_i}$ locator polynomial.

The construction of a code Goppa:

Goppa's code is a linear code on the field F_2, its construction requires the use of an extension F_{2^m}. Each element of the matrix H is then broken down into m elements of F_2 placed in columns, using a projection of F_{2^m} in F_2^m; we go from a size matrix $r \times n$ on F_{2^m} to a matrix of size $rm \times n$ on F_2 so it is a length code $n = |L|$ and dimension $k = n - mr$ and has a minimum distance at least equal to $d = r + 1$. Indeed the parity check matrix H is written as the product of a Vandermonde matrix and an invertible matrix therefore all under a square matrix $r \times r$ of H is invertible, then there are no code words with a weight less than or equal to r.

The decoding of a Goppa code:

Several techniques exist to decode Goppa codes but they work by the same principle. Let $c' = c + e$ and $w(e) < \frac{r}{2}$. We start by calculating the syndrome $R_{c'}(z)$ on F_{2^m}; from this syndrome we will write a key equation, and we will finish the decoding by solving the key equation to finde.

If $R_a(z) = 0$ the word will belong to the code.

The key equation

Let $\sigma_e(z) = \sum_{i=1}^{n}(z - \alpha_i)^{e_i}$ of degree $< \frac{r}{2}$. On introduit le polynôme $w_e(z) = \sigma_e(z)R_e(z) \bmod g(z)$ called evaluator polynomial.

$$\sigma_e(z)R_e(z) = \sum_{i=1}^{n} \frac{e_i}{z - \alpha_i} \prod_{j=1}^{n} (z - \alpha_j)^{e_j} \bmod g(z) = \sum_{i=1}^{n} e_i \prod_{\substack{j=1 \\ j \neq i}}^{n} (z - \alpha_j)^{e_j} \bmod g(z).$$

We can solve the key equation in two different ways: Berlekamp Massey's algorithm and the extended Euclidean algorithm. The latter has the advantage of being easier to present. Indeed we seek to find w_e and σ_e of degree $< \frac{r}{2}$ such as $w_e(z) = \sigma_e(z)R_e(z) \bmod g(z) = \sigma_e(z)R_e(z) + k(z)\, g(z)$. If we try to calculate the gcd of (g, R_e) with the extended Euclidean algorithm, we will calculate at each step the polynomials u_i, v_i, r_i checking $R_e u_i + g v_i = r_i$. At each step the polynomials u_i and v_i will be of degree $< i$ and the degree of r_i is equal to $r - i$. There is therefore a step at which if we stop the algorithm we will find a solution of the equation $\sigma_e = u_{i_0}$ and $w_{i_0} = r_{i_0}$ to a scalar coefficient.

3. Encryption/decryption systems

3.1 The basic system (McEliece)

We start by generating a code $[n, k, d]_q$ linear of a well-chosen family and its generator matrix G. We are going to mix this matrix to make it indistinguishable from a random matrix, so we need a permutation matrix P her size is $n \times n$ (having 1 in each row and column and 0 everywhere) and an invertible matrix S her size

$k \times k$ (S is jammer). The public key will be $G' = SGP$ which is indistinguishable from a random matrix (The definition of a random matrix comes from the definition of random code which be introduced in section four). The knowledge of S, P and G allows us to find the structure of the design code and provides us with the decoding algorithm.

3.1.1 The algorithms of the McEliece system

We cite the component algorithms of the McEliece cryptosystem [4].
The generation of keys
Input
A family of linear codes $[n, k, d]_q$ chosen for design.
Procedure
Choose a generator matrix G in systematic form of the design code.
Choose an invertible matrix S her size k with coefficients in F_q.
Choose a permutation matrix P her size is $n \times n$.
Calculate $G' = SGP$.
Output
The public key G'.
The private key (S, G, P).
Encryption of the plaintext.
Input
The public key G'.
The plaintext $x \in F_q^k$.
Procedure
Choose a vector $e \in F_q^n$ (an error) his weight less than or equal to the design code correction capacity.
Calculate $y = xG' + e$.
Output: The cipher text y.
Decryption of cipher text
Input: the cipher text y, The private key (S, G, P).
Procedure
Calculate $u = yP^{-1}$.
Calculate $x' = f_G(u)$ with f_G the design code decoding algorithm, whose generator matrix is G.
Calculate $x = x'S^{-1}$.
Output: the plaintext x.
Remark
The use of binary Goppa code as a secret key is initially proposed by McEliece in its original version. Where he took the following parameters: $m = 10, n = 2^n = 1024, r = 50, k = n - mr = 524$. So far it seems that this choice is perfectly safe, but it is not used in practice because the size of its public key is very large.
Example
We use the Hamming code with its generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$
and parity check matrix $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1. \end{bmatrix}$
The generation of keys

Let the private key S, G, P.

