A New Approach to Decoding of Rational Irreducible Goppa code

Ahmed DRISSI
LabSiv : Laboratoire des Systèmes informatiques et Vision
ESCAM : Equipe de la Sécurité, Cryptographie, Contrôle d’Accès et Modélisation
Departments of Mathematics and Computer Science
Faculty of Sciences, Ibn Zohr University, Agadir, Morocco
idrissi2006@yahoo.fr

Ahmed ASIMI
LabSiv : Laboratoire des Systèmes informatiques et Vision
ESCAM : Equipe de la Sécurité, Cryptographie, Contrôle d’Accès et Modélisation
Departments of Mathematics and Computer Science
Faculty of Sciences, Ibn Zohr University, Agadir, Morocco
asimiahmed2008@gmail.com

Abstract— The interesting properties of classical Goppa code and its effective decoding algorithm (algorithm of patterson) make the most appropriate candidate for use in the MC Eliece cryptosystem. Information leakage which results from the relationship between the error vector weight and the number of iterations in the decoding algorithm, presented a weakness of the cryptosystem. In this paper, we introduce a new approach to decoding, the use of binary Goppa code in system design MC Eliece which solve the problem of the leak of information, on the contrary in case of patterson algorithm. We treat this decoding method using the Newton identities and results of linear algebra.

Keywords: Binary Goppa code, the Newton identities, circulant matrix

I- INTRODUCTION

A motivation of this work is to find algorithms for decoding binary Goppa code where their use in the design of the MC Eliece leaves no information leakage. To attack the system Mc Eliece, the researchers H.Gregor Molter.Marc Stottinger.Abdulhadi Shoufan.Falko Strenzke have exploited in [1] an information leak, which results from the relationship between the weight error vector and the number of iterations of the Euclidean algorithm extended used in the algorithm of Patterson, and extract the error vector which is secret, and thereafter the plaintext. it prompts us to seek another decoding algorithm where this leak information about the error is remedied. Magali Bardet used in [2] and [3] the Newton identities for decoding cyclic codes but also used the Groebner basis calculation and the theory of elimination. The similarity in structure between the control matrix of a cyclic code and a Goppa code has encouraged us to try to follow the same path, but it has happened that the use of the properties of circular matrices and diagonalization better for our code.

In the next section, we state the notations used in this document and the third we define the Goppa code binary, its characterization and its correction capability. For the fourth section, it was replaced problem of solving a system in $F_2^n$, to $m$ systems in $F_2^m$. And its resolutions are discussed in the following two sections treating the relationship between Newton and elementary symmetric functions. Transforming this relationship in matrix form and use the properties of linear algebra, in particular the structure of a circulant matrix. We finally give our own method for decoding a binary irreducible Goppa code.

II- NOTATIONS AND PRELIMINARIES

$m$ : An integer.
$F_{2^m}$ : A finite field of $2^m$ elements.
$F_2 = \{0,1\}$.
$F_2^n$ : The set of vectors of length $n$ of a component 0 or 1.
$F_{2^m}^n$ : The set of vectors of length $n$ a component of $F_{2^m}$.
$I_n$ : The identity matrix of size $n$.
$I$ : an identity matrix.
$I_d$ : The application identity.
$\text{mat}_\beta(f)$ : The matrix associated with the endomorphism $f$ in the base $\beta$. 
The derivative of the polynomial \( \sigma_g(x) \) relative to \( x \).

\[
\Gamma(L,g) : \text{The Goppa code of support } L \text{ and polynomial } g.
\]

\[
\left[ \begin{array}{c}
\end{array} \right] : \text{The integer part.}
\]

\[
\left( w_1, ..., w_m \right) : \text{the basis of the vector space } F_{2^n} \text{ on the field } F_2.
\]

\[
F_{2^n}[x] : \text{The set of polynomials with coefficients in } F_{2^n}.
\]

\( N : \text{The set of integers.} \)

\( \text{card} : \text{the number of elements of a set.} \)

\( \text{rg}(C) : \text{the rank of a matrix } C \)

Let \( \alpha \in F_{2^n} \) and

\[
g(x) = g_0 + g_1 x + ... + g_{2^n-1} x^{2^n-1} \in F_{2^n}[x]
\]

with \( g \neq 0 \) and \( g(\alpha) \neq 0 \);

\[
g(x) - g(\alpha) = (x-\alpha) \sum_{i=0}^{2^n-1} g_i x^i
\]

Therefore

\[
\frac{-g(x)}{g(\alpha)} + 1 = (x-\alpha) \left[ -\frac{1}{g(\alpha)} \sum_{i=0}^{2^n-1} g_i \sum_{j=0}^{k_i-1} x^j \right]
\]

It is said that

\[
\frac{1}{x-\alpha} \mod g(x) = -\frac{1}{g(\alpha)} \sum_{i=0}^{2^n-1} g_i \sum_{j=0}^{k_i-1} x^j A_j
\]

III- The Binary Goppa code

1-Definition

Let \( L = (\alpha_1, ..., \alpha_n) \) a sequence of \( n \) distinct elements of \( F_{2^n} \) and \( g(x) \in F_{2^n}[x] \) a polynomial of degree \( r \) in \( F_{2^n}[x] \) such as \( 1 \leq r \leq n-1 \) and \( g(\alpha_i) \neq 0 \) for all \( i = 1, ..., n \).

