

A New Efficient Threshold Ring Signature Scheme based on Coding Theory

Abstract. Ring signatures were introduced by Rivest, Shamir and Tauman in 2001. Bresson, Stern and Szydlo extended the ring signature concept to t -out-of- N threshold ring signatures in 2002. We present in this paper a *generalization* of Stern's code based authentication (and signature) scheme to the case of t -out-of- N threshold ring signature. The size of our signature is in $\mathcal{O}(N)$ and does not depend on t . Our protocol is anonymous and secure in the random oracle model, it has a very short public key and has a complexity in $\mathcal{O}(N)$. This protocol is the first efficient code-based ring signature scheme and the first code-based threshold ring signature scheme. Moreover it has a better complexity than number-theory based schemes which have a complexity in $\mathcal{O}(Nt)$.

Keywords : Threshold ring signature, code-based cryptography, Stern's Scheme, syndrome decoding.

1 Introduction

In 1978, McEliece published a work where he proposed to use the theory of *error correcting codes* for confidentiality purposes. More precisely, he designed an asymmetric encryption algorithm whose principle may be sum up as follows: Alice applies a secret encoding mechanisms to a message and add to it a large number of errors, that can only be corrected by Bob who has information about the secret encoding mechanisms. The *zero-knowledge* authentication scheme proposed by Stern in [24] is based on a well-known error-correcting codes problem usually referred as the *Syndrome Decoding Problem* (*SD* in short). It is therefore considered as a good alternative to the numerous authentication schemes whose security relies on number theory problems, like the factorization and the discrete logarithm problems.

The concept of *ring signature* was introduced by Rivest, Shamir and Tauman [20] (called RST in the following). A ring signature is considered to be a simplified group signature without group managers. Ring signatures are related, but incomparable, to the notion of group signatures in [8]. On one hand, group signatures have the additional feature that the anonymity of a signer can be revoked (i.e. the signer can be traced) by a designated group manager, on the other hand, ring signatures allow greater flexibility: no centralized group manager or coordination among the various users is required (indeed, users may be unaware of each other at the time they generate their public keys). The original motivation was to allow secrets to be leaked anonymously. For example, a high-ranking government official can sign information with respect to the ring of all similarly high-ranking officials, the information can then be verified as coming from someone reputable without exposing the actual signer.

Bresson et al. [5] extended the ring signature scheme into a *threshold ring signature* scheme using the concept of partitioning and combining functions. Assume that t users want to leak some secret information, so that any verifier will be convinced that t users *among a select group* held for its validity. Simply constructing t ring signatures clearly does not prove that the message has been signed by different signers. A *threshold ring signature* scheme effectively proves that a minimum number of users of a certain group must have actually collaborated to produce the signature, while hiding the precise membership of the subgroup (for example the ring of public keys of all members of the President's Cabinet).

Contribution In this paper, we present a *generalization* of Stern’s authentication and signature scheme [24] for ring and threshold ring signature schemes. Our scheme’s performance does not depend on the number t of signers in the ring, the overall complexity and length of signatures only depend linearly in the maximum number of signers N . Our protocol also guarantees computational anonymity in the random oracle model. Besides these features and its efficiency, our protocol is also the first non generic coding theory based ring signature (and threshold ring signature) protocol and may constitute an interesting alternative to number theory based protocols. Overall our protocol has a very short public key size, a signature length linear in N and the best known complexity in $\mathcal{O}(N)$ when other number theory based threshold ring signature schemes have a complexity in $\mathcal{O}(Nt)$.

Organization of the paper The rest of this paper is organized as follows. In Section 2, we give a state of the art of ring signature and threshold ring signature. In Section 3, we describe Stern’s authentication and signature scheme and give some background and notation. In Section 4, we present our new *generalization* of Stern’s scheme in a threshold ring signature context. In Section 5, we study the security of the proposed scheme. In Section 6 we consider a variation of the protocol with double circulant matrices. In Section 7 we discuss the signature cost and length. Finally, we conclude in Section 8.

2 Overview of Ring Signatures

2.1 Ring signature

Following the formalization about ring signatures proposed in [20], we explain in this section the basic definitions and the properties eligible to ring signature schemes. One assumes that each user has received (via a PKI or a certificate) a public key p_{k_i} , for which the corresponding secret key is denoted s_{k_i} . A regular ring signature scheme consists of the following triple (Key-Gen, Sign and Verify):

- **Key-Gen** is a probabilistic polynomial algorithm that takes a security parameter(s) and returns the system, private, and public parameters.
- **Sign** is a probabilistic polynomial algorithm that takes system parameters, a private parameter, a list of public keys p_{k_1}, \dots, p_{k_N} of the ring, and a message M . The output of this algorithm is a ring signature σ for the message M .
- **Verify** is a deterministic algorithm that takes as input a message M , a ring signature σ , and the public keys of all the members of the corresponding ring, then outputs *True* if the ring signature is valid, or *False* otherwise.

