Shorter keys for code based cryptography

Philippe Gaborit *

September 8, 2004

Abstract

In this paper we propose a method to shorten the size of public keys for code based cryptosystem like the McEliece scheme or the Niederreiter scheme. Starting from subcodes of the class of primitive BCH codes, we achieve a size of public key of $O(n)$ for n the length of the code and for a suitable security. The idea is based on the use of cyclicity and quasi-cyclicity of BCH codes. As an example we propose parameters value with key of size as low as 12 kilobits for length 2047 and 20 kilobits for length 4095.

1 Introduction

Since the introduction of public key cryptography in the 70's many cryptosystems have been proposed and many have been broken. The most used cryptosystems rely on number theory problem like the factorization problem or the discrete logarithm problem over suitable groups. The MacEliece cryptosystem [13] which was introduced by McEliece in 1978 relies on coding theory, it is one of the few cryptosystems, which is not broken and which does not rely on number theory. This system presents many advantages: it is very fast for both encryption and decryption and the best known attacks are exponential in the length of the code, but this system has a very important drawback which explains why it is not as popular as the other cryptosystems: the size of the public key, a generator matrix of a long code, is very large, at least several hundred thousand bits.

In this paper we propose a method to severely decrease the size of the public key for such systems, making the public key almost linear, with a small factor inferior to 6 for the examples we consider. The idea of our method consists in considering quasi-cyclic generator matrices of a code, so that rather than giving the whole permuted generator matrix, it is only sufficient to give a few rows from which the whole matrix can be derived. This method permits us to obtain public keys of size 12 kilobits for length 2047 and 20 kilobits for length 4095, far below the 500 kilobits for length 2047 needed for the actual cryptosystem to assure a good security.

The paper is organized as follow: we first recall basic facts about code based cryptography, we then introduce our method after recalling basic theory of quasi-cyclic codes, eventually we present new public key parameters after analyzing general existing attacks and specific attacks on our new key description.

*LACO, Université de Limoges, 123,av. A. Thomas, 87000 Limoges, FRANCE **Email: gaborit@unilim.fr**

2 Code based cryptography

In this section we recall basic facts about code based cryptography. We refer to the work of Nicolas Sendrier in [18],[19] for a more general context on these problems and to [14] for a general context on coding theory. Every public key cryptosystem has to rely on a 'hard' problem. In the case of coding theory, the main problem is:

Syndrome decoding (SD) problem:
Let H be a $r \times n$ binary matrix H, let s be an element of F_2^r and let w be a positive integer. Does it exist a word of F_n^2 of weight smaller or equal to w such that $Hx^T = s$?

This problem was proven to be NP-complete in [3].

2.1 Schemes

The first cryptosystem based on codes was introduced by McEliece in 1978 in [13], this system is based on the decoding problem, which can be seen as a particular instance of the SD problem, later in 1986 Niederreiter proposed in [15] an equivalent scheme based directly on the syndrome decoding problem. More recently a signature scheme also based on these problems was proposed by Courtois, Finiasz and Sendrier in [5]. We now briefly recall these schemes.

- McEliece scheme

Private key: C a binary $[n, k, d]$ t-error correcting linear code, with G a generator matrix of C, S a $k \times k$ non singular matrix, P a $n \times n$ permutation matrix.
Public key: $G' = SGP$.
Encryption: $x \to y = xG' + e$, where e is a random word of weight t.
Decryption: $y \to \Phi_C(yP^{-1})S^{-1}$, where $\Phi_C(z)$ is a decoding algorithm up to distance t.

- Niederreiter scheme

Private key: C a binary $[n, k, d]$ t-error correcting linear code, with parity check matrix H, S a $(n-k) \times (n-k)$ invertible matrix and P a $n \times n$ permutation matrix.
Public key: $H' = SHP$.
Encryption: $x \to y = H'x^T$, with x of weight t.
Decryption: Decode s in z, zP^{-1} gives x.

The family of code proposed by McEliece was the family of Goppa codes, which has a fast decoding algorithm in $O(tmn)$ binary operations and many different codes with the same parameters. These codes can also be used for the Niederreiter system. The security of these two cryptosystem has been proven equivalent in [11] and rely on the difficulty to decode to solve an instance of the decoding problem and on the difficulty to recover the underlying structure of the permuted code.

