Improved identity-based identification and signature schemes using Quasi-Dyadic Goppa codes

Sidi Mohamed El Yousfi Alaoui, Pierre-Louis Cayrel, and Meziani Mohammed

CASED – Center for Advanced Security Research Darmstadt,
Mornewegstrasse 32, 64293 Darmstadt, Germany
{elyousfi, pierre-louis.cayrel, meziani}@cased.de

Abstract.
In this paper, we present an improved version of an identity-based identification scheme based on error-correcting codes. Our scheme combines the Courtois-Finiasz-Sendrier signature scheme using quasi-dyadic codes (QD-CFS) proposed in [2] and the identification scheme by Stern [18]. Following the construction proposed in [5], we obtain an identity-based identification scheme which has the advantage to reduce a public data size, the communication complexity and the signature length.

Keywords: Error-Correcting codes, Identity-based Cryptography, Quasi-dyadic Goppa codes.

1 Introduction

In 1984, Shamir introduced the concept of identity-based Public Key Cryptography ID-PKC [17] in order to simplify the management of public keys used for the authentication of users. In ID-PKC, the public key of a user is obtained from his identity *id* which can be a concatenation of any publicly known information that singles out the user: a name, an e-mail, or a phone number. ID-PKC requires a trusted third part called Key Generation Center (KGC), the KGC is the owner of a system-wide secret, thus called the *master key*. After successfully verifying (by non-cryptographic means) the identity of the user, the KGC computes the corresponding user private key from the master key, the user identity *id* and a trapdoor function. The motivation behind identity-based systems is to create a cryptographic system resembling an ideal mail system. In this ideal system, a knowledge of a person's name alone suffices for confidential mailing to that person, and for signature verification that only that person could have produced. In such an ideal cryptographic system, we get the following advantages:

1. users need no exchange neither of symmetric keys nor of public keys;
2. public directories (databases containing public keys or certificates) need not be kept;
3. the services of a trusted authority are needed solely during a set-up phase (during which users acquire authentic public system parameters).

Coding theory is one of few alternatives supposed to be secure in a post quantum world. The most popular cryptosystems in coding theory are the McEliece [13] and Niederreiter [15] cryptosytems. The main advantage of these two public cryptosystems is the provision of a fast encryption and decryption (about 50 times faster for encryption and 100 times faster for decryption than RSA), but they have a major disadvantage as requiring very large keys and consequently, large memory size allocation.
In order to make use of the benefits of ID-based cryptography, the authors in [5] proposed the first identity-based identification (IBI) scheme based on coding theory. This scheme combines the signature scheme of Courtois, Finiasz and Sendrier (CFS) [7] and Stern identification scheme [18]. The basic idea of this construction is to start from a Niederreiter-like problem which can be inverted by using 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

identification scheme.
An improvement of the CFS signature scheme using the quasi-dyadic (QD) structure was proposed in [2]. Using this improvement, we propose in this paper an identity based identification scheme built on quasi-dyadic codes.
The paper is organized as follows. In Section 2, we recall basic facts on code-based cryptography. Section 3 describes the first identity based on error correcting code proposed by Cayrel et. al. in [5]. Section 4 presents the improvement of the CFS signature scheme using the quasi-dyadic Goppa codes proposed in [2]. In Section 4, we introduce our improved identity based identification and the gain it offers in terms of performance. Finally, we conclude in Section 5.

2 Background of coding theory

Next, we provide some background for coding theory.
Let $\mathbb{F}_q$ to denote the finite field with q elements.
Let n and k be two integers such that $n \geq k$ and $\mathbb{F}_q^n$ be a finite field over $\mathbb{F}_q$. A code C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$.

Definition 1. ***(Minimum distance and Hamming weight)***
The minimum distance is defined by $d := \inf_{x,y \in C} dist(x,y)$*, where "dist" denotes the hamming distance.*
Let x *be a vector of* $\mathbb{F}_q^n$*, then we call* $wt(x) := dist(x,0)$ *the weight of* x*. It represents the number of non-zero entries.*

$C = C[n,k,t]$ *is a code with length* n*, dimension* k *and the ability of error-correcting in* C *is up to* t *errors (*t *is an integer).*

Definition 2. ***(Generator, Parity Check Matrix and Syndrome)***
A matrix $G \in \mathbb{F}_q^{k \times n}$ *is called generator matrix of* C*, if the rows of* G *span* C*.*
A matrix $H \in \mathbb{F}_q^{r \times n}$*, where* $r = n - k$*, is called parity check matrix of* C*, if* $Hx^{\mathsf{T}} = 0, \forall x \in C$*.*

