A zero knowledge identification scheme based on the q-ary SD problem

Pierre-Louis Cayrel, Pascal Véron, Sidi Mohamed El Yousfi Alaoui

A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem

Pierre-Louis Cayrel[1], Pascal Véron[2], and Sidi Mohamed El Yousfi Alaoui[1]

[1] CASED – Center for Advanced Security Research Darmstadt,
Mornewegstrasse 32, 64293 Darmstadt, Germany
{pierre-louis.cayrel,elyousfi}@cased.de
[2] IMATH
Université du Sud Toulon-Var.
B.P. 20132, F-83957 La Garde Cedex, France
veron@univ-tln.fr

Abstract. At CRYPTO'93, Stern proposed a 3-pass code-based identification scheme with a cheating probability of 2/3. In this paper, we propose a 5-pass code-based protocol with a lower communication complexity, allowing an impersonator to succeed with only a probability of 1/2. Furthermore, we propose to use double-circulant construction in order to dramatically reduce the size of the public key.

The proposed scheme is zero-knowledge and relies on an NP-complete coding theory problem (namely the q-ary Syndrome Decoding problem). The parameters we suggest for the instantiation of this scheme take into account a recent study of (a generalization of) Stern's information set decoding algorithm, applicable to linear codes over arbitrary fields $\mathbb{F}_q$; the public data of our construction is then 4 Kbytes, whereas that of Stern's scheme is 15 Kbytes for the same level of security. This provides a very practical identification scheme which is especially attractive for light-weight cryptography.

Keywords: post-quantum cryptography, code-based cryptography, Stern's scheme, identification, zero-knowledge.

1 Introduction

Shor's quantum algorithm for integer factorization, which was published in 1994, poses a serious threat to most cryptographic systems in use today. In particular, all constructions whose security relies on number theory (such as variants of the discrete logarithm problem or integer factorization) are vulnerable to this algorithm. If quantum computers will at one point exist, such schemes can be broken in polynomial time, whereas no quantum attacks are known for lattice-based, code-based, and multivariate cryptographic systems. On the other hand, even should such number-theoretic assumptions remain hard, it is not wise to rely on a single type of hard problems. Furthermore, as the capacity of current adversaries increases, so does the key size for classical constructions; it is possible

A. Biryukov, G. Gong, and D.R. Stinson (Eds.): SAC 2010, LNCS 6544, pp. 171–186, 2011.

that alternative post-quantum constructions may provide a better alternative in that sense.

In this paper, we consider a particular type of alternative cryptography, based on error-correcting code theory. Code-based cryptography was initiated a long time ago with the celebrated McEliece encryption algorithm.

We consider the question of public key identification (ID) protocols in this context. Such schemes allow a party holding a secret key to prove its identity to any other entity holding the corresponding public key. The minimum security of such protocols should be that a passive observer who sees the interaction should not then be able to perform his own interaction and successfully impersonate the prover.

Stern's code-based identification scheme, proposed at CRYPTO'93, is still the reference in this area [26]. 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 construction has two major drawbacks:

1. Since the probability of a successful impersonation is 2/3 for Stern's construction instead of 1/2 as in the case of Fiat-Shamir's protocol based on integer factorization [11], Stern's scheme uses more rounds to achieve the same security, typically 28 rounds for an impersonation resistance of 2^{-16}.
2. There is a common data shared by all users (from which the public identification is derived) which is very large, typically 66 Kbits. In Fiat Shamir's scheme, this common data is 1024 bits long.

The second issue was addressed by Gaborit and Girault in [12] and by Véron in [29]. In this paper, we focus on the first drawback. Using q-ary codes instead of binary ones, we define a 5-pass identification scheme for which the success probability of a cheater is 1/2. We then propose to use quasi-cyclic construction to address the second drawback.

Organization of the Paper

In Section 2, we give basic facts about code-based cryptography and describe the original scheme due to Stern; in Section 3 we show a new identification scheme which allows us to reduce the number of identification rounds. In Section 4, we describe the properties of our proposal and study its security. Section 5 presents some concluding remarks to our contribution.

2 Code-Based Cryptography

In this section we recall basic facts about code-based cryptography. We refer to [4], for a general introduction to these issues.

2.1 Definitions

Linear codes are k-dimensional subspaces of an n-dimensional vector space over a finite field $\mathbb{F}_q$, where k and n are positive integers with $k < n$, and q a prime

power. The error-correcting capability of such a code is the maximum number t of errors that the code is able to decode. In short, linear codes with these parameters are denoted (n, k, t)-codes.

Definition 1 (Hamming weight). *The (Hamming) weight of a vector x is the number of non-zero entries. We use $\mathsf{wt}(x)$ to represent the Hamming weight of x.*

Definition 2 (Generator and Parity Check Matrix). *Let $\mathscr{C}$ be a linear code over $\mathbb{F}_q$. A generator matrix G of $\mathscr{C}$ is a matrix whose rows form a basis of $\mathscr{C}$:*

$$\mathscr{C} = \{xG : x \in \mathbb{F}_q^k\}$$

A parity check matrix H of $\mathscr{C}$ is is an $(n-k) \times n$ matrix whose rows form a basis of the orthogonal complement of the vector subspace $\mathscr{C}$, i.e. it holds that,

$$\mathscr{C} = \{x \in \mathbb{F}_q^n : Hx^T = 0\}$$

Let n and r be two integers such that $n \geq r, \mathsf{Binary}(n, r)$ (resp. $\mathsf{q-ary}(n, r)$) be the set of binary (resp. q-ary) matrices with n columns and r rows of rank r. Moreover, denote by $x \xleftarrow{\$} A$, the random choosing of x amongst the elements of a set A.