Most of the existing ring signature schemes have a signature length linear in N , the size of the ring. Many schemes have been proposed, one can cite the work of Bendery, Katz and Morselli in [2] where they present three ring signature schemes which are provably secure in the standard model. Recently, Shacham and Waters [22] proposed a ring signature where for N members the signature consists of $2N + 2$ group elements and requires $2N + 3$ pairings to verify.

A breakthrough on the size of ring signature was obtained in [10] in which the authors proposed the first (and unique up to now) constant-size scheme based on accumulator functions and the Fiat-Shamir zero-knowledge identification scheme. However, the signature derived from the Fiat-Shamir scheme has a size of at least 160 kbits. Another construction proposed by Chandran, Groth and Sahai ([7]) has a size in $\mathcal{O}(\sqrt{N})$.

Recently in [32], Zheng, Li and Chen presented a code-based ring signature scheme with a signature length of $144 + 126N$ bits, but this scheme is based on the signature of [9] which remains very slow in comparison with other schemes.

Eventually a generalization of ring signature schemes in mesh signatures was proposed by Boyen in [4].

2.2 Threshold ring signature

In [5], Bresson, Stern and Szydlo introduced the notion of threshold ring signature. We explain in this section the basic definitions and the properties of threshold ring signature schemes.

One assumes that each user has created or received a secret key s_{k_i} and that a corresponding public key p_{k_i} is available to everyone.

Let A_1, \dots, A_N be the N potential signers of the ring with their p_{k_1}, \dots, p_{k_N} public keys. Then t of the N members form a group of signers, one of them, L , is the leader on the t -subgroup.

- Setup : initializes the state of the system. On input a security parameter 1^l , create a public database p_{k_1}, \dots, p_{k_N} , choose a leader L of the group and generate the system's parameters;
- Make-GPK : the Group Public Key construction algorithm;
- Commitment-Challenge-Answer : an electronic way to temporarily hide a sequence of bits that cannot be changed;
- Verification : takes as input the answers of the challenges and verifies the honesty of the computation, and returns a boolean.

In [5], the size of the signature grows with the number of users N and the number of signers t . More precisely, the size of such t -out-of- N signature is : $2^{\mathcal{O}(t)} \lceil \log_2 N \rceil \times (tl + Nl)$ computations in the easy direction where l is the security parameter.

Later, Liu et al. [15] proposed another threshold ring signature based on Shamir's secret sharing scheme. Their scheme is separable, with a signature length linear in N but a complexity in $\mathcal{O}(N^2)$ for $t \approx N/2$ (the cost of secret sharing scheme). The Mesh signature of [4] can also be used in that case: the signature length is also linear in N but the verification is in Nt bilinear pairings verifications.

A variation for ring signature was introduced in [26], where the author introduced the notion of *linkable ring signature* by which a signer can sign only once being anonymous, since a verifier can link a second signature signed by the same signer. Although this property may have interesting applications (in particular for e-vote) it does not provide full anonymity (in the sense that it cannot be repeated). Later their scheme was extended to threshold ring signature with a complexity in $\mathcal{O}(N)$, but again, only a linkable ring signature which does not correspond to original researched feature of [20] and [5], a fully anonymous scheme.

3 Notation and background on coding theory and Stern's signature scheme

3.1 Permutation notation

We first introduce two notions of *block permutation* that we will use in our protocol. Consider n and N two integers.

Definition 31 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 32 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 $(\sigma_1, \dots, \sigma_N)$ of $\{1, \dots, n\}$ on n positions and Σ a constant n -block permutation on N blocks defined on $\{1, \dots, N\}$. We consider a vector v of size nN of the form :

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

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

$$\Pi(w) = \Sigma \circ \sigma(w) = (\sigma_1(W_{\Sigma(1)}), \dots, \sigma_N(W_{\Sigma(N)})) = \Sigma(\sigma_1(W_1), \dots, \sigma_N(W_N)).$$

3.2 Difficult problems in coding theory

Let us recall that a linear binary code C of length n and dimension k , is a vector subspace of of dimension k of $GF(2)^n$. The weight of an element x of $GF(2)^n$ is the number of non zero coordinates of x . The minimum distance of a linear code is the minimum weight of any non-zero vector of the code. For any code one can define the scalar product $x.y = \sum_{i=1}^n x_i y_i$. A generator matrix G of a code is a generator basis of a code, the dual of code C is defined by $C^{perp} = \{y \in GF(2)^n | x.y = 0, \forall x \in C\}$. Usually a generator matrix of the dual of a code C is denoted by H . Remark that $c \in C \iff Hx^t = 0$. For $x \in GF(2)^n$, the value Hx^t is called the syndrome of x for H .

The usual hard problem considered in coding theory is the following Syndrome Decoding (SD) problem, proven NP-complete in [3] in 1978.

Problem:(SD) Syndrome decoding of a random code:

Instance: A $n - k \times n$ random matrix H over $GF(2)$, a non null target vector $y \in GF(2)^{(n-k)}$ and an integer ω .

