Secure Cryptographic Scheme based on Modified Reed Muller Codes

Cheikh Thiecoumba Gueye and EL. Hadji Modou Mboup

*Département Mathématiques et Informatique, Université Cheikh Anta DIOP,
Dakar, Sénégal
Laboratoire LACGAA
cheikht.gueye@ucad.edu.sn, domboups@yahoo.fr*

Abstract

It is devised a new cryptosystem based on modified Reed Muller codes RM(r,m). The new cryptosystem is a modified version of Sidel'nikov's one. This allows to increase the security of the public key, and to reconsider Reed Muller codes as good candidates for using in secure encryption scheme. An efficient decoding with the Reed Muller decoding algorithm RM(r,m) and an increased level of security against attacks of the Sidel'nikov's crypto- system due to Minder and Shokrolahi are the main advantages of the modified version.

Adding new columns implies longer codes, but this would not be a problem for decoding or deciphering because in decode one has only to deal with the words of the secret code belonging to the Reed Muller code RM(r,m). So the decoding phase would not suffer from this modification.

Keywords: *McEliece cryptosystem, Minder and Shokrolahi attack, Reed Muller code*

1. Introduction

The cryptosystem of McEliece [20] has been created in 1978 and use the coding theory. In the original McEliece cryptosystem, the Goppa code is used. It is one of the cryptosystems, which is not yet broken and which does not depend on computations in the group Z/nZ. This system is not as popular as the others cryptosystems, because of the size of the public-key, which is very large. Many cryptosystems based on coding theory have been proposed and many have been broken. It is the case of the cryptosystem of Sidel'nikov [9]. This asymmetric cryptosystem replaces the Goppa codes with Reed-Muller codes. One of the advantages of using Reed Muller code is that efficient decoding algorithms are known for these codes. In [21] L. Minder and A. Shokrolahi present a structural attack again the Sidel'nikov cryptosystem. This attack uses the filtration proprieties of Reed Muller codes and the fact that minimum-weight words in RM(r,m) are products of r minimum-weight words in RM(1,m).

In this paper we present a method, based on modified Reed Muller codes, that allows to preventing against the cryptanalysis of L. Minder and A. Shokrollahi used in Sidel'nikov cryptosystem. Or equivalently, we show that the main properties that are exploited in the Minder and Shokrolahi attack are no longer satisfied if one adds a random matrix.

We improve the Sidel'nikov cryptosystem: from a generator matrix G of a Reed Muller code RM(r,m), $\mathrm{d} = 2^{\mathrm{m}} - \mathrm{r}$, we build a secret key which is a generator matrix of our new code, by adding to G RM(r,m) a $k \times n'$ random matrix. So we propose this modified version of Sidel'nikov which allows us to restore the use of advantageous Reed Muller codes.

For instance, the Reed Muller code RM(r,m) with length $\mathrm{n} = 2058$ $(\mathrm{m} = 11, \mathrm{r} = 3)$, $\mathrm{n}' = 10$ and dimension $\mathrm{k} = 232$, and number of errors t =400 (we use in this case the decoding algorithm of RM(3, 11) which allows to correct almost always 400 errors) has a very low probability ($\frac{1}{2^{2320}}$) to be broken by Minder and Shokrolahi attack. In this case the work factor (WF) of Minder and Shokrolahi attack is greater than 2^{88}.

2. Reed Muller codes

For further details the reader is referred to [18] or [8].

Definition 2.1 (Reed Muller codes)

The Reed Muller $[n, k, d]$ $-$code RM(r,m) is defined by two integers m and r ($0 \leq r \leq m$) and have length n, dimension k and minimal distance d, where $n = 2^m, k = \sum_{i=1}^{r} C_i^m$ and $d = 2^m - r$.

This code is the set of all the vectors of the form $V_f = (f(a_1), f(a_2), \dots, f(a_n))$ where f is a boolean polynomial in m variables, with degree less than r and where $(a_1, a_1, \dots, a_1) = IF_2^m$ is the set of all binary vectors of length m.

