Lightweight code-based identification and signature

Philippe Gaborit
XLIM-DMI, Université de Limoges,
123 av. Albert Thomas,
87000, Limoges, France
Email: gaborit@unilim.fr

Marc Girault
France Télécom Division R&D
42 rue des Coutures,
14066 Caen, France
Email:marc.girault@orange-ftgroup.com

***Abstract*— We revisit the code-based identification protocol proposed by Stern at Crypto'93, and give evidence that the size of public keys can be dramatically reduced while preserving a high and well-understood level of security. More precisely, the public keys can be made even shorter than RSA ones (typically 347 bits), while their size is around 150 Kbits in the original scheme. This is achieved by using matrices which are double circulant, rather than purely random. On the whole, this provides a very practical identification (and possibly signature) scheme which is mostly attractive for light-weight cryptography.**

I. Introduction

As cryptography is more and more widely used in the real world, there is a strong need for public key schemes which are not based on number theory.

Firstly because it would be unreasonable to put all one's eggs in the same basket. At the time, nearly all public key cryptographic products are based on integer factorization or discrete logarithm. If a polynomial algorithm happened to be discovered for one these problems, the situation would become highly critical (notice that it would be the case if a quantum computer could be built).

Secondly, even if the above mentioned problems remain hard, practical progress in factorization and discrete logarithm computation leads to choose larger and larger keys.

Finally, arithmetic-based cryptography is slow, because it involves large exponentiations of large numbers. This makes it inappropriate to low-cost devices (such as smart card without cryptoprocessors), which require so-called light-weight cryptography.

In this paper, we consider another type of alternative cryptography, based on error-correcting code theory, and more specifically identification (or authentication) protocols , in which a prover proves to a verifier that he is who he claims to be. Code-based cryptography was initiated a long time ago with the celebrated McEliece encryption algorithm. Roughly speaking, this kind of cryptography has the same drawbacks as multivariate cryptography : the (also bit-based) computations are very fast, while public keys are large. Recently, Gaborit ([6]) has proposed a way to reduce the McEliece public key, decreasing its size from typically 500 Kbit to "only" 12 Kbit.

At Crypto'93, Stern proposed a new scheme, which is still today the reference in this area. The Stern's scheme is a multiple round zero-knowledge protocol, where each round is a three-pass interaction between the prover and the verifier. This protocol is similar in principle to factorization-based Fiat-Shamir's one, except that the cheater success probability is 2/3 at each round, instead of 1/2. Note that, in 1987, Guillou and Quisquater proposed a Fiat-Shamir variant in which only one round is required.

Stern's scheme is very nice but has two drawbacks : a) many rounds are required (typically 28 if we want the cheater success probability to be less than 2^{-16}), and b) the public key is very large, typically 150 Kbit). Unfortunately, the first drawback seems to be inherent to the usage of error-correcting codes, and the problem of deriving a "Guillou-Quisquater-like" variant of Stern's scheme is still open.

The second issue was first addressed in part by Veron, who worked with the generator matrix of the code rather than with on its dual matrix, and also proposed a specific construction of the public key which makes it much smaller. Unfortunately the coding theory problem on which security of this public key relies is somewhat unclear.

Here, we propose two new constructions of the Stern's scheme keys, one construction replaces a random matrix by a double circulant matrix and the other embedds directly the secret key in the public key. These constructions have the two following advantages : a) their security relies on a problem which is related to well known and well studied codes, namely the double circulant codes, so that security is much easier to appreciate (note that the NTRU cryptosystem uses a similar idea), and b) the size of the public key is very low, only 347 bits in a typical set-up, still smaller than in arithmetic-based cryptographic systems (note that the private key is also relatively small, typically 694 bits). Moreover the cyclic structure we use, makes the implementation easy and efficient, since the product of a circulant matrix and a vector can be obtained by multiplying only the first row of the circulant matrix with shifts of the vector.