- Signature scheme of Courtois, Finiasz and Sendrier

Constructing a signature scheme for codes is not as natural as for the RSA cryptosystem since the decoding operation is not reversible in the way that it is possible to decode a random element of the whole space only if this element is at a decodable distance of the code. In general the proportion of such decodable elements is very low. The scheme they propose uses long Goppa codes with small error-correcting capacity t, in that case the proportion of decodable words of the whole space is roughly $\frac{1}{t!}$. The signature scheme consists then in concatening to a hash of the message $h(M)$, a sequence of increasing elements $0, 1, 2, \cdots, i$: $h(M), i$, and compute the hash value until a hash value $h(h(M), i_0)$ corresponds to a decodable codeword. The signature is then the decoded codeword associated to the hash value $h(h(M), i_0)$. The parameters they consider are $n = 2^{16} - 1$ and $t = 9$.

2.2 Usual attacks

There are two kinds of attacks: attacks which try to decode directly a message or structural attacks which try to recover the structure of the code.

2.2.1 Decoding attack: Information Set Decoding

The most efficient algorithms in our case are based on the information set decoding. A first analysis was done by MacEliece in [13], then by Lee and in Brickell in [9] and also by Stern in [22] and Leon in [10] and at last by Canteaut and Chabaud in [4].

Consider a $[n, k, 2t+1]$ binary code, if one uses information set decoding, one chooses a random set of k columns, an error is decodable when its support does not meet the k random columns. The probability for an error to be decodable (see [19] for more details) is then $P_{dec} = \frac{\binom{n-k}{t}}{\binom{n}{t}}$, which leads with the usual binomial approximation to a probability:

$$P_{dec} = O(1).2^{-nH_2(t/n)-(1-k)H_2(t/(n-k))},$$

for $H_2(x) = -xlog_2(x) - (1-x)log_2(1-x)$.
Then the estimated work factor WF to find a word of weight t can be estimated as follow:

$$WF = \frac{P(k)}{P_{dec}},$$

where $P(k)$ corresponds to the cost of a Gaussian elimination, $P(k)$ can be first thought as a cost in $O(k^3)$, in fact the different improvements of the method dealt with improvement of this factor and in the best improvement of [4] one can consider $P(k)$ linear or even less. For the parameters we consider it is reasonable to consider it linear to fit the practical results of [4]. This algorithm is currently the best known.

2.2.2 Structural attacks

Structural attacks consist in recovering directly the original code from the permuted matrix. It was successfully done by Sidel'nikov and Shestakov in [21] for Generalized Reed-Solomon (GRS) codes and by Sendrier in [16] for concatened codes.

Another powerfull attack permits to recover the permutation between two equivalent codes, this algorithm developped by Sendrier in [17] is called the Support Splitting Algorithm and has a complexity related to the dimension of the hull of a code: the intersection of a code and its dual.

Note that this attack does not apply for Goppa codes although the dimension of their hull is small since there are many Goppa codes and since one does not know which Goppa code is used first. Meanwhile if one is to consider a unique code as it was proposed by Sidel'nikov with the Reed-Muller code in [20], the code must necessarily have a big hull to resist this attack.

For the family of Goppa codes an attack was proposed by Gibson in [7] and later improved by Loidreau and Sendrier in [12], which by the exhibition of special permutation groups permit to divide the total number ($n!$) of permutations to test by a factor mn or mn^3.

3 Shortening the size of the public key

We now explain our method to shorten the size of the public key. We first recall basic facts about quasi-cyclic codes.

3.1 Quasi-cyclic codes

Definition 3.1 *A code of length n is called quasi-cyclic of order s, for n a multiple of s if every cyclic shift of a codeword by s coordinates is again a codeword.*

Remark 1: A cyclic code is a quasi-cyclic code with $s = 1$.
One deduces the straightforward lemmas:

Lemma 3.2 *If C is a cyclic code of length n then C is also quasi-cyclic of order s, for any s which divides n.*

Lemma 3.3 *If C is a quasi-cyclic code of order s, then $C^\perp$ is also quasi-cyclic code of order s.*

Proof. It is deduced from the fact that a code and its dual have the same automorphism group.
□
We now consider a particular generator matrix of a quasi-cyclic code.

