Identity-based identification and signature schemes using correcting codes

Pierre-Louis Cayrel[1], Philippe Gaborit[1] and Marc Girault[2]

1 Université de Limoges, XLIM-DMI,
123, Av. Albert Thomas
87060 Limoges Cedex, France
{pierre-louis.cayrel,philippe.gaborit}@xlim.fr
2 France Télécom Recherche et Développement
42, rue des Coutures
14066 Caen, France
marc.girault@orange-ftgroup.com

Abstract. In this paper, we propose a new identity-based identification (and signature) scheme based on error-correcting codes. This scheme is up to date the first identity-based scheme not based on number theory. The scheme combines two well known code-based schemes: the signature scheme of Courtois, Finiasz and Sendrier and the zero-knowledge authentication scheme of Stern (which may also be used for signature). The scheme inherits from the characteristics of the previous schemes: it has a large public key of order 1Mo and necessitates a certain number of exchange rounds. The scheme can also work in signature but leads to a very large signature of size 1Mo.

Keywords : Identity based scheme, Error-Correcting codes, Stern protocol, Niederreiter scheme, CFS scheme.

1 Introduction

The most critical point of classical public key cryptography (RSA, El Gamal...) is in the management of the authenticity of the public key. In fact, if Alice manages to take Bob's identity by cheating her own public key as Bob's one, she would be able to decipher all messages sent to Bob and to sign any message using the stolen identity.

In 1984, Shamir introduced the concept of IDentity-based Public Key Cryptography ID-PKC [9] in order to simplify the management and the authentication of the public key, which, time passing by, had become more and more complex.

In the ID-PKC scheme of Shamir, the public key of an user is undeniably linked to his identity on the network (user-id): it can be a concatenation of any publicly known information: his name, his e-mail, his phone number, etc ... Hence it is not necessary to verify a certificate for the public key or to contact a data base to obtain it. At first glance it seems simple but producing private keys becomes more complex. And since a private user can not derivate his own private key by himself, it is necessary to introduce trusted third party which derivate the private key from the public key and sends it to the user (at least it has to be done once for each user).

In [9] Shamir calls this trusted third party the Key Generation Center (KGC). The KGC is the owner of a secret, namely the master key. After a protocol of authentication of the identity of the user, the KGC computes his private key from the master key, the user-id and a trapdoor function.

In his paper Shamir proposed systems based on RSA or Discrete Logarithm but which did not fulfilled the previous requirements. The first efficient identity-based cryptosystem was proposed in 2001 by Boneh and Franklin [2]. This system is based on Weil pairing and elliptic curves. The same year, Cocks [4] published a system based on quadratic residuosity but the system has a very large message expansion which makes it unefficient in practice.

Following the paper by Boneh and Franklin, researches on ID-PKI have made great progresses and lots of schemes have been published all of them based on elliptic curves and bilinear pairings, such as identity-based encryption (IBE) schemes [1, 6], identity-based key agreement schemes [10], identity-based signature (IBS) or identity-based identification (IBI) schemes [7, 17, 18] (see [3] for more references).In 2004 Bellare, Neven and Namprempre proposed in [3] a general framework to derivate IBI or IBS from signature or authentication scheme, and they applied it to known schemes, but they only considered number theory based schemes.

In this paper we consider a code-based scheme, which does not rely on previously studied schemes (in particular those of [3]).

Code-based cryptography was introduced at the same time than RSA by MacEliece [14], later a variation on the scheme was proposed by Niederreiter in 1986 [8]. The idea of using error-correcting codes for identification purposes is due to Harari, followed by Stern (first protocol) and Girault. But Harari and Girault protocols were subsequently broken, while Stern's one was five-pass and unpractical. At Crypto'93, Stern proposed a new scheme [16], which is still today the reference in this area.

For a long time no code-based signature scheme was known, eventually the first (non broken) code-based cryptosystem was proposed by Courtois, Finiasz and Sendrier [5] (CFS) in 2001. At the difference of RSA, the MacELiece or Niederreiter schemes do not rely on purely bijective problems like the modular exponentiation. The basic idea of the CFS signature scheme is to choose parameters such that such an inversion for the Niederreiter scheme is practically possible. This is done at the cost of obtaining rather large parameters (except for the length of the signature) when comparing to other signature schemes but at least it exists!