We describe here the main hard problems on which the security of code-based cryptosystems mostly relies.

Definition 3 (Binary Syndrome Decoding (SD) problem)
Input : $H \xleftarrow{\$} \mathsf{Binary}(n, r)$, $y \xleftarrow{\$} \mathbb{F}_2^r$, *and an integer* $\omega > 0$.
Output : *A word* $s \in \mathbb{F}_2^n$ *such that* $\mathsf{wt}(s) \leq \omega$, $Hs^T = y$.

This problem was proven to be NP-complete in 1978 [3]. An equivalent dual version of the SD problem can be presented as follows:

Definition 4 (General Binary Decoding (G-SD) problem)
Input : $G \xleftarrow{\$} \mathsf{Binary}(n, n-r)$, $y \xleftarrow{\$} \mathbb{F}_2^n$, *and an integer* $\omega > 0$.
Output : *A word* $x \in \mathbb{F}_2^{n-r}$, $e \in \mathbb{F}_2^n$ *such that* $\mathsf{wt}(e) \leq \omega$ *and* $xG + e = y$.

Finally, this problem can be considered over an arbitrary finite field.

Definition 5 (q-ary Syndrome Decoding (qSD) problem)
Input : $H \xleftarrow{\$} \mathsf{q-ary}(n, r)$, $y \xleftarrow{\$} \mathbb{F}_q^r$, *and an integer* $\omega > 0$.
Output : *A word* $s \in \mathbb{F}_q^n$ *such that* $\mathsf{wt}(s) \leq \omega$ *and* $Hs^T = y$.

In 1994, A. Barg proved that this last problem remains NP-complete [1, in russian].

The problems which cryptographic applications rely upon can have different numbers of solutions. For example, public key encryption schemes usually have exactly one solution, while digital signatures often have more than one possible solution. For code-based cryptosystems, the uniqueness of solutions can be expressed by the Gilbert-Varshamov (GV) bound:

Definition 6 (q-ary Gilbert-Varshamov bound)
Let $H_q(x)$ be the q-ary entropy function, given by:

$$H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$$

Suppose $0 \leq \xi \leq (q-1)/q$. Then there exists an infinite sequence of (n, k, d) q-ary linear codes with $d/n = \xi$ and rate $R = k/n$ satisfying the inequality:

$$R \geq 1 - H_q(\xi) \qquad \forall n.$$

2.2 SD and G-SD Identification Schemes

Stern's scheme is the first practical zero-knowledge identification scheme based on the Syndrome Decoding problem [26]. The scheme uses a binary $(n-k) \times n$ matrix H common to all users. If H is chosen randomly, it will provide a parity check matrix for a code with asymptotically good minimum distance given by the (binary) Gilbert-Varshamov (GV) bound. The private key for a user will thus be a word s of small weight $\mathsf{wt}(s) = \omega$ (e.g. $\omega \approx$ GV bound), which corresponds to the syndrome $Hs^T = y$, the public key. By Stern's 3-pass zero-knowledge protocol, the secret key holder can prove his knowledge of s by using two blending factors: a permutation and a random vector. However, a dishonest prover not knowing s can cheat the verifier in the protocol with probability $2/3$. Thus, the protocol has to be run several times to detect cheating provers. The security of the scheme relies on the hardness of the general decoding problem, that is on the difficulty of determining the preimage s of $y = Hs^T$.

As mentioned in [3], the SD problem stated in terms of generator matrices is also NP-complete since one can go from the parity-check matrix to the generator matrix (or vice-versa) in polynomial time. In [29], the author uses a generator matrix of a random linear binary code as the public key and defines this way a dual version of Stern's scheme in order to obtain, among other things, an improvement of the transmission rate : the G-SD identification scheme.

Fig. 1 sums up the performances of the two 3-pass SD identification schemes for a probability of cheating bounded by 10^{-6}. The prover's complexity is the number of bit operations involved for the prover in the protocol run, while the communication complexity is measured in the number of exchanged bits. We considered that hash values are 160 bits long and seeds used to generate permutations 128 bits long.

2.3 Attacks

For SD identification schemes, since the matrix used is a random one, the cryptanalyst is faced with the problem of decoding a random binary linear code. There are two main families of algorithms to solve this problem: Information Set Decoding (ISD) and (Generalized) Birthday Algorithm (GBA). The Information Set Decoding algorithm has the lowest complexity of the two; the strategy to recover the k information symbols is as follows: the first step is to pick k of the

	SD	G-SD
Rounds	35	35
Public data (bits)	65792	66048
Prover's complexity	$2^{22.14}$	$2^{22.13}$
Communication complexity	43750	37777

Fig. 1. Performances of SD schemes,security level 2^{70}, probability of cheating 10^{-6}

n coordinates randomly in the hope that all of them are error-free. Then try to recover the message by solving a $k \times k$ linear system (binary or over $\mathbb{F}_q$).

In [19], the author describes and analyzes the complexity of a generalization of Stern's information set decoding algorithm from [25] which permit the decoding of linear codes over arbitrary finite fields $\mathbb{F}_q$. We will choose our parameters with regards to the complexity of this attack.