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = S^{-1},\ P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

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

The public key: $G' = SGP = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$

Encryption

Let the plaintext $x = (0110)$ and let error vector $e = (0010000)$.

The cipher text is $y = xG' + e = (0111000) + (0010000) = (0101000)$.

Decryption

We decipher the text received $y = (0101000)$. We have $y = xG' + e = xSGP + e$ then $P^{-1} = xSG + eP^{-1} = (1100000) = y'$. $Hy'^{t} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, so the error is in the third position hence $u = (1110000) = xSG$. And since G is generator matrix of the systematic system then $xS = (1110)$ then $x = (1110)S^{-1} = (0110)$. x. Then the plaintext sought.

3.2 The Niederreiter variant

Let C a linear t-corrector code of length *n* and dimension *k*. Let H a parity check matrix of C her size is $(n - k) \times n$. We randomly choose an invertible matrix S and P a permutation matrix. We calculate $H' = SHP$. We will have H' a public key and (S, H, P) the private key, with the knowledge of a syndrome decoding algorithm in C. Let x a plaintext of length *n* and weight *t*, we calculate the cipher text $y = H'x^{t}$. The recipient receives *y* knowing the secret key, he can calculate $S^{-1}y = HPx^{t}$. Using the syndrome decoding algorithm of C, he can find Px^{t} and applying P^{-1} the plaintext x is found.

The algorithms of the Niederreiter cryptosystem [5]

The generation of keys

Input

A linear code $[n, k, d]_q$ is chosen for the design, of which we know a decoding algorithm by syndrome.

Procedure

Choose a parity check matrix H of design code.
Choose a matrix S, invertible of size k with coefficients in F_q.
Choose a permutation matrix P of size$n \times n$.
Calculate $H' = SHP$.
Output
The public key H'.
The private key(S, H, P).
Encryption
Input
The public key H'.
The plaintext $x \in F_q^n$ of weight less than or equal to the correction capacity.
Procedure
Calculate $y = H'x^t$.
Output
The cipher text y.
Decryption
Input
The private key (S, H, P).
The cipher text y.
Procedure
Calculate $y' = S^{-1}y$.
Calculate $x' = f_H(y')$ with f_H the code syndrome decoding algorithm, its parity check matrix is H.
Calculate $x = x'P^{-1}$.
Output
The plaintext x.
Remark
Reed-Solomon codes were originally proposed by Niederreiter as a family of codes that could be considered by his cryptosystem. In 1992 Sidelnikov and Shestakov have shown that it is easy to attack this cryptosystem [2].

4. The security of cryptosystems based on correcting codes

The security of cryptosystems based on error-correcting codes is based on the problem of distinguishing the design code (hidden) from a random code. We first give the following definitions:

- Code equivalence

Two codes are said to be equivalent if their generator matrices (respectively parity) are deduced from each other by permutation of columns.

- Random code

A random code is a linear code of which the k linearly independent lines of the generator matrix (or the n linearly independent columns of the parity matrix) have been generated randomly.

The main parameters for securing an McEliece cryptosystem and its variants are then the structure of the code family chosen for the design, which it is desirable that it will be difficult to find an equivalent code. Since the robustness of such a system lies in the difficulty of decoding and the hidden structure of the design code, then

the attacker can attempt to attack the system by two methods: decoding attack and structural attack. The resistance of the system to these two attack methods depends on the family of codes chosen for the design. The choice of code family is the essential point in the design of the cryptosystem.

4.1 Decoding attack

The attacker directly attempts to decode the cipher text in the *C* code (generator matrix *G* or public key parity *H*); the principle consists of decoding the intercepted cipher text relative to the public code using general decoding algorithms. We cite two decoding problems in a random code:

Problem 1

Given *G* a random binary matrix of size $k \times n$, generator of a *C* code of dimension *k*. *x* a random word of F_2^n and t a positive integer, find if there is an error word e of F_2^n such as $w(e) \leq t$ and $x + e \in C$.

