# Dual Construction of Stern-based Signature Schemes

Pierre-Louis Cayrel and Sidi Mohamed El Yousfi Alaoui

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

**Abstract.** In this paper, we propose a dual version of the first identity-based scheme based on error-correcting code proposed by Cayrel et.al [CGG07]. Our scheme combines the McEliece signature and the Véron zero-knowledge identification scheme, which provide better computation complexity than the Stern one. We also propose a generalization of the Véron identification scheme in order to build a threshold ring signature scheme, which is secure in the random oracle model and has the advantage to reduce the computation complexity as well as the size of storage.

**Key words:** Stern algorithm, Véron algorithm, CFS signature scheme, identity-based signature, threshold ring signature, post-quantum cryptography.

## 1 Introduction

The development in the field of quantum computing is a real menace of the security of many used public key cryptographic algorithms. Shor has demonstrated in 1994 that cryptographic schemes whose security relies on the difficulty of the factorization problem, such as RSA and the difficulty of discrete logarithm problem, such as Digital Signature Algorithm (DSA), can be broken using quantum computers. Consequently it is necessary to have available alternative signature and identification schemes.
Coding based cryptography is one of the few alternatives supposed to be secure in a post quantum world. The most popular cryptosystems in coding theory are the McEliece [McE78] and Niederreiter [Nie86] ones. 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 that they require very large keys, which need large memory spaces.
Secure identification schemes were introduced by Feige, Fiat and Shamir [FFS87]. These cryptographic schemes allow a prover to identify itself in polynomial time to a verifier without revealing any information of its private key to the verifier. These schemes could be turned into a digital signature via Fiat-Shamir paradigm [FS87].
In the last few years there were many tentatives to build practical identification or signature schemes based on error-correcting codes. Stern proposed at Crypto'93 [Ste94] an identification scheme based on syndrome decoding problem, and Véron proposed in 1995 a dual version of the first one based on search of low weight problem [Vér95]. In 2001, Courtois, Finiasz, and Sendrier [CFS01] introduced the first signature scheme based on McEliece and Niederreiter cryptosystems.
Identity-based public key cryptography was introduced in 1984 by Shamir [Sha85]. The main advantage of this construction was to simplify the key management and to avoid the need of digital certificates. This scheme needs a trusted third party called Key Generation Center

(KGC) or authority, which generates a private key for a user corresponding to its identity (e.g., name, e-mail,$\cdots$) using a secret, called master key, and then sends the generated private key to the user.
The concept of ring signatures was first introduced in 2001 by Rivest et al. [RST06]. Ring signatures permit a user from a set of possible signers with no existing group manager to sign a message and to convince the verifier that the author of the signature belongs to this set without revealing any information about its identity.
In 2002, Bresson et al. [BSS02] extended this concept in a $t$-out-of-$N$ threshold ring signature, which enables to any $t$ participating users belonging to a set of $n$ users to produce a signature. The anonymity of $t$ signers should be protected in both inside and outside the signing group.
In order to make use of the benefits of ID-based cryptography, the authors in [CGG07] proposed the first identity-based identification (IBI) scheme based on error-correcting code. This scheme combines the signature scheme of Courtois, Finiasz and Sendrier (CFS) and the identification algorithm of Stern. However, the performance of the IBI scheme depends on the performance of CFS. Therefore, the practical weaknesses of CFS parameters, such as large public key size and the long time required for signing, are also inherited. These drawbacks make it difficult to apply such schemes in devices with small memory spaces like smart cards.
The concept of threshold ring signatures in code-based cryptography was introduced by Aguilar et. al in [AMCG08]. This scheme is a generalization of Stern identification scheme. The major advantage of this construction is that its complexity depends linearly on a maximum number of signers $N$, comparing with the complexity of threshold ring signature schemes based on number theory whose complexity is $O(tN)$. However, the disadvantage of large signature sizes is still unsolved in this scheme.
**Our contribution:** In this paper, we propose a new identity-based identification scheme based on error-correcting code, which combines the signature scheme of Courtois, Finianz and Sendrier (CFS) and the zero knowledge identification scheme of Véron. Furthermore, we propose the generalization of Véron identification and signature in order to build threshold ring signature schemes. Using an improved version of Véron scheme, we obtain smaller public and private key sizes and better computation complexity for our scheme compared to the generalization of Stern scheme proposed in [AMCG08].
**Organization of the paper:** This paper is organized as follows: in Section 2 we briefly present basic background for code-based cryptography. In Section 3 we give a description of the CFS signature in Niederreiter's and McEliece's version. In Section 4 we present Stern and Véron schemes and we show in Section 5 how to use the last scheme to construct two identification schemes with special properties. Finally we conclude the paper in Section 6.

## 2 Background of Coding Theory

Next, we provide the necessary mathematical background to understand the schemes that we present in the next sections.
Let $n$ and $k$ be two integers such that $n \geq k$ and $\mathbb{F}_2^n$ be a finite field over $\{0,1\}^n$. A code $C$ is a $k$-dimensional subspace of the vector space $\mathbb{F}_2^n$.

**Definition 1 (Minimum distance and hamming weight).** The minimum distance is defined by $d := \inf_{x,y \in C} \mathrm{dist}(x,y)$, where "dist" denotes the hamming distance.
Let $x$ be a vector of $\mathbb{F}_2^n$, then we call $\mathrm{wt}(x) := \mathrm{dist}(x,0)$ the weight of $x$. It represents the number of non-zero entries.