For Reed Muller RM(r,m) codes we have the following properties see [18] and [8] :

Proposition 2.2 (filtration)

For any m, we have

$$(0,1) = RM(0, m) \subseteq RM(1, m) \subseteq \cdots \subseteq RM(m-1, m) \subseteq RM(m, m) = IF_2^m.$$

Proposition 2.3 (Minimum-weight codewords)

Let $f \in RM(r, m)$ be a word of minimum weight.
Then there exist $f_1, f_2, \dots, f_n \in RM(1, m)$ such that

$$f = f_1 . f_2 . \dots . f_n .$$

The f_i are of minimum weight in RM(1,m).

3. The New Code

Definition 3.1 (New code)

Let C be a Reed Muller [n,k,d]-code RM(r,m) and A a $k \times n'$ random matrix, where n' is a nonzero integer. The new [n+n', k, d']-code, denoted $RM^{+}(r, m)$, is the code defined by the generator matrix $G^{r,m} = [G_r^m | A]$ where G_r^m is a generator matrix of the Reed Muller code RM(r,m).

Proposition 3.2 (Cracking filtration)

The probability to obtain

$$RM^{+}(0, m) \subseteq RM^{+}(1, m) \subseteq \cdots \subseteq RM^{+}(m-1, m) \subseteq RM^{+}(m, m)$$

is very low.

Proof: Let us assume that $G^{i,m}$ is the $k \times N$ generator matrix of the new code $RM^{+}(i, m)$ and $G^{i+1,m}$ the $k' \times N$ generator matrix of the new code $RM^{+}(i+1, m)$ (with $k = \sum_{j=0}^{i} C_j^m$, $k' = \sum_{j=0}^{i+1} C_j^m$ and $N = n + n'$ where $n = 2^m$ and n' a nonzero integer.

Set $G^{i,m} = [G_i^m|A_i]$ where G_i^m is the $k \times n$ generator matrix of the Reed Muller code RM(i,m) and A_i is the $k \times n'$ random matrix and $G^{i+1,m} = [G_{i+1}^m|A_{i+1}]$ where G_{i+1}^m is the $k' \times n$ generator matrix of the Reed Muller code RM(i + 1,m) and A_{i+1} the $k' \times n'$ random matrix .

Set H^i the $(N - k) \times N$ control matrix of the new code $RM^+(i,m)$ and H^{i+1} the $(N - k') \times N$ control matrix of the new code $RM^+(i+1,m)$.

Then $H^i = \left(\frac{H_0^i|N_0^i}{D_0^i|D_1^i}\right)$ where H_0^i is the $(n - k) \times n$ control matrix of the Reed Muller code RM(i,m), N_0^i the $(n - k) \times n'$ random matrix, D_0^i the $(N - n) \times n$ random matrix and D_1^i the
$(N - n) \times n'$ random matrix are created by the random matrix A_i,

And $H^{i+1} = \left(\frac{H_0^{i+1}|N_0^{i+1}}{D_0^{i+1}|D_1^{i+1}}\right)$ where H_0^{i+1} is the $(n - k') \times n$ control matrix of the Reed Muller code RM(i+1,m), N_0^{i+1} the $(n - k') \times n'$ random matrix, D_0^{i+1} the $(N - n) \times n$ random matrix and D_1^{i+1} the $(N - n) \times n'$ random matrix are created by the random matrix A_{i+1},

- Let x be a element of $RM^+(i,m)$, x is not an element of $RM^+(i+1,m)$
  if and only if $H^{i+1}({}^t x) \neq 0$

Let's compute $H^{i+1}({}^t x) =$:
Set $x = [x_0^i|x_{A_i}]$ where x_0^i is the codeword of the Reed Muller code RM(i,m), so this is a codeword of the Reed Muller code RM(i+1,m), and x_{A_i} is given by a linear combination of rows of the random matrix Ai.
We obtain :

$$H^{i+1}({}^t x) = \left(\frac{H_0^{i+1}|N_0^{i+1}}{D_0^{i+1}|D_1^{i+1}}\right)({}^t[x_0^i|x_{A_i}])$$

$$H^{i+1}({}^t x) = \left(\frac{H_0^{i+1} \times {}^t x_0^i|N_0^{i+1} \times {}^t x_{A_i}}{D_0^{i+1} \times {}^t x_0^i|D_1^{i+1} \times {}^t x_{A_i}}\right)$$