In this paper we combine the previous signature scheme and the authentication scheme by Stern to obtain an IBI and an IBS scheme.

The basic idea of our scheme is to start from a Niederreiter-like problem which can be inverted like in the CFS scheme. This permits to associate a secret to a random (public) value obtained from the identity of the user. The secret and public values are then used for the Stern zero-knowledge authentication (or signature) scheme.

The paper is organized as follows: in section 2 we recall basic facts on code-based cryptography, in section 3, we recall the cryptosystem of Niederreiter, the signature scheme of Courtois, Finiasz and Sendrier and the protocol of Stern before developping our new protocol in section 4. At last in section 5 we give parameters and security analysis of our scheme and conclude in section 6.

2 Code-based cryptography

In this section we recall basic facts about code-based cryptography. We refer to the work of Nicolas Sendrier in [15], for a more general context on these problems.

2.1 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 [12].

2.2 Usual attacks

In term of 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.

Information set decoding The most efficient algorithms in our case are based on the information set decoding. A first analysis was done by MacEliece, then by Lee and in Brickell and also by Stern and Leon and at last by Canteaut and Chabaud (see [13] for all 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 [15] 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 the best improvement of [4] 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 [4]. This algorithm is currently the best known.

Structural attacks Structural attacks aim at recovering the structure of the permuted code, ie: recovering the permutation from the code and its permuted. The problem behind is the equivalence of codes, this problem was considered by Sendrier for which he gave a nice algorithm: the Support Splitting Algorithm [15]. In our context it is not relevant since we will be using Goppa codes, in which case his algorithm can not be applied since one knows only the permuted code and not the original code (which are too many).

3 CFS signature scheme and Stern identification protocol

Before decribing the CFS scheme of Courtois,Finiasz and Sendrier, and the Stern identification protocol, we first recall the Niederreiter scheme:

3.1 Niederreiter scheme

Let C be a q-ary linear code t-correcting of length n and of dimension k. Let H a matrix of parity of C. We will use an $\widetilde{H}$ matrix such that :

$$\widetilde{H} = VHP \begin{cases} V \text{ is invertible} \\ P \text{ is a permutation matrix} \end{cases}$$

$\widetilde{H}$ will be public and its decomposition will be secret, knowing a decoding by syndromes algorithm useful in C. To be clearer, we recall the various sizes of matrices. M is $n \times n-k$, V is $n-k \times n-k$, H is $n \times n-k$, P is $n \times n$.

Encryption For a chosen cleartext x in the $E_{q,n,t}$ space of $\mathbb{F}_q^n$ words which Hamming weight t, y is the cryptogramm corresponding to x if and only if :

$$y = \widetilde{H}x^T.$$

Decryption For $y = \widetilde{H}x^T$, the knowledge of the secrets allows :

1. to compute $V^{-1}y$ $(= HPx^T)$;
2. to find Px^T from $V^{-1}y$ thanks to the decoding by syndromes algorithm used in C;
3. to find x applying P^{-1} to Px^T.

The decoding by syndromes algorithm can be, for instance, in the case of Goppa's codes, Patterson's algorithm (see part 5.1).

3.2 CFS signature scheme

As we already mentionned at the difference of the RSA scheme which is naturally invertible, the MacEliece or the Niederreiter schemes are not invertible, ie, if one starts from a random element y of F_2^n and a code $C[n,k,d]$ that we are able to decode up to $d/2$, it is almost sure that we won't be able to decode y into a codeword of C. This comes from the fact that the density of the whole space which is decodable is very small. The idea of the CFS scheme is to fix parameters $[n,k,d]$ such that the density of decodable codewords is reasonable and pick up random elements until one is able to decode it.

More precisely, given M a message to sign and h a hash function of $\{0,1\}^{n-k}$. We try to find a way to build $s \in F_2^n$ of given weight t such that $h(M) = \widetilde{H}s^T$. For $D()$ a decoding algorithm, the algorithm works as follows:

1. $i \leftarrow 0$
2. while $h(M \oplus i)$ is decodable do $i \leftarrow i+1$
3. compute $s = D(h(M \oplus i))$

Fig. 1. The CFS signature scheme

We get at the end an $\{s,j\}$ couple, such that $h(M \oplus j) = \widetilde{H}s^T$. Let us notice that we can suppose that s has weight $t = [d/2]$.

