A New Efficient Threshold Ring Signature Scheme based on Coding Theory

Carlos Aguilar, Pierre-Louis Cayrel, Philippe Gaborit and Fabien Laguillaumie

***Abstract*—Ring signatures were introduced by Rivest, Shamir and Tauman in 2001 [26]. These signatures allow a signer to anonymously authenticate a message on behalf of a group of his choice. This concept was then extended by Bresson, Stern and Szydlo into t-out-of-N (threshold) ring signatures in 2002 [8]. We propose in this article a *generalisation* of Stern's code based identification (and signature) scheme [30] to design a practical t-out-of-N threshold ring signature scheme. The size of the resulting signatures is in $\mathcal{O}(N)$ and does *not* depend on t, contrary to most of the existing protocols. Our scheme is existentially unforgeable under a chosen message attack in the random oracle model assuming the hardness of the *minimum distance problem*, is unconditionally source hiding, it has a very short public key and has an overall 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 $\mathcal{O}(Nt)$. This paper is an extended version of [2] with complete proofs and definitions.**

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

I. Introduction

The constant need to electronically emulate real-life applications with strong security properties leads to the design of sophisticated identification schemes with specific properties. Ring signatures are such an identification technique, where a signer anonymously authenticates a message on behalf of a group of his own choice. The design of such special purpose signatures almost always relies on arithmetic in the ring $\mathbb{Z}/N\mathbb{Z}$ or in groups of points of an algebraic curve equipped or not with a pairing.

From the point of view of the efficiency of the computations involved in the whole cryptographic process, *error correcting codes* are a real alternative to such integral arithmetic. Indeed, in 1978 when McEliece published his seminal work where he proposed to use the theory of error correcting codes for confidentiality purposes, he designed one of the most efficient encryption schemes, which *still* resist to cryptanalysts. His asymmetric encryption algorithm 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. A long time after, Stern proposed in [30] a *zero-knowledge* identification protocol 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 identification schemes whose security relies on number theory problems, like the factorisation of large integers and the discrete logarithm problem.

The concept of *ring signature*, which is the subject of this article, was introduced in 2001 by Rivest, Shamir and Tauman [26] (called RST in the following). Ring signatures are often considered as simplified group signatures without group managers. If ring signatures are related to this notion of group signatures in [11], they are indeed quite different. 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 centralised 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). Moreover, the anonymity of the signer is unconditionally guaranteed. 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.* [8] 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. The trivial construction consisting in producing 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).

1) Related Work: The seminal work of Bresson *et al.* [8] suffers from a lack of efficiency since the size of the signature grows with the number of users N and the number of signers t. More precisely, the size of their t-out-

C. Aguilar and P. Gaborit are with University of Limoges, XLIM-DMI, 123, Av. Albert Thomas 87060 Limoges Cedex France. carlos.aguilar@unilim.fr,gaborit@unilim.fr

P.L Cayrel is with CASED Center for Advanced Security Research Darmstadt Mornewegstrasse, 32 64293 Darmstadt Germany pierre-louis.cayrel@cased.de

F. Laguillaumie is with University of Caen, GREYC fabien.laguillaumie@info.unicaen.fr

of-N signature is $2^{\mathcal{O}(t)}\lceil \log_2 N \rceil \times (tl + Nl)$ where l is the security parameter. A number of t inversions are necessary to perform a signature and $\mathcal{O}(2^t N \log_2 N)$ computations are needed in the easy direction.

Later, Liu et al. [21] proposed another threshold ring signature based on Shamir's secret sharing scheme. Their scheme is separable (which means that the signers are free to choose their own parameters), with a signature length *linear* in N but a *quadratic* complexity for $t \approx N/2$ (the cost of secret sharing scheme). The notion of *mesh signature*, introduced by Boyen in [7] can also be used in that case: the signature length is also linear in N but the verification is in $\mathcal{O}(Nt)$ bilinear pairings computations.

A variation for ring signature was introduced in [32] by Tsang, Wei, Chan, Au, Liu and Wong: the authors 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 required feature of [26] and [8], namely a fully anonymous scheme.

A first attempt to design ring signatures within the error correcting code setting was performed by Zheng, Li and Chen [38], but their scheme is still inefficient. Very recently, Dallot and Vergnaud proposed a code-based threshold ring signature scheme [13], inspired by Bresson *et al.*'s construction with Courtois, Finiasz and Sendrier's signatures [12]. Both previous schemes use [12], which makes them very difficult to use in practice.