Rational Goppa code of support \( L \) (vector generator) and of generator polynomial \( g \) (Goppa polynomial) noted \( \Gamma(L,g) \) is the set

\[
\Gamma(L,g) = \left\{ c = (c_1, ..., c_r) \in F_2^r \mid \sum_{i=1}^{r} c_i \left( \frac{1}{x-\alpha_i} \mod g(x) \right) = 0 \right\}
\]

If \( g \) is irreducible, we say that \( \Gamma(L,g) \) is an irreducible binary Goppa code.

2- Characterization of Goppa code

Theorem

Let \( L = (\alpha_1, ..., \alpha_n) \) a sequence of \( n \) distinct elements of \( F_{2^n} \) and \( g(x) \in F_{2^n}[x] \) a polynomial of degree \( r \) in \( F_{2^n}[x] \), such as \( 1 \leq r \leq n-1 \) and \( g(\alpha_i) \neq 0 \) for all \( i = 1, ..., n \).

The following assertions are equivalent:

i) \( \sum_{i=1}^{n} a_i \left( \frac{1}{x-\alpha_i} \mod g(x) \right) = 0 \).

ii) \( H \alpha^t = 0 \)

\[
H = \begin{pmatrix}
1 & 1 & 1 & \ldots & 1 \\
\alpha_i & \alpha^2_i & \alpha^3_i & \ldots & \alpha^{r-1}_i \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
\alpha^{r-1}_i & \alpha^{2(r-1)}_i & \alpha^{3(r-1)}_i & \ldots & \alpha^{(r-1)(r-1)}_i
\end{pmatrix}
\]

\( H \) is called control matrix Goppa code \( \Gamma(L,g) \)

iii) \( g(x) \) divide \( \frac{d \sigma_g(x)}{dx} \) with

\[
\sigma_g(x) = \prod_{i=1}^{n} (x-\alpha_i)
\]

proof

we have

\[
\frac{1}{x-\alpha} \mod g(x) = -\frac{1}{g(\alpha)} \sum_{i=0}^{2^n-1} g_i \sum_{j=0}^{k_i-1} x^j A_j
\]

\[
\sum_{i=1}^{n} a_i \frac{1}{x-\alpha_i} \mod g(x) = -\sum_{i=1}^{n} a_i g(\alpha_i) \sum_{j=0}^{k_i-1} \sum_{j=0}^{k_i-1} x^j A_j
\]

\[
= -\sum_{i=1}^{n} g_i \sum_{j=0}^{k_i-1} x^j A_j
\]

we denote

\[
A_j = \sum_{i=1}^{n} a_i g(\alpha_i)^{-1} \alpha_i^{j} , \ j = 0, 1, ..., r - 1.
\]

ii) \( \Rightarrow i) \)

\[
H \alpha^t = 0 \Rightarrow \sum_{i=1}^{n} a_i \ g(\alpha_i)^{-1} \alpha_i^{j} = 0 \text{ for } j = 0, 1, ..., r - 1 \text{ then }
\]

\[
\sum_{i=1}^{n} a_i \frac{1}{x-\alpha_i} \mod g(x) = 0.
\]

i) \( \Rightarrow ii) \)

Let

\[
\sum_{k=1}^{r} g_k \sum_{j=0}^{k-1} x^{k-j} A_j = 0 \text{ then }
\]
$$g_1A_0 + g_2(xA_0 + A_1) + g_3(x^2A_0 + xA_1 + A_2) +$$
$$g_4(x^3A_0 + x^2A_1 + xA_2 + A_3) + g_5(x^4A_0 + x^3A_1 +$$
$$+ x^2A_2 + xA_3 + A_4) + \ldots$$

$$+ g_r(x^{-r}A_0 + x^{-r+1}A_1 + \ldots + xA_{r-2} + A_{r-1}) = 0$$

Then
$$g_1A_0 + g_2A_1 + \ldots + g_rA_{r-1} = 0$$
$$g_2A_0 + g_3A_1 + \ldots + g_rA_{r-2} = 0$$
$$g_3A_0 + \ldots + g_rA_{r-3} = 0$$
$$\ldots$$

$$g_{r-1}A_0 + g_rA_1 = 0$$

Since \( g_r \neq 0 \), it was \( A_0 = 0 \).

By recurrence we find that \( A_j = 0 \) for

\( j = 0, 1, \ldots, r - 1 \).