The security of the most code-based cryptosystems relies on the difficulty of solving a syndrome decoding problem (SD), which is defined as follows:

Definition 3. ***(Syndrome Decoding (SD) Problem)***
Input: *A* $r \times n$ *random binary matrix* H *over* $\mathbb{F}_q$*, a target vector* $y \in \mathbb{F}_q^r$ *and an integer* $t > 0$*.*
Problem: *Find a vector* $x \in \mathbb{F}_q^n$ *with* $wt(x) \leq t$*, such that* $Hx^{\mathsf{T}} = y$*.*

This problem is proven NP-complete in [3].

2.1 Quasi-dyadic codes

Since a large public matrix size is one of the drawbacks of code-based cryptography, there have been many attempts to reduce the matrix size. Miscozki and Barreto proposed in [14] the use of quasi-dyadic Goppa codes which admit a compact parity-check matrix and permit then to store it more efficiently.
In what follows we recall some definitions from [14] that we need in this paper, and we refer the reader to [14] for a detailed description of the quasi-dyadic codes construction.

Definition 4. *Given a vector* $h = (h_0, \ldots, h_{n-1}) \in \mathbb{F}_q^n$*, where* q *is a power of 2. The* dyadic *matrix* $\Delta(h) \in \mathbb{F}_q^{n \times n}$ *is the symmetric matrix with components* $\Delta_{ij} = h_{i \oplus j}$*, where* $\oplus$ *stands for bitwise exclusive-or on the binary representations of the indices. The sequence* h *is called its* signature*. The set of dyadic* $n \times n$ *matrices over* $\mathbb{F}_q$ *is denoted* $\Delta(\mathbb{F}_q^n)$*.*

Given $t > 0$, $\Delta(t, h)$ denotes $\Delta(h)$ truncated to its first t rows.
We call a matrix quasi-dyadic matrix if it is a block matrix whose component blocks are dyadic submatrices.

If n is a power of 2, then every $2^k \times 2^k$ dyadic matrix M can be recursively characterized as

$$M = \begin{bmatrix} A & B \\ B & A \end{bmatrix},$$

where A and B are $2^{k-1} \times 2^{k-1}$ dyadic matrices.

We remark that the signature $h = (h_0, \ldots, h_{n-1})$ of a dyadic matrix coincides with its first row.

Definition 5. *A* quasi-dyadic (QD) code *is a linear error-correcting code that admits a quasi-dyadic parity-check matrix.*

Definition 6. *Given two disjoint sequences $z = (z_0, \ldots, z_{t-1}) \in \mathbb{F}_q^t$ and $L = (L_0, \ldots, L_{n-1}) \in \mathbb{F}_q^n$ of distinct elements, the* Cauchy matrix $C(z, L)$ *is the $t \times n$ matrix with elements $C_{ij} = 1/(z_i - L_j)$, i.e.*

$$C(z, L) = \begin{bmatrix} \frac{1}{z_0 - L_0} & \cdots & \frac{1}{z_0 - L_{n-1}} \\ \vdots & \ddots & \vdots \\ \frac{1}{z_{t-1} - L_0} & \cdots & \frac{1}{z_{t-1} - L_{n-1}} \end{bmatrix}.$$

Cauchy matrices have the property that all of their submatrices are nonsingular [16]. Notice that, Goppa codes admit a parity-check matrix in cauchy form under certain assumption [12]. Misoczki and Barreto showed in [14] Theorem 2 that the intersection of these two classes is non-empty if the code is defined over a field with characteristic 2.
This result was given in the following theorem.

Theorem 1 ([14]). *Let $H \in \mathbb{F}_q^{n \times n}$ with $n > 1$ be simultaneously a dyadic matrix $H = \Delta(h)$ for some $h \in \mathbb{F}_q^n$ and a Cauchy matrix $H = C(z, L)$ for two disjoint sequences $z \in \mathbb{F}_q^n$ and $L \in \mathbb{F}_q^n$ of distinct elements. Then $\mathbb{F}_q$ is a binary field, h satisfies*

$$\frac{1}{h_{i \oplus j}} = \frac{1}{h_i} + \frac{1}{h_j} + \frac{1}{h_0}, \tag{1}$$

and $z_i = 1/h_i + \omega$, $L_j = 1/h_j + 1/h_0 + \omega$ for some $\omega \in \mathbb{F}_q$.