Question: Is there $x \in GF(2)^n$ of weight $\leq \omega$, such that $Hx^t = y^t$?

This problem was used by Stern for his protocol [24], but in fact a few years later a variation on this problem called the Minimum Distance (MD) problem was also proven NP-complete in [27]:

Problem: (MD) Minimum Distance:

Instance: A binary $n - k \times n$ matrix H and an integer $\omega > 0$.

Question: Is there a non zero $x \in GF(2)^n$ of weight $\leq \omega$, such that $Hx^t = 0$?

It was remarked in [12] that this problem could also be used with Stern's scheme, the proof works exactly the same. Notice that the practical difficulty of both SD and MD problems are the

same: the difficulty of finding a word of small weight in a random code. The associated intractable assumptions associated to these problems are denoted by **SD assumption** and **MD assumption**, see [25] for a precise formal definition of the SD assumption related to the SD problem.

3.3 Stern's authentication scheme

This scheme was developed in 1993 (see [24]). It provides a zero-knowledge authentication scheme, not based on number theory problems. Let h be a hash function. Given a public random matrix H of size $(n - k) \times n$ over \mathbb{F}_2 . Each user receives a secret key s of n bits and of weight ω . A user's public identifier is the secret's key syndrome $i_L = Hs^t$. It is calculated once in the lifetime of H . It can thus be used by several future identifications. Let us suppose that L wants to prove to V that he is indeed the person corresponding to the public identifier i_L . L has his own private key s_L such that the public identifier is its syndrome $i_L = Hs_L^t$.

Our two protagonists run the following protocol :

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

$$c_1 = h(\sigma|Hy^t); \quad c_2 = h(\sigma(y)); \quad c_3 = h(\sigma(y \oplus s))$$

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

2. [Challenge Step] V sends $b \in \{0, 1, 2\}$ to L .
3. [Answer Step] Three possibilities :
 - if $b = 0$: L reveals y and σ .
 - if $b = 1$: L reveals $(y \oplus s)$ and σ .
 - if $b = 2$: L reveals $\sigma(y)$ and $\sigma(s)$.
4. [Verification Step] Three possibilities :
 - if $b = 0$: V verifies that c_1, c_2 have been honestly calculated.
 - if $b = 1$: V verifies that c_1, c_3 have been honestly calculated.
 - if $b = 2$: V verifies that c_2, c_3 have been honestly calculated, and that the weight of $\sigma(s)$ is ω .
5. Iterate the steps 1,2,3,4 until the expected security level is reached.

Fig. 1. Stern's protocol

Remark 1 During the fourth Step, when b equals 1, it can be noticed that Hy^t derives directly from $H(y \oplus s)^t$ since we have:

$$Hy^t = H(y \oplus s)^t \oplus i_A = H(y \oplus s)^t \oplus Hs^t .$$

It is proven in [24] that this scheme is a zero-knowledge Fiat-Shamir like scheme with a probability of cheating in $2/3$ (rather than in $1/2$ for Fiat-Shamir).

Remark 2 In [12] the authors propose a variation on the scheme by taking the secret key to be a small word of the code associated to H . The Minimum Distance problem MD, defined in the previous section. This results in exactly the same protocol except that, as the secret key is a codeword, the public key (i.e. the secret key's syndrome) is not the matrix H and the syndrome but only the matrix H . The protocol remains zero-knowledge with the same feature. The problem of finding a small weight codeword in a code has the same type of complexity that the syndrome decoding problem (and is also NP-complete). The only drawback of this point of view is that it relates the secret key with the matrix H but in our case we will be able to take advantage of that.

4 Our Threshold Ring Signature Scheme

In this section, we describe a new efficient threshold ring identification scheme based on coding theory. This scheme is a *generalization* of Stern’s scheme. Furthermore, by applying the Fiat-Shamir heuristics [11] to our threshold ring identification scheme, we immediately get a t -out-of- N threshold ring signature which size is in $\mathcal{O}(N)$.

4.1 High-level overview

Consider a ring of N members (P_1, \dots, P_N) and among them t users who want to prove that they have been cooperating to produce a ring signature. Each user P_i computes a public matrix H_i of $(n - k) \times n$ bits. A user’s public key consists of the public matrix H_i and an integer w (common to all public keys). The associated secret key is s_i a word of weight w of the code C_i associated to the dual of H_i .

The general idea of our protocol is that each of the t signers performs by himself an instance of Stern’s scheme using matrix H_i and a null syndrome as parameters (as in the scheme’s variation proposed in [12]). The results are collected by a leader L among the signers in order to form, with the addition of the simulation of the $N - t$ non-signers, a new interactive Stern protocol with the verifier V . The master public matrix H is created as the direct sum of the ring members’ public matrices. Eventually, the prover P , formed by the set of t signers among N (see Fig 2), proves (by a slightly modified Stern’s scheme - one adds a condition on the form of the permutation) to the verifier V that he knows a codeword s of weight $t\omega$ with a particular structure: s has a null syndrome for H and a special form on its N blocks of length n : each block of length has weight 0 or ω . In fact this particular type of word can only be obtained by a cooperation processus between t members of the ring. Eventually the complexity is hence the cost of N times the cost of a Stern authentication for a single prover (the multiplication factor obtained on the length of the matrix H used in the protocol) and this *for any value of t* .