\( \Rightarrow \) \( i \) \( \iff \) \( iii \)

$$\frac{d\sigma_a}{dx} = \sum_{i=1}^{n} a_i (x - \alpha_i)^{-1} \prod_{j=1}^{n} (x - \alpha_j)^{-1} + \sum_{i=1}^{n} a_i \prod_{j=1, j \neq i}^{n} (x - \alpha_j)^{-1}$$

$$= \sigma_a \sum_{j=1}^{n} \frac{a_j}{x - \alpha_j} = \sigma_a R_a(x).$$

It was \( R_a(x) = \sum_{i=1}^{n} \frac{a_i}{x - \alpha_i} = \frac{P(x)}{Q(x)} \) with

\( Q(x) = \prod_{i=1}^{n} (x - \alpha_i) \) and

\( u_i(x) = \frac{1}{x - \alpha_i} \mod g(x). \)

It was

\( u_i(x)(x - \alpha_i) = 1 + k_i(x)g(x) \)

\( \sum_{i=1}^{n} a_i \left( \frac{1}{x - \alpha_i} \mod g(x) \right) = \sum_{i=1}^{n} a_i u_i(x) \)

\( = \sum_{i=1}^{n} \frac{a_i}{x - \alpha_i} + \sum_{i=1}^{n} \frac{a_i k_i(x)g(x)}{x - \alpha_i} \)

\( = R_a(x) + g(x) \sum_{i=1}^{n} \frac{a_i k_i(x)}{x - \alpha_i} \)

\( = \frac{P(x)}{Q(x)} + g(x) \sum_{i=1}^{n} \frac{a_i k_i(x)}{x - \alpha_i} \)

Where

\( Q(x) \sum_{i=1}^{n} a_i \left( \frac{1}{x - \alpha_i} \mod g(x) \right) = P(x) + g(x)Q(x) \sum_{i=1}^{n} \frac{k_i(x)}{x - \alpha_i} \) (1)

If \( \sum_{i=1}^{n} a_i \left( \frac{1}{x - \alpha_i} \mod g(x) \right) = 0 \) then \( g(x) \) divide \( P(x) \) (indeed \( Q(x) \sum_{i=1}^{n} a_i \frac{k_i(x)}{x - \alpha_i} \) is a polynomial) gold it was \( \frac{d\sigma_a}{dx} = \sigma_a R_a(x) \) then

\( Q(x) \frac{d\sigma_a}{dx} = \sigma_a P(x) \) therefore \( g(x) \) divide \( Q(x) \frac{d\sigma_a}{dx} \); gold \( Q(x) \) and \( g(x) \) are mutually prime (because \( g(\alpha_i) \neq 0 \) for \( i = 1, \ldots, n \) ) therefore \( g(x) \) divide

\( \frac{d\sigma_a}{dx} \)

\( \Leftarrow \)

If \( g(x) \) divide \( \frac{d\sigma_a}{dx} \) therefore \( g(x) \) divide

\( Q(x) \sum_{i=1}^{n} a_i \left( \frac{1}{x - \alpha_i} \mod g(x) \right) \) and since \( g(x) \) and \( \sigma_a(x) \) are mutually prime therefore \( g(x) \) divide \( P(x) \) and according to (1) \( g(x) \) divided

\( Q(x) \sum_{i=1}^{n} a_i \left( \frac{1}{x - \alpha_i} \mod g(x) \right) \) and since \( g(x) \) and \( Q(x) \) are mutually prime then \( g(x) \) divide

\( \sum_{i=1}^{n} a_i \left( \frac{1}{x - \alpha_i} \mod g(x) \right) \). We know that
deg \( g(x) = r \) and

deg \( \sum_{i=1}^{n} a_i \left( \frac{1}{x - \alpha_i} \mod g(x) \right) = r - 1 \) then

\( \sum_{i=1}^{n} a_i \left( \frac{1}{x - \alpha_i} \mod g(x) \right) = 0 \)
3- correction capacity

The parity matrix $H$ can be written as the product of a Vandermonde matrix and a nonsingular matrix so any square submatrix $r \times r$ of $H$ is invertible, then there is no code word of weight less or equal to $r$, then it has a minimum distance of at least $d = r + 1$ (of capacity correction $\left\lfloor \frac{r}{2} \right\rfloor$).

If we add an additional constraint on $g$ to be without multiple factors, we can double the capacity of correction. (in particular irreducible codes).

Indeed $g(x)$ divide \( \frac{d \sigma_s(x)}{dx} \), on $F_{2^m}$ the derivative of a polynomial does not contain coefficients of odd degree, therefore there exists a polynomial satisfying \( \frac{d \sigma_s(x)}{dx} = f^2(x) \).

If $g$ has no multiple factors and $g$ divide $f^2$ then, $g$ necessarily divided $f$.