2.2 Usual attacks

Any public-key cryptosystem primarily requires to be resistant to an adversary who manages either to extract the private data given only public data, or to invert the trapdoor encryption function given the ciphertexts of his choice (and public data). Against code-based cryptosystem there are two classes of attacks : structural attacks which try to recover the structure of the code and decoding attacks which try to decode directly a plaintext. The most threatening attacks are based on decoding algorithms for generic, but because we deal with Goppa codes, one has to take care as well of structural attacks.

3 Identity-based identification and signature scheme

Identity-based (IB) public key cryptography was introduced in 1984 by Shamir [17] in order to simplify public key management and to avoid the need for digital certificates. However, identity

based PKC need a third party called Key Generation Center (KGC) or trusted, which generates user private keys corresponding to user identities (e.g., name, e-mail,...); the key generation requires a secret, called master key.
The first identity-based scheme based on error-correcting codes was proposed by Cayrel et. al in [5]. This scheme consists of two phases: the key generation part using the signature scheme of Courtois, Finiasz, and Sendrier (CFS) [7] and the interaction part, which uses the Stern identification scheme [18].
In this section, we recall the description of the CFS and Stern schemes, then we show how the authors in [5] combined them in order to construct an identity-based identification scheme.

3.1 Description of CFS signature scheme

In 2001, Courtois, Finiasz and Sendrier proposed in [7] the first practical signature scheme in coding theory, which is based on the Niederreiter cryptosystem. Due to the fact that not all syndromes are decodable, the idea of CFS is to hash the message M, which has to be signed after a counter has been appended to it. If the resulting hash value is not decodable, it has to try successive counter values until a decodable syndrome is found. The actual signature on the message M consists of both the error pattern of weight t corresponding to the syndrome, and the value of the counter giving this syndrome.
Let $\mathcal{H} : \{0,1\}^* \times \mathbb{N} \rightarrow \mathbb{F}_q^k$ be a random oracle for a given vector space $\mathbb{F}_q^k$ over a finite field $\mathbb{F}_q$. Formally, the CFS signature scheme consists of the following algorithms:

- Keygen: For the desired security level expressed by suitable integers q, n, k, t, choose a linear t-error correcting $[n,k,t]$-code over $\mathbb{F}_q$ defined by a public parity-check matrix H with a private decoding trapdoor $\mathcal{T}$. The private-public key pair is $(\mathcal{T}, H)$.
- Sign: Let $M \in \{0,1\}^*$ be the message to sign. Find $i_0 \in \mathbb{N}$ (either sequentially or by random sampling) such that $x \leftarrow \mathcal{H}(M, i_0)$ is a decodable syndrome. Using the decoding trapdoor $\mathcal{T}$, find $s \in \mathbb{F}_q^n$ of weight $\mathsf{wt}(s) \leqslant t$ such that $Hs^{\mathrm{T}} = x$. The signature is the pair (s, i_0).
- Verify: Let (s, i_0) be a purported signature of a message M. Compute $x \leftarrow \mathcal{H}(M, i_0)$, and accept iff $\mathsf{wt}(s) \leqslant t$ and $Hs^{\mathrm{T}} = x$.

The authors of [7] used Goppa codes, which have a good proportion of decodable words, and choose parameters such that this proportion is reasonable. For a t-error correcting Goppa code $[n = 2^m, n - mt, t]$ (m integer), the number of decoding attempt required to get one signature will be approximately around $(t!)$. The security of this scheme can be reduced to the syndrome decoding (SD) problem.

3.2 Description of the Stern identification scheme

At CRYPTO'93, Stern proposed the first identification scheme based on error-correcting codes [18]. This construction is an interactive zero-knowledge protocol which enables a prover (P) to identify himself to a verifier (V).
Let H be a public random $(n-k) \times n$ binary matrix ($n \geq k$) and h a hash function returning a binary word n. Each prover P receives a n-bit secret key s_k of Hamming weight t ($t \geq n$) and computes a public identifier id_P such that $id_P = Hs_k^T$. This identifier is calculated once in the lifetime of H and can be used for several identifications.
We now describe this protocol:

- Commitment Step: P randomly chooses $y \in \mathbb{F}_2^n$ and a permutation σ of $\{1, 2, \ldots, n\}$. Then P sends to V the commitments c_1, c_2, and c_3 such that :

$$c_1 = h(\sigma \| Hy^T);\ c_2 = h(\sigma(y));\ c_3 = h(\sigma(y \oplus s_k)),$$

  where $h(a\|b)$ denotes the hash of the concatenation of the sequences a and b.