3.3 Stern authentication (or identification) protocol

This scheme was developed in 1993 (see [11]) to aim at providing zero-knowledge authentication scheme, not based on number theory problems. Given $\widetilde{H}$ a matrix of size $(n-k) \times n$ over $\mathbb{F}_2$. This matrix is public. Each user receives a secret key s of n bits and of weight t. A user's public identifier is obtained from :$i = \widetilde{H}s^T$. It is calculated once in the lifetime of $\widetilde{H}$. It can thus be used by several future identifications. Let us suppose that A wants to prove to B that he is indeed the person corresponding to the public identifier i_A. A has his own private key s_A s.t. $i_A = \widetilde{H}s_A^T$. Our two protagonists can then follow the protocol:

1. A chooses randomly any word y of n bits and a permutation σ of $\{1, 2, \ldots, n\}$. Then A sends to B : c_1, c_2, c_3 such that :

$$c_1 =< \sigma, \widetilde{H}y^T >;\ c_2 =< y.\sigma >;\ c_3 =< (y \oplus s).\sigma >$$

where arg_1, arg_2 notes the concatenation of arg_1 and arg_2, $< arg_1 >$ the action of a hash function on arg_1 and $arg.\sigma$ is the image of arg by σ.
2. B sends to A, $b \in \{0, 1, 2\}$.
3. Three possibilities:
   - if $b = 0$: A reveals y and σ.
   - if $b = 1$: A reveals $(y \oplus s)$ and σ.
   - if $b = 2$: A reveals $y.\sigma$ and $s.\sigma$.
4. Three possibilities:
   - if $b = 0$: B verifies that the c_1, c_2 received at the second round have really been honestly calculated.
   - if $b = 1$: B verifies that the c_1, c_3 received at the second round have really been honestly calculated. For c_1 we can note that $\widetilde{H}y^T$ derives directly from $\widetilde{H}(y \oplus s)^T$ by :

$$\widetilde{H}y^T = \widetilde{H}(y \oplus s)^T \oplus i = \widetilde{H}(y \oplus s)^T \oplus \widetilde{H}s^T = \widetilde{H}y^T$$

   - if $b = 2$: B verifies that the c_2, c_3 received at the second round have really been honestly calculated, and that the weight of $s.\sigma$ is really equal to t.
5. Reiterate the steps 1,2,3,4 while the expected security is not reached.

Fig. 2. Stern's protocol

The protocol has to be iterated long enough to make the k numbers of rounds $(2/3)^k$ close to the level of confidence wanted, where $(2/3)$ is the probability that a dishonest person cheats during a round. Apart from the number of turns, the security of this scheme relies on the difficulty to invert the function :

$$x \mapsto \widetilde{H}x^T.$$

4 An identity-based identification protocol : the Stern-Niederreiter protocol

Given C a q-ary linear code of length n and of dimension k. Let H be a matrix of parity of C. Given $\widetilde{H} = VHP$ with V invertible and P a matrix of permutation. Let h a hash function with values in $\{0, 1\}^{n-k}$. Let id_A Alice's identity, id_A can be compute by everyone. Similarly, $\widetilde{H}$ is public. The decomposition of $\widetilde{H}$ is, on the contrary, a secret of the authority and not of Alice.
We shall describe an identity-based authentication method : Alice the prover is identifying herself to Bob the verifier.

Preliminary : key deliverance Alice has to authentify herself in a classic way, to get the private key which will then allow her to authentify herself to a third

person as Bob. For that purpose, we use variation on identity. Let us admit that we know Bob's identity id_B. Given h a hash function with values in $\{0,1\}^{n-k}$. We search a way to find $s \in E_{q,n,t}$ such that $h(id_B) = \widetilde{H}s^T$.
The main point is to decode $h(id_B)$. The main problem is that $h(id_B)$ is not *in principle* in the arrival space of $x \rightarrow \widetilde{H}x^T$. That is to say that $h(id_B)$ is not *in principle* in the space of decodable elements of F_2^n. That problem can be solved thanks to the following algorithm. Given $D()$ a decoding algorithm for the hidden code: We get at the end a couple $\{s, j\}$, such that $h(id_B \oplus j) = \widetilde{H}s^T$.