A word $a$ which belongs to the code $\Gamma(L, g)$ with $g$ without multiple factors belong to the code $\Gamma(L, g^2)$ which has a minimum distance $2r + 1$ and a decoding algorithm to $r$ errors.

4- The decoding

Formally the decoding problem can be stated as follows: let the received word $r = (r_1, r_2, ..., r_n)$ and the codeword sent $c = (c_1, c_2, ..., c_n)$ such as $r = c + e$ with $e = (e_1, e_2, ..., e_n)$ a weight vector less or equal to the correction capacity

\[
\begin{pmatrix}
S_0 \\
S_1 \\
\vdots \\
S_{r-1}
\end{pmatrix} =
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
a_1 & a_2 & \cdots & a_s \\
\vdots & \vdots & \ddots & \vdots \\
a_t^{-1} & a_{t+1}^{-1} & \cdots & a_s^{-1}
\end{pmatrix}
\begin{pmatrix}
\sigma_1 \\
\sigma_2 \\
\vdots \\
\sigma_s
\end{pmatrix}
\begin{pmatrix}
r_1 \\
r_2 \\
\vdots \\
r_s
\end{pmatrix}
\]

\[
Hr' = Hc' + He' = 0 + He' = He'
\]

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
a_1 & a_2 & \cdots & a_s \\
\vdots & \vdots & \ddots & \vdots \\
a_t^{-1} & a_{t+1}^{-1} & \cdots & a_s^{-1}
\end{pmatrix}
\begin{pmatrix}
\sigma_1 \\
\sigma_2 \\
\vdots \\
\sigma_s
\end{pmatrix}
\begin{pmatrix}
e_1 \\
e_2 \\
\vdots \\
e_s
\end{pmatrix}
\]

\[
S_i + \sum_{j=1}^{k} \sigma_j S_{i-j} = 0 \quad \text{for} \quad i \geq k.
\]

Proof

We denote the polynomial

\[
\sigma(x) = \prod_{j=1}^{k} (x - x_j) = \sum_{j=0}^{k} \sigma_s x^{k-j} = \sigma + \sigma x + \cdots + \sigma_x + \sigma_n
\]

with $\sigma_0 = 1$. For $j$ fixed $\sigma(x_j) = 0$ therefore $\sigma_0 x_j^p + \sigma_1 x_j^{p-1} + \cdots + \sigma_n x_j^{p-k} + \sigma_n x_j^{p-k} = 0$

Let for $p \geq k$

\[
\sigma_0 x_j^p + \sigma_1 x_j^{p-1} + \cdots + \sigma_n x_j^{p-k} + \sigma_n x_j^{p-k} = 0
\]

We must find the vector

\[
\begin{pmatrix}
g(\alpha_1)^{-1} e_1 \\
g(\alpha_2)^{-1} e_2 \\
\vdots \\
g(\alpha_s)^{-1} e_s
\end{pmatrix}
\]

IV - The identity newton

Let $k \in N$ and $x_1, x_2, ..., x_k \in F_{2^n}$ , the following theorem known as Newton's identity gives a relation between the elementary symmetric functions $\sigma_j = \sum_{i_1 < ... < i_j} x_{i_1} ... x_{i_j}$ and the sum of newton $S_p = \sum_{i=0}^{k} x_i^p$, $\forall p \in N$.

Theorem - circular identity of Newton-

Let $k \in N$ and $x_1, x_2, ..., x_k \in F_{2^n}$ , the sum of Newton $S_j = \sum_{j=0}^{k} x_j^p$, $\forall i \in N$ , the elementary symmetric functions $\sigma_1, ..., \sigma_k$ of $x_1, x_2, ..., x_k$ defined by

\[
\sigma_j = \sum_{1 \leq i_1 < ... < i_j \leq k} x_{i_1} ... x_{i_j}
\]

then we will have relations

\[
S_i + \sum_{j=1}^{k} \sigma_j S_{i-j} = 0 \quad \text{for} \quad i \geq k.
\]
Summing over $j$ we will

$$\sigma_0 S_p + \sigma_1 S_{p-1} + \ldots + \sigma_{k-1} S_{p-k+1} + \sigma_k S_{p-k} = 0$$

Since $S_{i+2^m-1} = S_i$ (indeed $S_{i+2^m-1} = \sum_{j=0}^{2^m-1} x_j = \sum_{j=0}^{i-1} x_j = S_i$)

therefore for

$1 \leq p \leq k$ we will $S_{p+2^m-1} = S_p$ and $p + 2^m - 1 \geq k$

then we can write this relation in matrix form as follows

**Lemma 1:**

$
\text{form matrix identity newton}$

Let $x_1, x_2, \ldots, x_k \in F_{2^n}$ and

$$
\sigma(x) = \sum_{j=0}^{k} (x-x_j) = \sum_{j=0}^{k} \sigma_j x^{k-j} = \sigma_0 + \sigma_1 x + \ldots + \sigma_{k-1} x + \sigma_k
$$

and

$$
S_i = \sum_{j=0}^{2^m-1} x_j, \forall i = 0,1,2^m-2
$$

it was

$$
\begin{bmatrix}
S_{2^m-2} & S_{2^m-3} & \ldots & S_0 & 0 \\
S_0 & S_{2^m-2} & \ldots & S_1 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
S_{2^m-3} & S_{2^m-4} & \ldots & S_{2^m-2} & \sigma_i
\end{bmatrix}
= 0
$$