3 An Identification Scheme Based on qSD

To our knowledge, amongst all the identification schemes whose security does not depend upon some number theoretic assumptions, only three of them involve 5-pass, have a probability of cheating bounded by 1/2, and deal with values over a finite field $\mathbb{F}_q$ ($q > 2$) : PKP, Chen's scheme and CLE ([24],[8], [27]). Stern's 5-pass variant of SD is on a binary field, PPP [22] 5-pass variant has a probability of cheating bounded by 2/3 and $\mathcal{MQ}^*$-IP is a 2-pass protocol [30].

PKP, Chen's scheme and CLE have one thing in common : once the commitments sent, the verifier sends a random challenge which is an element $\alpha \in \mathbb{F}_q$. Then the prover sends back his secret vector scrambled by : a random vector, a random permutation and the value α. We proposed in this paper to show how to adapt this common step in the context of the qSD problem. Notice that while it is known since Barg's paper in 1994, that the qSD problem is NP-complete, it's only from the recent works developed in [18,19] that it was possible to set up realistic parameters for the security of an identification scheme based on the qSD problem. To end this remark, we just mention that Chen's scheme based on rank metric codes is not secured [7].

In what follows, we write elements of $\mathbb{F}_q^n$ as n blocks of size $\lceil \log_2(q) \rceil = N$. We represent each element of $\mathbb{F}_q$ as N bits. We first introduce a special transformation that we will use in our protocol.

Definition 7. *Let Σ be a permutation of $\{1, \ldots, n\}$ and $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{F}_q^n$ such that $\forall i, \gamma_i \neq 0$. We define the transformation $\Pi_{\gamma,\Sigma}$ as :*

$$\begin{array}{rccc} \Pi_{\gamma,\Sigma} : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & v & \mapsto & (\gamma_{\Sigma(1)} v_{\Sigma(1)}, \ldots, \gamma_{\Sigma(n)} v_{\Sigma(n)}) \end{array}$$

Notice that $\forall \alpha \in \mathbb{F}_q, \forall v \in \mathbb{F}_q^n, \Pi_{\gamma,\Sigma}(\alpha v) = \alpha \Pi_{\gamma,\Sigma}(v),$ and $\mathsf{wt}(\Pi_{\gamma,\Sigma}(v)) = \mathsf{wt}(v)$.

Our identification scheme consists of two parts: a key generation algorithm (Fig. 2) and an identification protocol (Fig. 3); in the following we will describe these parts.

3.1 Key Generation

For $r = n - k$, the scheme uses a random $(r \times n)$ q-ary matrix H common to all users which can be considered to be the parity check matrix of a random linear (n, k) q-ary code. We can assume that H is described as $(I_r|M)$ where M is a random $r \times r$ matrix; as Gaussian elimination does not change the code generated by H, there is no loss of generality. Let κ be the security parameter. Fig. 2 describes the key generation process ($\mathrm{WF}_{\mathrm{ISD}}$ denotes the workfactor of the Information Set Decoding algorithm).

KeyGen:
Choose n, k, ω, and q such that $\mathrm{WF}_{\mathrm{ISD}}(n, r, \omega, q) \geq 2^{\kappa}$
$H \xleftarrow{\$} \mathbb{F}_q^{r \times n}$
$s \xleftarrow{\$} \mathbb{F}_q^n$, s.t. $\mathsf{wt}(s) = \omega$.
$y \leftarrow Hs^T$
Output $(\mathrm{sk}, \mathrm{pk}) = (s, (y, H, \omega))$

Fig. 2. Key generation algorithm: parameters n, k, w, q are public

3.2 Identification Protocol

The secret key holder can prove his knowledge of s by using two blending factors: the transformation by means of a permutation and a random vector. In the next section we will show how a dishonest prover not knowing s can cheat the verifier in the protocol with probability of $q/2(q-1)$. Thus, the protocol has to be run several times to detect cheating provers. The security of the scheme relies on the hardness of the general decoding problem, that is on the difficulty of determining the preimage s of $y = Hs^T$. In Fig. 3, h denotes a hash function and S_n the symmetric group of degree n.

4 Properties and Security of the Scheme

4.1 Zero-Knowledge-Proof

Let $I = (H, y, \omega)$ be the public data shared by the prover and the verifier in our construction, and let $P(I, s)$ be the predicate:

$P(I, s) =$ "s is a vector which satisfies $Hs^T = y, \mathsf{wt}(s) = \omega$". We show in this section that the protocol presented in Fig. 3 corresponds to a zero-knowledge interactive proof. To this end, we provide in the following proofs for the completeness, soundness, and zero-knowledge properties of our identification scheme.