1. $i \leftarrow 0$
2. while $h(id_B \oplus i)$ is not decodable do $i \leftarrow i + 1$
3. compute $s = D(h(id_B \oplus i))$

Fig. 3. key deliverance

We can note that we have necessarily s of weight t.

Identification by Bob. We use a slight derivation of Stern's protocol (section 3.3 figure 3.3). We suppose in that protocol that A obtained a couple $\{s, j\}$ verifying : $h(id_A \oplus j) = \widetilde{H}s^T$. $h(id_A \oplus j)$ is A's public key. The new protocol is based on Stern's protocol but with two changes, first A sends j to B at the step one and second, we change the step 4 with : The knowledge of j doesn't permit

4bis. Three possibilities:

- if $b = 0$: *Bob* verifies that the c_1, c_2 received at the second round have really been honestly computed.
- if $b = 1$: *Bob* verifies that the c_1, c_3 received at the second round have really been honestly computed. For c_1 we can note that $\widetilde{H}y^T$ derives directly from $\widetilde{H}(y \oplus s)^T$ by :

$$\widetilde{H}y^T = \widetilde{H}(y \oplus s)^T \oplus h(id_A \oplus j) = \widetilde{H}(y \oplus s)^T \oplus \widetilde{H}s^T$$

- if $b = 2$: *Bob* verifies that the c_2, c_3 received at the second round have really been honestly commputed, and that the weight of $s.\sigma$ is really equal to t.

Fig. 4. Authentication by Bob

to find s such that $h(id_A \oplus j) = \widetilde{H}s^T$. The security of this system is the same as the security of Stern's one (see section 2).
Remark: Identity-based signature scheme: it is possible to derive a signature scheme from the zero-knowledge authentication scheme of Stern by classical constructionc. Hence it permits to derive an IBS scheme.

5 Security Analysis

We shall here deal with the security of *classical* protocol as their applicability and finally end with our protocol.

Remind that in the case of Niederreiter's cryptosystem, its security relies on the *supposed* difficulty of the decoding of a linear code (see section 2).

5.1 Parameters and security of the scheme

The protocol has two parts: in the first part one inverts the syndrome decoding problem for a matrix $\widetilde{H}$ in order to construct a private key for the prover and in second part one applies Stern authentication protocol with the same matrix $\widetilde{H}$. This shows that the overall parameters of the scheme are equivalent to the security of the CFS scheme, since the security of the Stern scheme with the same matrix parameters is implicitly included in the signature scheme.

In particular the scheme has to respect two imperative conditions:

1. make the computation of $\{s, j\}$ (defined in advance) difficult without the knowledge of the description of H,
2. make the number of trials to determine the correct j not too important in order to reduce the cost of the computation of s.

Following [5] the Goppa $[2^m, 2^m - tm, t]$ codes are a large class of codes which are compatible with condition 2. Indeed, for such a code, the proportion of the decodable syndromes is about $1/t!$ (which is a relatively good proportion). We also have to choose a relatively small t.

The $\{s, j\}$ production process will thus be iterated, about $t!$ times before finding the correct j. But each iteration forces to compute $D(h(id_A \oplus j))$.
The decoding of the Goppa codes consists of :

- computing a syndrome : $t^2m^2/2$ binary operations;
- computing a localisator polynomial : $6t^2m$ binary operations;
- computing its roots : $2t^2m^2$ binary operations.

We thus get a total cost for the computation of Alice's private key of about :

$$t!t^2m^2(1/2 + 2 + 6/m) \text{ binary operations}$$

The cost of an attack by decoding thanks to the *split syndrome decoding* is estimated to :

$$2^{tm(1/2+o(1))}.$$

The choice of parameters will have to be pertinent enough to conciliate cost and security. Althought less crippling, some sizes have also to remain reasonable : the length of $\{s, j\}$, the cost of the verification and the size of $\widetilde{H}$.

The size of $\widetilde{H}$ is $(n - k) \times n$, that is for a Goppa code : $2^m tm$. The following figure sums up the different parameters :

signature cost	$t!t^2m^2(1/2+2+6/m)$
signature size	tm
verification cost	t^2m
attack cost	$2^{tm(1/2+o(1))}$
size of $\widetilde{H}$	$2^m tm$

Following [5] we can for example take $t = 9$ and $m = 16$. The cost of the signature stays then relatively reasonable for a security of about 2^{80}. The others sizes remain in that context very acceptable.