V. The circulant matrix

**Definitions**

A circulant matrix with coefficients in a finite field $F_{2^n}$ of size $n$ is a matrix of the form

$$C = \begin{bmatrix}
c_0 & c_1 & \ldots & c_{n-1} \\
c_{n-1} & c_0 & \ldots & c_{n-2} \\
\vdots & \vdots & \ddots & \vdots \\
c_1 & c_2 & \ldots & c_0
\end{bmatrix}
$$

with

$$c_i \in F_{2^n}, \forall i \in \{0,1,\ldots,n-1\}$$

The matrix $A = \begin{bmatrix}
0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 1 & \ldots & 0 \\
0 & \ldots & 0 & \ldots & 0 \\
1 & 0 & \ldots & 0
\end{bmatrix}$ is said to be elementary.

**Lemma 1**

Let $A$ the circulant matrix elementary of size $n$ and $E_j$ the $j^{th}$ line of the identity matrix $I_n$, it was

i) $A^n = I_n$

ii) $E_j A^k = E_{(j+k) \mod n}, \forall k = 1, \ldots, n$

**Proof**

i) let $\beta$ be a base and $f$ the endomorphism such as $A = \text{mat}_f(\beta)$, we see that $f(e_i) = e_j$ and $\forall k = 2, \ldots, n$, $f(e_i) = e_{k+i}$, we deduce easily that $f^n = I_d$ that is to say $A^n = I_n$.

ii) by recurrence on $k$ it was for $k = 1$, $E_j A = E_{j+1}$. Suppose that $E_j A^k = E_{(j+k) \mod n}$ then $E_j A^{k+1} = E_j A^k A = E_{(j+k) \mod n} A = E_{(j+k+1) \mod n}$

**Lemma 2**

We can decompose the circulant matrix $C$ defined above in the following manner $C = c_0 I + c_1 A + \ldots + c_{n-1} A^{n-1}$

**Proof**

Using the fact that $E_j A^k = E_{(j+k) \mod n}$ it was

$$E_j (c_1 I + c_1 A + \ldots + c_{n-1} A^{n-1}) = c_j E_j + c_1 E_{j+1} + \ldots + c_{n-1} E_{j+n-1} = E_j C$$

Therefore a $j^{th}$ line of $C$ and of $c_0 I + c_1 A + \ldots + c_{n-1} A^{n-1}$ are equal.

**Lemma 3**

Let $\alpha$ be a primitive element of the finite field $F_{2^n}$, therefore

$$\alpha^{2^n-1} = 1$$

and the matrix

$$P = \begin{bmatrix}
1 & 1 & \ldots & 1 \\
1 & \alpha & \alpha^{2^n-2} & \ldots & \alpha^{(2^n-2)(\mod 2^n-2)} \\
1 & \alpha^{2^n-2} & \alpha^{(2^n-2)(\mod 2^n-2)} & \ldots & \alpha^{(2^n-2)(\mod 2^n-2) - 1} \\
1 & \alpha^{2^n-2} & \alpha^{(2^n-2)(\mod 2^n-2)} & \ldots & \alpha^{(2^n-2)(\mod 2^n-2) - 1}
\end{bmatrix}
$$

invertible and its inverse is

$$P^{-1} = \begin{bmatrix}
1 & 1 & \ldots & 1 \\
1 & \alpha^{2^n-2} & \alpha^{(2^n-2)(\mod 2^n-2)} & \ldots & \alpha^{(2^n-2)(\mod 2^n-2) - 1} \\
1 & \alpha^{2^n-2} & \alpha^{(2^n-2)(\mod 2^n-2)} & \ldots & \alpha^{(2^n-2)(\mod 2^n-2) - 1}
\end{bmatrix}
$$

**Proof**

Let $a = \sum_{j=0}^{2^n-2} \alpha^j = \sum_{j=0}^{2^n-2} \alpha^{j(\mod 2^n)} = \begin{bmatrix}
1 & 1 & \ldots & 1 \\
0 & si & i \neq l
\end{bmatrix}$

it was $1 + \alpha + \alpha^2 + \ldots + \alpha^{2^n-2} = 0$ indeed

$$(1-\alpha)(1 + \alpha + \alpha^2 + \ldots + \alpha^{2^n-2}) = 1 - \alpha^{2^n-1} = 1 - 1 = 0$$
Lemma 4