These features make our variant highly attractive for light-weight implementations, especially in environments where memory (RAM, PROM etc.) is a rare resource, e.g. a smart card, and where authentication can be achieved gradually, e.g. in pay TV or in systems where a machine (e.g. a copy printer or a coffee dispenser) wants to authenticate a physical resource (e.g. an ink or coffee cartridge). Moreover, by using the so-called Fiat-Shamir paradigm, it is theoretically possible to convert Stern's protocol into a signature scheme, even if it is practically questionable, since the signatures are around

120Kbit-long.

The organisation of the paper is as follows : in Section 2 we recall main tools of code-based cryptography, then we explain in Section 3 how to decrease the size of keys by using double circulant codes. In Section 4 we consider the security of this new key construction, while Section 5 compares the performances of the new protocols with previous ones, and finally provide a conclusion in Section 6.

II. Code-based cryptography

In this section we recall basic facts about code-based cryptography. We refer to the work of Nicolas Sendrier in [12] for a more general context on these problems and to [9] for a general context on coding theory.

A. A hard problem

Every public key cryptosystem has to rely on a hard problem. In the case of coding theory, the main problem used is:

Problem: SYNDROME DECODING (SD)

Instance: An $m \times n$ matrix H over F_q, a target vector $s \in F_q^m$ and an integer $w > 0$.

Question: Is there a vector $x \in F_q^n$ of weight $\leq w$, such that $Hx^T = s^T$?

This problem was proven to be NP-complete in [1].

B. Stern identification scheme

In this section we recall Stern scheme [13], notice that we also considered our construction with Veron's scheme but we do not mention it in this short version [14]. In the following '+' stands for bit-wise modulo 2 addition.

Let H be a $(n-k) \times n$ binary matrix. The private key of the system is x, an element of F_2^n of Hamming weight $w > 0$, the public key s is then constructed as the syndrome associated to x:

$$s^T = Hx^T.$$

The protocol operates as follows:

1. The prover P randomly chooses a word y of length n and a permutation σ on $\{1, \cdots, n\}$. He then sends to V: c_1, c_2 and c_3 such that:

$$c_1 =< \sigma, Hy^t >; c_2 =< y, \sigma >; c_3 =< (y+x), \sigma >$$

where $< arg_1, arg_2 >$ stands for the action of a hash function on the concatenation of arg_1 and arg_2, and $arg.\sigma$ is the image of arg by σ.

2. The verifier V sends to P a random challenge b in $\{0, 1, 2\}$.

3. P receives b and three possibilities occur:
- if $b = 0$: P reveals y and σ,
- if $b = 1$: P reveals $(y + x)$ and σ,
- if $b = 2$: P reveals $y.\sigma$ and $x.\sigma$.

4. Three possibilities may occur:

- if $b = 0$: V checks that c_1 and c_2 received at step 2 were correctly computed.

- if $b = 1$: V checks that c_1 and c_3 received at step 2 were correctly computed. One remarks that:

$$Hy^T = H(y + x)^T + s^T$$

- if $b = 2$: V checks that c_2 and c_3 received at step 2 were correctly computed and that the weight of $x.\sigma$ is exactly w.

5. Repeat steps $1, 2, 3$ and 4 until the necessary security level is reached.

The protocol has been proved zero-knowledge in [13] with a probability of cheating of $2/3$. This protocol as an authentication scheme has two drawbacks, first the size of the public key is very large as in the usual McEliece cryptosystem (more than 150000 bits for the matrix) and because of the probability of cheating of $2/3$ it needs a certain number of repetition rounds to reach the desired security. For instance to reach the weak and strong authentication probabilities of 2^{-16} and 2^{-32} of the norm ISO/IEC-9798-5, it needs respectively 28 and 56 repetitions.

C. Signature from authentication

As zero-knowledge protocols it is possible to use these protocols as signature schemes ([5]) but then the signature is large and has a size of roughly 120 Kbits.