- Challenge Step: V sends $b \in \{0, 1, 2\}$ to P.
- Answer Step: There are three possibilities :
  - if $b = 0$: P reveals y and σ.
  - if $b = 1$: P reveals $(y \oplus s_k)$ and σ.
  - if $b = 2$: P reveals $\sigma(y)$ and $\sigma(s_k)$.

- Verification Step: There are three possibilities :
  - if $b = 0$: V verifies that c_1, c_2 are correct.
  - if $b = 1$: V verifies that c_1, c_3 are correct.
  - if $b = 2$: V verifies that c_2, c_3 are correct, and that the weight of $\sigma(s_k)$ is t.

- Soundness Amplification Step: Iterate the above steps until the expected security level is reached.

For the verification step and when b equals 1, it can be noticed that Hy^T derives directly from $H(y \oplus s_k)^T$ since we have: $Hy^T = H(y \oplus s_k)^T \oplus id_p = H(y \oplus s_k)^T \oplus Hs_k^T$. It is proven in [18] that this protocol verifies the zero-knowledge proof and for each iteration, the probability that a dishonest party succeeds in cheating is (2/3). Therefore, to get a confidence level of β, the protocol must be iterated a number α of times with $(2/3)^\alpha \leq \beta$ holds.

3.3 Identity based identification (IBI) protocol

The identity based identification protocol proposed in [5] is an interactive identification protocol between a prover and a verifier, consisting of two parts: the first one, called key deliverance, uses the CFS signature scheme to create the private key for the prover, while the Stern's protocol is used for the identification in the second part. We describe these two parts as follows:

- Key deliverance: Let h be a hash function with values in $\{0, 1\}^{n-k}$ and let id_p be the prover's identifier identities. The goal of this part is to generate a prover's secret key by using the CFS signature. The prover receives a secret key s_k such that $Hs_k^{\mathsf{T}} = h(id_p|i_0)$, where i_0 is the smallest value of i for which it is possible to decode $h(id_p|i_0)$. The secret key corresponding to the prover's identifier consists then of $\{s_k, i_0\}$.
- Prover and verifier's interaction: Each prover is associated now with the tuple $\{s, i_0\}$. In this case a prover P wishes to identify to a verifier V using the same matrix H and proving that he knows the secret key. This is achieved by Stern's protocol such that in the commitment step, the prover has to submit the counter i_0 together with the other commitments c_1, c_2 and c_3. The knowledge of i_0 is needed for the verification step when b equals 1, since we have: $Hy^T = H(y \oplus s_k)^T \oplus h(id_v|i_0) = H(y \oplus s_k)^T \oplus Hs_k^T$.

By virtue of the so-called Fiat-Shamir Paradigm [9], it is possible to convert this identity based identification scheme into an identity based signature scheme, but the resulting signature size is long (about 1.5 Mbyte long for 2^{80} security).

A proof of security for this scheme in the random oracle model is given in [4], assuming the hardness of the two problems: Goppa Parametrized Bounded Decoding (GPBD) and Goppa Code Distinguishing (GD). However, due to the recently work proposed in [8] , the hardness of GD problem is no longer valid.

Suggested parameters Because the IBI scheme uses CFS scheme in the first part of the protocol, its security relies on CFS parameters. The authors of IBI scheme in [4] suggest $t = 9$ and $m = 16$, which gives the following properties:

- Public Key: tm (180 Bits)
- Private Key: tm (180 Bits)
- Matrix size: $2^m tm$ (1 Mbyte)

- Communication cost for IBI $\approx 2^m \times \#rounds$ (500 Kbyte), where $\#rounds = 58$.
- Signature length for IBS $\approx 2^m \times \#rounds$ (2.2 Mbyte), where $\#rounds = 150$.

Due to Daniel Bleichenbacher attack's described in [11] are these suggested parameters not realistic for 2^{80} as security level, to ensure this security level, the authors of [11] suggested $t = 12$ and $m = 15$.

4 Identity-based identification using quasi-dyadic codes

In what follows, we give the main idea of the quasi-dyadic CFS signature construction, which consists of using a family of quasi-dyadic codes described in Section 2 instead of Goppa codes. The use of such family of codes allows to reduce the public key size by almost a factor of 4, but the number of signing attempts is increased by a factor of 2. For more detail, we refer the reader to [2].