Proposition 3.4 *Let C be a $[n,k]$ quasi-cyclic code of order s with $n = rs$ then there exists a $k' \times n$ matrix G (with $k' \geq k$), which generates C of the form:*

$$G = \begin{pmatrix} A_1 & A_2 & A_3 & \cdots & A_r \\ A_r & A_1 & A_2 & \cdots & A_{r-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_2 & A_3 & A_4 & \cdots & A_1 \end{pmatrix},$$

where the A_i are $\frac{k'}{r} \times s$ matrices.

Proof. The proof works by induction. Starting from a nul $(1, n)$ matrix G^0, one considers a random word $c = (c_1, \cdots, c_n)$ of C.
Separating c into $r = \frac{n}{s}$ equal parts: $(c_1, \cdots, c_s), (c_{s+1}, \cdots, c_{2s}), \cdots, (c_{n-s+1}, \cdots, c_n)$, one constructs the $(1, s)$ matrices $A_i^1 = (c_{s(i-1)+1}, \cdots, c_{si})$, $1 \leq i \leq r$, obtained by r cyclic shifts. One then considers the matrix G^1:

$$G^1 = \begin{pmatrix} A_1^1 & A_2^1 & A_3^1 & \cdots & A_r^1 \\ A_r^1 & A_1^1 & A_2^1 & \cdots & A_{r-1}^1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_2^1 & A_3^1 & A_4^1 & \cdots & A_1^1 \end{pmatrix},$$

Now G^1 generates a code C_1, if $C_1 = C$ then one stops, else one considers a codeword c_2 of C which does not belong to C_1. Separating again c_2 in s equal parts we add a second row to the matrices A_i^1 to obtain the matrices A_i^2. One then considers the matrices $G^2, G^3, \cdots, G^j$ and so on. Since the rank of the matrices G^j increases strictly with j, it will stop for a certain j_0 satisfying $k' = j_0.r \geq k$ since G^{j_0} generates C. Note that j_0 may vary and depends on the random elements $c_1, c_2, \cdots$. $\square$

Remark 1: The previous form of the generator matrix implies that it is sufficient to know the matrices $A_1, \cdots, A_r$ to derive the whole matrix G.
Remark 2: The matrix G generates the code C but is not necessarily a generator matrix of C since k' may be greater than k.

We now explain how to construct quasi-cyclic subcode of order s from a quasi-cyclic code of order s.

Proposition 3.5 *Let C be a $[n, k]$ quasi-cyclic code of order s with $n = rs$ then there exist quasi-cyclic subcodes strictly included in C of order s with dimension greater or equal to $k - r = k - \frac{n}{s}$.*

Proof. If C is quasi-cyclic of order s then the dual $C^\perp$ of C is also quasi-cyclic of order s. Now take a random codeword x of $F_2^n - C^\perp$ and consider the generator matrix G_x obtained by adding x and its $r - 1$ s-shifts to a generator matrix of $C^\perp$. The code C_x generated by G_x is then by construction quasi-cyclic of order s and dimension at most $n - k + r$. The dual of $C_x^\perp$ is then quasi-cyclic of order s with the announced dimension. $\square$

Proposition 3.6 *Let C be a s quasi-cyclic $[n, k, d]$ code, then at least 2^{k-r} distinct codes can be constructed by Proposition 3.5.*

Proof. The previous proposition explains how it is possible to construct a quasi-cyclic subcode of C with dimension at least $k - r$. Counting the different distinct subcodes is equivalent to counting the distinct duals of these codes. The dual code has dimension at most $n - k + r$. Now the union of all the possible dual has to be the whole space, therefore since each code has dimension at most $n - k + r$ there are at least $2^{n-(n-k+r)} = 2^{r-k}$ distinct such quasi-cyclic subcodes. $\square$