With $x_0^i \in RM(i+1,m)$ and then $H_0^{i+1} \times^t x_0^i = 0$

So $H^{i+1}({}^t x) = \left(\frac{0 \qquad |N_0^{i+1} \times {}^t x_{A_i}}{D_0^{i+1} \times {}^t x_0^i|D_1^{i+1} \times {}^t x_{A_i}}\right)$

Thus $H^{i+1}({}^t x) \neq 0$ if and only if $N_0^{i+1} \times^t x_{A_i} \neq 0$ or $D_0^{i+1} \times^t x_0^i \neq 0$ or $D_1^{i+1} \times^t x_{A_i} \neq 0$

Now let's find the probability to obtain $N_0^{i+1} \times^t x_{A_i} \neq 0$ or $D_0^{i+1} \times^t x_0^i \neq 0$ or $D_1^{i+1} \times^t x_{A_i} \neq 0$.

The matrices N_0^{i+1}, D_0^{i+1} and D_1^{i+1} are given by the random matrix A_{i+1}.
The filtration of the **proposition 2.2** cannot be applied if and only if

$$N_0^{i+1} \times^t x_{A_i} \neq 0 \text{ or } D_0^{i+1} \times^t x_0^i \neq 0 \text{ or } D_1^{i+1} \times^t x_{A_i} \neq 0$$

Let us prove that $N_0^{i+1} \times^t x_{A_i} = 0$, $D_0^{i+1} \times^t x_0^i = 0$ and $D_1^{i+1} \times^t x_{A_i} = 0$ $<=>$ $A_{i+1} = \left(\frac{A_i}{D}\right)$, where D is the $(n - k) \times n'$ matrix.

1. Suppose that $N_0^{i+1} \times^t x_{A_i} = 0 , D_0^{i+1} \times^t x_0^i = 0$ and $D_1^{i+1} \times^t x_{A_i} = 0$:

Then we have $H^{i+1}({}^t x) = \left(\frac{H_0^{i+1} \times^t x_0^i | N_0^{i+1} \times^t x_{A_i}}{D_0^{i+1} \times^t x_0^i | D_1^{i+1} \times^t x_{A_i}}\right)$

Finally

$$H^{i+1}({}^t x) = 0$$

Thus $x \in RM^+(i+1, m)$, but $x \in RM^+(i, m)$, which implies that $RM^i(i, m) \subseteq RM^+(i+1, m)$

So $A_{i+1} = \left(\frac{A_i}{D}\right)$.

2. Suppose that $A_{i+1} = \left(\frac{A_i}{D}\right)$,

We have $G^{i+1,m} = [G^{i,m} | A_{i+1}]$ with $A_{i+1} = \left(\frac{A_i}{D}\right)$ and $G_0^{i+1} = \frac{G_0^i}{D_0}$ **(cf. proposition 2.2**).

Then $G^{i+1,m} = \left(\frac{G_0^i}{D_0} | \frac{A_i}{D}\right)$ and we have $G^{i,m} = [G_0^i | A_i]$.

Let us put $D_1 = [D_0 | D]$

So we have $RM^+(i, m) \subseteq RM^+(i+1, m)$, and this implies that

$$N_0^{i+1} \times^t x_{A_i} = 0 , D_0^{i+1} \times^t x_0^i = 0 \text{ and } D_1^{i+1} \times^t x_{A_i} = 0$$

Set p the probability for $A_{i+1} \neq \left(\frac{A_i}{D}\right)$ and q the complementary probability (q = 1 − p).

Then the number of random matrix A_i is: $2^{n' \times k}$.

Thus $q = \frac{1}{2^{n' \times k}}$ and $p = 1 - \frac{1}{2^{n' \times k}}$.

Thus the probability to obtain the filtration is very low for some parameters of the code.

Example 3.3:

For a new code $RM^+(3, m)$, the following array describes the values of the probabilities p and q.