Let \((c_1, c_2, ..., c_{n-1}) \in F_{2^n}^n\) and the polynomial

\[C(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}\]

it was if \(n = 2^m - 1\) and \(\alpha\) primitive root of the finite field \(F_{2^n}\)

\[
\begin{bmatrix}
\alpha^n & \alpha^{n-1} & \cdots & \alpha & 1 \\
\alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha^2 & \alpha \\
\cdot & \cdot & \cdots & \cdot & \cdot \\
\alpha & \alpha^2 & \cdots & \alpha^{n-2} & \alpha^{n-1} \\
1 & 1 & \cdots & 1 & 1 \\
\end{bmatrix}
\]

\(\beta = \alpha^{2^{m-1}}\)

And \(\text{rg}(C) = \text{card}\{i \in [0,1,...,n-1]; C(\beta^i) \neq 0\}\)

Proof

Calculate the eigenvalues of the elementary circulate matrix \(A\) of size \(n\).

It was \(A^{2^m - 1} = I\) by Lemma 1.

Let \(\alpha\) primitive root of the finite field \(F_{2^n}\) (that is to say \(\alpha^{2^m - 1} = 1\)) we have

\[
\begin{bmatrix}
0 & 1 & 0 & ... & 0 \\
0 & 0 & 1 & \cdots & ... \\
0 & ... & 0 & 1 \\
1 & 0 & ... & ... & \alpha \\
\end{bmatrix}
\]

\[= \alpha^{(2^m-2)}\]

\(i = 0,1,...,2^m - 2\) so we can diagonalize \(A\) as follows

\[A = P \alpha P^{-1}\]

with

\[P = \begin{bmatrix}
1 & \alpha & \cdots & \alpha^{2^m - 2} \\
1 & \alpha & \cdots & \alpha^{2^m - 2} \\
\cdot & \cdot & \cdots & \cdot \\
1 & \alpha & \cdots & \alpha^{2^m - 2(2^m - 2)} \\
\end{bmatrix}\]

Lemma 2

\[C(\alpha) = \begin{bmatrix}
1 & \alpha & \cdots & \alpha^{2^m - 2} \\
1 & \alpha & \cdots & \alpha^{2^m - 2} \\
\cdot & \cdot & \cdots & \cdot \\
1 & \alpha & \cdots & \alpha^{2^m - 2(2^m - 2)} \\
\end{bmatrix} \begin{bmatrix}
C(\alpha) \\
C(\alpha^2) \\
\vdots \\
C(\alpha^{2^m - 2}) \\
\end{bmatrix}
\]

and we deduce that also

\[\text{rg}C = \text{card}\{i \in [0,1,...,n-1]; C(\alpha^i) \neq 0\}\]

VI- FOR \(F_{2^n}\) TO \(F_{2^m}\)

we put \(v = [v_1,...,v_n] \in F_{2^n}\) and we must solve the following system in \(F_{2^n}\) : \(Av = S\) with the matrix \(A\) and the vector \(S\) are known.

In this section we will replace this system by \(m\) systems unknown in \(F_{2^m}\)

\[Av^i = S^i, \ A = 1,....,m\]

Let \((\omega_1, ..., \omega_m)\) a base of \(F_{2^m}\) as a vector space on field \(F_2\)

\[\forall v \in F_{2^n}; v = \sum_{j=1}^{m} v_j \omega_j \] and \(\forall s \in F_{2^m}; s = \sum_{j=1}^{m} s_j \omega_j\)

Let \(A = (a_{ij})_{j=1,...,r}\) a matrix of elements in \(F_{2^m}\)

Let the system \(Av^j = s\)

For \(i = 1,...,r\) it was

\[s_j = \sum_{j=1}^{m} a_{ij} v_j\]

\[= \sum_{j=1}^{m} a_{ij} \omega_j\]

therefore \(s_j^2 = \sum_{j=1}^{m} a_{ij} v_j^2\) we conclude that

\[\forall j = 1,...,r\]

\[v_j^2 = \sum_{j=1}^{m} a_{ij} \omega_j\]

\[A = \begin{bmatrix}
v_1 & \cdots & v_n \\
v_1 & \cdots & v_n \\
\vdots & \cdots & \vdots \\
v_1 & \cdots & v_n \\
\end{bmatrix}
\]

VII- SOLVING SYSTEMS OF VANDERMONDE MATRIX \(F_{2^n}\)

Let the system \(A \vdots v = S\) ; if \(A\) is of the form

\[A = \begin{bmatrix}
1 & 1 & \cdots & 1 \\
\alpha_1 & \alpha_2 & \cdots & \alpha_n \\
\vdots & \vdots & \cdots & \vdots \\
\alpha_1^{2^m-2} & \alpha_2^{2^m-2} & \cdots & \alpha_n^{2^m-2} \\
\end{bmatrix}
\]