4.1 Quasi-dyadic codes for CFS signature

The strategy to get shorter keys is due to the fact that the CFS signature scheme needs only a very small t, so most rows of the parity matrix H are unused anyway when defining the code. Therefore, we can have some undefined entries in H, as long as the corresponding rows are not used to define the code. This leads to extend the code length to $2^m - t$.
Algorithm 1 picked from [2] describes this construction.

Parameter combinations proposed in [2] are put forward on Table 1.

Table 1. Suggested parameters for practical security levels.

level	m	t	$n = \lfloor 2^{m-1/t} \rceil$	$k = n - mt$	key size (Kbyte)
80	15	12	30924	30744	169
100	20	12	989724	989484	7248
120	25	12	31671168	31670868	289956

Implementation of QD-CFS signature scheme: To attract the attention of QD-CFS scheme, the authors in [1] proposed an GPU implementation of this scheme, it was demonstrated that signing a document using a QD-CFS can be performed in acceptable time (around 5 minutes). A GTX 295 running CUDA Version 3.0 has been used for the implementation process.

4.2 Improved identity-based identification and signature schemes using quasi-dyadic Goppa codes (QD-IBI)

The main advantage of the QD-CFS signature scheme presented in subsection 4.1 is to reduce the size of the public key. But, the drawback is the high signature cost, which originates in the elaborate key deliverance process of the IBI scheme. However, since the key deliverance is a one-time process, the long-term computational cost is reduced by the smaller parity check matrix. We extend this result by using quasi-dyadic codes in the identity based identification (IBI) scheme presented in subsection 3.3. The main idea consists in replacing the CFS signature scheme by the QD-CFS signature scheme during the key deliverance in the IBI-protocol. In the second part of our IBI scheme, the prover can identify itself through Stern's protocol using the same matrix H and proving that he knows the private key s_k. The quasi-dyadic structure of the matrix used as public key permits to

Algorithm 1 Constructing a purely dyadic, CFS-friendly code [2]

INPUT: m, n, t.

OUTPUT: A dyadic signature h from which a CFS-friendly t-error correcting binary Goppa code of length n can be constructed from a code over $\mathbb{F}_{2^m}$, and the sequence b of all consistent blocks of columns (i.e. those that can be used to define the code support).

$q \leftarrow 2^m$
repeat
  $U \leftarrow \mathbb{F}_q \setminus \{0\}$
  $h_0 \xleftarrow{\$} U,\ U \leftarrow U \setminus \{h_0\}$
  for $s \leftarrow 0$ **to** $m-1$ **do**
    $i \leftarrow 2^s$
    $h_i \xleftarrow{\$} U,\ U \leftarrow U \setminus \{h_i\}$
    for $j \leftarrow 1$ **to** $i-1$ **do**
      if $h_i \neq 0$ **and** $h_j \neq 0$ **and** $1/h_i + 1/h_j + 1/h_0 \neq 0$ **then**
        $h_{i+j} \leftarrow 1/(1/h_i + 1/h_j + 1/h_0)$
      else
        $h_{i+j} \leftarrow 0$ ▷ undefined entry
      end if
      $U \leftarrow U \setminus \{h_{i+j}\}$
    end for
  end for
  $c \leftarrow 0$ *also:* $U \leftarrow \mathbb{F}_q$
  if $0 \notin \{h_0, \ldots, h_{t-1}\}$ **then** ▷ consistent root set
    $b_0 \leftarrow 0,\ c \leftarrow 1$ ▷ also: $U \leftarrow U \setminus \{1/h_i, 1/h_i + 1/h_0 \mid i = 0, \ldots, t-1\}$
    for $j \leftarrow 1$ **to** $\lfloor q/t \rfloor - 1$ **do**
      if $0 \notin \{h_{jt}, \ldots, h_{(j+1)t-1}\}$ **then** ▷ consistent support block
        $b_c \leftarrow j,\ c \leftarrow c+1$ ▷ also: $U \leftarrow U \setminus \{1/h_i + 1/h_0 \mid i = jt, \ldots, (j+1)t-1\}$
      end if
    end for
  end if
until $ct \geqslant n$ ▷ consistent roots and support
$h \leftarrow (h_0, \ldots, h_{q-1}),\ b \leftarrow (b_0, \ldots, h_{c-1})$ ▷ also: $\omega \xleftarrow{\$} U$
return $h,\ b$ ▷ also: ω

reach better performance compared to the original IBI scheme in [5]. We can mention, that the use of a quasi-dyadic matrix in Stern's protocol preserves the security against Simple Analysis (SPA) and Differential Power Analysis (DPA) attacks, this can be achieved by adapting the masking technique suggested in [6] for the case of quasi-cyclic codes.
By virtue of the so-called Fiat-Shamir Paradigm [9], it is possible to convert the identity based identification scheme using quasi-dyadic codes (QD-IBI) into an identity based signature scheme (QD-IBS).