3.2 A new way to describe the public key

In this section we apply the quasi-cyclic property to shorten the size of a key.
For code based cryptosystems, the public key consists in a particular generator matrix of a code $C[n,k,d]$ permuted on its coordinates, and the whole matrix has to be known, so that the size of the key is $k(n-k)$ bits for a generator matrix in systematic form. To be sure to resist to attacks, the necessary values of n and k lead to a size of key which is too big for many applications.
Now our idea consists in starting from a quasi-cyclic code and use the fact that the generator matrix can be described with less information. Indeed, let C be a quasi-cyclic code of order s. From Proposition 3.4 it is possible to associate to C a matrix G, which can be described as in the proposition with the r sub matrices $A_1,\cdots,A_r$ of size $\frac{k'}{r}\times s$. Now consider a given permutation π on s coordinates and apply it on the r sets of s coordinates $(1,\cdots,s),\cdots,(n-s+1,\cdots,n)$. The matrix G is changed into a matrix G', which can still be described because of the particular structure of G, only with the knowledge of the action of the permutation π on the A_i:$A_1\pi,\cdots,A_r\pi$.
Let us denote by Π the permutation matrix which acts on the sequences of s coordinates:

$$\Pi=\begin{pmatrix} \pi & 0 & \cdots & 0 \\ 0 & \pi & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \pi \end{pmatrix},$$

The knowledge of the $A_1\pi,\cdots,A_r\pi$ permits to retrieve the whole matrix G':

$$G'=\begin{pmatrix} A_1\pi & A_2\pi & A_3\pi & \cdots & A_r\pi \\ A_r\pi & A_1\pi & A_2\pi & \cdots & A_{r-1}\pi \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_2\pi & A_3\pi & A_4\pi & \cdots & A_1\pi \end{pmatrix},$$

So for our scheme we propose to start from a quasi-cylic code of order s and to consider a random permutation π on s coordinates, the public key consists only the knowledge of the matrices $A_1\pi,\cdots,A_r\pi$, rather than the whole matrix.
So this way of considering the key permits to have a public of size $n\frac{k'}{r}$, with k' in general close to k, to be compared to $n(n-k)$.

An extraction procedure:
Note that for all the schemes we consider, both sides have to start from the same matrix. In our case the expansion of the public key to the matrix G' does not necessarily lead to a matrix with exactly k rows, the dimension of the code. So to extract the matrix M which will actually be used for the encryption as xM, from the $A_1\pi,\cdots,A_r\pi$, one has to do it in particular way.
Consider v_1 the codeword of G' constructed from the concatenation of the first rows of $A_1\pi,\cdots,A_r\pi$, now consider the matrix M_1 consisting of the vector v_1, consider then the vector v_1' obtained by shifting all the coordinates of v by s coordinates, if v_1' does not belong to the code generated by M_1 then one considers the new matrix M_2 obtained by adding the row v_1' to M_1 else we take M_2

equal to M_1. Repeating the process $r = \frac{n}{t}$ times by shifting v_1 by is coordinates for $1 \leq i \leq r$, one obtains a matrix M_r, then one consider the vector v_2 obtained from the second row of the concatenation of the matrices $A_1\pi, \cdots, A_r\pi$, one then adds one by one all the s shifts of v_2, checking each time whether the dimension of the matrix M_i increases. One repeats the process up to the last row of the concatenation of the A_i. This process leads necessarily to a unique matrix M with k rows and n columns which generates the permuted code C and is used to send the message.

Remark: the same method applies, if the dual code rather than the code is considered. One extracts a generator matrix for the parity check in the special form described earlier. Then it is possible to apply a Gaussian elimination to this matrix from which one may deduce a generator matrix for the code in a unique way.

3.3 New scheme

We now describe the variation on the classical McEliece with this new key.

- **Key creation:**

Let C be a $[n, k, d]$ s-quasi-cyclic code.
Choose a random permutation π on s coordinates.
Construct a (n, k') matrix G associated to C as in Proposition 3.4. Apply the permutation Π to G and construct $G' = G\Pi$. The public key K_P consists in the first $\frac{k'}{r}$ rows of G', the number of decodable errors t and the order of quasi-cyclicity s. The secret key is the permutation π.

- **Encryption:**

From the public key, one recovers the matrix G' by quasi-cyclicity. One then extracts the encryption matrix M from G' as in the extraction procedure previously described.

Now one proceeds as usual, let x be the message, send $c = xM + e$, where e is an error vector of appropiate weight.