2) Contributions: In this paper, we present a *generalisation* of Stern's identification and signature scheme [30] that we use to design new 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 unconditional anonymity of the signers. 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 $\mathcal{O}(Nt)$.

3) Organisation of the paper.: The rest of this paper is organised as follows. In Section II, we give a state of the art of ring signatures and threshold ring signatures. In Section III, we describe Stern's identification and signature scheme and give some background and notation. In Section IV, we present our new *generalisation* of Stern's scheme in a threshold ring signature context. In Section V, we study the security of the proposed scheme. In Section VI we consider a variation of the protocol with double circulant matrices. In Section VII we discuss the signature cost and length. Finally, we conclude in Section VIII.

II. Overview of Ring Signatures

A. Ring signature

Following the formalisation of ring signatures proposed in [26], we review in this section some basic definitions and properties eligible to ring signature schemes.

Definition 1 (Ring Signature) *Let λ be an integer. A* ring signature scheme *RS consists of the following four algorithms:*

- *Setup: is a probabilistic algorithm which takes the unary string 1^λ as input and outputs the* public parameters *$\mathcal{P}$. The integer λ is the* security parameter *and will be an input of all algorithms.*
- *KeyGen: is a probabilistic algorithm which takes public parameters as input and outputs a pair of secret and public keys (sk, pk).*
- *Sign: is a probabilistic algorithm which takes as input public parameters, a set $\{pk_1, \ldots, pk_n\}$ of public keys, a secret key sk_i for $1 \leq i \leq n$, a message m, and which outputs a ring signature σ on m.*
- *Verify: is a deterministic algorithm which takes as input public parameters, a set $\{pk_1, \ldots, pk_N\}$ of public keys, a putative pair message/signature (m, σ), and outputs 1 if σ is a valid signature on m with respect to the set of public keys $\{pk_1, \ldots, pk_N\}$, and 0 otherwise.*

The crucial security property expected from a ring signature scheme (besides its unforgeability) is the *source hiding*, which is a very strong anonymity property. Indeed, it means that an attacker, even with unbounded computation capabilities, is not able to determine which member of the ring actually produced a given signature. This property is required to be unconditionnaly fulfilled (*i.e.* in the information theoretic sense), not only computationnaly. Precise definition of the security requirements will be detailed in the next section concerning *threshold* ring signatures.

From a practical point of view, most of the existing ring signature schemes have a signature length linear in N, the size of the ring. Among the many schemes appearing in the literature, one can mention the work of Bendery, Katzyz and Morselli in [3] where they present three ring signature schemes which are provably secure in the *standard model*. Recently, Shacham and Waters [28] proposed a ring signature scheme where the signature consists of $2N + 2$ group elements and requires $2N + 3$ pairings to be verified.

A breakthrough on the size of ring signature was obtained in [14] 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, and the security proof is conducted in the random oracle model. Another construction proposed by Chandran, Groth and Sahai ([10]) has a size in $\mathcal{O}(\sqrt{N})$.

Recently in [38], 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 from [12] which remains very slow in comparison with other schemes.

Eventually a generalisation of ring signature schemes in mesh signatures was proposed by Boyen in [7].

B. Threshold ring signature: definition and security model

In [8], Bresson, Stern and Szydlo introduced the notion of threshold ring signature as an extension of the original concept of ring signature from Rivest *et al.* [26]. We formally define in this section the notion of threshold ring signature scheme together with the security requirements.

Definition 2 (Threshold Ring Signature) *Let λ, t and N be three integers. A (t, N)-*threshold ring signature scheme *TRS consists of the following four algorithms:*

- *Setup: is a probabilistic algorithm which takes the unary string 1^λ as input and outputs the* public parameters *$\mathcal{P}$.*
- *KeyGen: is a probabilistic algorithm which takes public parameters as input and outputs a pair of secret and public keys (sk, pk).*
- *Sign: is a probabilistic interactive protocol between t users, involving public parameters, a set $\{pk_1, \ldots, pk_N\}$ of public keys, a set of t secret keys $\{sk_{i_1}, \ldots, sk_{i_t}\}$, a message m, and which outputs a (t, N)-threshold ring signature σ on m.*
- *Verify: is a deterministic algorithm which takes as input public parameters, a threshold value t, a set $\{pk_1, \ldots, pk_N\}$ of public keys, a putative pair message/signature (m, σ), and outputs 1 if σ is a valid signature on m with respect to the set of public keys $\{pk_1, \ldots, pk_N\}$, and 0 otherwise.*