$C[n, k, w]$ is a code with length $n$, dimension $k$ and the ability of error-correcting in $C$ is up to $w$ errors.

**Definition 2 (Generator, Parity Check Matrix and Syndrome).** A matrix $G \in \mathbb{F}_2^{k \times n}$ is called generator matrix of $C$, if the rows of $G$ span $C$.
A matrix $H \in \mathbb{F}_2^{(n-k) \times n}$ is called parity check matrix of $C$, if $H^\mathsf{T}$ is the right kernel of $C$ (i.e. $Hx^\mathsf{T} = 0, \forall x \in C$).
A code generated by $H$ is called the dual code of $C$ and denoted $C^\perp$.
Given a word $x$ of $\mathbb{F}_2^n$, a syndrome of $x$ is defined as a vector $s$ of length $(n-k)$ such that $Hx^\mathsf{T} = s$.

### 2.1 Syndrome Decoding (SD) Problem

The security of most code-based cryptosystems relies on the difficulty of solving a syndrome decoding problem (SD), which is defined as follows:
**Input:** A $m \times n$ random binary matrix $H$ over $\mathbb{F}_2$, a target vector $s \in \mathbb{F}_2^m$ and an integer $w > 0$.
**Question:** Is there a vector $x \in \mathbb{F}_2^n$ with $wt(x) \leq w$, such that $Hx^\mathsf{T} = s$.

This problem is proven NP-complete in [Nie86].
An equivalent version of the SD problem (dual version) can be presented as follows:
**Input:** A $k \times n$ random binary matrix $G$ over $\mathbb{F}_2$, binary vector $x$ of length $n$ of $\mathbb{F}_2^n$ and $w > 0$.
**Question:** Is there a vector $(m, e)$ with $m$ a vector of length $k$, $e$ a vector of length $n$ and weight $w$ such that $x = mG + e$.

### 2.2 Usual attacks: Information Set Decoding

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. Information Set Decoding (ISD) is one of the known decoding attacks, which has the advantage of low complexity. We calculate our suggested parameters of all scheme, in this paper using the following proposition introduced by Finianz and Sendrier [FS09].
$WF_{ISD}(n, r, w)$ is defined as the minimum binary work factor (number of binary operations) of the binary ISD algorithm to find a solution on input parameters $(n, k = n - r, w)$ of a code over $\mathbb{F}_2^n$.

**Proposition:**
Let $k$ be $n-r$, if $\binom{n}{w} < 2^r$ (single solution) or if $\binom{n}{w} > 2^r$ (multiple solutions) and $\binom{r}{w-p}\binom{k}{p} \ll 2^r$

$$WF_{ISD}(n, r, w) \approx \min_p \frac{2l \min(\binom{n}{w}, 2^r)}{\lambda \binom{n}{w} \sqrt{\binom{k+l}{p}}} \text{ with } l = \log(K_{w-p} \sqrt{\binom{k}{p}})$$

with $\lambda = 1 - e^{-1} \approx 0.63$. If we have $\binom{n}{w} > 2^r$ (multiple solutions) and $\binom{r}{w-p}\binom{k}{p} \gg 2^r$, we have:

$$WF_{ISD}(n, r, w) \approx \min_p \frac{2l 2^{r/2}}{\sqrt{\binom{r-l}{w-p}}} \text{ with } l = \log(K_{w-p} \frac{2^{r/2}}{\sqrt{\binom{r-l}{w-p}}})$$

According to the authors, the variable $p$ should be very small ($p \leq 8$) and $K_{w-p} = 2(t-p)$.

### 2.3 The McEliece Cryptosystem

The McEliece cryptosystem is the first cryptosystem based on the difficulty of decoding without knowledge of the structure of the code. It has shown resistance against attacks for more than 20 years and is still unbroken in its original version. The original version of McEliece uses Goppa codes, which are hard to distinguish from a random code and have an efficient decoding algorithm. This cryptosystem is very fast but the drawback is the public key size (about 500000 bits).
We now briefly describe this cryptosystem. For more details we refer to [McE78].

**Algorithm 1** McEliece cryptosystem

**Parameters:** $n, k, w \in \mathbb{N}$, where $w \ll n$
▷ Key generation:
$G'$: a $k \times n$ binary generator matrix of $C[n, k, w]$
$S$: a $k \times k$ random binary non singular matrix
$P$: a $n \times n$ random binary permutation matrix
compute the $k \times n$ matrix $G = SG'P$
**Public key:** $(G, w)$
**Private key:** $(S, D_C, P)$, where $D_C$ is an efficient decoding algorithm for $C$
▷ Encryption:
$m \to c = mG + e$, where $e$ is a random word of weight $w$, $m$ is the plaintext and $c$ is the ciphertext
▷ Decryption:
$c \to D_C(cP^{-1})S^{-1}$
get $m$

### 2.4 The Niederreiter Cryptosystem

Niederreiter cryptosystem is a dual version of McEliece cryptosystem, which uses a parity check matrix of a code $C$ as public key. This cryptosystem is as secure and efficient as the McEliece cryptosystem. The following algorithm presents this cryptosystem. See [Nie86] for more details.

