International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:4, No:3, 2010

Dual Construction of Stern-based Signature Scheme

Pierre-Louis Cayrel and Sidi Mohamed El Yousfi Alaoui
CASED–Center for Advanced Security Research Darmstadt
Mornewegstrasse 32, 64293 Darmstadt, Germany
Email: {pierre-louis.cayrel, elyousfi@cased.de}

Abstract—In this paper, we propose a dual version of the first threshold ring signature scheme based on error-correcting code proposed by Aguilar et. al in [1]. Our scheme uses an improvement of Véron zero-knowledge identification scheme, which provide smaller public and private key sizes and better computation complexity than the Stern one. This scheme is secure in the random oracle model.

Keywords—Stern algorithm, Véron algorithm, threshold ring signature, post-quantum cryptography.

I. 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), could 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 [9] and Niederreiter [11] 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 [6]. 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 [5].

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 [14] 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 [15]. In 2001, Courtois, Finiasz, and Sendrier [4] introduced the first signature scheme based on McEliece and Niederreiter cryptosystems.

The concept of ring signatures was first introduced in 2001 by Rivest et al. [13]. Ring signatures permit any user from a set of intended signers to sign a message with no existing group manager 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. [3] 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.

The concept of threshold ring signatures in code-based cryptography was introduced by Aguilar et. al in [1]. 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 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 [1].

Organization of the paper: This paper is organized as follows: in Section II we briefly present basic background for code-based cryptography. In Section III we present Stern and Véron schemes and we show in Section IV how to use the last scheme to construct an identification schemes with special properties. Finally we conclude the paper in Section V.

II. 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 $d := \inf_{x,y \in C} \text{dist}(x,y)$, where "dist" denotes the hamming distance.

Let x be a vector of $\mathbb{F}_2^n$, then we call $\text{wt}(x)$:= $\text{dist}(x,0)$ 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 its rows span C.

A matrix $H \in \mathbb{F}_2^{(n-k) \times n}$ is called parity check matrix of C,

if $Hx^{\mathsf{T}} = 0, \forall x \in C$.
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 $Hx^{\mathsf{T}} = s$.

A. 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 [2].
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 $x = mG + e$.

B. 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 [7].
$WF_{ISD}(n, r, w)$ 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 $K_{w-p} = 2(t - p)$.

C. 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 in Algorithm 1. For more details we refer to [9].

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:
$m \rightarrow c = mG + e$, where e is a random word of weight w, m is the plaintext and c is the ciphertext
▷ Decryption:
$c \rightarrow D_C(cP^{-1})S^{-1}$
get m

D. 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 Algorithm 2 presents this cryptosystem. See [11] 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:
$m \rightarrow s = He^{\mathsf{T}}$, 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^{T}
get e

III. 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 [14] 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 [15] and is a dual version of Stern scheme, which uses a generator matrix G of a random binary linear code C as public key.

A. 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 of length 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 in Algorithm 3 as follows:

Algorithm 3 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 σ 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 σ to Verifier
else if $b = 1$ **then** send $u \oplus s$ and σ 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

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 β, 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 [5], it is possible to convert this scheme into a signature scheme.

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

- Random linear codes satisfy a Gilbert-Varshamov type lower bound [8].
- For large n almost all linear codes lie over the Gilbert-Varshamov bound [12].
- Solving the syndrome decoding problem for random codes is NP-complete [2].

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.

*2) **Suggested parameters**:*
Considering $n = 614$, $k = n/2 = 307$ and $w = 68$, we have the following results:

- ISD attack complexity: 2^{80}
- Public Data size: $k^2 + k$ (94556 Bits)
- Private Data size: $k^2 + 2k$ (94863 Bits)
- Prover's Work Factor: $r(k(2(n-k)+1)+n+\frac{n}{3})$ binary operations ($\simeq 2^{24,6}$)

B. Dual construction: Véron Signature Scheme

As mentioned above, in [15] 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 is described in Algorithm 4.

*1) **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.

*2) **Suggested parameters**:*
Considering $n = 614$, $k = 307$ and $w = 68$, we have the following results:

- ISD attack complexity: 2^{80}
- Public Data size: $k^2 + 2k$ (94863 Bits)
- Private Data size: $k^2 + 3k$ (95170 Bits)
- Prover's Work Factor: $r(\frac{8}{3}(k(n-k)+n+\frac{5}{3}k)$ binary operations ($\simeq 2^{25}$)

Algorithm 4 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
1: Choose u from $\mathbb{F}_2^k$ at random
2: Choose σ permutation over $\{1, \ldots, k\}$ at random
3: Set $c_1 \leftarrow h(\sigma)$
4: Set $c_2 \leftarrow h(\sigma((u + m)G))$
5: Set $c_3 \leftarrow h(\sigma(uG + x))$
6: Send c_i to Verifier, i =1, 2, 3
▷ Verifier: make a challenge
7: Choose challenge b from $\{0, 1, 2\}$ at random
8: Send b to Prover
▷ Prover: answer the challenge
9: **if** $b = 0$ **then** send $u + m$ and σ to Verifier
10: **else if** $b = 1$ **then** send $\sigma((u+m)G)$ and $\sigma(e)$ to Verifier
11: **else if** $b = 2$ **then** send σ and u to Verifier
12: **end if**
▷ Verifier: checks the answer complies with commitments
13: **if** $b = 0$ **then** check if c_1 and c_2 were honestly computed
14: **else if** $b = 1$ **then** check if c_1 and c_3 are correct, and $wt(\sigma(e)) = w$
15: **else if** $b = 2$ **then** check if c_2 and c_3 are correct.
16: **end if**