- **Decryption:**

Extract the matrix M from the public key K_P. As usual, apply Π^{-1} to c, find $xM\Pi^{-1} + e\Pi^{-1}$, decode $xM\Pi^{-1} + e\Pi^{-1}$ in $xM\Pi^{-1}$, recover x from M.

Remark : Note that the extraction procedure has only to be done once.

3.4 Choice of type of codes

Now in order to apply our scheme one has to find a family of codes which is s quasi-cyclic and which resists to known attacks. We propose to start from the family of BCH codes, and in particular from the primitive BCH codes of lengths $n = 2^m - 1$. The set of codes we consider will consist in the set of s quasi-cyclic subcodes of a given BCH $[2^m - 1, k, 2t+1]$ constructed as in Proposition 3.5.

This family presents all the properties we are searching for:
- these codes are s quasi-cyclic with s divides $2^m - 1$,
- there are many of them: more than 2^{k-r} by Proposition 3.6,
- they can be decoded very quickly in $O(tmn)$ elementary operations.

Remark 1: the idea of considering subcodes of a code to mask the structure was also used in [2] to counter the Sidel'nikov Shestakov attack on GRS codes.

Remark 2: one may also choose to iterate anew the algorithm of Proposition 3.4 to obtain an even more important set of quasi-cyclic subcodes, meanwhile the drawback is that it decreases both the security and the transmission rate.

Remark 3: One could also start from the family of Reed-Muller codes, but they propose less choices of parameters and the decoding algorithm is not so obvious as for BCH codes. Another possibility would be to consider a large non trivial subfamily of quasi-cyclic Goppa codes, but for now, no such family has been described in the litterature.

4 Security of the new key

As we saw previously two kind of attacks have to be considered: direct decoding attacks on the message and structural attacks.

4.1 Attack on the message

As we saw in a previous section the best known algorithms to decode are exponential, and are all based on information set decoding. In our case the only new things the attacker knows is the quasi-cyclicity of the code, but this does not help for information decoding attack since one has to consider random information sets, and since the algorithm relies on finding random information sets, the knowledge of the quasi-cyclicity does not seem to be of any particular use to do that. Then the estimated work factor WF to decode an error of weight t remains as previously mentionned in Section 4.2.

4.2 Structural attacks

4.2.1 Attack on the size of the key

The first natural attack is related to the number of possible keys. In our case, for quasi-cyclic codes of order s, one chooses a permutation on s coordinates, therefore the number of keys is $s!$, then for each key one has to test whether this key is the good one and this surely asks to compare two rows or two columns of the code, so a factor k should be added. So the complexity of the attack should be at least in $k.s!$ elementary operations.

4.2.2 Support puncturing attack

This attack is specific to our construction and was found by T. P. Berger [1].
Let us denote by s-sets S_i the r possible sets of columns of the form $\{si+1, \cdots, si+s\}$ for

$0 \leq i \leq r-1$. From the very definition of the permutation Π, one deduces that if one punctures the permuted code on some s-sets, this punctured code will also be equivalent through a repetition of the small permutation π to the non-permuted code punctured on the same s-sets, with the same property for the dual of the permuted code.
In our case the attacker does not know the initial subcode used and can possibly not test them all since there are too many of them. Meanwhile if the attacker punctures particular combinations of s-sets, he will decrease the length of the code to attack. If the punctured code is equal to the whole space then the attacker will deduce no information, so the punctured code has to be at least of co-dimension one to be of practical interest. Nonetheless for the parameters we will consider a simple dimension analysis of the punctured dual shows that in that case there are still at least 2^r codes to test, which makes the attack infeasable for $r \geq 80$.

Remark : this attack would be very efficient if we only considered a BCH code: although the BCH by itself resists the support splitting algorithm since it has a big hull, this is not the case of the punctured dual of BCH codes.

4.2.3 Gibson attack

For the key construction we propose, the set of possible secret permutations has the very special form of the permutation Π, which corresponds to a repetition of S_s, the symmetric group acting on s elements. The special permutation group exhibited by Gibson belongs to the much more bigger group S_n, and has no reason to belong to the repetition of S_s.