5.2 Practical values

The big difference when using the parameters associated to the CFS scheme is that the code used is very long, 2^{16} against 2^9 for the basic Stern scheme, it dramatically develops communication costs.

In the next table we sum up for the parameters $m = 16$, $t = 9$ the general paramaters of the IBI and IBS schemes.

public key	private key	matrix size	communication cost	key generation
tm	tm	$2^m tm$	$\approx 2^m \times \#rounds$	
144	144	1 Mo	500 Ko (58 rounds)	1 s

Practical values for the IBI scheme: $m = 16, t = 9$

public key	private key	matrix size	signature length	key generation
tm	tm	$2^m tm$	$\approx 2^m \times 150$	
144	144	1 Mo	1 Mo	1 s

Practical values for the IBS scheme: $m = 16, t = 9$

Reduction of the size of the public matrix: At the difference of a pure signature scheme in which one wants to be able to sign fast, in our scheme the signature is only computed once for sending it to the prover, hence the time for signing may be judged less determinant and a longer time of signature may be accepted at the cost of reducing (a little) the parameters of the public matrix (we shall precise it in a longer version of our paper).

6 Conclusion

In this paper we presented an IBI and a related IBS scheme based on error-correcting code. This scheme is the first non number theory based identity based scheme. The scheme combines two well known schemes and inherits from bad properties of these schemes: the public data is large, the communication cost for the IBI scheme is large and the signature length for the IBS scheme is also very large but besides these weaknesses our scheme presents the first alternative to number theory for ID-based cryptography and may open a new area of research.

References

1. Boneh D. and Boyen X. . Efficient selective-id secure identity based encryption without random oracles. Eurocrypt 2004, LNCS 3027:223–238, 2004.
2. Franklin M. and Boneh D. . Identity-based encryption from the weil pairing. Advances in Cryptology-Crypto'01, 2001.
3. Bellare M.,Namprempre C. and Neven G. Security proofs sor identity-based authentication and signature schemes. Eurocrypt 2004, volume 3027 of Lecture Notes in Computer Science:268–286, 2004.
4. Cocks C. An identity based encryption scheme based on quadratic residues. Lecture Notes in Computer Science, Vol 2260:360–363, 2001.
5. Courtois Nicolas, Finiasz Matthieu , and Sendrier Nicolas . How to achieve a maceliece-based digital signature scheme. Asiacrypt 2001 volume 248, 2001.
6. Gentry Craig , Silverberg Alice . Hierarchical id-based cryptography. Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology:548–566, December 01-05,2002.
7. Hess Florian. Efficient identity based signature schemes based on pairings. Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography:310–324, August 15-16, 2002.
8. Niederreiter Harald. Knapsack-type cryptosystems and algebraic coding theory. Prob. Contr. Inform. Theory, 1986.
9. Shamir Adi. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto'84, 1984.
10. Smart N. A id-based authenticated key agreement protocol based on the weil pairings. Electron. Lett. 38(13):630–632, 2002.
11. Stern Jacques. A new identification scheme based on syndrome decoding. Lecture Notes in Computer Science 773, 1994.
12. MacEliece R. Berlekamp E. and van Tilborg H. On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory, IT-24(3), 1978.
13. Canteaut Anne and Chabaud Florent. A new algorithm for finding minimum-weight words in a linear code: application to primitive narrow-sense bch codes oflength| 511. IEEE Transactions on Information Theory, IT-44:367–378, 1988.
14. MacEliece R.J. A public-key cryptosystem based on algebraic coding theory. JPL DSN Progress Report 42-44:114–116, 1978.
15. Sendrier N. On the security of the maceliece public-key cryptosystem. In: M. Blaum, P.G. Farrell and H. van Tilborg,editors, Information, Coding and Mathematics:141–163, 2002.
16. Stern Jacques. A method for finding codewords of small weight. coding theory and applications. Lecture Notes in Comput. Sci., 388, New York:106–113, 1989.
17. Yi X. An identity-based signature scheme from the weil pairing. IEEE Communications Letters 7(2):76–78, 200.
18. Yoon H., Cheon J. H. and Kim Y. Batch verifications with id-based signatures. ICISC 2004, LNCS 3506:223–248, 2005.