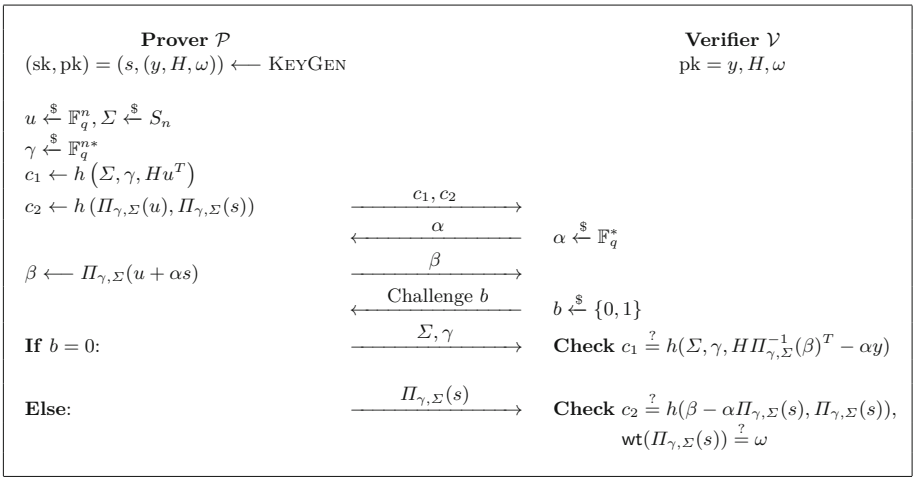

Fig. 3. Identification protocol

Completeness. Clearly, each honest prover which has the knowledge of a valid secret s, the blending mask u, and the permutation $\Pi_{\gamma,\Sigma}$ for the public data can answer correctly any of the honest verifier's queries in any given round, thus the completeness property of the scheme is satisfied.

Zero-Knowledge. The zero-knowledge property for our identification protocol (Fig. 3) is proved in the random oracle model assuming that the hash function h has statistical independence properties.

Theorem 1. *The construction in Fig. 3 is a zero-knowledge interactive proof for $P(I, s)$ in the random oracle model.*

Proof. The proof uses the classical idea of resettable simulation [13]. Let M be a polynomial-time probabilistic Turing machine (simulator) using a dishonest verifier. Because of the two interaction with the prover, we have to assume that the dishonest verifier could contrive two strategies : $St_1(c_1, c_2)$ taking as input the prover's commitments and generating a value $\alpha \in \mathbb{F}_q^*$, $St_2(c_1, c_2, \beta)$ taking as input the prover's commitments, the answer β and generating as output a challenge in the set $\{0, 1\}$. M will generate a communication tape representing the interaction between prover and verifier. The goal is to produce a communication tape whose distribution is indistinguishable from a real tape by an honest interaction. The simulator M is constructed as follows :

Step 1. M randomly picks a query b from $\{0, 1\}$.

– If $b = 0$, M randomly chooses: u, γ, and Σ, and solves the equation: $Hs'^T = y$ for some s' not necessarily satisfying the condition $\mathsf{wt}(s') = \omega$. The commitments are taken as $c_1 = h(\Sigma, \gamma, Hu^T)$, and c_2 as a random string. By simulating the verifier, M applies $St_1(c_1, c_2)$ to get $\alpha \in \mathbb{F}_q^*$, and then computes

$\beta = \Pi_{\gamma,\Sigma}(u + \alpha s')$, and has the information needed to derive the simulated communication data between prover and verifier. Therefore the candidates to be written in the communication tape consist of elements $A = c_1||c_2$, β and $ans = \gamma||\Sigma$. Taking into account the uniform distribution of the random variables used in the computation of A, ans and β, it follows that the distribution of these elements is indistinguishable from those resulting from a fair interaction.

– If $b = 1$ the machine also chooses u, γ, and Σ at random. This time it picks s as random from the set $\mathbb{F}_q^n$ with weight ω. The commitment c_1 will be given uniformly at random value and $c_2 = h(\Pi_{\gamma,\Sigma}(u), \Pi_{\gamma,\Sigma}(s))$. Again, from $St_1(c_1, c_2)$, the machine computes $\beta = \Pi_{\gamma,\Sigma}(u+\alpha s)$, and has the information needed to derive the simulated communication data. The communication set features elements $A = c_1||c_2$, β and $ans = \Pi_{\gamma,\Sigma}(s)$. The uniformly random character of the choices made will render these elements indistinguishable from those resulting from a fair interaction.

Step 2. M applies the verifier's strategy $St_2(c_1, c_2, \beta)$ obtaining b' as result.
Step 3. When $b = b'$, the machine M writes on its communication tape the values of A, α, β, b and ans. If the values differ, however, nothing is written and the machine returns to step 1.

Therefore, in 2δ rounds on average, M produces a communication tape indistinguishable from another that corresponds to a fair identification process execution that takes δ rounds. This concludes the proof. □

Soundness: We now show that at each round, a dishonest prover is able to cheat a verifier to accept his identity with a probability limited by $q/(2(q-1))$.

Let us suppose that a dishonest prover has devised the following strategies to cope with the challenges that the verifier is expected to send. The first strategy (st_0) corresponds to the actions the prover takes when hoping to receive 0 as challenge. He chooses u, γ, and Σ at random and solves the equation $Hs'^T = y$ without satisfying the condition $\mathsf{wt}(s') = \omega$. Then he computes c_1 according to these values and randomly generates c_2. Thus, he will be able to answer the challenge $b = 0$, regardless of the value of α chosen by the verifier. The second strategy (st_1) is successful in case a value 1 is received as challenge. He chooses u, γ and Σ at random and picks an s' with Hamming weight w. With this choice, the commitment c_2 can be correctly reconstructed, and the Hamming weight of the fake private key validated. The commitment c_1 is randomly generated.

Now, these two strategies can be improved. Indeed a dishonest prover can try to make a guess on the value α sent by the verifier. Let α_c be the guessed value, so that β would be $\Pi_{\gamma,\Sigma}(u + \alpha_c s')$.

In st_0, instead of randomly generating c_2, he computes $c_2 = h(\beta - \alpha_c\tilde{s}, \tilde{s})$ where $\tilde{s}$ is a random word of Hamming weight w which will be sent as answer (if $b = 1$) instead of $\Pi_{\gamma,\Sigma}(s')$. With such a strategy, the cheater can answer to $b = 0$ regardless the value of α chosen by the verifier and to $b = 1$ if $\alpha = \alpha_c$.