N	k	n'	p	q
1034 (m=10)	176	10	$1 - \frac{1}{2^{1760}} \cong 1$	$\frac{1}{2^{1760}} \cong 0$
2058 (m=11)	232	10	$1 - \frac{1}{2^{2320}} \cong 1$	$\frac{1}{2^{2320}} \cong 0$
1033 (m=10)	176	9	$1 - \frac{1}{2^{1584}} \cong 1$	$\frac{1}{2^{1584}} \cong 0$
2057 (m=11)	232	9	$1 - \frac{1}{2^{2088}} \cong 1$	$\frac{1}{2^{2088}} \cong 0$
1032 (m=10)	176	8	$1 - \frac{1}{2^{1408}} \cong 1$	$\frac{1}{2^{1408}} \cong 0$
2056 (m=11)	232	8	$1 - \frac{1}{2^{1856}} \cong 1$	$\frac{1}{2^{1856}} \cong 0$

n : length of the code $RM^+(r, m)$,

k : dimension of the code $\mathrm{RM}^{+}(\mathrm{r},\mathrm{m})$,
n' : number of columns of the random matrix A.

We notice that the probability $p \cong 1$ and the probability $q \cong 0$.

Then the **proposition 2.2** cannot be applied for the new code.

Proposition 3.4 Let G_r be the automorphism group of the RM(r,m) and G_r^{+} the automorphism group of the $RM^{+}(r,m)$. We have $G_r \subseteq G_r^{+}$.

Proof: Without lost of generality, a RM(r,m) code can be considered as a $RM^{+}(r,m)$ if the random matrix A is the null matrix.

Remark 3.5 (Comparison with Reed Muller codes)

- Unlike Reed Muller Codes, for the new codes, there are several codes for a given length and dimension. This fact is interesting for a cryptographic use.
- The number of correctable errors by the new codes has to be very large, which renders general linear decoding algorithms inefficient. this fact is a advantage of security over.
- The fact that $\mathrm{G_r} \subseteq \mathrm{G_r^{+}}$ (**Proposition 3.4**) render the attack which uses the support splitting algorithm [8] ineffective, likewise in the case of the Reed Muller codes.

4. The New Cryptosystem

This cryptosystem uses the new code defined above. We present in the sequel the algorithms for the new cryptosystem.

A. Generating keys algorithm:

1. Choose randomly a generator matrix G_m^r of the Reed Muller code RM(r,m),
2. Lay δ_0 the t-corrector decoding algorithm of the Reed Muller code RM(r,m).
3. Choose randomly a $\mathrm{k} \times \mathrm{n'}$ matrix A.
4. Build a generator matrix of the new code $\mathrm{G^{r,m}} = [\mathrm{G_m^r}|\mathrm{A}]$
5. Choose two matrices: S a non-singular $\mathrm{k} \times \mathrm{k}$ matrix and P a $\mathrm{N} \times \mathrm{N}$ permutation matrix where $\mathrm{N} = \mathrm{n} + \mathrm{n'}$.
6. Compute $\mathrm{G_p} = \mathrm{SG^{r,m}P}$.
   Then the keys of this cryptosystem are:
   - the public-key $\mathrm{P_k} = (\mathrm{G_p}, \mathrm{t})$,
   - the private-key $\mathrm{S_k} = (\mathrm{G^{r,m}}, \mathrm{S}, \mathrm{P}, \delta_0\ )$,
7. Return$\mathrm{S_k}$ and $\mathrm{P_k}$.

B. Ciphering algorithm:

```
1. input: $x, e$ and $G_p$  // x plaintext, e error and $G_p$ the public-key
2. output: c //c ciphertext
3. $c = xG_p + e$
4. Return c.
```

C. Deciphering algorithm:

```
1. input : c //ciphertext
2. output : x //the plaintext
3. $c' = cP^{-1}$ ,
4. Lay $c' = [c'^{r}_{0}|\square'_{\square^{\square}_{\square},}]$  //where $c'^{r}_{0}$ is the ciphertext of the Reed Muller code RM(r,m)
5. $x' = \delta_0(c'^{r}_{0})$ //Decode $c'^{r}_{0}$ by the algorithm $\delta_0$
6. $x = x'S^{-1}$ ,
7. Return x.
```

Remark 4.1: Adding a random matrix is not a problem for decoding or deciphering since in the decoding algorithm we decode the elements of the code-word belonging to the Reed-Muller code.