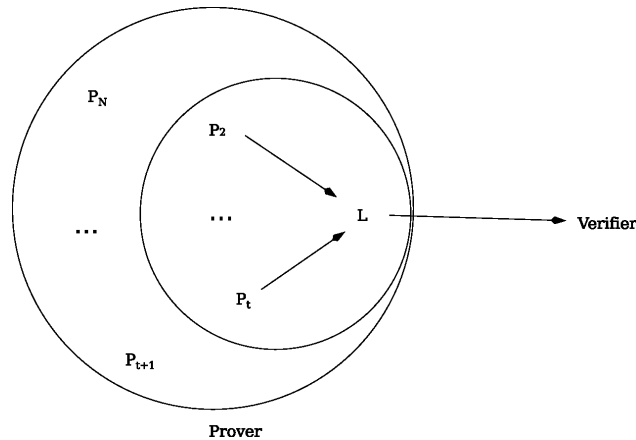


Fig. 2. Threshold ring signature scheme in the case where the t signers are P_1, \dots, P_t and the leader $L = P_1$, for a group of N members.

Besides the combination of two Stern protocols (one done individually by each signer P_i with the leader, and one slightly modified done by the leader with the verifier), our scheme relies on the three following main ideas:

1. The master public key H is obtained as the direct sum of all the public matrices H_i of each of the N users.
2. Indistinguishability among the members of the ring is obtained first, by taking a common syndrome value for all the members of the ring: the null syndrome, and second, by taking secret keys s_i with the same weight ω (public value) associated to public matrices H_i .
3. Permutation constraint: a constraint is added in Stern's scheme on the type of permutation used: instead of using a permutation of size Nn we use a n -block permutation on N blocks, which guarantees that the prover knows a word with a special structure, which can only be obtained by the interaction of t signers.

4.2 Setup

The Setup algorithm is run to obtain the values of the parameters l, n, k, t, w . l is the security parameter, n and $n - k$ the matrix parameters, ω the weight of the secret key s_i , t the number of signers. This algorithm also creates a public database p_{k_1}, p_{k_N} , (here matrices H_i). remark that parameters: n, k and ω are fixed once for all, and that any new user knowing these public parameters can join the ring. The parameter t has just to be precised at the beginning of the protocol.

The matrices H_i are constructed in the following way: choose s_i a random vector of weight ω , generate $k - 1$ random vectors and consider the code C_i obtained by these k words (the operation can be reiterated until the dimension is exactly k). The matrix H_i is then a $(n - k) \times n$ generator matrix of the dual code of C_i . Remark that this construction lead to a rather large public matrix H_i , we will consider in Section 7, an interesting variation of the construction.

4.3 Make-GPK

Each user owns a $(n - k) \times n$ -matrix H_i (public) and a n -vector s_i (secret) of small weight ω (public) such that

$$H_i s_i^t = 0.$$

The problem of finding s of weight ω is a MD problem defined earlier. The t signers choose a leader L among them which sends a set of public matrices H_1, \dots, H_N .

Remark: in order to simplify the description of the protocol (and to avoid double indexes), we consider in the following that the t signers correspond to the first t matrices H_i ($1 \leq i \leq t$) (although more generally their order can be considered random in $\{1, \dots, N\}$ since the order depends of the order of the N matrices sent by the leader.

Construction of a public key for the ring

The RPK (Ring Public Key) is constructed by considering, the matrix H described as follow:

$$H = \begin{pmatrix} H_1 & 0 & 0 & \cdots & 0 \\ 0 & H_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & H_N \end{pmatrix}.$$

H, ω and $H_i, \forall i \in \{1; \dots; N\}$ are public. The $s_i, \forall i \in \{1; \dots; N\}$ are private.

4.4 Commitment-Challenge-Answer and Verification steps

We now describe formally our scheme.

The leader L collects the commitments given from the $t - 1$ other signers, simulates the $N - t$ non-signers and chooses a random constant n -block permutation Σ on N blocks. From all these commitments L creates the master commitments C_1, C_2 and C_3 which are sent to the verifier V , who answers by giving a challenge b in $\{0, 1, 2\}$. Then L sends the challenge to each of the other $t - 1$ signers and collects their answers to create a global answer for V . Upon reception of the global answer, V verifies that it is correct by checking the commitments as in the regular Stern's scheme.

All the details of the protocol are given in Fig. 3. *Recall that in the description of the protocol, in order to avoid complex double indexes in the description we considered that the t signers corresponded to the first t matrices H_i .*

5 Security

5.1 Our Security model

The security of our protocol relies on two notions of unforgeability and anonymity secure under the Minimum Distance problem assumption in the random oracle model.