In st_1, instead of randomly generating c_1, he computes $c_1 = h(\Sigma, \gamma, Hu^T + \alpha_c(Hs'^T - y))$. With such a strategy, the cheater can answer to $b = 1$ regardless the value of α chosen by the verifier and to $b = 0$ if $\alpha = \alpha_c$.

Therefore, when we consider the probability space represented by the random variables b and α, the success probability of a strategy st for one round is given by:

$$P[\text{successful impersonation}] = \sum_{i=0}^{1} P(st = st_i)P(b = i) + P(st = st_i)P(b = 1 - i)P(\alpha = \alpha_c) = \frac{q}{2(q-1)}.$$

Though it was calculated for the particular strategies above, this value also corresponds to the upper limit for generic cheating strategies as shown below. The security assumptions that we make are as follows: we require that the commitment scheme be computationally binding and that the qSD problem be hard. We now show that if a cheating prover manages to answer more than $(\frac{q}{2(q-1)})^\delta$ of the queries made by a verifier after δ rounds, either of the security assumptions above was broken, as stated in the theorem below.

Let us denote by $\overline{B}$ an honest verifier and by $\tilde{A}$ a cheating prover.

Theorem 2. *If $\overline{B}$ accepts $\tilde{A}$ proof with probability $\geqslant (\frac{q}{2(q-1)})^\delta + \varepsilon$, then there exists a polynomial time probabilistic machine M which, with overwhelming probability, either computes a valid secret s or finds a collision for the hash function.*

Proof. Let T be the execution tree of $(\tilde{A}, \overline{B})$ corresponding to all possible questions of the verifier when the adversary has a random tape RA. $\overline{B}$ may ask $2(q-1)$ possible questions at each stage. Each question is a couple (α, b) where $\alpha \in \mathbb{F}_q^*$ and $b \in \{0, 1\}$. First we are going to show that, unless a hash-collision has been found, a secret key s can be computed from a vertex with $q + 1$ sons. Then we will show that a polynomial time M can find such a vertex in T with overwhelming probability.

Let V be a vertex with $q + 1$ sons. This corresponds to a situation where 2 commitments c_1, c_2 have been made and where the cheater has been able to answer to $q+1$ queries. That is to say that there exists $\alpha \neq \alpha'$ such that the cheater answered correctly to the queries $(\alpha, 0)$, $(\alpha, 1)$, $(\alpha', 0)$ and $(\alpha', 1)$. Now let :

- (β, Σ, γ) the answer sent for the query $(\alpha, 0)$,
- (β, z) the answer sent for the query $(\alpha, 1)$,
- $(\beta', \Sigma', \gamma')$ the answer sent for the query $(\alpha', 0)$,
- (β', z') the answer sent for the query $(\alpha', 1)$,

the value z (resp. z') represents the expected value $\Pi_{\gamma,\Sigma}(s)$, (resp. $\Pi_{\gamma',\Sigma'}(s)$), hence $\mathrm{wt}(z) = \omega$. Notice also that the same value β (resp. β') is used for $(\alpha, 0)$ and $(\alpha, 1)$ (resp. $(\alpha', 0)$ and $(\alpha', 1)$) since it is sent before the bit challenge b. Then, because commitment c_1 (resp. c_2) is consistent with both queries $(\alpha, 0)$ and $(\alpha', 0)$ (resp. $(\alpha, 1)$ and $(\alpha', 1)$), we have:

$$h(\Sigma, \gamma, H\Pi_{\gamma,\Sigma}^{-1}(\beta)^T - \alpha y) = c_1 = h(\Sigma', \gamma', H\Pi_{\gamma',\Sigma'}^{-1}(\beta')^T - \alpha' y)\,,$$

and

$$h(\beta - \alpha z, z) = c_2 = h(\beta' - \alpha' z', z')\,.$$

The equations are satisfied by finding collisions on the hash function or having the following equalities:

$$\begin{aligned} \Sigma &= \Sigma' \\ \gamma &= \gamma' \\ z &= z' \\ H\Pi^{-1}_{\gamma,\Sigma}(\beta)^T - \alpha y &= H\Pi^{-1}_{\gamma',\Sigma'}(\beta')^T - \alpha' y \\ \beta - \alpha z &= \beta' - \alpha' z'\,. \end{aligned}$$

Hence:

$$\begin{aligned} H\Pi^{-1}_{\gamma,\Sigma}(\beta - \beta')^T(\alpha - \alpha')^{-1} &= y \\ (\beta - \beta')^T(\alpha - \alpha')^{-1} &= z\,. \end{aligned}$$

Then:

$$H\Pi^{-1}_{\gamma,\Sigma}(z) = y\,.$$

Therefore, the value $s = \Pi^{-1}_{\gamma,\Sigma}(z)$ with $\mathsf{wt}(\Pi^{-1}_{\gamma,\Sigma}(z)) = \mathsf{wt}(z) = \omega$, obtained from the equalities above, constitutes a secret key that can be used to impersonate the real prover.

Now, the assumption implies that the probability for T to have a vertex with $q+1$ sons is at least ε. Indeed, let us consider RA the random tape where $\tilde{A}$ randomly picks its values, and let Q bet the set $\mathbb{F}_q^* \times \{0,1\}$. These two sets are considered as probability spaces both of them with the uniform distribution.