4.2.4 Translating to F_2^r

Quasi-cyclic codes have been considered for a long time, and it is well known that there is a link between quasi-cyclic codes of order s and length n with codes over F_2^r, for $r = \frac{n}{s}$. In particular this approach was used by C. Huffman in [8] to construct good self-dual binary codes from self-dual codes over F_2^r for a special scalar product. The attack would then consist in translating the decoding attack on the binary code to an attack over shorter code of length $\frac{n}{r}$ over F_2^r. But this attack does not seem to apply since over F_2, the number of error is high and will therefore lead to a big number of errors for the code over F_2^r, beyond the decoding capacity of such a code.

4.2.5 Quasi-cyclic decoding

Another kind of structural attack would be to consider the quasi-cyclic codes as a concatenation of several cyclic codes of length r and decode the errors separately for each cyclic code. This approach may work of course but only for codes with very low rate which is not the kind of parameters we consider. As far as we know there is no general 'good' decoding algorithm for quasi-cyclic codes
One may also think to the attack developped by Sendrier for concatenated codes but this attack relied on the fact that these codes have small words in their dual which is not the case for BCH codes and has no reason to be the case for a random quasi-cyclic subcode.

5 Applications and new parameters

In this section we give new parameters derived from the new way of describing the key.
We consider primitive BCH codes since we obtained codes with better parameters than with non primitive BCH codes.
In the following, message security consists in the complexity of the decoding attack and structural security consists in the minimum cost of testing all possible permutation keys or the cost of the support puncturing attack.
When constructing the quasi-cyclic form of the matrix, the number of rows will vary with the A_i considered. We will denote by the *matrix generation order* the number of rows of the A_i, this number is necessarily greater than $\frac{k}{r}$. In the following we give the number we found after a few trials of the algorithm of Proposition 3.4.
Of course it is possible to give many parameters, we try to emphasize solution with small size of key. The public key corresponds to the dual of the code considered. The transmission rate corresponds to k/n.
In the following we give two sets of parameters A and B. The set of parameters A corresponds to a public key of 20 kbits and has strong security parameters. The set of parameters B has a key of shorter size, 12 kbits but with tight security parameters.

- McEliece scheme

Security Parameters A : $n = 4095, t = 26, s = 45$.
Parameters of the code:$[4095, 3692, 53]$
Matrix generation order: 5
Public Key: 20475 bits
Transmission rate: 0.9
Message security : 2^{100}
Structural security : 2^{91}

Security Parameters B : $n = 2047, t = 31, s = 23$.
Parameters of the code:$[2047, 1617, 63]$
Matrix generation order: 5
Public Key: 12282 bits
Transmission rate: 0.79
Message security : 2^{80}
Structural security : 2^{85}

- Niederreiter scheme

For this scheme the type of public key used is the same than for McEliece cryptosystem.

6 Conclusion and perspective

We have presented a method which reduces in an important way the size of the public key cryptosystem for the McEliece and the Niederreiter schemes. Our method uses a very large set of subcodes of a given BCH code as a large set of Goppa codes is used in the original McEliece scheme.

Now a question arise concerning the signature scheme proposed by Courtois, Finiasz and Sendrier: the method cannot by applied as such since their signature scheme relies heavily on the fact that a random codeword has a probability $\frac{1}{t!}$ to be decoded. The method we propose decreases the dimension of the code used by r which makes the probability to decode a random codeword too small.
Meanwhile the construction of a random quasi-cyclic subcode may be done in another way than in Proposition 3.5: one may start directly from the BCH code and add r random shifted codewords one after the other. One then directly constructs a nested sequence a quasi-cyclic codes included in the initial BCH code. In fact practical implementation of this method shows that depending on the parameters of the BCH code, it is possible to construct quasi-cyclic subcodes of the BCH code with small co-dimension (typically 1 or 2) rather than r. Meanwhile we could not prove that in this case the number of such quasi-cyclic subcodes is still very big, although we conjecture it is.

If one were able to show that the number of such code is still very big, it would permit to construct keys with paramaters respectively 16 kbits and 10 kbits rather than 20 kbits and 12 kbits.