Suppose that the indexes \(i_1,...,i_k\) of vector \(v\) are not zero

\[v_{i_1} = \cdots = v_{i_k} = 1;\] it follows

\[v_i = \begin{bmatrix}
v_1 \\
\vdots \\
v_n \\
\end{bmatrix}
\]
\[ S_0 = 1 + \ldots + 1 \]
\[ S_i = \alpha_i + \ldots + \alpha_i \]
\[ S_2 = \alpha_i^2 + \ldots + \alpha_i^2 \]
\[ \ldots \]
\[ S_{n-1} = \alpha_i^{n-2} + \ldots + \alpha_i^{n-2} \]

We pose \( \alpha_i = x_1, \ldots, \alpha_i = x_k \) therefore
\[ S_i = \sum_{j=1}^{k} x_j^i, i = 0,1,\ldots,2^n - 2 \]

Let \( \sigma(x) = \prod_{j=1}^{k} (x - x_j) = \sum_{j=0}^{k} \sigma_j x^j \)
\[ v_i = 1 \iff \sigma(\alpha_i) = 0 \]

Just find the polynomial \( \sigma(x) \) and exhaustive search method known as one dog finds its roots and can be detected by following the indexes \( i_1, \ldots, i_k \).

According to Newton's identity we have:
\[
\begin{bmatrix}
S_{2^n-2} & S_{2^n-3} & \ldots & S_0 & 0 \\
S_0 & S_{2^n-2} & \ldots & S_1 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
S_{2^n-3} & S_{2^n-4} & \ldots & S_{2^n-2} & \sigma_k
\end{bmatrix} = 0; \text{ so we have to solve this system, first study the uniqueness of solution.}
\]

**Lemma**
\[
\begin{bmatrix}
S_{2^n-2} & S_{2^n-3} & \ldots & S_0 & 0 \\
S_0 & S_{2^n-2} & \ldots & S_1 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
S_{2^n-3} & S_{2^n-4} & \ldots & S_{2^n-2} & \sigma_k
\end{bmatrix} = k
\]

**Proof**
\[ S_i = \sum_{j=1}^{k} x_j^i = \sum_{j=1}^{n} v_i \alpha_j^i, \forall i \in N \]
\[
\begin{bmatrix}
S_i \\
S_{i+1} \\
\vdots \\
S_{i+n-1}
\end{bmatrix} = \begin{bmatrix}
1 & 1 & \ldots & 1 \\
\alpha_1 & \alpha_2 & \ldots & \alpha_n \\
\alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1}
\end{bmatrix} \begin{bmatrix}
v_i \alpha_1^i \\
v_2 \alpha_2^i \\
\vdots \\
v_n \alpha_n^i
\end{bmatrix}
\]
\[
\begin{bmatrix}
S_i \\
S_{i+1} \\
\vdots \\
S_{i+n-1}
\end{bmatrix} = \begin{bmatrix}
1 & 1 & \ldots & 1 \\
\alpha_1 & \alpha_2 & \ldots & \alpha_n \\
\alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1}
\end{bmatrix} \begin{bmatrix}
v_i \alpha_1^i \\
v_2 \alpha_2^i \\
\vdots \\
v_n \alpha_n^i
\end{bmatrix}
\]

\[ F = \begin{bmatrix}
v_1 & 0 & \ldots & 0 \\
0 & v_2 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & v_n
\end{bmatrix} \quad \text{with } F \text{ and } F' \text{ two matrix}
\]

Vandermonde invertible therefore
\[ \text{rg}(C) = \text{card}\{j \in \{1,\ldots,n\}/v_j = 1\} = k \]

**Lemma**
For all \( i = 0,1,\ldots,2^n - 2 \), \( S_i = \sum_{j=1}^{n} v_i \alpha_j^i \) and
\[ \sigma(x) = \sum_{j=0}^{k} \sigma_j x^j \]

The solution \( \text{of system} \)
\[
\begin{bmatrix}
S_{2^n-2} & S_{2^n-3} & \ldots & S_0 & 0 \\
S_0 & S_{2^n-2} & \ldots & S_1 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
S_{2^n-3} & S_{2^n-4} & \ldots & S_{2^n-2} & \sigma_k
\end{bmatrix} = 0 \text{ of unknown } \begin{bmatrix}
\sigma_1 \\
\sigma_2 \\
\vdots \\
\sigma_k
\end{bmatrix} \text{ is unique.}
\]

**Proof**
Repeat the same proof as above we obtain the lemma
\[
\begin{bmatrix}
S_i & S_{i+1} & \ldots & S_0 \\
S_{i+1} & S_{i+2} & \ldots & S_1 \\
\vdots & \vdots & \ddots & \vdots \\
S_{i+n-1} & S_{i+n} & \ldots & S_{i+n-1}
\end{bmatrix} = \begin{bmatrix}
1 & 1 & \ldots & 1 \\
\alpha_1 & \alpha_2 & \ldots & \alpha_n \\
\alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1}
\end{bmatrix} \begin{bmatrix}
v_1 \alpha_1^i \\
v_2 \alpha_2^i \\
\vdots \\
v_n \alpha_n^i
\end{bmatrix}
\]

\[ \text{So } \text{rg}(C) = k \text{ then } \begin{bmatrix}
S_k & S_{k+1} & \ldots & S_0 \\
S_{k+1} & S_{k+2} & \ldots & S_1 \\
\vdots & \vdots & \ddots & \vdots \\
S_{k+n-1} & S_{k+n} & \ldots & S_{k+n-1}
\end{bmatrix} \text{ is invertible.} \]
\[ S_k \] is invertible then \[ \sigma_i \] is unique.