The scheme TRS must be *correct*, which means that for all $(\lambda, N, t) \in \mathbb{N}^3$, for all $m \in \{0,1\}^*$, for all $\mathcal{P} \leftarrow \mathsf{TRS.Setup}(1^\lambda)$, $\mathsf{TRS.Verify}(\mathcal{P}, t, \{pk_1, \ldots, pk_N\}, (m, \sigma)) = 1$ as long as $(sk_i, pk_i) \leftarrow \mathsf{TRS.KeyGen}(\mathcal{P}) \ \ \forall \ \ 1 \leq i \leq N$, and $\sigma \leftarrow \mathsf{TRS.Sign}(\mathcal{P}, \{pk_1, \ldots, pk_N\}, \{sk_{i_1}, \ldots, sk_{i_t}\}, m)$ with $\{sk_{i_1}, \ldots, sk_{i_t}\} \subset \{sk_1, \ldots, sk_N\}$.

Let us now discuss the security criteria which must be fulfilled by a threshold ring signature scheme.

1) Unforgeability: The conventional notion of security for signatures was introduced by Goldwasser, Micali and Rivest in [17]. A signature scheme is said to be secure if it is indeed *existentially unforgeable* under a *chosen message attack*. We formally describe by the following game between an existential forger $\mathcal{F}$ and its challenger $\mathcal{C}$, the similar notion of security for a threshold ring signature scheme.

Definition 3 *A threshold ring signature scheme is said to be existentially unforgeable under a chosen message attack if no PPT adversary $\mathcal{F}$ has a non-negligible advantage in the following game.*

1) *The challenger $\mathcal{C}$ chooses a security parameter λ and executes $\mathcal{P} \leftarrow \mathsf{TRS.Setup}(1^\lambda)$ and $(sk_i, pk_i) \leftarrow \mathsf{TRS.KeyGen}(\mathcal{P})$ for $1 \leq i \leq N$. It gives all pk_i's to the forger $\mathcal{F}$ and keeps the corresponding secret keys to itself.*
2) *The forger $\mathcal{F}$ can issue the following queries:*
   a) *a signing query for some message m; the challenger $\mathcal{C}$ executes $\sigma \leftarrow \mathsf{TRS.Sign}(\mathcal{P}, \{pk_1, \ldots, pk_N\}, \{sk_{i_1}, \ldots, sk_{i_t}\}, m)$ and hands σ to $\mathcal{F}$;*
   b) *a corrupt query for some $pk_i \in \{pk_1, \ldots, pk_N\}$: $\mathcal{C}$ gives $\mathcal{F}$ the corresponding secret key sk_i.*
3) *$\mathcal{F}$ outputs a (t, N)-threshold ring signature $\tilde{\sigma}^\star$ for a new message $m^\star$.*

The adversary $\mathcal{F}$ succeeds if $\mathsf{TRS.Verify}\big(\mathcal{P}, t, \{pk_1, \ldots, pk_N\}, (m^\star, \sigma^\star)\big) = 1$, $m^\star$ has not been asked by $\mathcal{F}$ in a signing query in step 1 of the game and the number of corrupt queries is strictly less than t. An attacker $\mathcal{F}$ is said to $(\tau, q_s, q_c, \varepsilon)$-break the unforgeability of the TRS scheme if he succeeds in the game within running time τ and with probability ε after having made q_s signing queries and q_c corrupt queries.

2) Anonymity of signers: The essential notion of security for ring signatures is an anonymity property, called *source hiding*. Roughly speaking, a (t, N)-threshold signature scheme is *source hiding* (or has perfect anonymity) if a signature on a message m produced by a set of signers S_0 of a given ring R looks exactly the same as a signature on the message m produced by another set S_1 of signers of the ring R. More formally, this notion is extended to the threshold setting in the following definition.

Definition 4 (Source hiding) *Let t and N be two integers. A (t, N)-threshold ring signature scheme TRS is said to be* unconditionnaly source hiding *if there exists a probabilistic polynomial time algorithm Fake taking as inputs some public parameters, a set $\{pk_1, \ldots, pk_N\}$ of public keys, a set of t secret keys $\{sk_{i_1}, \ldots, sk_{i_t}\}$ and a message m, which outputs a a bit string such that*

$\mathsf{TRS.Sign}(\mathcal{P}, \{pk_1, \ldots, pk_N\}, \{sk_{i_1}, \ldots, sk_{i_t}\}, m) = \mathsf{Fake}(\mathcal{P}, \{pk_1, \ldots, pk_N\}, \{sk_{j_1}, \ldots, sk_{j_t}\}, m)$

with $\#\{sk_{i_1}, \ldots, sk_{i_t}\} \cap \{sk_{j_1}, \ldots, sk_{j_t}\} < t$, for all $m \in \{0,1\}^*$, for all $\mathcal{P} \leftarrow \mathsf{TRS.Setup}(1^\lambda)$ and $(sk_i, pk_i) \leftarrow \mathsf{TRS.KeyGen}(\mathcal{P}) \ \ \forall \ \ 1 \leq i \leq N$.