5. Attacks against the New Cryptosystem

A. Size of the key for the new cryptosystem :

This new cryptosystem is a variant of Sidel'nikov cryptosystem. Then we can compare the new cryptosystem with Sidel'nikov's one. For instance we take a Reed Muller code RM(3,m) and n'=10 for the new code. Therefore the following array describes this comparison:

……………….	N	K	Size of the key (bit)
Sidel'nikov cryptosystem	1024 (m=10)	176	10240
New cryptosystem	1034 (m=10)	176	10340
Sidel'nikov cryptosystem	2048 (m=11)	232	22528
New cryptosystem	2058 (m=11)	232	22638

N: the length of the code
$k = \sum_{i=0}^{r} C_i^m$: the dimension of the Reed Muller code RM(r,m)

n' The length of the random matrix.
In the sequel we give the security of the new cryptosystem.

B. Usual attack:

The basic security of codes based cryptosystems depend on the difficulty of the following two attacks :

- **Structural attacks**: Recover the secret transformation and the description of the secret code(s) from $\mathrm{P_k} = (\mathrm{G_p}, \mathrm{t})$.
- **Ciphertext-Only Attack**: Recover the original message from the ciphertext and the public-key.

The difficulty of the Ciphertext-Only Attack is related to the general decoding problem. However in general the difficulty of structural attacks is not related to any classic coding theoretic problem. It mainly depends on the class of codes and the secret transformation used.

1. Structural attacks:

These attacks permit to find the private key after that the public key is given.
One of the nice features of Reed-Muller codes for using in cryptographic scheme is the fact that they are weakly self-dual and thus optimally resistant to the support splitting algorithm [8] (SSA). The reason for that is that SSA has to compute the weight enumerator of the hull (intersection of the code with its dual) which is intractable for Reed-Muller code. This feature will be essentially unchanged with the Reed-Muller codes modified. These codes are also resistant to L. Minder and A. Shokrolahi attack [21]. In **Proposition 3.3**, we have proved that the filtration cannot work for the new cryptosystem. Since the heart of that attack is destroyed. By **Proposition 3.3** the probability to found the subcode $\mathrm{RM}^{+}(\mathrm{r}-1,\mathrm{m})^{\sigma}$ such that $\mathrm{RM}^{+}(\mathrm{r}-1,\mathrm{m})^{\sigma} \subseteq \mathrm{RM}^{+}(\mathrm{r},\mathrm{m})^{\sigma}$ is very low. So, the cryptanalysis of Sidel'nikov by Minder and Shokrollahi in [21] do not allow to reduce the order r of a code $\mathrm{RM}^{+}(\mathrm{r}-1,\mathrm{m})^{\sigma}$ in order to find $\mathrm{RM}^{+}(1,\mathrm{m})^{\sigma}$.

So, the most powerful structural attack procedure on this new cryptosystem is to remove the added coordinates in order to return to the original system and apply the Sidel'nikov cryptanalysis [9].

2. Cryptanalysis exploiting the added coordinates :

There are two differents ways to find the original system: **find the random matrix directly** or **distinguish the added positions from the others**.

- **Find the random matrix directly**: This attack consists to find the random matrix A in the generator matrix of the new code RM+. After finding A, we apply the same method that cryptanalysis of Sidel'nikov describe in [21]. There exist $\mathrm{C}_{\mathrm{n}'}^{\mathrm{N}}$ random matrices in the generator matrix of order (N × k). So the work factory (WF) is:

$$\mathrm{W} = \mathrm{C}_{\mathrm{n}'}^{\mathrm{N}}$$

In [21] the cost of the cryptanalysis of Sidel'nikov cryptosystem is:

$$\mathrm{CostSh} = 2^{-\frac{\mathrm{m}-\mathrm{r}+1}{\mathrm{m}-2\mathrm{r}+1}\times\frac{\mathrm{m}^{\mathrm{r}}}{\mathrm{r}!}\times\log_2(1-2^{-\mathrm{r}})-\mathrm{mr}+\mathrm{r}(\mathrm{r}-1)+(\mathrm{m}+\mathrm{r}^2+4\mathrm{r}+2)}$$

The cost of the cryptanalysis exploiting the random matrix is:

$$\mathrm{CostMG} = \mathrm{CostSh} + \mathrm{C}_{\mathrm{n}'}^{\mathrm{N}}$$

Now we compute the cost of the cryptanalysis with different parameters in the following array in order to give suggested parameters security.