To prove the first notion we prove that our protocol is an Honest-Verifier Zero-Knowledge (HZVZK) Proof of Knowledge. It has been proven in [11] that every HVZK protocol can be turned into a signature scheme by setting the challenge to the hash value of the commitment together with the message to be signed. Such a scheme has been proven secure against existential forgery under adaptatively chosen message attack in the random oracle model in [19].

The second notion of anonymity for our scheme in a threshold context is defined as follows:

Definition 51 (Threshold ring signature anonymity) *Let $R = \{R_k(\cdot, \cdot)\}$ be a family of threshold ring signature schemes.*

We note $SIG \leftarrow S(G, M, R_k)$ a random choice among the signatures of a t user group G concerning a message M using the ring signature scheme R_k .

R is said to be anonymous if for any $c > 0$, there is a K such that for any $k > K$, any two different subgroups G_1, G_2 of t users, any message M and any polynomial-size probabilistic circuit family $C = \{C_k(\cdot, \cdot)\}$,

$$Pr(C_k(SIG, G_1, G_2, \mathcal{P}(k)) = G | SIG \leftarrow S(G, M, R_k)) < 1/2 + k^{-c}$$

G being randomly chosen among $\{G_1, G_2\}$, and $\mathcal{P}(k)$ being the set of all the public information about the ring signature scheme.

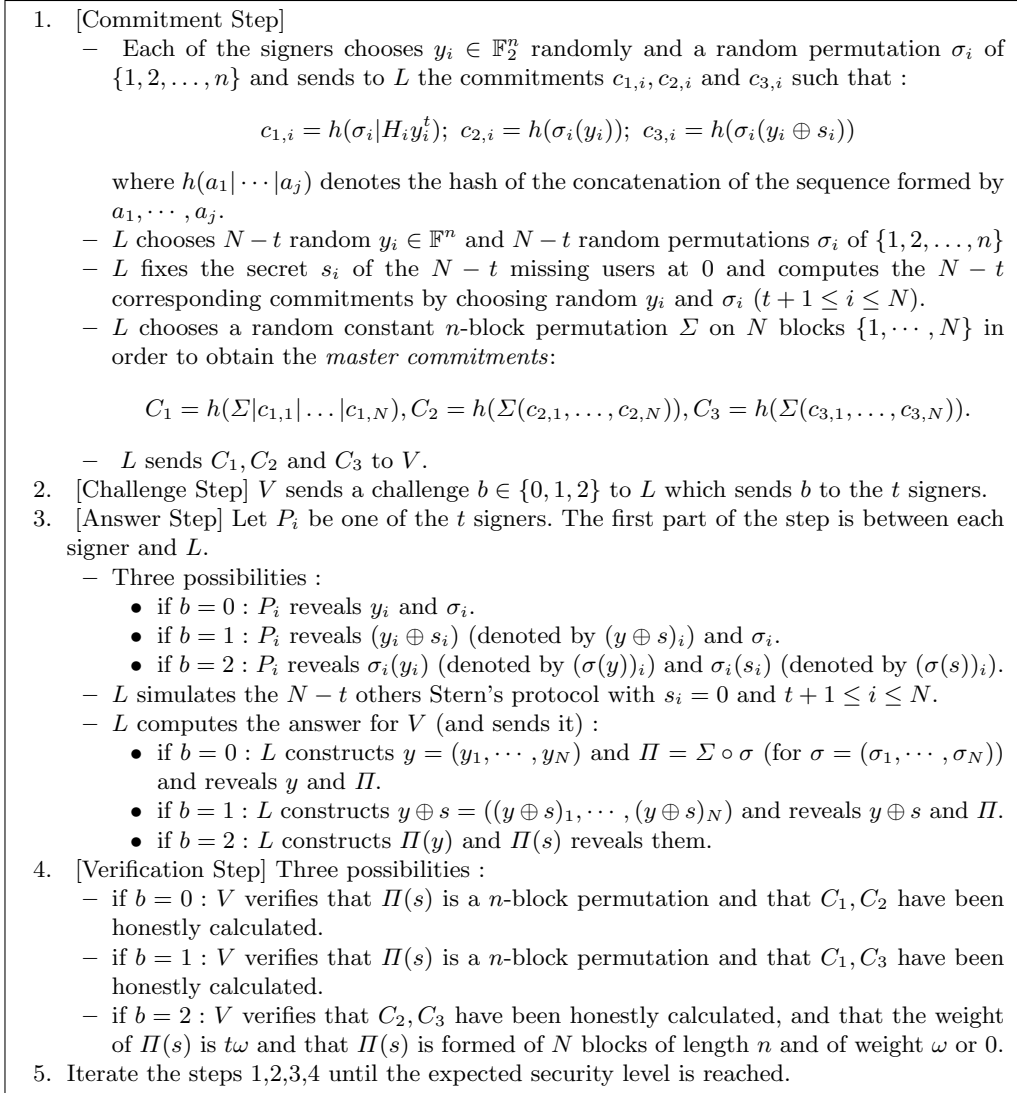


Fig. 3. Generalized Stern's protocol

5.2 Security of our scheme

We first prove that our scheme is HVZK with a probability of cheating of $2/3$. We begin by a simple lemma.