C. Fiat-Shamir Heuristic

Fiat and Shamir proposed in [15] a general paradigm for designing a secure signature scheme from a secure identification scheme. The idea is to start from a secure 3-round public coin identification scheme (with a commitment α from the prover, a random challenge β from the verifier and the response γ from the prover), and then to turn into a digital signature scheme with the help of a random oracle $\mathcal{H}$. Indeed, to sign a message m, the signer (who knows the secret) produces a valid transcript (α, β, γ) of the interactive identification protocol where $\beta = \mathcal{H}(\alpha, m)$.

Its efficiency and ease of design make the Fiat-Shamir protocol very popular. As indicated by Pointcheval and Stern in [25], an honest-verifier zero-knowledge protocol leads to a secure signature scheme in the random oracle model. This framework will be used to obtain our ring signature scheme from our generalised Stern's identification protocol.

III. Notations and background on coding theory and Stern's identification protocol

A. Permutation notation

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

Definition 5 *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 is 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 6 *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 a 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 $(\sigma_1, \ldots, \sigma_N)$ of $\{1, \ldots, n\}$ on n positions and Σ a constant n-block permutation on N blocks defined on $\{1, \ldots, N\}$. We consider a vector v of size nN of the form :

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

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

$$\Pi(v) = \Sigma \circ \sigma(v) =$$

$$(\sigma_1(V_{\Sigma(1)}), \ldots, \sigma_N(V_{\Sigma(N)})) = \Sigma(\sigma_1(V_1), \cdots, \sigma_N(V_N)).$$

B. 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 dimension k of $\mathbb{F}_2^n$. The *weight* of an element x of $\mathbb{F}_2^n$ 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. One define the scalar product between x and y from $\mathbb{F}_2^n$ as $x.y = \sum_{i=1}^{n} x_i y_i$. A generator matrix G of a code is a generator basis of a code, the dual of a code C is defined by $C^\perp = \{y \in \mathbb{F}_2^n | x.y = 0, \forall x \in C\}$. Usually a generator matrix of the dual of a code C is denoted by H. Remark that $x \in C \iff Hx^t = 0$. For $x \in \mathbb{F}_2^n$, 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 to be NP-complete in [5] in 1978.

Problem: (SD) Syndrome decoding of a random code
Instance: A $(n-k) \times n$ random matrix H over $\mathbb{F}_2$, a non null target vector $y \in \mathbb{F}_2^{(n-k)}$ and an integer $\omega > 0$.
Question: Is there $x \in \mathbb{F}_2^n$ of weight $\leq \omega$, such that $Hx^t = y^t$?

This problem was used by Stern to design his identification protocol [30], but in fact a few years later a variation on this problem called the *minimum distance (MD) problem* was also proven to be NP-complete in [33]:

Problem: (MD) Minimum Distance
Instance: A binary $(n-k) \times n$ matrix H and an integer $\omega > 0$.
Question: Is there a non zero $x \in \mathbb{F}_2^n$ of weight $\leq \omega$, such that $Hx^t = 0$?

It was remarked in [16] 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 [31] for a precise formal definition of the SD assumption related to the SD problem.

C. Stern's Identification Protocol

This scheme was developed in 1993 (see [30]). It provides a zero-knowledge identification protocol, 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 L receives a secret key s_L of n bits and of weight ω. A user's public identifier is the secret key's syndrome $i_L = Hs_L^t$. 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 satisfies $i_L = Hs_L^t$. The two protagonists run the protocol depicted in Fig. 1.

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

$$Hy^t = H(y \oplus s_L)^t \oplus i_L = H(y \oplus s_L)^t \oplus Hs_L^t \ .$$

∎

It is proven in [30] 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).

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

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

   where $h(a|b)$ denotes a hash value of the concatenation of the sequences a and b.
2) Challenge Step: V sends $b \in \{0, 1, 2\}$ to L.
3) Answer Step:
   - 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:
   - 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: In [16] the authors propose a variation on the scheme by taking the secret key to be a small word of the code associated to H. This results is 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 together with 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. ∎

IV. 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 *generalisation* of Stern's scheme. Furthermore, by applying the Fiat-Shamir heuristic [15] to our threshold ring identification scheme, we immediately get a t-out-of-N threshold ring signature scheme with signature's size in $\mathcal{O}(N)$.