Suggested parameters of the QD-IBI scheme We suggest the same parameters suggested for the QD-CFS in subsection 4.1, i.e.$(m,t) = (15,12)$; these parameters are enough to ensure a security of more than 2^{80} binary operations.against all currently known attacks.

In the following table, we compare the QD-IBI and QD-IBS schemes using the QD-CFS with the original IBI and IBS schemes for the parameters $m = 15$, $t = 12$.

Table 2 shows the advantage of QD-IBI and QD-IBS schemes concerning the size of public data, the signature size, and the communication overhead.

Table 2. Comparison of IBI/IBS and IBI (QD-IBI/IBS)

	IBI/IBS	**IBI (QD-IBI/IBS)**
Private key size	180 Bit	180 Bit
Public key size	180 Bit	180 Bit
Matrix size	720 kByte	169 kByte
Communication cost	232 kByte	219 kByte
Signature length	600 kByte	560 kByte

5 Conclusion

In this paper, we have proposed an improved identity based identification and signature scheme based on coding theory using quasi-dyadic codes. Our scheme has the advantage to reduce a public data size, the communication complexity and the signature length. For further improvements, we can imagine the use of Parallel-CFS proposed in [10]. Unfortunately, as often in code-based cryptography our improved scheme suffers from large system parameters, therefore we encourage the cryptography community to work in this area because a lot of proposals are needed to make code based schemes more practical and then to be a good alternative for the classic cryptography.

References

1. P. S. L. M. Barreto, P.-L. Cayrel, G. Hoffman, and R. Misoczki. GPU implementation of the quasi-dyadic CFS signature scheme. preprint 2010.
2. P. S. L. M. Barreto, P.-L. Cayrel, R. Misoczki, and R. Niebuhr. Quasi-dyadic CFS signature. *Inscrypt 2010*, 2010.
3. E. Berlekamp, R. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.
4. P.-L. Cayrel, P. Gaborit, D. Galindo, and M. Girault. Improved identity-based identification using correcting codes. *CoRR*, abs/0903.0069, 2009.
5. P.-L. Cayrel, P. Gaborit, and M. Girault. Identity-based identification and signature schemes using correcting codes. In *International Workshop on Coding and Cryptography, WCC 2007*, pages 69–78. editors : Augot, D., Sendrier, N., and Tillich, J.-P.
6. P.-L. Cayrel, P Gaborit, and E. Prouff. Secure implementation of the Stern authentication and signature schemes for low-resource devices. In *CARDIS*, pages 191–205, 2008.
7. N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology – Asiacrypt'2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 157–174, Gold Coast, Australia, 2001. Springer.
8. J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. A distinguisher for high rate mceliece cryptosystem – extended abstract. In P. Véron, editor, *Yet Another Conference on Cryptography, YACC 2010*, pages 1–4, Toulon, 2010.
9. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology — Crypto '86*.
10. M. Finiasz. Parallel-CFS, strengthening the CFS mceliece-based signature scheme. to appear at SAC 2010.
11. M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. In *to appear in Advances in Cryptology – Asiacrypt'2009*, 2009. http://eprint.iacr.org/2009/414.pdf.
12. F. J. Macwilliams and N. J. A. Sloane. The theory of error-correcting codes. 1978.
13. R. McEliece. A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report, DSN PR 42–44, 1978. http://ipnpr.jpl.nasa.gov/progress report2/42-44/44N.PDF.
14. P. S. L. M. Misoczki and P. S. L. M. Barreto. Compact McEliece keys from Goppa codes. In *Selected Areas in Cryptography – SAC'2009*, volume 5867 of *LNCS*, pages 276–392. Springer, 2009.
15. H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.
16. S. Schechter. On the inversion of certain matrices. *Mathematical Tables and Other Aids to Computation*, 13(66):73–77, 1959. http://www.jstor.org/stable/2001955.

17. A. Shamir. Identity-based cryptosystems and signature schemes. *Advances in Cryptology-Crypto'84*, 1984.
18. J. Stern. A new identification scheme based on syndrome decoding. volume Lecture Notes in Computer Science vol. 773 Springer 1993, pages 13–21, 1993.