A triple $(c, \alpha, b) \in (RA \times Q)^\delta$ represents the commitments, answers and queries exchanged between $\tilde{A}$ and $\tilde{B}$ during an identification process (c represents commitments and answers). We will say that (c, α, b) is "valid", if the execution of $(\tilde{A}, \tilde{B})$ leads to the success state.

Let V be the subset of $(RA \times Q)^\delta$ composed of all the valid triples. The hypothesis of the lemma means that:

$$\frac{\mathrm{card}(V)}{\mathrm{card}((RA \times Q)^\delta)} \geq \left(\frac{q}{2(q-1)}\right)^\delta + \varepsilon.$$

Let Ω_δ be a subset of RA^δ such that:

- If $c \in \Omega_\delta$, then $q^\delta + 1 \leq \mathrm{card}\{(\alpha, b),\ (c, \alpha, b) \text{ be valid }\} \leq (2(q-1))^\delta$,
- If $c \in RA^\delta \setminus \Omega_\delta$, then $0 \leq \mathrm{card}\{(\alpha, b),\ (c, \alpha, b) \text{ be valid }\} \leq q^\delta$.

Then, $V = \{\text{valid } (c, \alpha, b), c \in \Omega_\delta\} \cup \{\text{valid } (c, \alpha, b), c \in RA^\delta \setminus \Omega_\delta\}$, therefore:

$$\mathrm{card}(V) \leqslant \mathrm{card}(\Omega_\delta)(2(q-1))^\delta + (\mathrm{card}(RA^\delta) - \mathrm{card}(\Omega_\delta))q^\delta.$$

Thus

$$\frac{\mathrm{card}(V)}{\mathrm{card}((RA\times Q)^{\delta})} \leqslant \frac{\mathrm{card}(\Omega_{\delta})}{\mathrm{card}(RA^{\delta})} + q^{\delta}\left((2(q-1))^{-\delta} - \frac{\mathrm{card}(\Omega_{\delta})}{\mathrm{card}((RA\times Q)^{\delta})}\right)$$

$$\leq \frac{\mathrm{card}(\Omega_{\delta})}{\mathrm{card}(RA^{\delta})} + \left(\frac{q}{2(q-1)}\right)^{\delta}.$$

It follows that:

$$\frac{\mathrm{card}(\Omega_{\delta})}{\mathrm{card}(RA^{\delta})} \geq \varepsilon.$$

This shows that the probability that an intruder might answer to (at least) $q^{\delta}+1$ of the verifier's queries, by choosing random values, is greater than ε. Now, if more than $q^{\delta}+1$ queries are bypassed by an intruder then $T(RA)$ has at least $q^{\delta}+1$ leaves, i.e. $T(RA)$ has at least a vertex with $q+1$ sons.

So, by resetting $\tilde{A}$ $\frac{1}{\varepsilon}$ times, and by repeating again, it is possible to find an execution tree with a vertex with $q+1$ sons with probability arbitrary close to one. This theorem implies that either the hash function h is not collision free, or the qSD problem is not intractable. Therefore, the soundness property was demonstrated, given that one must have the probability negligibly close to 1/2.

4.2 Security and Parameters

As for binary SD identification schemes, the security of our scheme relies on three properties of random linear q-ary codes:

1. Random linear codes satisfy the q-ary Gilbert-Varshamov lower bound [15];
2. For large n almost all linear codes lie over the Gilbert-Varshamov bound [20];
3. Solving the q-ary syndrome decoding problem for random codes is NP-complete [1].

We now have to choose parameters for an instantiation of the construction in Fig. 3. We take into account the bounds corresponding to the Information Set Decoding algorithm over $\mathbb{F}_q$ in [18] and propose parameters for a security level of at least 2^{80}. The number of rounds must then be chosen in order to minimize the success probability of a cheater.

Since we deal with random codes, we have to select parameters with respect to the Gilbert-Varshamov bound (see Definition 6), which is optimal for $k = r = n/2$. We assume this to be true in the remainder of the paper.

Let N be the number of bits needed to encode an element of $\mathbb{F}_q$, ℓ_h the output size of the hash function h, ℓ_{Σ} *(resp.* ℓ_{γ}*)* the size of the seed used to generate the permutation Σ *(resp. the permutation* γ*)*, and δ the number of rounds. We have the following properties for our scheme:

Size of the matrix in bits:

$$k \times k \times N (\text{we use the systematic form of } H)$$

Size of the public identification:

$$kN$$

Size of the secret key:

$$nN$$

Total number of bits exchanged:

$$\delta(2\ell_h + N + nN + 1 + (\ell_\Sigma + \ell_\gamma + nN)/2)$$

Prover's computation complexity over $\mathbb{F}_q$:

$$\delta((k^2 + \mathsf{wt}(s)) \text{ multiplications} + (k^2 + \mathsf{wt}(s)) \text{ additions})$$

To obtain a precise complexity on the workfactor of ISD algorithms over $\mathbb{F}_q$ we've used the code developed by C. Peters, which estimates the number of iterations needed for an attack using a Markov chain implementation [19]. ISD algorithms depend on a set of parameters and this code allows to test which ones can minimize the complexity of the attack.

For our scheme, we suggest the following parameters:

$$q = 256, n = 128, k = 64, \mathsf{wt}(s) = 49.$$

The complexity of an attack using ISD algorithms is then at least 2^{87}. For the same security level in SD schemes, we need to take $n = 700, k = 350, \mathsf{wt}(s) = 75$.