**Algorithm 2** Niederreiter cryptosystem

**Parameters:** $n, k, w \in \mathbb{N}$, where $w \ll n$
▷ Key generation:
$H'$: a $k \times n$ binary parity check matrix of $C[n, k, w]$
$S$: a $(n-k) \times (n-k)$ random binary non singular matrix
$P$: a $n \times n$ random binary permutation matrix
compute the $k \times n$ matrix $H = SH'P$
**Public key:** $(H, w)$
**Private key:** $(S, D_C, P)$ where $D$ is an efficient decoding algorithm for $C$
▷ Encryption:
$m \to s = He^{\mathsf{T}}$, where $e$ is a random word of weight $w$
▷ Decryption:
compute $S^{-1}c = H'Pe^{\mathsf{T}}$
decode $H'Pe^{\mathsf{T}}$ in $Pe^{\mathsf{T}}$
get $e$

## 3 CFS Signature

Using error-correcting code, Courtois, Finiasz and Sendrier (CFS) signature scheme is the first practical signature scheme in code theory [CFS01]. However, it is not quite as successful as RSA signature. The main reason is that it is not guaranteed to decode any random element of $\mathbb{F}_2^n$ into a codeword for a given code $C[n, k, w]$. Therefore, the authors of this scheme uses Goppa codes, which have a good proportion of decodable words, and choose parameters such that this proportion is reasonable. For $w$-error correcting Goppa code of length $n = 2^m$, the number of decoding attempt to get one signature will be approximately around $w!$, in praxis $w$ should not be greater than 10. The security of this scheme can be reduced to the syndrome decoding problem.
We describe in the following the CFS signature in Niederreiter and McEliece versions.

### 3.1 CFS Signature in Niederreiter's version

Let $h$ be a hash function returning a binary word $n - k$ and $x$ be a message to be signed. We denote $x_i = h(x||i)$ the hashed value of the concatenation of the message and the index $i$. The idea of the CFS algorithm is to compute $x_i$ starting for $i$ by 0 and increasing at each try until $x_i$ is decodable. This syndrome $x_i$ will then be decoded into a word $s$ of length $n$ using the decoding algorithm, such that $Hs^\mathsf{T} = x_{i_0}$, where $i_0$ is the smallest value of $i$ for which decoding is possible. The signature consists of $\{s, i_0\}$.
The CFS algorithm works as follows:

**Algorithm 3** CFS algorithm

**Parameters:** $H \in \mathbb{F}_2^{(n-k)\times n}$:parity-check matrix of Goppa code $C[n, k, w]$, $h$ a collision resistant hash function returning a binary word $n - k$.
▷ Signature:
1: hash the message $x$ into $h(x)$
2: compute $x_i = h(x||i)$ for $i = 0, 1, 2 \cdots$
3: find $i_0$ the smallest value of $i$ such that $x_i$ decodable
4: using the decoding algorithm to compute $s$ such that $Hs^\mathsf{T} = x_{i_0}$
5: signature: $\{s, i_0\}$
▷ Verification:
6: compute $b_1 = Hs^\mathsf{T}$
7: compute $b_2 = h(x||i_0)$
8: compare $b_1$ and $b_2$, if they are equal the signature is valid

***Performance and security***

| | |
|---|---|
| signature cost | $w!w^2m^3$ |
| signature length | $(w-1)m + log_2 w$ |
| verification cost | $w^2m$ |
| public key size | $wm2^m$ |

The security of the CFS algorithm relies on the syndrome decoding problem (SD). In the original paper the authors proposed the parameters $m = 16$ and $w = 9$ for a security about $2^{80}$ binary operations. In this case the signature length in average is 144 bits.

In [FS09], the authors proposed an attack against CFS signature, which implies a change of the original parameters, the new parameters are $m = 22$ and $w = 9$ for a security about $2^{80}$ binary operations. The signature length for this new parameters is about 198 bits.

### 3.2 CFS signature in McEliece's version

Let $G$ be a generator matrix of the Goppa code $C[n, k, w]$. In the case of McEliece CFS signature one chooses $h$ a hash function producing $n$-bit values.
The way to compute a signature for one message $x$ is the same as Niedrreiter's version. From the hashed $n$-bits $h(x)$ one can construct a couple $(m, e)$ corresponding to the decrypted $h(x||i)$ using the decoding algorithm, such that $mG + e = h\,(x||i_0)$ ($i_0$ the smallest value of $i$ for which the decoding is possible). The signature in this case is $\{e, i_0\}$.
The verification step consists of proving that $h(x||i_0) + e$ is an element of the space span by $G$, which is publicly given.

***Performance and security.*** In the case of McEliece CFS signature one has the same performance and parameters for the security as Niederreiter version.
The only difference between the two versions (McEliece and Niederriter of CFS) is the value returned by the hash-function, this value is smaller ($n - k < n$) in the case of Niederreiter, therefore the authors of this scheme use this version.

## 4 Identification and Signature Schemes

In this section, we present two identification schemes based on error-correcting codes. Both are three-pass schemes and proved to satisfy a perfect zero-knowledge interaction proof, which is an interactive method for one party to prove to another that a statement is true, without revealing any additional information. The security of both schemes is based on the syndrome decoding problem (SD). The first identification scheme is proposed by Stern [Ste94] and uses a parity check matrix $H$ of a random binary linear code $C$ as public key, which is common to all users. The second is called Véron identification scheme. It was introduced by Véron [Vér95] and is a dual version of Stern scheme, which uses a generator matrix $G$ of a random binary linear code $C$ as public key.