D. Usual attacks: Information Set Decoding

For code-based cryptography 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, in the case of Stern authentication scheme only decoding attacks are relevant.

The most efficient algorithms in our case are based on the information set decoding. A first analysis was done by MacEliece in [8], then by Lee and in Brickell and also by Stern and Leon and at last by Canteaut and Chabaud (see [2] or references).

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 [12] 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:

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

where $H_2(x) = -xlog_2(x) - (1-x)log_2(1-x)$.
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 deal with improvement of this factor and in the best improvement of [2] one can consider $P(k)$ linear or even less. For the parameters we are

envisaging it is reasonable to consider them linear to fit the practical results of [2]. This algorithm is currently the best known.

III. A VARIATION ON THE SCHEME WITH VERY SHORT KEYS

In this section we explain how to obtain very short public keys for the Stern scheme by using double circulant codes. We propose two ways to do so.

A. Keys of type A: a double circulant form for the matrix

In the NTRU cryptosystem [10] the public key consists of the ratio $\frac{f}{g}$ where f and g are truncated polynomial of the ring $R = Z_q[x]/(x^n - 1)$ for n and q some parameters of the system (typically 251 and 128). To encrypt we have to multiply polynomials in the ring R. This product can be seen as a multiplication of two circulant matrices. So a natural idea to avoid the large size of the key (a matrix) is to consider a $n \times 2n$ double circulant matrix H of the form

$$H = (I|A)$$

for A a random circulant matrix of the form:

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}.$$

The matrix H is simply described from the a_i's which can be randomly chosen. By doing so we obtain (the term 'data' includes all the data necessary for the prover/verifier to run the protocol (private/public key + public matrix)):

Private data: the secret x of length $2n$ and the first row of A of size n: $3n$ bits.
Public data: the syndrome s of size n and the half row of H of size n: $2n$.

Remark : As in the original scheme proposed by Stern, all the users can work with the same matrix H, only the secrets x and the syndrome s are individual.

B. Keys of type B: the secret is embedded in the matrix

In fact it is possible to still decrease the sizes obtained in the previous subsection. The idea consists in embedding the secret key x in the public matrix. To achieve that, we consider the secret as a word of the dual code of the code generated by the public matrix H. This means that we will use a null syndrom, which does not change the zero-knowledge property. Suppose $b = (b_1, \cdots, b_n)$ and $a = (a_1, \cdots, a_n)$. Then construct the matrix: $G = (A|B)$, for A and B two circulant matrices:

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix},$$

and

$$B = \begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ b_n & b_1 & b_2 & \cdots & b_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_2 & b_3 & b_4 & \cdots & b_1 \end{pmatrix},$$

One must randomly choose $a = (a_1, \cdots, a_n)$ and $b = (b_1, \cdots, b_n)$ such that the weight of (a, b) satisfies the conditions of weight in Stern protocol. Without loss of generality, we can assume that the matrix A is invertible (one may simply choose another a if not). Then one can construct

$$G' = A^{-1}G = (I|A^{-1}B) = (I|D).$$

Note that since A and B are circulant, the matrix $D := A^{-1}B$ is also circulant.

Consider now for public matrix, the matrix $H = (C|I)$ where $C = D^t$, the transposed circulant matrix of D. The matrix H corresponds to the matrix of the dual code generated by G and hence x has a null syndrome by H.

In such a case, the secret x is the couple (a, b) and the public key is simply the vector c derived from C. One then obtains:

Private data: the secret $x = (a, b)$ of length $2n$: $2n$ bits.
Public data: the vector c of size n: n bits.

Remark : The vector c can be theoretically reconstructed from a and b with a small complexity.

IV. SECURITY OF THE NEW SCHEME

A. Security of Stern scheme and random codes

Recall that a $[n, k, d]$ code satisfy a Gilbert-Varshamov bound ([9],p.30) if the parameters n, k and d satisfy $\sum_{i=0}^{d-1} \binom{n}{i} \approx 2^{n-k}$. This bound assures that a code on this bound has a good minimum weight difficult to obtain by usual attacks.