In [26], Stern has proposed two 5-pass variants of his scheme. The first one to lower the computing load. However, this variant slightly increases the probability of cheating rather than lowering it, and thus increases the communication complexity. The other one minimizes the number of rounds and lower the probability of cheating to $(1/2)^\delta$. The following table shows the advantage regarding the communication cost and the size of the matrix of our scheme in comparison with Stern's initial proposal and his second variant, for the same security level of 2^{87} and an impersonation resistance of 2^{-16}. We considered that all seeds used are 128 bits long and that hash values are 160 bits long.

	SD	G-SD	Stern 5-pass	Our scheme
Rounds	28	28	16	16
Matrix size (bits)	122500	122500	122500	32768
Public Id (bits)	350	700	2450	512
Secret key (bits)	700	1050	4900	1024
Communication (bits)	42019	35486	62272	31888
Prover's Computation	$2^{22.7}$op. over $\mathbb{F}_2$	$2^{22.7}$op. over $\mathbb{F}_2$	$2^{21.92}$op. over $\mathbb{F}_2$	2^{16}mult + 2^{16}add op. over $\mathbb{F}_{256}$

Fig. 4. SD schemes vs. q-ary SD scheme, security level 2^{87}, probability of cheating 2^{-16}

To obtain a security level of 2^{128} the indicated parameters are,

$$q = 256, n = 208, k = 104, \mathsf{wt}(s) = 78,$$

which gives a scheme with the following properties:

Number of Rounds : 16
Matrix size (bits) : 86528
Public Id (bits) : 832
Secret key (bits) : 1664
Communication (bits) : 47248
Prover's Computation : $2^{17.4}$mult. and $2^{17.4}$add. over $\mathbb{F}_{256}$

4.3 Comparison with Other Schemes

We compare our scheme to some other zero-knowledge schemes whose security does not depend upon number theoretic assumptions, and where the whole probability of cheating is bounded by $(1/2)^{\delta}$ (except for PPP). We use some results given in [21], [22], [23] and [14] and try to adapt parameters such that the security level be as near as possible than 2^{87} for a fair comparison. Notice that for CLE, the result given in our table does not fit with what is given in [22] and [23]. Indeed, as mentioned in [27], the zero-knowledge property of the scheme can only be stated if two quantities ($S\sigma$ and $T\tau$) are public in addition to the public identification. For PPP, we considered the 3 pass version instead of the five one because, as stated by the authors in [22], it is more efficient from a computational point of view and furthermore easier to implement. As for our scheme, only a part of the matrix can be stored in PKP. All these schemes uses a random matrix shared by all users. In Fig. 5, we considered that all seeds used are 128 bits long and that hash values are 160 bits long. We have not considered for the prover's complexity the cost of the computation of hash values but the number of hash values to compute is mentioned in Fig. 5.

Notice that for a level of security near from 2^{80} we could have used smaller parameters. This would improve the general performances of our scheme, but we think that the suggested parameters fit well for practical implementation.

	PKP	CLE	PPP	Our scheme
Rounds	16	16	39	16
Matrix size	24×24	24×24	161×177	64×64
over the field	$\mathbb{F}_{251}$	$\mathbb{F}_{257}$	$\mathbb{F}_2$	$\mathbb{F}_{256}$
Public Id (bits)	384	288	245	512
Secret key (bits)	128	192	177	1024
Communication (bits)	13456	16528	51441	31888
Prover's Computation	$2^{13.28}$add., $2^{13.28}$ mul.	$2^{13.28}$add., $2^{13.34}$ mul.	$2^{21.1}$ add., $2^{21.1}$ mul.	2^{16} add. +, 2^{16} mul.
over the field	$\mathbb{F}_{251}$	$\mathbb{F}_{257}$	$\mathbb{F}_{127}$	$\mathbb{F}_{256}$
Number of hash values	2	2	8	2
Security level	2^{85}	$\simeq 2^{84}$	$> 2^{74}$	2^{87}

Fig. 5. qSD scheme vs. other schemes, probability of cheating 2^{-16}

To see how the performances are modified with a lower probability of cheating, interested readers can consult [9].

4.4 Reducing Public Key Size

Double-circulant construction. The authors of [12] propose a variation of the Stern identification scheme by using double-circulant codes. The circulant structure of the matrix used as a public key requires very little storage and greatly simplifies the computation, as the binary matrix needs never to be wholly generated. Still in this context, the authors show that all random double-circulant $[2k, k]$ codes such that k be prime and 2 be a primitive root of $\mathbb{Z}/k\mathbb{Z}$ lie on the Gilbert-Varshamov bound. They propose a scheme with a public key of size 347 bits and a private key of size 694 bits.

We can use this construction in our context by replacing the random q-ary matrix H by a random q-ary double-circulant matrix. In this case, the parameters using this construction are $q = 256, n = 134, k = 67, \mathsf{wt}(s) = 49$; this gives a size for the public data of 1072 bits (536 for the matrix and 536 for the public identification) and a private key of size 1072 bits for almost the same complexity for an ISD attack.

We can also imagine a construction based on double-dyadic codes or embedding the syndrome in the matrix as proposed in [17] and [12].

Against these aforementioned constructions, there are recently several *new* structural attacks appeared in [28] and [10]; these attacks extract the private key of some parameters of the variants presented in [2] and [17]. Since in our context we deal with random codes, we are not addressed by this kind of attacks.