### 4.1 Stern Identification Scheme

Let $H$ be a public random $(n - k) \times n$ binary matrix and $h$ be a hash function returning a binary word $n$.
The prover $P$ constructs its public key $x$ associated to its secret key $s$ such that $Hs^{\mathsf{T}} = x$. The syndrome $x$ is calculated once during the lifetime of $H$.
We now describe the scheme that enables the prover to identify itself to the verifier. The scheme includes $r$ rounds, each of them is performed as follows:

This scheme has for each single round the knowledge error of 2/3. The number $r$ of consecutive rounds depends on the required level of security denoted by $\beta$, i.e. the scheme must be iterated $r$ times until $(2/3)^r \leq \beta$, for 80 bits security level one needs about 140 rounds.
By using Fiat-Shamir paradigm [FS87], it is possible to convert this scheme into a signature scheme.

**Algorithm 4** Stern Identification Scheme

**Parameters:** $n$ : code length; $k$ : code dimension; $H \in \mathbb{F}_2^{(n-k)\times n}$ : parity-check matrix, $h$ a collision resistant hash function returning a binary word $n$.
**Private key**: $s \in \mathbb{F}_2^n$, such that $\mathsf{wt}(s) = \omega$
**Public key**: $x \in \mathbb{F}_2^{n-k}$, such that $Hs^T = x$
▷ Prover: make commitments
Choose $u$ from $\mathbb{F}_2^n$ at random
Choose $\sigma$ permutation over $\{1, \ldots, n\}$ at random
Set $c_1 \leftarrow h\left(\sigma, Hu^T\right)$
Set $c_2 \leftarrow h(\sigma(u))$
Set $c_3 \leftarrow h(\sigma\left(u \oplus s\right))$
Send $c_i$ to Verifier
▷ Verifier: make a challenge
Choose challenge $b$ from $\{0, 1, 2\}$ at random
Send $b$ to Prover
▷ Prover: answer the challenge
**if** $b = 0$ **then** send $u$ and $\sigma$ to Verifier
**else if** $b = 1$ **then** send $u \oplus s$ and $\sigma$ to Verifier
**else if** $b = 2$ **then** send $\sigma(u)$ and $\sigma(s)$ to Verifier
**end if**
▷ Verifier: checks the answer complies with commitments
**if** $b = 0$ **then** check if $c_1$ and $c_2$ were honestly computed
**else if** $b = 1$ **then** check if $c_1$ and $c_3$ are correct.
**else if** $b = 2$ **then** check if $c_2$ and $c_3$ are correct, and that $\mathsf{wt}(\sigma(s)) = \omega$.
**end if**

***Performance and security.*** The security of stern scheme is based on all of the following conditions:

1. Random linear codes satisfy a Gilbert-Varshamov type lower bound [MS77].
2. For large $n$ almost all linear codes lie over the Gilbert-Varshamov bound [Pie67].
3. Solving the syndrome decoding problem for random codes is NP-complete [BMvT78].

Let $C[n, k, w]$ be a random linear code. When $n$ equals $2k$, the first condition implies that $w$ is approximately $0.22n$.
The first condition assures the existence of good random codes. It permits to estimate a lower bound on the minimum weight of the definite code and thereby to provide an evaluation of the usual attack by information set decoding. The second condition affirms that all random codes satisfy such a bound and the last condition assures the difficulty to solve the decoding problem.

***Suggested parameters.***
Considering $n = 614$, $k = 307$ and $w = 68$, we have the following results:
**ISD attack complexity:** $2^{80}$
**Public Data size:** $n^2 + n$ (94556 Bits)
**Private Data size:** $n^2 + 2n$ (94863 Bits)
**Prover's Work Factor**: $r(k(2(n-k)+1) + n + \frac{n}{3})$ binary operations ($\simeq 2^{24,6}$)

### 4.2 Dual construction: Véron Signature Scheme

As mentioned above, in [Vér95] the author of this scheme uses a $k \times n$ generator matrix $G$ of a random binary linear code $C$ as a public key, this matrix is common to all users. Each of them receives a secret key $(m, e)$, where $m$ is a vector of $k$ bits, $e$ a vector of $n$ bits and weight $w$. A user's identifier $x$ is obtained by:

$$x = mG + e$$

Suppose that the prover $P$ wants to prove to the verifier $V$ that $P$ is indeed the person corresponding to the public identifier $x$ using Véron identification scheme.
This scheme can be described as follows:

**Algorithm 5** Véron Identification Scheme

**Parameters:** $n$: code length; $k$: code dimension; $G \in \mathbb{F}_2^{k \times n}$:generator matrix, $h$ a collision resistant hash function.
**Private key** : $(m, e) \in \mathbb{F}_2^k \times \mathbb{F}_2^n$, such that $\mathsf{wt}(e) = \omega$
**Public key** : $x \in \mathbb{F}_2^n$, such that $mG + e = x$
▷ Prover: make commitments
Choose $u$ from $\mathbb{F}_2^k$ at random
Choose $\sigma$ permutation over $\{1, \ldots, k\}$ at random
Set $c_1 \leftarrow h(\sigma)$
Set $c_2 \leftarrow h(\sigma(u + m)G)$
Set $c_3 \leftarrow h(\sigma(uG + x))$
Send $c_i$ to Verifier, $i$ =1, 2, 3
▷ Verifier: make a challenge
Choose challenge $b$ from $\{0, 1, 2\}$ at random
Send $b$ to Prover
▷ Prover: answer the challenge
**if** $b = 0$ **then** send $u + m$ and $\sigma$ to Verifier
**else if** $b = 1$ **then** send $\sigma(u + m)G$ and $\sigma(e)$ to Verifier
**else if** $b = 2$ **then** send $\sigma$ and $u$ to Verifier
**end if**
▷ Verifier: checks the answer complies with commitments
**if** $b = 0$ **then** check if $c_1$ and $c_2$ were honestly computed
**else if** $b = 1$ **then** check if $c_1$ and $c_3$ are correct, and $wt(\sigma(e)) = w$
**else if** $b = 2$ **then** check if $c_2$ and $c_3$ are correct.
**end if**

***Performance and security.*** The security of Véron identification scheme relies on the three conditions of random linear codes, which have been already discussed in the Stern identification scheme.

***Suggested parameters.***
Considering $n = 614$, $k = 307$ and $w = 68$, we have the following results:
**ISD attack complexity**: $2^{80}$
**Public Data size:** $n^2 + 2n$ (94863 Bits)
**Private Data size:** $n^2 + 3n$ (95170 Bits)
**Prover's Work Factor**: $r(\frac{8}{3}(k(n-k) + n + \frac{5}{3}k)$ binary operations ($\simeq 2^{25}$)

### 4.3 Improved Véron Signature Scheme

In this subsection, we briefly describe an improvement of the original scheme [Vér96]. The idea of this improvement is to start with two arbitrary vectors chosen in a finite field, and among them a generator matrix $G$ of a binary linear code $C$ can be built. The storage space required by the prover, in this case, is reduced, because the prover only needs to store the two vectors and not the whole matrix. Further advantage of this idea is that the complexity of the computation has considerably decreased comparing to Stern identification scheme and the original version of Véron scheme.
Let $\mathbb{F}_{2^k}$ be a finite field and $\beta = \{\beta_1, \ldots, \beta_k\}$ be a basis of $\mathbb{F}_{2^k}$.
Let $\gamma = \sum_{i=1}^{k} \beta_i \gamma_i$ be an arbitrary element of $\mathbb{F}_{2^k}$, $\gamma$ can be represented then as $(\gamma_1, \cdots, \gamma_k)$.
The $\beta$ product matrix of $\gamma$, denoted by $[\gamma]_\beta$, is the $(k \times k)$ matrix defined as follows:

$$[\gamma]_\beta = \begin{bmatrix} \gamma.\beta_1 \\ \vdots \\ \gamma.\beta_k \end{bmatrix}$$

**Example:**
Consider the finite Field $\mathbb{F}_2^3$ generated by $p(x) = x^3 + x + 1$ and $\alpha$ root of $p(x)$.
Let $\beta = \{1, \alpha, \alpha^2\}$ basis of $\mathbb{F}_2^3$
Then we have : $0 = (000)$; $1 = (100)$; $\alpha = (010)$; $\alpha^2$=(001)
$\alpha^3 = (110)$; $\alpha^4 = (011)$; $\alpha^5 = (111)$; $\alpha^6 = (101)$
For $\gamma = \alpha^4$, we have:

$$[\gamma]_\beta = \begin{pmatrix} 0\ 1\ 1 \\ 1\ 1\ 1 \\ 1\ 0\ 1 \end{pmatrix}$$

As mentioned above, a generator matrix $G$ of a binary linear code $C$ is replaced by the following $(k \times 2k)$ matrix: $([\gamma_1]_\beta, [\gamma_2]_\beta)$, for two arbitrary vectors $(\gamma_1, \gamma_2)$ of $\mathbb{F}_{2^k}$ such that $w_\beta(\gamma_1)$ and $w_\beta(\gamma_2)$ be small.
where $w_\beta(\gamma)$ is defined as the Hamming weight of $(\gamma_l, ..., \gamma_k)$, for given vector $\gamma$ of $\mathbb{F}_{2^k}$.
For more details of this construction we refer to [Vér96].

***Performance and security.*** The security of this scheme depends on syndrome decoding problem and linked to the parameters $n, k$ and $w$.

***Suggested parameters.***
Considering $n = 614$, $k = 307$ and $w = 68$, we have the following results:
**ISD attack complexity**: $2^{80}$
**Public Data size:** $4n$ (1228 Bits)
**Private Data:** $5n$ (1535 Bits)
**Prover's Work Factor**: $r(2k(\frac{11}{3} + \frac{5}{3}t_1 + t_2) - \frac{10}{3})$ binary operations ($\simeq 2^{23.4}$)

The results of the three above schemes are summarized in table 1. As you can see, the size of public and private data has been significantly reduced by the improved Véron scheme. In addition the computation complexity has been optimized. Both advantages allow the application of such schemes in devices with low storage capacities, such as smart cards.

In the next section, we describe how these advantages can be applied to optimize the performance of the identity-based identification and the threshold ring signature schemes.