A. A Code-Based Construction of Threshold Ring Signature

Consider a ring of N members $(P_1, \cdots, P_N)$ 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 [16]). 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 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 n has weight 0 or ω. In fact this particular type of word can only be obtained by a cooperation process between t members of the ring. Eventually the complexity is hence the cost of N times the cost of a Stern identification 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.

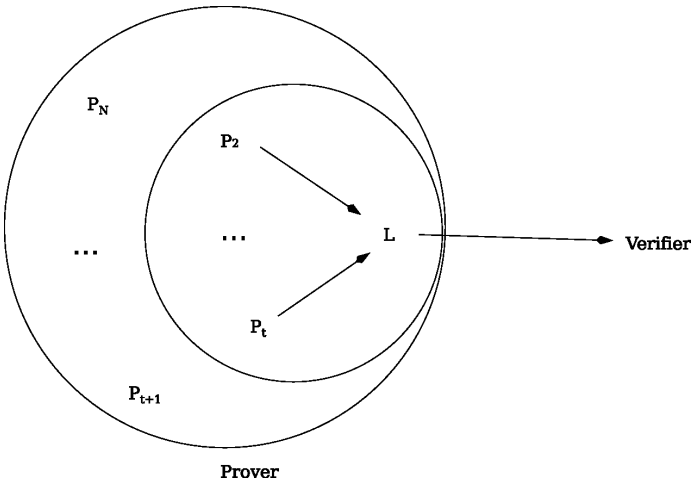

Fig. 2. Threshold ring signature scheme in the case where the t signers are $P_1, \cdots, P_t$ and the leader $L = P_1$, for a group of N members.

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.

The overall scheme is described by the following algorithms.

1) TRS.Setup: Given a security parameter λ, TRS.Setup outputs a length n, a dimension k, an integer (the weight) ω and the threshold value t.

2) TRS.KeyGen: Given the public parameters $\{\lambda, n, k, \omega, t\}$, TRS.KeyGen outputs a pair of keys where the public key consists of a $(n-k) \times n$ parity check matrix H and the secret key of a single codeword of weight ω from the code C with parity check matrix H.

3) TRS.Sign: The signing algorithm will be composed of the following sub-procedures

- Lead: this phase consists in agreeing on a leader.
- Make-RPK: a group public key is defined as the direct sum of the N public keys $pk_i = H_i$, for $1 \leq i \leq N$. The matrix H is then a $N(n-k) \times Nn$ matrix such that $H = \oplus_{i=1}^{N} H_i$.
- NIZKPK: this phase consists in the combination of t zero-knowledge proofs of the knowledge of the secret keys. The paradigm of Fiat-Shamir is applied to this global proof to obtain a (t, N)-threshold ring signature σ on m.

4) TRS.Verify: Given the public parameters, the threshold value, N public keys $\{pk_i\}_{1 \leq i \leq N}$ and a putative pair message/signature (m, σ), this phase consists in recovering the group public-key and checking the validity of the Fiat-Shamir signature on m.

B. TRS.Setup

With 1^λ as input, where λ is the security parameter, the Setup algorithm is run to obtain the values of the parameters n, k, t, w. The integers n and $n-k$ are the matrix parameters, ω is the weight of the secret key s_i and t is the number of signers (the threshold). This algorithm also creates a public database $p_{k_1}, \ldots, p_{k_N}$, (which are indeed matrices H_i).. Note that the parameters n, k and ω are set once for all, and that any new user knowing these public parameters can join the ring. The parameter t has to be defined 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 leads to a rather large public matrix H_i, we will consider in Section VI, an interesting variation of the construction.

C. Make-RPK

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

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 $\{1, .., N\}$ since the order depends of the order of the N matrices sent by the leader). ∎

The RPK (Ring Public Key) is then constructed as follows:

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

D. TRS.Sign and TRS.Verify

We now describe the core of tour identification protocol in Fig. 3. The TRS.Sign and TRS.Verify are obtained by applying the Fiat-Shamir paradigm on this protocol.

The leader L collects the commitments given from the $t-1$ other signers (L is also a signer), 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.

Recall that in the description of the protocol, in order to avoid disturbing double indexes, we consider that the t signers correspond to the first t matrices H_i.