It would also permit to adapt our method to the signature scheme of Courtois, Finiasz and Sendrier, indeed in that case considering a subcode with a small codimension will only decrease the probability of decoding a random codeword by a small factor. But it would permit either to shorten the size of the key for the scheme they propose ($m = 16, t = 9$) from 8 megabits to approximatively 128 kbits, or either to keep a big size of key but with smaller t which would considerably decrease the time of computation (less than one second) of the signature ($m = 18, t = 7$ or $m = 20, t = 6$).

ACKNOWLEDGEMENT

We thank T. Berger and G. Kabatiansky for helpful discussions.

References

[1] T. P. Berger, private communication.

[2] T. P. Berger and P. Loidreau, How to mask the structure of codes for a cryptographic use, to in *Designs, Codes and Crypt.*. ,

[3] E. Berlekamp, R. McEliece and H. van Tilborg, On the inherent intractability of certain coding problems, IEEE Transactions on Information Theory, IT-24(3) (1978).

[4] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to primitive narrow-sense BCH codes of length— 511. IEEE Transactions on Information Theory, IT-44(1998), 367-378.

[5] N. Courtois, M. Finiasz and N. Sendrier, How to achieve a MCEliece based digital signature scheme. In Advances in Cryptology-ASIACRYPT 2001, Springer-Verlag.

[6] E. Gabidulin, A. Paramonov and O. Tretjakov, Ideals over a non commutative ring and their application to cryptology. In Advances in Cryptology-EUROCRYPT 1991, D. Davies, Ed. New York: Springer-Verlag,pp.482-489.

[7] J. K. Gibson, Equivalent Goppa codes and trapdoors to McEliece public key cryptosystem, In Advances in Cryptology-EUROCRYPT 1991, D. Davies, Ed. New York: Springer-Verlag,pp. 517-521.

[8] W. C. Huffman,*Automorphisms of codes with applications to extremal doubly even codes of length* 48, IEEE Trans. Inform. Theory 28 (1982), no. 3, 511–521.

[9] P. Lee and E. Brickell, An observation on the security of MacEliece's public-key cryptosystem, in Advances in Cryptology-EUROCRYPT '88, C. Gunter, Ed. New York: Springer-Verlag, 1988, pp. 275-280.

[10] J. Leon, A probabilistic algorithm for computing minimum weights of large error correcting codes, IEEE Trans. on Information Theory, IT-34 (1988) pp. 1354-1359.

[11] Y. Li, R. Deng and X. Wang, On the equivalence of McEliece's and Niederreiter's cryptosystems, IEEE Trans. on Information Theory, IT-40 (1994) pp. 271-273.

[12] P. Loidreau and N. Sendrier, Weak keys in McEliece public key cryptosystem, *IEEE Trans. Inf. Theory*, (2001).

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

[14] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland (1977).

[15] H. Niederreiter, Knapsack-type cryptosystems and algebraic coding theory, *Prob. Contr. Inform. Theory*, vol 15, n 2, (1986), pp. 157-166.

[16] N. Sendrier, *On the concatened structure of a linear code*, Jour. Appl. Alg. Err. Corr. Codes, vol. 9, n.3, (1998),pp. 221-242.

[17] N. Sendrier, Finding the permutation between equivalent codes: the support splitting algorithm, *IEEE Trans. Inf. Theory*, vol. 46, n.4 , pp. 1193-1203.

[18] N. Sendrier, *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs*, Mémoire d'habilitation, Inria 2002, available at: http://www-rocq.inria.fr/codes/Nicolas.Sendrier/pub.html

[19] N. Sendrier, On the security of the McEliece public-key cryptosystem, In: M. Blaum, P.G. Farrell and H. van Tilborg, editors, Information, Coding and Mathematics , pages 141-163. Kluwer, 2002.

[20] V. M. Sidel'nikov, *A public-key cryptosystem based on Reed-Muller codes*, Discr. Math. Appli., vol 4, n.3, (1994), pp. 191-207.

[21] V. M. Sidel'nikov and S. O. Shestakov, *On cryptosystem based on general Reed-Solomon codes*, Discrete Mathematics (in Russian), vol. 4, n.3, (1992), pp. 57-63.

[22] J. Stern, A method for finding codewords of small weight, Coding theory and applications (Toulon, 1988), 106–113, Lecture Notes in Comput. Sci., 388, Springer, New York, 1989.