**Table 1.** Comparison of the three schemes

| | Public Data | Privat Data | Prover's Work Factor |
|---|---|---|---|
| **Stern scheme** | 94556 Bits | 94863 Bits | $2^{24.6}$ |
| **Véron scheme** | 94863 Bits | 95170 Bits | $2^{25}$ |
| **Improved Véron scheme** | 1228 Bits | 1535 Bits | $2^{23.4}$ |

## 5 Identity-based Identification and Threshold Ring Signature

In order to make use of the benefits of the improved Véron identification scheme, we present in this section a novel variant of the existing identity-based identification and threshold signature schemes in coding theory that were based on Stern scheme.

### 5.1 Identity-based McEliece Véron signature scheme

Identity-based Identifications (IBI) were introduced in cryptography as an alternative form of public key cryptography, which do not use certification authorities or certificates. The first identity-based scheme based on error-correcting code was proposed by Cayrel et. al in [CGG07]. This scheme combines the signature scheme of Courtois, Finiasz, and Sendrier (CFS) and the Stern identification scheme.
Our idea is to construct a dual version of the above identity-based scheme. Our scheme combines two parts: a CFS Signature (version McEliece) with the zero-knowledge identification scheme of Véron presented in Section 3. In the first part an authority computes the prover's private key $(m, e)$ from its identity using the public matrix $G$. In the second part the prover can identify itself through the Véron scheme using the same matrix $G$ and proving that he knows the private key $(m, e)$.
We suppose a prover (P) wants to identify itself to a verifier (V). In the following we describe in short our algorithm:

**Algorithm 6** Identity-based with Véron scheme

**Parameters:** $n, k, w \in \mathbb{N}$, where $w \ll n$
**Public key:**
$G$: generator matrix of a linear code $C[n, k, w]$
$h$: a hash function with values in $\{0,1\}^k$
$id_V$: prover identity
▷ Step1: key deliverance:
1: The authority gives to the prover its private key $(m, e)$ from its identity (public) using McEliece scheme such that: $mG + e = h(id_V||i_0)$ (see 3.1 for definition of $i_0$ )
▷ Step2: Identification of a prover by a verifier
2: The prover sends the index $i_0$ to the verifier
3: The prover identify itself to a verifier using Véron scheme with $(m, e)$ as private key and $(id_V||i_0)$ as public key.

***Security and parameters of IBI.*** A proof of security for this scheme in the random oracle model is similar to the the proof given in [CGGG09]. Due to the limit size of our paper, we do not present it here.

The IBI scheme consists of two parts: In the first part we apply the CFS scheme in order to create the private key for the prover and in the second part we use Véron identification scheme for identification. This implies that the security of our scheme (IBI) relies on the choice of the parameters of CFS scheme, which are based on two assumptions:

1. The complexity for computing the signature should be difficult without knowledge of the description of $G$.
2. The cost of computation for the correct index $i_0$ should not be to high.

To respect the second assumption, one uses the Goppa code $[2^m, 2^m - wm, w]$, which have a good portion of decodable syndromes (about $1/w!$). $w$ should be relatively small.
The decoding of the Goppa code consists of:

– computing a syndrome: $w^2m^2/2$ binary operations;
– computing a localisator polynomial: $6w^2m$ binary operations;
– and $2w^2m^2$ binary operations.

The cost for the computation of private key in our scheme is about:

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

***Suggested parameters.***
For $w = 9$ and $m = 22$ is a security about $2^{80}$ binary operations.

***Advantage of our scheme.*** Using an improved Véron signature scheme in step 2 of our scheme, a prover's work factor is about $(2^{37.6})$, which is smaller than the prover's work factor $(2^{51.5})$ for the scheme proposed in [CGG07] for the same suggested parameters. The size of the private and public data remains unchanged.

### 5.2 Threshold ring Véron-based signature scheme

In this section we propose a new threshold ring scheme based on error correcting codes, called threshold ring Véron scheme. The construction of this scheme can be considered as a generalization of Véron identification scheme, which can be afterwards converted to a signature scheme by using Fiat-Shamir paradigm.
More precisely, we consider one set of $N$ members $(P_1, \ldots, P_N)$. Let $t$ be a subset of this set consisting of the members which want to sign a message whereas one of them is a leader $L$.
Each user of the group $(P_1, \ldots, P_N)$ chooses its own $k \times n$ generator matrix $G_i$. The leader collects all these matrices and forms among them the following matrix $G$ called master public key.

$$G = \begin{pmatrix} G_1 & 0 & \cdots & 0 \\ 0 & G_2 & 0 & 0 \\ \vdots & \ddots & G_i & 0 \\ 0 & 0 & \cdots & G_N \end{pmatrix}$$

We first define two notions of block permutation that we will use in our scheme.

Let $n$ and $N$ be two integers.

**Definition 1**
A constant $n$-block permutation $\Sigma$ on $N$ blocks is a permutation by block which permutes together $N$ blocks of length $n$ block by block. Each block being treated as a unique position as for usual permutations.

A more general type of permutation is the $n$-block permutation $\Sigma$ on $N$ blocks.