The security of Stern scheme relies on three properties of random linear codes:

- 1) Random linear codes satisfy a Gilbert-Varshamov type lower bound [9],
- 2) For large n almost all linear codes lie over the Gilbert-Varshamov bound [11]
- 3) Solving the syndrome decoding problem for random codes is NP-complete [1].

The first point proves the existence of good random codes (in the sense that they satisfy a Gilbert-Varshamov bound), the second point shows that in fact almost all random codes satisfy such a bound and hence they have a high minimal weight, at last the third point implies the difficulty of finding a polynomial algorithm to solve the syndrome decoding problem in general, although of course solving a particular instance of a problem is not equivalent to solving the general problem.

Practically the two first points are essential to estimate the attacks against Stern scheme since they give a lower bound on the minimum weight of the considered code and hence permit to give an estimation of the usual attack by information set decoding. The third point gives a theoretical assurance on the difficulty of the problem.

B. Random double circulant codes

Basically our new scheme proposes to use random double circulant codes rather than pure random codes. So what can we say about such double circulant codes ?

In fact if we accept a small constraint on the length of the code, it is possible to show that random double circulant $[2n, n, d]$- codes satisfy the first two previous points. More precisely if one considers a length n such that n is prime and such that 2 is primitive root of Z/nZ, then almost all random double circulant $[2n, n]$-codes lie on the Gilbert-Varshamov bound. This is because for such a n, $x^n - 1 = (x + 1)(1 + x + x^2 + \cdots + x^{n-1}$ and in that case the circulant matrix generated by any random word of odd weight is invertible. This ensures that basically one gets the same type of random properties in term of minimum weights than for linear codes. This result is showed by Chen, Peterson and Weldon in [3] (see also [9],p.507 and [7]).

Hence random double circulant codes with adequate length have a very good minimum weight and satisfy, like random codes, the two previous first points 1) and 2), which are truly the two points which assure Stern's scheme practical security.

Now what about the third point ?

We first define a new problem, which adapts the syndrome decoding problem to the case of double circulant codes :

Problem: SYNDROME DECODING of DOUBLE CIRCULANT LINEAR CODES

Instance: An $n \times 2n$ double circulant matrix H over F_q, a target vector $s \in F_q^n$ and an integer $w > 0$.

Question: Is there a vector $x \in F_q^n$ of weight $\leq w$, such that $Hx^t = s^t$?

It is not known whether this problem is NP-complete (as is the syndrome decoding problem), but we can argue that this problem is presumably very hard. Indeed if this problem was not NP-complete it would mean that we are able decode in a sub-exponential or polynomial time a family of binary codes up to the Gilbert-Varshamov bound. Until now no family of binary codes is known with such a property and finding it would certainly be a major breakthrough in coding theory. Moreover no particular algorithm is known to decode general quasi-cyclic codes up to the Gilbert-Varshamov bound.

These arguments show that although the previous problem is not proven NP-complete, there is a strong evidence that this problem is difficult to solve.

Remark: notice that if one uses another compact way to describe the public matrix (like LFSR for instance) one would also reduce the size of the public data but in that case nothing could be said about the minimum distance of the matrix and the security would be more difficult to evaluate.

C. Security parameters for the type A scheme

Let x be the secret of weight w. In the original Stern protocol w is chosen just a little below the Gilbert-Varshamov bound. The reason why is that as we previoulsy mentioned, the minimum weight of a random code lies on the GV bound. Hence by choosing such a value for w it assures that this is the highest value for which there are no other codewords which optimizes the difficulty of the attack by decoding.