Lemma 1. *Finding a vector v of length nN such that the global weight of v is $t\omega$, the weight of v for each of the N blocks of length n is 0 or ω and such that v has a null syndrome for H , is hard under the MD assumption.*

Proof: The particular structure of H (direct sum of the H_i of same length n) implies that finding such a n -block vector of length nN is exactly equivalent to finding a solution for the local hard problem of finding s_i of weight ω such that $H_i s_i^t = 0$, which is not possible under our assumption. \square

Theorem 1. *Our scheme is a proof of knowledge, with a probability of cheating $2/3$, that the group of signers P knows a vector v of length nN such that the global weight of v is $t\omega$, the weight of v for each of the N blocks of length n is 0 or ω and such that v has a null syndrome for H . The scheme is secure under the MD assumption in the random oracle model.*

Proof:(sketch) We need to prove the usual three properties of completeness, soundness and zero-knowledge. The property of completeness is straightforward since for instance for $b = 0$, the knowledge of y and Π permits to recover Σ , σ_i and the y_i so that it is possible for the verifier to recover all the c_i and hence the master commitment C_1 , the same for C_2 . The cases $b = 1$ and $b = 2$ works the same. The proof for the soundness and zero-knowledge follow the original proof of Stern in [25] for the problem defined in the previous lemma, by remarking that the structure of our generalized protocol is copied on the original structure of the protocol with Σ in Fig.3 as σ in Fig.1, and with the fact that one checks in the answers $b = 0$ and $b = 1$ in the protocol that the permutation Π is an n -block permutation on N blocks. \square

Remark: It is also not possible to have information leaked between signers during the protocol since each signer only gives information to L (for instance) as in a regular Stern's scheme which is zero-knowledge.

Now we consider anonymity of our protocol, the idea of the proof is that if an adversary has the possibility to get more information on who is a signer among the N potential signers or who is not, it would mean in our case that the adversary is able to know with a better probability than $2/3$ that a block s_i of $s = (s_1, \dots, s_N)$ of size n among the N such blocks associated to the created common secret s is completely zero or not. But since we saw that our protocol was zero-knowledge based on a light modification of the Stern protocol, it would mean that the adversary is able to get information on the secret s during the interaction between L and V , which is not possible since the protocol is zero-knowledge. Formally we obtain:

Theorem 2. *Our protocol satisfies the threshold ring signature anonymity.*

Proof:Suppose that for a given M , a given $c > 0$ and two given subgroups G_1, G_2 of t users there is a family of circuits $C = \{C_k(\cdot, \cdot)\}$ such that for any K there is a $k > K$ such that

$$Pr(C_k(SIG, G_1, G_2, \mathcal{P}(k)) = G | SIG \leftarrow S(G, M, R_k)) > 1/2 + k^{-c}.$$

Consider a user $P_i \in G_1$ such that $U \notin G_2$ (such a user exists as the groups are different), and the following circuit: - Whenever the circuit C_k outputs G_1 : output that the i -th (out of N) block of size n of the secret s associated to the matrix H is not null. - Whenever the circuit C_k outputs G_2 : output that the i -th (out of N) block of size n of the secret s associated to the matrix H is null. Such a circuit guesses with non-negligible advantage whether a part of the secret s associated to the ring key matrix H is null or not, and therefore breaks the zero-knowledge property of the protocol. the family of circuits $C' = \{C_k(\cdot, \cdot)\}$ \square

5.3 Practical Security of Stern's Scheme from [24]

The security of Stern's Scheme relies on three properties of random linear codes:

1. Random linear codes satisfy a Gilbert-Varshamov type lower bound [16],
2. For large n almost all linear codes lie over the Gilbert-Varshamov bound [18],

3. Solving the syndrome decoding problem for random codes is NP-complete [3].

In practice Stern proposed in [24] to use rate 1/2 codes and ω just below the Gilbert-Varshamov bound associated to the code. For such code the exponential cost of the best known attack [6] is in $\approx O(n) \frac{\binom{n}{\omega}}{\binom{n-k}{\omega}}$, which gives a code with today security (2^{80}) of $n = 634$ and rate 1/2 and $\omega = 69$.

6 An interesting variation of the scheme based on double-circulant matrices

In Section 5 we described a way to create the public matrices H_i , this method as in the original Stern's paper, leads to a large size of the public keys H_i in $n^2/2$ bits. It was recently proposed in [12], to use double-circulant random matrices rather than pure random matrices for such matrices. A double circulant matrix is a matrix of the form $H_i = (I|C)$ for C a random $n/2 \times n/2$ cyclic matrix and I the identity matrix. Following this idea one can construct the matrices H_i as follows: consider $s_i = (a|b)$ where a and b are random vectors of length $n/2$ and weight $\approx \omega/2$, then consider the matrix $(A|B)$ obtained for A and B square $(n/2 \times n/2)$ matrices obtained by the $n/2$ cyclic shifts of a and b (each row of A is a shift of the previous row, beginning with first row a or b).