**Definition 2**
A $n$-block permutation $\Sigma$ on $N$ blocks is a permutation which satisfies that the permutation of a block of length $n$ among $N$ blocks is exactly included in a block of length $n$.
A constant $n$-block permutation is a particular $n$-block permutation in which the blocks are permuted as such. For instance the permutation $(6, 5, 4, 3, 2, 1)$ is 2-block permutation on 3 blocks and the permutation $(3, 4, 5, 6, 1, 2)$ is a constant 2-block permutation on 3 blocks since the order on each block ($(1, 2), (3, 4)$ and $(5, 6)$) is preserved in the block permutation.
The notion of product permutation is then straightforward. Let us define $\sigma$, a family of $N$ permutations $(\sigma_1, \cdots, \sigma_N)$ of $\{1, \cdots, n\}$ on $n$ positions and $\Sigma$ a constant $n$-block permutation of $N$ blocks defined on $\{1, \cdots, N\}$. We consider a vector $v$ of size $nN$ of the form:

$$v = (v_1, v_2, \cdots, v_n, v_{n+1}, \cdots, v_{n+n}, v_{2n+1}, \cdots, v_{nN}),$$

we denote $V_1$ the first $n$ coordinates of $v$ and $V_2$ the $n$ following coordinates and so on, to obtain: $v = (V_1, V_2, \cdots, V_N)$. There we can define a $n$-block permutation on $N$ blocks, $\Pi = \Sigma \circ \sigma$ as $\Pi(v) = \Sigma \circ \sigma(v) = \Sigma(\sigma_1(V_1), \cdots, \sigma_N(V_N))$.

Let $w$ be an integer. To ensure the anonymity, each user of $t$ signers generates a couple $(m_i, e_i)$ such that $m_i G_i + e_i = 0$ where each $e_i$ has a weight $w$. The $N - t$ non signers choose $(m_i, e_i) = (0, 0)$. Then we obtain the public key $(G, w)$ and the secret key $(m, e)$ such that $mG + e = 0$ where $e$ is a $nN$ vector of weight $tw$. For more anonymity the leader uses special permutations to mix the permutations used of each $t$-signers in order to mask, which matrices are used in the scheme. The prover $P$, consists of the set of $t$ signers among $N$, proves to the verifier that he knows a secret key $(m, e)$, with $e$ is a $nN$ vector of weight $tw$.
Algorithm 7 gives a full description of this scheme.

***Performance and security.*** Due to the limit size of our paper, we do not give the full proofs of the following statements, but the proofs can be realized in the same way as in [AMCG08].

- Threshold Véron scheme is an interactive zero-knowledge scheme with a probability of cheating 2/3.
- The scheme satisfies the threshold signature anonymity.

**Algorithm 7** Threshold Véron scheme

**Parameters:** $n$ : code length; $k$ : code dimension; $G \in \mathbb{F}_2^{k\times n}$ : generator matrix, $h$ a collision resistant hash function.
**Private key**: $(m, e) \in \mathbb{F}_2^{nN}$, such that $\mathsf{wt}(e) = N\omega$
**Public key**: $x \in \mathbb{F}_2^{(n-k)N}$, such that $mG + e = x$
▷ Each signer: make master commitments
Each signer chooses $u_i$ from $\mathbb{F}_2^k$ at random
Each signer chooses $\sigma_i$ permutation over $\{1, \ldots, n\}$ at random
Set $c_{1,i} \leftarrow h(\sigma_i)$
Set $c_{2,i} \leftarrow h(\sigma_i(u_i + m_i)G_i)$
Set $c_{3,i} \leftarrow h(\sigma_i(u_iG_i))$
Send $c_{1,i}, c_{2,i}$ and $c_{3,i} \forall i$ to Leader
▷ Leader: make commitments
$L$ chooses $N - t$ random values $u_i$ of $\mathbb{F}_2^k$ and $N - t$ random permutations $\sigma_i$ of $\{1, 2, \ldots, n\}$
$L$ fixes the secret keys $(m_i, e_i)$ of the $N - t$ missing users at 0
$L$ computes the $N - t$ corresponding commitments by choosing random $u_i$ and $\sigma_i$ $(t + 1 \leq i \leq N)$
$L$ chooses a random constant $n$-block permutation $\Sigma$ on $N$ blocks $\{1, 2, \ldots, N\}$ in order to obtain the master commitments:
Set $C_1 \leftarrow h(\Sigma(c_{1,1}, \ldots, c_{1,N}))$
Set $C_2 \leftarrow h(\Sigma(c_{2,1}, \ldots, c_{2,N}))$
Set $C_3 \leftarrow h(\Sigma(c_{3,1}, \ldots, c_{3,N}))$
$L$ sends $C_1, C_2$ and $C_3$ to Verifier
▷ Verifier: make a challenge
Choose challenge $b$ from $\{0, 1, 2\}$ at random
Send $b$ to Leader
▷ Leader: answer the challenge
▷ Let $P_i$ be one of the signers. The first part of the step is between each signer and $L$
**if** $b = 0$ **then** $P_i$ sends $u_i + m_i$ and $\sigma_i$ to Leader
**else if** $b = 1$ **then** $P_i$ sends $\sigma_i(u_i + m_i)G$ and $\sigma_i(e_i)$ to Leader
**else if** $b = 2$ **then** $P_i$ sends $\sigma_i$ and $u_i$ to Leader
**end if**
▷ $L$ simulates the $N - t$ others Véron scheme with $(m_i, e_i) = (0, 0)$ where $t + 1 \leq i \leq N$
▷ $L$ computes the answer for $V$ (and sends it)
**if** $b = 0$ **then** $L$ constructs $u + m = (u_1 + m_1, \ldots u_N + m_N)$ and $\Pi = \Sigma \circ \sigma$ and sends $u + m$ and $\Pi$ to verifier
**else if** $b = 1$ **then** $L$ constructs
$\Pi(u + m)G = (\Sigma \circ \sigma_1(u_1 + m_1)G_1, \ldots, \Sigma \circ \sigma_N(u_N + m_N)G_N)$ and $\Pi(e) = (\Sigma \circ \sigma_1(e_1), \ldots, \Sigma \circ \sigma_N(e_N))$ and sends $\Pi(u + m)G$ and $\Pi(e)$ to verifier
**else if** $b = 2$ **then** $L$ constructs $\Pi = \Sigma \circ \sigma$ and $u = (u_1, \ldots, u_N)$ and sends them to verifier
**end if**
▷ Verifier: checks the answer complies with commitments
**if** $b = 0$ **then** $V$ verifies that $\Pi(m, e)$ is a $n$-block permutation and that $C_1, C_2$ have been honestly calculated
**else if** $b = 1$ **then** $V$ verifies that $\Pi(m, e)$ is a $n$-block permutation and that $C_2, C_3$ have been honestly calculated
**else if** $b = 2$ **then** $V$ verifies that $\Pi(m, e)$ is a $n$-block permutation and that $C_1, C_3$ have been honestly calculated
**end if**