Table 1. The code RM+(3, 10)

Parameters	WF	CostSh	CostMG
N=1034 (m=10), k=176 and n'=10	2^{78}	2^{36}	$\cong 2^{78}$
N=1035 (m=10), k=176 and n'=11	2^{85}	2^{16}	$\cong 2^{85}$

Table 5.2. The code RM+(3, 11)

Parameters	WF	CostSh	CostMG
N=2056 (m=11), k=232 and n'=8	2^{73}	2^{39}	$\cong 2^{73}$
N=2057 (m=11), k=232 and n'=9	2^{80}	2^{39}	$\cong 2^{80}$
N=2058 (m=11), k=232 and n'=10	2^{88}	2^{39}	$\cong 2^{88}$
N=2059 (m=11), k=232 and n'=11	2^{96}	2^{19}	$\cong 2^{96}$

- **Distinguish the added positions from the others by using the Hull dimension of the modified code:**

In general, added one coordinate to the Reed Muller-code will have as effect to reduce the hull dimension by the one unit. Someone can think that the Hull dimension of the modified code is $\mathrm{k} - \mathrm{n}'$. It is not so in general because the probability for it to be the case is weak. The probability P that the Hull dimension of the modified codes is equal to $\mathrm{k} - \mathrm{n}'$ is :

- if m > 2r + 1 : then the probability P is:

$$P = \frac{1}{2^{n' \times (k - n')}}$$

- if m < 2r + 1 : then the probability P is:

$$P = \frac{1}{2^{n' \times (n - k - n')}}$$

So, just observing the Hull dimension will not provided enough information to distinguish the added position from the others.

- **Distinguish the added positions from the others by using the public key $\boldsymbol{G_p}$:**

The probability P to find directly the added position by using a row of the public key $\boldsymbol{G_p}$ is

$$\boldsymbol{P(r,m,n') = \frac{n!}{A_N^n}}$$

Where $n = 2^m$ the length of the Reed Muller code RM(r,m) and $N = n + n'$ the length of the modified Reed Muller code $RM^+(r,m)$.

For example:

$$\boldsymbol{P(3,11,10) = \frac{2048!}{A_{2058}^{2048}} = 2^{-90}}$$

Remark 5.3: We suggest, to resist to the attack against the Sidel'nikov scheme, the $\left[n+n^{'},k,d^{'}\right] - code\ \ RM^+(r,m)$ with $(n^{'} = 10, m = 11\ and\ r = 3)$ or $(n^{'} = 10, m = 10\ and\ r = 3)$.

3. **Decoding attacks:**

Since the new codes can decode many more errors (decoding algorithm of Reed Muller codes), with high probability, than even the minimum distance of the code. Thus the direct decoding attack [12, 11] is impractical, including the low weight word finding algorithm [2].

6. Conclusion

We have presented a new scheme based on the Reed Muller code modified $RM^+(r,m)$. This allows to prevent against, our knowledge, the first known effective attack again Sidel'nokov's cryptosytem.

An efficient decoding with Reed Muller decoding algorithm RM(r,m) and an increased level of security against attack of Sidel'nikov's cryptosystem due to Minder and Shokrolahi are the main advantages of the modified version. This allows to reconsider Reed Muller codes as good candidates for using in cryptography. Adding new columns implies longer codes, but this would not be a problem for decoding or deciphering because in decoding one has only to deal with the words of the secret code belonging to the Reed Muller code RM(r,m). So the decoding phase would not suffer from this modification.

References

[1] E. R. Berlekamp, R. J. McEliece and H. C. A. V. Tilborg, “On the inherent intractability of certain coding problems”, IEEE Trans. Inform. Theory, vol. IT-24, **(1978)** May, pp. 384-386.

[2] A. Canteaut and F. Chabaut, “A new algorithm for finding minimum-weigth words in a linear code: application to primitive narrow-sense BCH-codes of length 511”, IEEE Transactions on information Theory, vol. 44, **(1998)**, pp. 367-378.