Now consider the code G_i generated by the matrix $(A|B)$, the matrix H_i can then be taken as $H_i = (I|C)$ such that H_i is a dual matrix of G_i and C is cyclic since A and B are cyclic, and hence can be described with only its first row). It is explained in [12] that this construction does not decrease the difficulty of the decoding but clearly decrease dramatically the size of the description of H_i : $n/2$ bits against $n^2/2$.

It is then possible to define a new problem:

Problem: (MD-DC) Minimum Distance of Double circulant codes:

Instance: A binary $n/2 \times n$ double circulant matrix H and an integer $\omega > 0$.

Question: Is there a non zero $x \in GF(2)^n$ of weight $\leq \omega$, such that $Hx^t = 0$?

It is not known whether this problem is NP-complete or not, but the problem is probably as hard as the MD problem, and on practical point of view (see [12] for details) the practical security is almost the same for best known attack that the MD problem. Practicly the author of [12] propose $n = 347$.

Now all the proof of security we considered in this paper can also be adapted to the $MD-DC$ problem, since for the generalized Stern protocol we introduced we can take any kind of H_i with the same type of problem: knowing a small weight vector associated to H_i (in fact only the problem assumption changes).

7 Length and Complexity

In this section examine the complexity of our protocol and compare it to other protocol.

7.1 The case $t = 1$

This case corresponds to the case of classical ring signature scheme, our scheme is then not so attractive in term of length of signature since we are in \mathcal{N} but more precisely in $\approx 20ko \times N$ (for $20ko$ the cost of one Stern signature), meanwhile since the Stern protocol is fast in term of speed our protocol is faster than all others protocols for $N = 2$ or 3 which may have some applications.

7.2 The general case

Signature length

It is straight forward to see that the signature length of our protocol is in $\mathcal{O}(N)$, more precisely in $\approx 20ko \times N$, for 20ko the length of one signature by the Fiat-Shamir paradigm applied to the Stern scheme (a security of 2^{-80} is obtained by 140 repetitions of the protocol). For instance consider a particular example with $N = 100$ and $t = 50$, we obtain a $2Mo$ signature length, which is quite large, but still tractable. Of course other number theory based protocols like [4] or [15] have shorter signature lengths (in 8Ko or 25Ko) but are slower.

Public key size

If we use the double-circulant construction described in Section 6, we obtain, a public key size in $347N$ which has a factor 2 or 3 better than [15] and of same order than [4].

Complexity of the protocol

The cost of the protocol is N times the cost of one Stern signature protocol hence in $\mathcal{O}(N)$, (more precisely in $140n^2N$ operations) and this *for any* t . When all other fully anonymous threshold ring signature protocol have a complexity in $\mathcal{O}(tN)$ operations (multiplications or modular exponentiations in large integer rings, or pairings). Hence on that particular point our algorithm is faster than other protocols.

8 Conclusion

In this paper we presented a new (fully anonymous) t -out-of- N threshold ring signature scheme based on coding theory. Our protocol is a very natural generalization of the Stern authentication scheme and our proof is based on the original proof of Stern. We showed that the notion of weight of vector particularly went well in the context of ring signature since the notion of ad hoc group corresponds well to the notion of direct sum of generator matrices and is compatible with the notion of sum of vector of small weight. Eventually we obtain a fully anonymous protocol based on a proof of knowledge in the random oracle model. Our protocol is the first non-generic protocol based on coding theory and (as usual for code based protocol) is very fast compared to other number theory based protocols

Moreover the protocol we described can also be easily generalized to the case of general access scenario. Eventually the fact that our construction is not based on number theory but on coding theory may represent an interesting alternative. We hope this work will enhance the potential of coding theory in public key cryptography.

References

1. ABE M., OHKUBO M., and SUZUKI K. : 1-out-of- N signatures from a variety of keys, To appear in Advances in Cryptology-Asiacrypt 2002, 2002
2. BENDER A., KATZ J. and MORSELLI R. : Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles Theory of Cryptography, Lecture Notes in Computer Science, page 60-79, Volume 3876/2006
3. BERLEKAMP E. MCELIECE R. and VAN TILBORG H.: On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, IT-24(3), 1978.
4. Xavier Boyen: Mesh Signatures. EUROCRYPT 2007: 210-227
5. BRESSON E., STERN J. and SZYDLO M. : Threshold ring signatures and applications to ad-hoc groups. In Advances in Cryptology, Crypto 2002.