***Advantage of our scheme.*** If we use the improved Véron scheme to create each matrix $G_i$, the prover have to store only the two vectors described in Section 4, we obtain then the following key sizes:
**Public key size:** $5nN$ instead $(n^2+n)N$ for public key size in the original Stern threshold scheme.
**Private key size:** $4nN$ instead $(n^2+2n)N$ for private key size in the original Stern threshold scheme.

Table 2 gives a comparison of Stern threshold scheme and our scheme considering the following parameters $N = 50$ and $n = 307$.

**Table 2.** Comparison of Stern threshold scheme and our scheme

| | Public Data size | Privat Data size | Prover's Work Factor for each user |
|---|---|---|---|
| **Stern threshold scheme** | 4727800 Bits | 4743150 Bits | $2^{24.6}$ |
| **Our scheme** | 76750 Bits | 61400 Bits | $2^{23.4}$ |

## 6 Conclusion

In this paper, we have proposed a variant of identity-based and threshold identification scheme based on error-correcting codes to reduce the complexity computation of the prover and the size of the data stored by the latter. Unfortunately, as often in code-based cryptography, our proposed schemes suffer from large system parameters, that could be reduced by using specific codes such quasi-dyadic codes introduced in [MB09].
To the best of our knowledge, up to present there exist neither identity-based nor threshold signature schemes except a few code-based systems in post-quantum world. Therefore, we encourage the cryptography community to work in this area because a lot of proposals are needed in post-quantum cryptography like schemes with additional properties.

## References

[AMCG08] Carlos Aguilar Melchor, Pierre-Louis Cayrel, and Philippe Gaborit. A new efficient threshold ring signature scheme based on coding theory. In *PQCrypto '08: Proceedings of the 2nd International Workshop on Post-Quantum Cryptography*, pages 1–16, Berlin, Heidelberg, 2008. Springer-Verlag.

[BMvT78] 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.

[BSS02] Emmanuel Bresson, Jacques Stern, and Michael Szydlo. Threshold ring signatures and applications to ad-hoc groups. In *CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, pages 465–480. Springer-Verlag, 2002.

[CFS01] 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.

[CGG07] 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, 2007.

[CGGG09] Pierre-Louis Cayrel, Philippe Gaborit, David Galindo, and Marc Girault. Improved identity-based identification using correcting codes. *CoRR*, abs/0903.0069, 2009.

[FFS87] U. Fiege, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. In *STOC '87: Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 210–217, 1987.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: practical solutions to identification and signature problems. In *Proceedings on Advances in cryptology—CRYPTO '86*, pages 186–194. Springer-Verlag, 1987.

[FS09] Matthieu Finiasz and Nicolas Sendrier. Security bounds for the design of code-based cryptosystems. Cryptology ePrint Archive, Report 2009/414, 2009. `http://eprint.iacr.org/`.

[MB09] R. Misoczki and P. S. L. M. Barreto. Compact mceliece keys from goppa codes. Preprint, 2009. `http://eprint.iacr.org/2009/187.pdf`.

[McE78] 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/progressreport2/42-44/44N.PDF`.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, volume 16. North-Holland Mathematical Library, 1977.

[Nie86] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[Pie67] J. N. Pierce. Limit distribution of the minimum distance of random linear codes. In *IEEE Trans. Inf. Theory*, pages 595–599, Vol. IT-13 (1967).

[RST06] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret: Theory and applications of ring signatures. In *Essays in Memory of Shimon Even*, pages 164–186, 2006.

[Sha85] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53. Springer-Verlag New York, Inc., 1985.

[Ste94] Jacques Stern. A new identification scheme based on syndrome decoding. In *CRYPTO '93: Proceedings of the 13th annual international cryptology conference on Advances in cryptology*, pages 13–21. Springer-Verlag, 1994.

[Vér95] Pascal Véron. Probleme sd, opérateur trace, schemas d´identification et codes de goppa. PhD thesis, Université de Toulon et du Var, 1995.

[Vér96] Pascal Véron. Improved identification schemes based on error-correcting codes. *Appl. Algebra Eng. Commun. Comput.*, 8(1):57–69, 1996.