Problem 2

Given H a binary random parity matrix; her size $(n - k) \times n$ of a *C* code its dimension k, s a random vector of F_2^{n-k} and t a positive integer, find if there is a word x of F_2^n such as $w(x) \leq t$ and $Hx^t = s$.

Decoding in random code is behind the following attacks:

- Algorithme de décodage par ensemble d'information

The principle is based on two steps: the selection of a set of information and the search for low-weight word. There are several variants which propose to optimize one or the other of these two steps.

Definition

Let C a linear code of generator matrix G and length n. A set of information I is a subset of $\{1, 2, ...n\}$ such as G_I, her size $k \times k$ formed of columns of G labeled by the elements of I, is invertible.

Remark

The matrix $(G_I|G_J)$ with $I \cup J = \{1, 2, ...n\}$ is equivalent to G.

Algorithm

Input

G: a matrix generating of a code C.

t: a positive integer.

y: a word of F_2^n such as $d(y, C) \leq t$.

Output

The couple (x, e) such as $y = xG + e$ where $w(e) \leq t$.

Procedure

Randomly draw a set of information I of the code C (let J such as $I \cup J = \{1, 2, ...n\}$).

Calculate $R = G_I^{-1}G_J$.

Write $y = \left(y_I|y_J\right)$.

Calculate $e_J = y_J - y_IR$.

Repeat the previous operations until you find e_J such as $w(e_J) \leq t$.

Returne $= (0|e_J)$.

Determine the word x such as $y - e = xG$.

Proof

We have a $y = xG + e$ and $y = \left(y_I|y_J\right) = x(G_I|G_J) + (e_I|e_J)$. Hence $e_I = y_I - xG_I$ and $e_J = y_J - xG_J$.

If the set of information I does not contain an error position $(e_I = 0)$ and like G_I is invertible, we obtain $y_I = xG_I$, $e_J = y_J - y_I G_I^{-1} G_J$. Then $e = \left(0|y_J - y_I G_I^{-1} G_{J.}\right)$ is the solution sought.

Remark

We have C_n^k possibilities to choose $k = |I|$ positions of $\{1, 2, ...n\}$ ($|I|$ is a cardinally of I). And we have C_{n-t}^k possibilities to choose $k = |I|$ positions among $n - t$ positions where $e_i = 0$. So the probability of getting the set of information I with $e_I = 0$ is $p = \frac{C_{n-t}^k}{C_n^k}$ and the average number of iterations will be $\frac{1}{p}$.

Example

Let us try to attack the following system by this method: We have$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$.

The cipher text $y = (10101011)$ ett $= 1$.

looking (m, e) such as $mG + e = y$.

Let $I = \{1, 5\} \subset \{1, 2, ...8\}$ then $G_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = G_I^{-1}$

and$G_J = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$.

$y_I = (1, 1)$ and $y_J = (0, 1, 0, 0, 1, 1)$. Then $e_J = y_J - y_I G_I^{-1} G_J = (001000)$, it follows that $\left(e_I|e_J\right) = (00001000)$.

$$\left(y_I|y_J\right) + \left(e_I|e_J\right) = (11010011) + (00001000) = (11011011) = m\left(G_I|G_J\right)$$
$$= m\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

then $m = (11)$.

- Decoding by paradox of birthdays

Consider an instance of problem 2. For a parity check matrix H of size $r \times n$, a syndrome s and a weight t. If the weight t is even, let us separate the columns of H in two sets of the same size H_1 and H_2 such as $H = (H_1|H_2)$.

Let us build $L_1 = \left\{H_1 e_1^t, e_1 \text{of length} \frac{n}{2} \text{and the weight} \frac{t}{2}\right\}$ et $L_2 = \left\{s + H_2 e_{2,}^t e_2 \text{of length} \frac{n}{2} \text{and the weight} \frac{t}{2}\right\}$. Common elements of L_1 and L_2 are such that $H_1 e_1^t = s + H_2 e_2^t$, that is to say $(e_1|e_2)$ is solution of problem 2.

The probability that one of the solutions splits into two equal parts of the parity matrix is $p = \frac{\left(C_{n/2}^{t/2}\right)^2}{C_n^t}$; to solve problem 2 you have to repeat these operations $\frac{1}{p}$ on different permutations of the public code.