In the figure 3, $h(a_1|\cdots|a_j)$ denotes the hash of the concatenation of the sequence formed by $a_1, \cdots, a_j$.

V. Security

A. 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

1) Commitment Step:
- Each of the signers chooses $y_i \in \mathbb{F}_2^n$ randomly and a random permutation σ_i of $\{1, 2, \ldots, n\}$ and sends to L the commitments $c_{1,i}, c_{2,i}$ and $c_{3,i}$ such that :

$$c_{1,i} = h(\sigma_i | H_i y_i^t);\ c_{2,i} = h(\sigma_i(y_i));$$

$$c_{3,i} = h(\sigma_i(y_i \oplus s_i))$$

- L sets the secret s_i of the $N-t$ missing users at 0 and computes the $N-t$ corresponding commitments by choosing random y_i and σ_i $(t+1 \leq i \leq N)$.
- L chooses a random constant n-block permutation Σ on N blocks $\{1, \cdots, N\}$ in order to obtain the *master commitments*:

$$C_1 = h(\Sigma | c_{1,1} | \ldots | c_{1,N}), C_2 = h(\Sigma(c_{2,1}, \ldots, c_{2,N})),$$

$$C_3 = h(\Sigma(c_{3,1}, \ldots, c_{3,N})).$$

- L sends C_1, C_2 and C_3 to V.

2) Challenge Step: V sends a challenge $b \in \{0, 1, 2\}$ to L which sends b to the t signers.

3) Answer Step: Let P_i be one of the t signers. The first part of the step is between each signer and L.
- Three possibilities :
  - if $b = 0 : P_i$ reveals y_i and σ_i.
  - if $b = 1 : P_i$ reveals $(y_i \oplus s_i)$ (denoted by $(y \oplus s)_i$) and σ_i.
  - if $b = 2 : P_i$ reveals $\sigma_i(y_i)$ (denoted by $(\sigma(y))_i$) and $\sigma_i(s_i)$ (denoted by $(\sigma(s))_i$).
- L simulates the $N-t$ others Stern's protocol with $s_i = 0$ and $t+1 \leq i \leq N$ and sets $s = (s_1, \ldots, s_N)$.
- L computes the answer for V (and sends it) :
  - if $b = 0 : L$ constructs $y = (y_1, \cdots, y_N)$ and $\Pi = \Sigma \circ \sigma$ (for $\sigma = (\sigma_1, \cdots, \sigma_N)$) and reveals y and Π.
  - if $b = 1 : L$ constructs $y \oplus s = ((y \oplus s)_1, \cdots, (y \oplus s)_N)$ and reveals $y \oplus s$ and $\Pi = \Sigma \circ \sigma$.
  - if $b = 2 : L$ constructs and reveals $\Pi(y)$ and $\Pi(s)$.

4) Verification Step:
- if $b = 0 : V$ verifies that $\Pi(s)$ is a n-block permutation and that C_1, C_2 have been honestly calculated.
- if $b = 1 : V$ verifies that $\Pi(s)$ is a n-block permutation and 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 $\Pi(s)$ is $t\omega$ and that $\Pi(s)$ is formed of N blocks of length n and of weight ω or 0.

5) Iterate the steps 1,2,3,4 until the expected security level is reached.

Fig. 3. Generalised Stern's protocol

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. □

Theorem 2 *Our scheme is an honest verifier 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: 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 [31] for the problem defined in the previous lemma, by remarking that the structure of our generalised 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. □

This result naturally leads to the following theorem:

Corollary 3 *The resulting threshold ring signature scheme obtained from the application of the Fiat-Shamir heuristic on our generalised Stern's protocol is existentially unforgeable under a chosen message attack in the random oracle model assuming the hardness of the MD problem.*

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 the anonymity provided to the signers by our protocol.Formally we obtain:

Theorem 4 *Our threshold ring signature scheme is unconditionally source hiding.*

Our protocol generalises Gaborit and Girault's flavour of Stern's protocol [16] in the sense that the small weight secret codeword in their protocol is "expanded" into a vector where blocks of secret non-zero vectors (the secret key of user i) correspond to 1 in the small secret (at the ith position), whereas the blocks of zeros correspond to 0 in the small secret. The source hiding essentially comes from the fact that this Gaborit and Girault's variant of Stern's original protocol perfectly hides the position of 1s and 0s in the secret. Then, any subset of t users can produce a given ring signature with equal probability.