6. CANTEAUT A. and CHABAUD F.: A new algorithm for finding minimum-weight words in a linear code: application to primitive narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, IT-44:367–378, 1988.
7. CHANDRAN N., GROTH J. and SAHAI A.: Ring signatures of sub-linear size without random oracles. In ICALP, LNCS 4596, pages 423-434, 2007.
8. CHAUM D. and VAN HEYST E.: Group signatures. In *Advances in Cryptology, Eurocrypt'91*.
9. N. Courtois, M. Finiasz and N. Sendrier, How to achieve a McEliece based digital signature scheme. In *Advances in Cryptology-ASIACRYPT 2001*, Springer-Verlag.
10. DODIS Y., KIAYIAS A., NICOLOSI A. and SHOUP V. : Anonymous identification in ad-hoc groups. In *Advances in Cryptology, Eurocrypt 2004*.
11. FIAT A. and SHAMIR A. : How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Advances in Cryptology-CRYPTO'86*, volume 263 of LNCS, pages 186-194. Springer, 1986.
12. GABORIT P. and GIRAULT M. : Lightweight code-based authentication and signature ISIT 2007
13. HERRANZ J. and SAEZ G. : Forking lemmas for ring signature schemes, in *Indocrypt'03*, LNCS 2904, pp.266-279, Springer-verlag, 2003.
14. KUWAKADO H. and TANAKA H. : Threshold Ring Signature Scheme Based on the Curve, *Transactions of Information Processing Society of Japan* volume 44, number 8, page 2146-2154(2003)
15. LIU J.K., WEI V.K. and WONG D.S. : A Separable Threshold Ring Signature Scheme. In Jong In Lim and Dong Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003*, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers, volume 2971 of *Lecture Notes in Computer Science*, pages 352-369. Springer, 2003.
16. MACWILLIAMS F.J., SLOANE N.J.A. : *The Theory of Error Correcting Codes*, North-Holland (1977).
17. NAOR M. : Deniable Ring Authentication, *Advances in Cryptology-Crypto 2002*, LNCS 2442, pp.481-498, Springer-Verlag, 2002
18. PIERCE J.N. : Limit distributions of the minimum distance of random linear codes, *IEEE Trans. Inf. theory*, Vol IT-13 (1967), pp. 595-599.
19. D. Pointcheval and J. Stern: Security proofs for signature schemes, *Advances in Cryptology-EuroCrypt 1996*, LNCS 1070, pp.387-398, Springer-Verlag, 1996.
20. RIVEST R.L. , SHAMIR A. and TAUMAN Y. : How to leak a secret, *Advances in Cryptology-Asiacrypt 2001*, LNCS 2248, pp.552-565, Springer-Verlag, 2001.
21. SENDRIER N. : *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs*, Mémoire d'habilitation, Inria 2002, available at: <http://www-rocq.inria.fr/codes/Nicolas.Sendrier/pub.html>
22. SHACHAM H. and WATERS B. : Efficient Ring Signatures without Random Oracles, *Public Key Cryptography - PKC 2007* page 166-180, Volume 4450/2007
23. SHAMIR A.: How to share a secret. In *Com. of the ACM*, 22(11):612-613,1979.
24. STERN J.: A new identification scheme based on syndrome decoding. *Lecture Notes in Computer Science 773*, 1994.
25. STERN J.: A new paradigm for public key identification *IEEE Transactions on Information Theory* 42 (6) 2996, 2757–2768
<http://www.di.ens.fr/~stern/publications.html>
26. TSANG P.P., WEI V.K., CHAN T.K., AU M.H., LIU J.K. and WONG D.S. : Separable Linkable Threshold Ring Signatures. In Anne Canteaut and Kapalee Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004*, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings, volume 3348 of *Lecture Notes in Computer Science*, pages 384-398. Springer, 2004.
27. VARDY A. : The intractability of computing the minimum distance of a code. *IEEE Transactions on Information Theory* 43(6): 1757-1766 (1997)
28. VÉRON P.: A fast identification scheme. *Proceedings of IEEE, International Symposium on Information Theory'95, Whistler, Canada, Septembre 1995*.
29. WONG D.S., FUNG K., LIU J.K. and WEI V.K. : On the RSCode Construction of Ring Signature Schemes and a Threshold Setting of RST. In Sihan Qing, Dieter Gollmann, and Jianying Zhou, editors, *Information and Communications Security*, 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13, 2003, Proceedings, volume 2836 of *Lecture Notes in Computer Science*, pages 34-46. Springer, 2003
30. XU J., ZHANG Z. and FENG D. : A ring signature scheme using bilinear pairings. In *Workshop on Information Security Applications (WISA)*, 2004.
31. ZHANG F. and KIM K.: ID-Based Blind Signature and Ring Signature from Pairings, *Advances in Cryptology-ASIACRYPT*, 2002

32. ZHENG D., LI X. and CHEN K. : Code-based Ring Signature Scheme, International Journal of Network Security, Vol.5, No.2, PP.154-157, Sept. 2007 available at <http://ijns.nchu.edu.tw/contents/ijns-v5-n2/ijns-2007-v5-n2-p154-157.pdf>