- The recovery of a plaintext encrypted twice by the same McEliece system

This is an active attack that only applies to the McEliece encryption system (because it is not deterministic) and does not apply to the Niederreiter system. Suppose the plaintext x is encrypted in two different ways. We will have $y_1 = xG + e_1$, $y_2 = xG + e_2$ où e_1 et e_2 sont deux vecteurs d'erreur distincts de poids t. We get the word $y_1 - y_2 = e_1 - e_2$ which is less than or equal to 2t. Once an attacker has detected that the two cipher texts y_1 and y_2 correspond to the same plaintext, this information will reduce the number of iterations of the decoding algorithm set

of information. Message forwarding is detected by observing the weight of the two cipher texts. If the two plaintexts are identical then, the weight of the sum of the two numerical texts remains less than 2t in general (t the correction capacity).

Algorithm

Input

G: The public key of sizek $\times$ n.

Two words y_1 and y_2 such as $y_1 = xG + e_1$, $y_2 = xG + e_2$ where e_1 and e_2 are two distinct error vectors of weightt.

Output

The plaintext x.

Procedure

Calculate $y_1 - y_2$.

Randomly draw a set of information $I \subset \{1, 2, ...n\}$ which label the zero positions of $y_1 - y_2$.

Calculate $e_J = y_J - y_I G_I^{-1} G_J$ où $y_1 = \left(y_I | y_J\right)$ et$I \cup J = \{1, 2...n\}$.

Repeat the previous operations until the weight of e ($\leq$t).

Return $x = y_I G_I^{-1}$.

Example

Let us try to attack by this method the system of the previous example.

Either plaintext encrypted two ways in which the public key is

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

$$y_1 = mG + e_1 = (11)\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} + (00010000) = (10101011)$$

$$y_2 = mG + e_2 = (11)\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} + (00100000) = (10011011)$$

$$y_1 + y_2 = (00110000).$$

Draw a set of information that labels the zero positions of $y_1 + y_2$ let $I = \{7, 8\}$.

$G_I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = G_I^{-1}$, $G_J = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$;

$y_1 = (10101011), y_I = (11), y_J = (101010)$.

$$e_J = y_J - y_I G_I^{-1} G_J = (101010) - (11)\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = (000100).$$

$$\left(y_I | y_J\right) + \left(e_I | e_J\right) = (11101010) + (00000100) = (11101110)$$

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

So we extract $m = (11)$.

4.2 Structural attack

The attacker tries to find a decomposition of the key $G' = S_1 G_1 P_1$, which allows it to develop its own decoding algorithm. Succeeding in a structural attack generally amounts to finding a code equivalent to the public code for which we know a decoding algorithm. This attack depends exclusively on the structure of the space of

the keys used. We quote here a successful attack on an McEliece system with the Reed-Solomon code as the design code.

- The attack of Sidelnikov and Shestakov

Sidelnikov and Shestakov showed [6] that generalized Reed-Solomon codes were so structured that one could find a decoder of the public code in polynomial time. The systematic form of the matrix generating a *GRS* code can be obtained from the following proposition:

Proposal

Let $G = \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \ldots & v_n\alpha_n \\ \ldots & \ldots & \ldots & \ldots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \ldots & v_n\alpha_n^{k-1} \end{pmatrix}$ a matrix generating a Reed-Solomon code generalized on F_{q^m} then there is a matrix $k \times k$ invertible S coefficient in F_{q^m} and a matrix $R = \left(R_{ij}\right)_{\substack{i = 1\ldots k \\ j = k+1\ldots n}}$ such that $(I|R) = SG$ and $R_{ij} = \frac{v_j}{v_i}\prod_{\substack{s=1 \\ s \neq i}}^{k} \frac{\alpha_j - \alpha_s}{\alpha_i - \alpha_s}$

Proof

For $i = 1, 2\ldots k$ we define the following interpolation polynomial $f_i(x) = \prod_{\substack{s=1 \\ s \neq i}}^{k} \frac{\alpha_j - \alpha_s}{\alpha_i - \alpha_s} = \sum_{j=1}^{k} f_{ij}x^{j-1}$ of degree $k-1$ such that $f_i(\alpha_i) = 1$, $f_i(\alpha_j) = 0$ for $j = 1, 2\ldots k$ and $j \neq i$. We note $S = \left(\frac{f_{ij}}{v_i}\right)_{\substack{i = 1\ldots k \\ j = 1\ldots k}}$.