Proof:

The basic idea is that the distributions of the signatures produced by any subset of t users are actually the same. The Fake algorithm to exhibit is just the Sign algorithm used with any set of t secret keys. We can see that each commitment produced by a signer involving its secret corresponds to a one-time pad of the secret, which means that the distribution of this commitment is perfectly indistinguishable from a random one, as well as a distribution coming from any other secret. Therefore, the whole protocol perfectly hide the signers.

□

B. Practical Security of Stern's Scheme from [30]

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 [22],
2) For large n almost all linear codes lie over the Gilbert-Varshamov bound [24],
3) Solving the syndrome decoding problem for random codes is NP-complete [5].

In practice Stern proposed in [30] 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 [9] (or the more recent [6] can be lower bounded by an approximation in $O(n)\frac{\binom{n}{\omega}}{\binom{n-k}{\omega}}$, which gives a code with today security (2^{80}) of $n = 634$ and rate 1/2 and $\omega = 69$.

VI. An Interesting Variation of the Scheme Based on Double-Circulant Matrices

In Section IV 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 [16], to use double-circulant random matrices rather than pure random matrix 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 [16] 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 $x \in \mathbb{F}_2^n$ of weight $\leq \omega$, such that $Hx^t = 0$?

It is not known whether this problem is NP-complete or not (although the problem of decoding quasi-cyclic code in general, has been proven NP-complete in [4]), but the problem is probably as hard as the MD problem, and on practical point of view (see [16] for details) the practical security is almost the same for best known attack that the MD problem. Practically the author of [16] 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 generalised 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).

VII. Length and Complexity

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

A. The case $t = 1$

This case corresponds to the case of classical ring signature schemes. Our proposal is then not so attractive in term of signature length since we are in $\mathcal{O}(N)$, or more precisely $20ko \times N$ (where $20ko$ is the cost of one Stern signature). On the other hand, since Stern's protocol is fast in terms of speed, our protocol is faster that all others protocols for small values of N ($N = 2$ or 3) which may have some applications. In particular, the case $N = 2$ corresponds to a designated verifier signature scheme [19].

B. The general case

Signature length.

It is straightforward to see that the signature length of our protocol is in $\mathcal{O}(N)$, more precisely around $20ko \times N$, 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 [7] or [21] have shorter signature lengths (in $8ko$ or $25ko$) but are slower.

Public key size.

If we use the double-circulant construction described in Section VI, we obtain, a public key size in $347N$ which has a factor 2 or 3 better than [21] and of same order than [7].

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.

VIII. 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 generalisation of the Stern identification 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 vectors of small weight. Eventually we obtain a unconditionally source hiding protocol. 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 generalised 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. Proc. of Asiacrypt 2002, Springer LNCS Vol. 2501, pp. 415–432 (2002)

[2] Aguilar Melchor C., Cayrel P., Gaborit P.: A New Efficient Threshold Ring Signature Scheme Based on Coding Theory. Proc. of PQCrypto 2008: 1-16 (2008)

[3] Bender A., Katz J. and Morselli R. : Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles. Proc. of TCC 2006, Springer LNCS Vol. 3876, pp. 60–79 (2006)

[4] Berger T., Cayrel P.-L., Gaborit P. and Otmani A.: Reducing Key Length of the McEliece Cryptosystem, Proc. AFRICACRYPT 2009, LNCS,: 77-97 (2009).

[5] Berlekamp E., McEliece R. and van Tilborg H.: On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory, IT-24(3), pp. 384–386 (1978)

[6] Bernstein D.,Lange T. and Peters C.: Attacking and Defending the McEliece Cryptosystem, Proceedings of PQCrypto 2008,LNCS pp. 31-46 (2008).

[7] Boyen X.: Mesh Signatures. Proc. of Eurocrypt 2007, Springer LNCS Vol. 4515, pp. 210–227 (2007)

[8] Bresson E., Stern J. and Szydlo M. : Threshold ring signatures and applications to ad-hoc groups. Proc. of Crypto 2002, Springer LNCS Vol. 2442, pp. 465–480 (2002)

[9] Canteaut A. and Chabaud F. : A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. IEEE Transactions on Information Theory, IT-44(1), pp. 367–378 (1988)

[10] Chandran N., Groth J. and Sahai A. : Ring signatures of sub-linear size without random oracles. Proc. of ICALP 2007, Springer LNCS Vol. 4596, pp. 423–434 (2007)

[11] Chaum D. and van Heyst E. : Group signatures. Proc. of Eurocrypt 1991, Springer LNCS Vol. 546, pp. 257-265 (1991)