C. Improved Véron Signature Scheme

In this subsection, we briefly describe an improvement of the original scheme [16]. 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 $\mathbb{F}_{2^k}$, γ can be represented then as $(\gamma_1, \cdots, \gamma_k)$.
The β product matrix of γ, 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 α root of $p(x)$.
Let $\beta = \{1, \alpha, \alpha^2\}$ basis of $\mathbb{F}_{2^3}$
Then we have : $0 = (000)$; $1 = (100)$; $\alpha = (010)$; α^2=(001)
$\alpha^3 = (110)$; $\alpha^4 = (011)$; $\alpha^5 = (111)$; $\alpha^6 = (101)$
For $\gamma = \alpha^4$, we have:

TABLE I
COMPARISON OF THE THREE SCHEMES

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

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

Definition 1.
Let q be a power of a primzahl p.
A trace operator $Tr_{F_{q^m}:F_q}$ is defined as follows:

$$Tr_{F_{q^m}:F_q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$$
$$z \longmapsto \textstyle\sum_{i=1}^{m-1} z^{q^i}$$

Definition 2.
Let $\beta = \{\beta_1, \cdots, \beta_m\}$ be a basis of F_{2^m}.
$\beta = \{\beta_1, \cdots, \beta_m\}$ is called duale trace basis if :

$$\forall i, j \quad Tr_{F_{2^m}:F_2}(\beta_i {\beta^*}_j) = \delta_{ij}.$$

Where δ_{ij} is the Kronecker symbol.

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 (γ_1, γ_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 γ of $\mathbb{F}_{2^k}$. For more details of this construction we refer to [16].

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

*2) **Suggested parameters**:*
Considering $n = 614$, $k = 307$ and $w = 68$, we have the following results:

- ISD attack complexity: 2^{80}
- Public Data size: $4k$ (1228 Bits)
- Private Data size: $5k$ (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 I. 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 a threshold ring signature scheme.

IV. 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 Aguilar et.al [1] threshold signature scheme in coding theory that was based on Stern scheme.

A. 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 Σ 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 Σ on N blocks.
Definition 2
A n-block permutation Σ 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 σ, a family of N permutations $(\sigma_1, \cdots, \sigma_N)$ of $\{1, \cdots, n\}$ on n positions and Σ 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 $\Pi(v) = \Sigma \circ \sigma(v) = \Sigma(\sigma_1(V_1), \cdots, \sigma_N(V_N))$.

TABLE II
COMPARISON OF STERN THRESHOLD SCHEME AND OUR SCHEME

	Public Data (Bits)	Privat Data (Bits)	Prover's Work Factor
Stern threshold scheme	4727800	4743150	$2^{24.6}$
Our scheme	76750	61400	$2^{23.4}$

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 matrices 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 5 gives a full description of this scheme.

*1) **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 [1].

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

*2) **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 III, we obtain then the following key sizes:

- Public key size: $5kN$ instead $(k^2 + k)N$ for public key size in the original Stern threshold scheme.
- Private key size: $4kN$ instead $(k^2 + 2k)N$ for private key size in the original Stern threshold scheme.

Table II gives a comparison of Stern threshold scheme and our scheme considering the following parameters $N = 50$, $n = 614$ and $k = n/2 = 307$

V. CONCLUSION

In this paper, we have proposed a variant of 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 scheme suffer from large system parameters, that could be reduced by using specific codes such quasi-dyadic codes introduced in [10].
To the best of our knowledge, up to present there exist no 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.

Algorithm 5 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 σ_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 σ_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 σ_i $(t+1 \leq i \leq N)$
L chooses a random constant n-block permutation Σ 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 σ_i to Leader
else if $b = 1$ **then** P_i sends $\sigma_i((u_i + m_i)G_i)$ and $\sigma_i(e_i)$ to Leader
else if $b = 2$ **then** P_i sends σ_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 Π 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

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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/.
[8] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, volume 16. North-Holland Mathematical Library, 1977.
[9] 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.
[10] R. Misoczki and P. S. L. M. Barreto. Compact mceliece keys from goppa codes. Preprint, 2009. http://eprint.iacr.org/2009/187.pdf.
[11] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.
[12] 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).
[13] 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.
[14] 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.
[15] Pascal Véron. Probleme sd, opérateur trace, schemas dt'identification et codes de goppa. PhD thesis, Université de Toulon et du Var, 1995.
[16] Pascal Véron. Improved identification schemes based on error-correcting codes. *Appl. Algebra Eng. Commun. Comput.*, 8(1):57–69, 1996.