The ith row of the matrix produces SG is $\left(f_i(\alpha_1)\frac{v_1}{v_i}, f_i(\alpha_2)\frac{v_2}{v_i}, \ldots f_i(\alpha_n)\frac{v_n}{v_i}\right)$

By construction of polynomials f_i, the k first columns of the matrix SG form the identity matrix, therefore S is invertible and $SG = (I|R)$ where $R = R_{ij}$ and $R_{ij} = f_i(\alpha_j)\frac{v_j}{v_i}$.

Corollary

Let I the identity matrix its order k and $R = \left(R_{ij}\right)_{\substack{i = 1\ldots k \\ j = k+1\ldots n}}$ where $R_{ij} = \frac{v_j}{v_i}\prod_{\substack{s=1 \\ s \neq i}}^{k} \frac{\alpha_j - \alpha_s}{\alpha_i - \alpha_s}$. Alors la matrice $(I|R)$ is the generator matrix in systematic form of the generator matrix *GRS* code $G = \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \ldots & v_n\alpha_n \\ \ldots & \ldots & \ldots & \ldots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \ldots & v_n\alpha_n^{k-1} \end{pmatrix}$.

Proof

Can be deducted from the definition of the generalized Reed-Solomon code and the latest proposal.

Algorithm

Input

A family of generalized Reed-Solomon code of length n, of dimension k constituting the key space.

The public key G'.

Results

The matrix $G = \left(v_j\alpha_j^i\right)_{\substack{i = 0,..k-1 \\ j = 1\ldots n}}$ and S invertible matrix its size $k \times k$ such that $G' = SG$.

Procedure

Put the matrix G' in form $(I|R)$ by Gaussian elimination.

Determine the matrix $G = \left(v_j \alpha_j^i\right)_{\substack{i = 0,..k-1 \\ j = 1...n}}$ such that $\alpha_1, ...\alpha_n$ et $v_1, ...v_n$ check the equations $R_{ij} = \frac{v_j}{v_i} \prod_{\substack{s = 1 \\ s \neq i}}^{k} \frac{\alpha_j - \alpha_s}{\alpha_i - \alpha_s}$.

Determine the matrix S such that $G' = SG$.

5. Conclusion

In conclusion, the security of cryptosystems based on error-correcting codes is strongly linked to the family of code used in the design of the system. The cryptosystem based on the Reed-Solomon code was broken by Sidelnikov and Shestakov in 1992. The version of McEliece using Goppa codes has been studied for 40 years and it seems perfectly secure from a cryptographic point of view; but it is not used in practice because the size of its public key is much larger that we know how to do with systems from other fields (RSA for example), hence the importance of finding a way to reduce the size of their public key. In the end, the McEliece system based on Goppa's code remains a preferred system as a post-quantum cryptosystem. We have not covered in this chapter other cryptographic applications of error-correcting codes, including hash functions [3, 7–11], pseudo-random generators, identification protocols, etc.

Author details

Ahmed Drissi
National School for Applied Sciences, ENSA, Abdelmalek Essaadi University, Tangier, Morocco

*Address all correspondence to: idrissi2006@yahoo.fr

References

[1] Cayrel PL. Nouveaux résultats en cryptographie basée sur les codes correcteurs d'erreurs.

[2] Loidreau P. Etude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs [doctoral dissertation]; Thèse de doctorat. ENSTA Paris. 2001

[3] Drissi A. Formation doctorale [doctoral dissertation]. Thèse de doctorat. Université Ibn Zohr; 2014

[4] McEliece RJ. A Public-Key Cryptosystem Based on Algebraic Coding Theory, 42441978. pp. 114-116

[5] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory. 1986;**15**(2): 159-166

[6] Sidelnikov VM, Shestakov SO. On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Mathematics and Applications. 1992;**2**(4):439-444

[7] Drissi A, Asimi A. One-way hash function based on goppa codes «OHFGC». Applied Mathematical Sciences. 2013;**7**(143):7097-7104

[8] Dallot L. Sécurité de protocoles cryptographiques fondés sur les codes correcteurs d'erreurs [doctoral dissertation]; France: Université de Caen/Basse-Normandie; 2010

[9] Merkle R. One way hash functions and DES. In: Crypto 1989, LNCS. Vol. 435. 1990

[10] Pretzel O. Error-Correcting Codes and Finite Fields. Student ed. Oxford University Press, Inc.; 1996

[11] Kumar R, Naidu AS, Singh A, Tentu AN. McEliece cryptosystem: Simulation and security vulnerabilities. International Journal of Computing Science and Mathematics. 2020;**12**(1): 64-81