In the case of double circulant codes, there is no particular decoding attack besides the general information set decoding attack described at section 2.2.1. Now we want to choose n such that the cost of finding a unique word of weight w in a $[2n, n]$ code for w just below the GV bound is at least 2^{80} (by the complexity of section 2.2.1) and such that 2 is primitive root of n. A fast complexity analysis leads to a value of $n = 317$, which leads for this type of keys to a public key of size 634 and a private key of size 951.

Proposed parameters for Type A: $n = 317, w = 69$
Decoding attack security: 2^{85}

D. Security parameters for the type B scheme

In that case one knows that there is a certain vector of given weight w in the matrix G (dual of H). The type of matrix for this case corresponds exactly to the case of the NTRU problem in the case of $q = 2$. We first choose a vector $x = (a, b)$ of weight w, just a little below the GV bound. We saw in the previous section that for adequate n almost all random double-circulant code were on the Gilbert-Varshamov bound. If one starts from a codeword with a weight slightly less than the GV bound it seems then reasonable to consider that this is exactly the minimum weight of the code (which is confirmed by simulation for lengths up to $n = 120$). The same reasonable assumption is made for NTRU.

There are then two main way to use the (quasi-)cyclicity of x to improve the usual information set decoding attack.

One remarks that by cyclicity all the shifts of a codeword are still in the code, which means that there is not one codeword of weight w to search for but n. This means that the complexity of the decoding attack has to be divided by n. This does not really change strongly the complexity.

There exist particular attacks on NTRU which can be adapted for our case but all the attacks can be countered by taking a n a little greater than for case A,$n \approx 350$ is enough to reach the security level superior to 2^{80}. Therefore for that case we can take a public key with size: 347 bits, and the private key has size 694 bits.

Remark: for that case the LLL attack for NTRU does not apply since LLL is not efficient when it has to deals with $\{0,1\}$ matrices.

Proposed parameters for Type B : $n = 347, w = 76$
Decoding attack security: 2^{83}

V. Comparison with other public key authentication schemes

A. Comparison to Stern and Veron schemes

The following tables show a comparison between our schemes, Stern and (improved) Veron (the one with a short key)[14] ones for $[2n, n]$ public matrices. Since for the same security level, the protocols require the same number of rounds, we only give the computation cost (without permutations and vector additions) and the transmission rate in one round.

	$Stern$	$Veron$	$typeA$	$typeB$
$public\,data$	$2n^2+n$	$4n$	$2n$	n
$private\,data$	$2n^2+2n$	$5n$	$3n$	$2n$
$transmission$ $(1round)$	c_S	c_V	c_S	c_S
$work\,factor$ $(1\,round)$	$2n^2$	nw_β	$n(0.22n+1)$	$\frac{n(n+1)}{2}$

Where $w_\beta = (w_\beta(\gamma_1)+w_\beta(\gamma_2))-2$ (for $w_\beta(\gamma_1)$ and $w_\beta(\gamma_2)$ the Hamming weights of γ_1 and γ_2 (see [14] for details)), where h is the size of the hash and l_s the size of the seed for the permutation. The complexities c_S and c_V are respectively $3h+\frac{2}{3}(4n+l_s)$ and $3h+\frac{2}{3}(3n+l_s)$. In the case of $n=256$, the common value of 80 was proposed for $w_\beta(\gamma_1)$ and $w_\beta(\gamma_2)$, we kept it for our increased n. The term $0.22n$ comes from the GV bound for a $[2n,n]$ code.