Furthermore in [6] the authors describe a secure implementation of the Stern scheme using quasi-circulant codes. Our proposal inherits the advantages of the original Stern scheme against leakage of information, such as SPA and DPA attacks.

5 Conclusion

We have defined an identification scheme which among all the schemes based on the SD problem has the best parameters for the size of the public data as well as for the communication complexity. Moreover, we propose a variant with a reduced public key size.

The improvement proposed here to the Stern scheme can be applied to all the Stern-based identification and signature schemes (such as identity-based identification and signature scheme [5] or threshold ring signature scheme [16] for example).

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

References

1. Barg, S.: Some new NP-complete coding problems. Probl. Peredachi Inf. 30, 23–28 (1994)
2. Berger, T.P., Cayrel, P.-L., Gaborit, P., Otmani, A.: Reducing key length of the mcEliece cryptosystem. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 77–97. Springer, Heidelberg (2009)
3. Berlekamp, E., McEliece, R., van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory 24(3), 384–386 (1978)
4. Bernstein, D.J., Buchmann, J., Dahmen, E.: Post-Quantum Cryptography. Springer, Heidelberg (2008)
5. Cayrel, P.-L., Gaborit, P., Girault, M.: Identity-based identification and signature schemes using correcting codes. In: Augot, D., Sendrier, N., Tillich, J.-P. (eds.) International Workshop on Coding and Cryptography, WCC 2007, pp. 69–78 (2007)
6. Cayrel, P.-L., Gaborit, P., Prouff, E.: Secure implementation of the stern authentication and signature schemes for low-resource devices. In: Grimaud, G., Standaert, F.-X. (eds.) CARDIS 2008. LNCS, vol. 5189, pp. 191–205. Springer, Heidelberg (2008)
7. Chabaud, F., Stern, J.: The cryptographic security of the syndrome decoding problem for rank distance codes. In: Kim, K.-c., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 368–381. Springer, Heidelberg (1996)
8. Chen, K.: Improved girault identification scheme. Electronics Letters 30(19), 1590–1591 (1994)
9. Interactive comparison of some zero knowledge identification schemes, `http://tinyurl.com/32gxn8w`
10. Faugère, J.-C., Otmani, A., Perret, L., Tillich, J.-P.: Algebraic cryptanalysis of mcEliece variants with compact keys. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 279–298. Springer, Heidelberg (2010)
11. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)
12. Gaborit, P., Girault, M.: Lightweight code-based authentication and signature. In: IEEE International Symposium on Information Theory – ISIT 2007, Nice, France, pp. 191–195. IEEE, Los Alamitos (2007)
13. Goldreich, O.: Zero-knowledge twenty years after its invention (2002), `http://eprint.iacr.org/`
14. Jaulmes, É., Joux, A.: Cryptanalysis of pkp: a new approach. In: Kim, K.-c. (ed.) PKC 2001. LNCS, vol. 1992, pp. 165–172. Springer, Heidelberg (2001)
15. MacWilliams, F.J., Sloane, N.J.A.: The theory of error correcting codes. North-Holland, Amsterdam (1977)
16. Aguilar Melchor, C., Cayrel, P.-L., Gaborit, P.: A new efficient threshold ring signature scheme based on coding theory. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 1–16. Springer, Heidelberg (2008)
17. Misoczki, R., Barreto, P.S.L.M.: Compact mcEliece keys from goppa codes. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 376–392. Springer, Heidelberg (2009)
18. Niebuhr, R., Cayrel, P.-L., Bulygin, S., Buchmann, J.: On lower bounds for information set decoding over Fq. In: SCC 2010 (2010) (preprint)

19. Peters, C.: Information-set decoding for linear codes over Fq (2009), http://eprint.iacr.org/
20. Pierce, J.N.: Limit distributions of the minimum distance of random linear codes. IEEE Trans. Inf. theory 13, 595–599 (1967)
21. Pointcheval, D.: A new identification scheme based on the perceptrons problem. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 319–328. Springer, Heidelberg (1995)
22. Pointcheval, D., Poupard, G.: A new NP-complete problem and public-key identification. Des. Codes Cryptography 28(1), 5–31 (2003)
23. Poupard, G.: A realistic security analysis of identification schemes based on combinatorial problems. European Transactions on Telecommunications 8(5), 471–480 (1997)
24. Shamir, A.: An efficient identification scheme based on permuted kernels. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 606–609. Springer, Heidelberg (1990)
25. Stern, J.: A method for finding codewords of small weight. In: Wolfmann, J., Cohen, G. (eds.) Coding Theory 1988. LNCS, vol. 388, pp. 106–113. Springer, Heidelberg (1989)
26. Stern, J.: A new identification scheme based on syndrome decoding. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 13–21. Springer, Heidelberg (1994)
27. Stern, J.: Designing identification schemes with keys of short size. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 164–173. Springer, Heidelberg (1994)
28. Gauthier Umana, V., Leander, G.: Practical key recovery attacks on two McEliece variants (2009), http://eprint.iacr.org/2009/509.pdf
29. Véron, P.: Improved identification schemes based on error-correcting codes. Appl. Algebra Eng. Commun. Comput. 8(1), 57–69 (1996)
30. Wolf, C., Preneel, B.: $\mathcal{MQ}^*$-ip: An identity-based identification scheme without number-theoric assumptions (2010), http://eprint.iacr.org/