**Proposition**

For all \( i = 0, 1, \ldots, 2^m - 2 \), \( S_i = \sum_{j=1}^{n} v_j \alpha_j \) and

\[
\sigma(x) = \sum_{j=0}^{k} \sigma_j x^{k-j}
\]

and

\[
Q(x) = S_{2^n-2} + S_{2^n-3} x + \ldots + S_1 x^{2^n-3} + S_0 x^{2^n-2}
\]

\[
\begin{bmatrix}
S_{2^n-2} & S_{2^n-3} & \ldots & S_0 \\
S_{2^n-2} & S_{2^n-3} & \ldots & S_1 \\
\vdots & \vdots & \ddots & \vdots \\
S_{2^n-2} & S_{2^n-3} & \ldots & S_{2^n-2}
\end{bmatrix} = 0 \Rightarrow Q(\alpha') \sigma(\alpha') = 0
\]

\[
\forall i = 1, \ldots, 2^m - 2
\]

**Proof**

By lemma 4 we have

\[
\begin{bmatrix}
1 & 1 & 1 & \ldots & 1 \\
1 & 1 & 1 & \ldots & 1 \\
1 & 1 & 1 & \ldots & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
1 & 1 & 1 & \ldots & 1
\end{bmatrix} = \begin{bmatrix}
Q(1) \\
Q(0) \\
\vdots \\
Q(0)
\end{bmatrix} \Rightarrow
\begin{bmatrix}
0 \\
0 \\
\vdots \\
0
\end{bmatrix}
\]

therefore

\[
\begin{bmatrix}
\sigma(0) \\
\sigma(1) \\
\vdots \\
\sigma(0)
\end{bmatrix}
\]

**VIII – Our decoding algorithm**

The syndrome vector all received word not exceeding the correction capacity is calculated by simple matrix product control word received by the. We still have to find a method to calculate the extended syndromes. We must convert each element of \( F_{2^n} \) a column vector \( m \) component of \( F_2 \) taken with respect to a natural base \( \{1, \alpha, \ldots, \alpha^{m-1}\} \).

**Algorithm**

Input: \( \{S_{\lambda}^{\delta}\}_{\lambda=0,1,...,2^n-2} \)

Output: \( \{e_1, \ldots, e_m\} \)

for \( \lambda = 1, \ldots, m \)

\( Q(x) = S_{2^n-2} + S_{2^n-3} x + \ldots + S_1 x^{2^n-3} + S_0 x^{2^n-2} \)

for \( i = 1, \ldots, n \)

\( i \neq \alpha \Rightarrow e_i = 1 \) else \( e_i = 0 \)

for \( i = 1, \ldots, n \)

\( F_{2^n} \rightarrow F_{2^n} \left( e'_1, \ldots, e'_m \right) \rightarrow E_i \) and if

\( E_i = 0 \) then \( e_i = 0 \) else \( e_i = 1 \)
IX- Conclusion

Our approach overcomes the vulnerability of cryptosystems MC Eliece, incurred as information leakage, caused by the fact that the number of iterations in the Euclidean algorithm is influenced by the number of error bits that this cryptosystem must hide. This approach requires to find an effective method for calculate the syndromes of extended classical irreducible Goppa codes.

X- bibliographie

[1]: H. Gregor Molter, Marc Stottinger, Abdulhadi Shoufan, Falko Strenzke-2011 A simple power analysis attack on a McEliece cryptoprocessor

[2]: Daniel Augot Magali Bardet Jean-charles Faugère On the decoding of binary cyclic codes with the Newton identities 2009.

[3]: Magali Turrel Bardet Thes de doctorat de l’université Paris 6 Etude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie 2004.

[4]: Houssam Khalil Matrices structures et matrices de Toeplitz par blocs de Toeplitz en calcul numérique et formel Thèse de doctorat 2008 université Claude Bernard-Lyon1

[5]: Kequin Fenga, Lanju Xu Fred J. Hickernellb Linear error-block codes 2005

[6]: Error-Correcting Codes and finite Fields OliverPRETZEL Imperial college lo,ndon 1992

[7]: Quelques applications des transformations discrètes de Galois-Fourier aux codes de Goppa. Jean Conan Ecole polytechnique canada 1987.