[3] W. Diffie and M. E. Hellman, “New direction in Cryptography”, IEEE Trans. Inform, Theory, vol. IT-22, **(1976)** November, pp. 644-654.

[4] I. Dumer, “Recursive decoding and its performance for low-rate Reed-Muller codes”, IEEE Trans. Info. Theory, vol. 50, no. 5, **(2004)** May, pp. 811-823.

[5] I. Dumer and K. Shabunov, “Recursive error correction for general Reed-Muller codes”, Discret Applied Mathematics, vol. 154, **(2006)**, pp. 253-269.

[6] H. Niederreiter, “Knapsack-type cryptosystems and algebraic coding theory”, Problems of Control and Information Theory, vol. 15, no. 2, **(1986)**, pp. 159-166.

[7] E. Prange, "The use of information sets in decoding cyclic codes", IEEE Transactions, vol. IT-8, **(1962)** September, pp. S5-S9.

[8] N. Sendrier, "Finding the permutation between equivalent linear codes: The support spliting algorithm", IEEE Transaction on Information Theory, vol. 46, **(2000)**, pp. 1279-1280.

[9] V. M. Sidelnikov, "A public-key cryptosystem based on binary Reed-Muller codes", Discret Math. Appl, vol. 4, no. 3, **(1994)**, pp. 191-207.

[10] A. Stern, "A method for finding codewords of small weight", in Coding Theory and applications, Lecture Notes in Computer Science, Springer-Verlag, vol. 388, **(1989)**, pp. 106-113.

[11] A. Becker, A. Joux, A. May and A. Meurer, "Decoding Random Binary Linear Codes in 2n/20: How 1 + 1 = 0 Improves Information Set Decoding", EUROCRYPT2012.

[12] A. Bernstein and T. Lange et C. Peters, "Attacking and defending the McEliece cryptosystem", Lecture Notes in Computer Science, PQCrypto 2008, Springer-Verlag, aout , vol. 5299, **(2008)**, pp. 31-46.

[13] T. A. Berson, "Failure of the McEliece public-key cryptosystem under messageresend and related-message attack", Lecture Notes in Computer Sciences, Advances in Cryptology-CRYPTO '97, aout, vol. 1294, **(1997)**, pp. 213-220.

[14] F. Chabaud, "Asymptotic analysis of probabilistic algorithms for finding short codewords", CISM Courses and Lectures-EUROCODE 92, vol. 339, **(1992)**, pp. 175-183.

[15] A. Canteaut, "Attaques de cryptosystèmes à mots de poids faible et construction de fonctions trésilientes", Ph.D. dissertation, Univ. Paris 6, **(1996)** October.

[16] A. Canteaut and H. Chabane, "A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem", EUROCODE 94, P. Charpin, Ed., INRIA, **(1994)** March.

[17] A. Canteaut and N. Sendrier, "Cryptanalysis of the Original McEliece Cryptosystem", Advances in cryptology-ASIACRYPT'98 Proceedings, Springer, janvier, **(1998)**, pp. 187-199.

[18] W. C. Huffman and V. Pless, "Fundamentals of Error-Correcting Codes", Cambridge University Press, **(2003)**.

[19] P. J. Lee et E. F. Brickell, "An observation on the security of McEliece's public-key cryptosystem", Lecture Notes in Computer Science, Advances in Cryptology-EUROCRYPT'88, Springer-Verlag, mai, vol. 330, **(1988)**, pp. 275-280.

[20] R. J. McEliece, "A public-Key cryptosystem based on algebraic coding theory", JPL DSN Progress Report 42-44, janvier, **(1978)**, pp. 114-116.

[21] A. Shokrollahi and L. Minder, "Cryptanalysis of the Sidel'nikov cryptosystem", 2007 IACR, Advances in cryptology-Eurocrypt 2007, LNCS, vol. 4515, Springer.

[22] N. Sendrier, "On security of the McEliece public-key cryptosystem", Proceeding of Worshop honoring Prof. Bob McEliece on his 60th birthday (M. Blaum, P.G. Farrell, and H. van Tilborg, eds.), Kluwer, **(2002)**, pp.141-163.

[23] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Code", North-Holland, **(1978)**.