[12] Courtois N., Finiasz M. and Sendrier N. : How to achieve a McEliece based digital signature scheme. Proc. of Asiacrypt 2001, Springer LNCS Vol. 2248, pp. 157–174 (2001)

[13] Dallot L. and Vergnaud D. : Provably Secure Code-based Threshold Ring Signature. To appear in Proc. of IMA Conference on Cryptography and Coding, Springer LNCS (2009)

[14] Dodis Y., Kiayias A., Nicolosi A. and Shoup V. : Anonymous identification in ad-hoc groups. Proc. of Eurocrypt 2004, Springer LNCS Vol. 3027, pp. 609–626 (2004)

[15] Fiat A. and Shamir A. : How to Prove Yourself: Practical Solutions to Identification and Signature Problems. Proc. of Crypto 1986, Springer LNCS Vol. 263, pp. 186–194 (1986)

[16] Gaborit P. and Girault M. : Lightweight code-based identification and signature. ISIT 2007

[17] Goldwasser S., Micali S. and Rivest R. L.. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. SIAM J. Comput. 17(2), 281–308 (1988)

[18] Herranz J. and Saez G. : Forking lemmas for ring signature schemes. Proc. of Indocrypt 2003, Springer LNCS Vol. 2904, pp. 266–279 (2003)

[19] Jakobsson, M., Sako, K. and Impagliazzo, R. : Designated Verifier Proofs and their Applications. Proc. of Eurocrypt 1996, Springer LNCS 1070, pp.142–154 (1996)

[20] Kuwakado H. and Tanaka H. : Threshold Ring Signature Scheme Based on the Curve, Transactions of Information Processing Society of Japan Vol. 44(8), pp. 2146–2154 (2003)

[21] Liu J.K., Wei V.K. and Wong D.S. : A Separable Threshold Ring Signature Scheme. Proc. of ICISC 2003, Springer LNCS Vol. 2971, pp. 352–369 (2003)

[22] MacWilliams F.J., Sloane N.J.A. : The Theory of Error Correcting Codes, North-Holland (1977).

[23] Naor M. : Deniable Ring identification. Proc. of Crypto 2002, Springer LNCS Vol. 2442, pp. 481–498 (2002)

[24] Pierce J.N. : Limit distributions of the minimum distance of random linear codes, IEEE Transactions on Information Theory, IT-13, pp. 595–599 (1967)

[25] Pointcheval P., and Stern J. : Security proofs for signature schemes, Proc. of Eurocrypt 1996, Springer LNCS Vol. 1070, pp. 387–398 (1996)

[26] Rivest R. L. , Shamir A. and Tauman Y. : How to leak a secret. Proc. of Asiacrypt 2001, Springer LNCS Vol. 2248, pp. 552–565 (2001)

[27] 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

[28] Shacham H. and Waters B. : Efficient Ring Signatures without Random Oracles. Proc. of PKC 2007, Springer LNCS Vol. 4450, pp. 166–180 (2007)

[29] Shamir A. : How to share a secret. In *Com. of the ACM*, 22(11), pp. 612-613 (1979)

[30] Stern J. : A new identification scheme based on syndrome decoding. Proc. of Crypto 1993, Springer LNCS Vol. 773, pp. 13–21 (1994)

[31] Stern J. : A new paradigm for public key identification. IEEE Transactions on Information Theory, IT 42(6), pp. 2757–2768 (1996)

[32] Tsang P.P., Wei V.K., Chan T.K.,Au M.H., Liu J.K. and Wong D.S. : Separable Linkable Threshold Ring Signatures. Proc. of Indocrypt 2004, Springer LNCS Vol. 3348, p. 384–398 (2004)

[33] Vardy A. : The intractability of computing the minimum distance of a code. IEEE Transactions on Information Theory IT 43(6): pp. 1757–1766 (1997)

[34] Véron P. : A fast identification scheme. Proc. of IEEE International Symposium on Information Theory'95 (1995)

[35] 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. Proc. of ICICS 2003, Springer LNCS Vol. 2836, pp. pages 34–46 (2003)

[36] Xu J., Zhang Z. and Feng D. : A ring signature scheme using bilinear pairings. Proc. of WISA 2004, Springer LNCS Vol. 3325, pp. 160-169 (2005)

[37] Zhang F. and Kim K.: ID-Based Blind Signature and Ring Signature from Pairings. Proc. of Asiacrypt 2002, Springer LNCS Vol. 2501, pp. 533–547 (2002)

[38] Zheng D., Li X. and Chen K. : Code-based Ring Signature Scheme, International Journal of Network Security, 5(2), pp. 154–157 (2007)