We need 28 rounds for a weak authentication (security level: 2^{-16}) and 56 for a strong authentication (security level: 2^{-32}). Considering $n=317, w=69$ for all schemes except for type B ($n=347, w=76$), $h=160$ and considering the size of the seed generating the permutation is $l_s=160$ we get:

	$Stern$	$Veron$	$typeA$	$typeB$
$public\,data$	201295	1268	634	347
$private\,data$	201612	1585	951	694
$bits(weak)$	40096	35858	40096	42336
$bits(strong)$	80192	71716	80192	84672
$cost(weak)$	$2^{22.4}$	$2^{21.8}$	$2^{19.2}$	$2^{20.7}$
$cost(strong)$	$2^{23.4}$	$2^{21.8}$	$2^{20.2}$	$2^{21.7}$

With our schemes, the size of the public data is lower than with Veron's. Concerning the private data all our schemes give shorter data than Veron's one. Our global transmission rate is higher than Veron's for types A and B. The difference of the work factors comes from the difference of weights of the codewords of the matrix. Notice that it is also possible to adapt Veron's scheme with double circulant codes to obtain a rate as low as his but with shorter keys.

B. Comparison with some number theory public key authentication schemes

In the norm ISO/IEC9798-5 of 2004, some specifications are given for the Fiat-Shamir scheme and the Guillou-Quisquater scheme with an authentication of security 2^{-16}.

For the Fiat-Shamir scheme the storage capacity is 5 Kbits, the complexity of the operations for the prover and the verifier are 11 modular multiplications hence with an average complexity of $5/2n^2$ binary operations, for $n=1024$, we obtain $11.5/2.1024^2$ operations with 8 Kbits of exchange datas. For the Guillou-Quisquater scheme the storage capacity is 2 Kbits and the number of mudular multiplications is between 20 and 30, with 2 Kbits of exchange datas.

Now if we compare these schemes with our Type B scheme for instance, we see that the storage capacity of the prover is 1 Kbits, the total complexity is $28\frac{n^2}{2}$ with $n=347$. This leads to a protocol which is 10 times faster than Fiat-Shamir and 30 times faster than Guillou-Quisquater.

VI. Conclusion

In this paper we have proposed a variation of the Stern authentication scheme by using double circulant codes. We discussed the security of this construction by relating it to a difficult problem. We saw that the 2 types of schemes that we proposed permit to get rid of the large size of public matrix which made Stern protocol unpractical. Moreover the circulant structure of the public matrix makes the computation very easy without having to generate the whole matrix, indeed the whole scheme only needs very few memory storage. We propose a scheme with a public key of size 347 bits and a private key of size 694 bits which has a complexity of 2^{83} to be broken. Moreover the complexity of the best know attacks on the scheme is exponential. We also compared to Veron's shorter key improvement for which we showed that not only our variation had smaller keys, but also relied on a problem which complexity can be evaluated more easily.

Finally, we saw by comparing them to the well known Fiat-Shamir and Guillou-Quisquater schemes that our schemes were at least 10 to 30 times as fast.

We therefore believe that this type of scheme is a realistic alternative to the usual number theory authentication schemes in the case of constrained environments such as smart cards and of applications such as Pay-TV or vending machines.

References

[1] 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).

[2] 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.

[3] C. Chen, W. Peterson and E. Weldon, Some results on quasi-cyclic codes, Information and Control 15 (1969) pp. 407–423.

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

[5] A. Fiat and A. Shamir, How to prove yourself: practical solutions to identification and signature problems, Crypto '86, LNCS 263, pp 186-194.

[6] P. Gaborit, Shorter keys for the McEliece cryptosystem, Proceedings of WCC 2005.

[7] P. Gaborit and G. Zémor, Asymptotic improvement of the Gilbert-Varshamov bound for linear codes, Proceedings of ISIT 2006, Seattle, USA (2006), 287-291.

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

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

[10] www.ntru.com

[11] J. N. Pierce, Limit distributions of the minimum distance of random linear codes, IEEE Trans. Inf. theory, Vol IT-13 (1967), pp. 595-599.

[12] 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.

[13] J. Stern, A new identification scheme based on syndrome decoding, Crypto '93, p. 13-21.

[14] P. Veron, Improved Identification Schemes Based on Error-Correcting Codes, Applicable Algebra in Engineering, Communication and Computing, vol. 8 no. 1, Springer-Verlag, pp. 57-69, Janvier 1997.