Improved Lattice-Based Threshold Ring Signature Scheme

Slim Bettaieb[1] and Julien Schrek[1]

XLIM-DMI, Université de Limoges,
123, av. Albert Thomas
87060 Limoges Cedex, France
{slim.bettaieb,julien.schrek}@xlim.fr

Abstract. We present in this paper an improvement of the lattice-based threshold ring signature proposed by Cayrel, Lindner, Rückert and Silva (CLRS) [LATINCRYPT '10]. We generalize the same identification scheme CLRS to obtain a more efficient threshold ring signature. The security of our scheme relies on standard lattice problems. The improvement is a significant reduction of the size of the signature. Our result is a t-out-of-N threshold ring signature which can be seen as t different ring signatures instead of N for the other schemes. We describe the ring signature induced by the particular case of only one signer. To the best of our knowledge, the resulted signatures are the most efficient lattice-based ring signature and threshold signature.[3]

Keywords: Threshold ring signatures, lattices.

1 Introduction

Lattices were first used in cryptography with the LLL algorithm [1] in order to cryptanalyse some number theory primitives [2]. In 1996, the NTRU cryptosystem proposed an original idea to base cryptography on lattices assumptions.

In 1996, Ajtai [3] showed how to use the standard lattice problem GapSVP in order to build cryptographic schemes. More specifically he proved that the worst-case hardness of GapSVP is reduced to the average-case hardness of SIS problem. Lattice-based cryptography became a good alternative to number theory cryptography in regard to the quantum computer assumption. Nowadays several lattice-based cryptosystems show good results with strong security proofs.

The notion of group signature was first formalised by Chaum and van Heyst in 1991 [4]. A group signature scheme allows a user in a group to sign anonymously a message on behalf of the group. The group is administered by a group manager, who can accept to add users to the group and has the ability to determine the real identity of the signer when needed. Motivated by the following situation: a high-ranking official in the government wants to leak anonymously an important information to a journalist. Rivest, Shamir, and Tauman [5] introduced the concept of ring signature and proposed a scheme based on RSA. As opposed to group signatures, ring signatures have no group manager and no anonymity revocation system.

The concept of ring signature was extended by Bresson, Stern and Szydlo to threshold ring signatures [6]. In this setting, t-out-of-N users interact together in order to produce a signature without giving any information of the set of signers which produced the signature. Since their introduction, several threshold ring signature schemes were proposed [7–9]. Those constructions have a particularity in common: a complexity in $\mathcal{O}(Nt)$.

Aguilar, Cayrel and Gaborit [10] proposed a new threshold ring signature in 2008 of size in $\mathcal{O}(N)$. It is a code-based signature considered as a very efficient scheme due to its complexity.

In 2010, Cayrel, Lindner, Rückert and Silva [11] presented a lattice based version of the scheme in [10]. This version generalised an identification scheme given in [12], which is more efficient than Stern's identification protocol used by Aguilar et al. [10]. The security of the new scheme is based on the shortest independent vectors problem SIVP.

Our Contributions. In this work, we present an improvement of the lattice-based threshold ring signature scheme given in [11]. The improvement is due to a different way to achieve anonymity. Our scheme looks like t different digital signature. The difference is an extra challenge-answer part to deal with anonymity. The first part has the same size as t digital signatures (we use seeds to represent random permutations and other masks). The other part which deals with anonymity is in complexity $O(Nt)$ which is more important than $O(N)$ in [11] but implies smaller signatures when Nt is smaller than the size of t digital signatures. We also detail a ring signature in the particular case $t = 1$, which has the smallest size among others lattice-based ring signatures [13, 14, 11]. A table of comparison can be found in section 6.

Organization. In Section 2, we give some definitions and notions related to lattices and cryptography as well as a description of the identification scheme from [12]. In section 3, we present and detail our ring signature scheme. In section 4, we construct the lattice-based threshold ring signature scheme. The proofs of security for the scheme are detailed in section 5. In section 6, we give some concrete instantiations of our schemes and a comparison with the schemes from [11].

2 Preliminaries

This section is split into three parts. In the first one we give some basic definitions about lattices and cryptography. The second part details formal security definitions about ring signatures. In the third part we describe the identification scheme CLRS presented in [12].

Notations. We use bold upper-case letters to denote matrices and bold lower-case letters to denote vectors. We denote the Euclidean norm of the vector $\mathbf{v}$ by $\|\mathbf{v}\|$. For q an integer, $\mathbb{Z}_q$ denotes the group of integers modulo q. For a set E, we use the notation $w \overset{\$}{\leftarrow} E$ to mean that w is chosen randomly at uniform from E. Let $wh(\mathbf{v})$ denote the Hamming weight of $\mathbf{v}$ (the number of non-zero elements in $\mathbf{v}$) and for any integer m we denote by S_m the set of permutation of $\{1, \ldots, m\}$. Let $N \in \mathbb{N}$, we denote by δ_j the vector in $\{0,1\}^N$ with 1 in the j-th position and 0 elsewhere.

2.1 Lattices in cryptography

We recall the definition of lattices, the small integer solution problem SIS, the inhomogeneous small integer solution problem ISIS, the standard hard lattice problem SIVP and a lattice-based commitment scheme.

Definition 1. *Let $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ be set of n linearly independent vectors in $\mathbb{R}^m$. The lattice generated by B is the set*

$$\mathcal{L}(B) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}$$

of all integer combination of vectors in B. We denote by $\lambda_1(\mathcal{L}(B))$ the shortest vector of the lattice $\mathcal{L}(B)$. For $i \in \{1, \ldots, n\}$, we denote by $\lambda_i(\mathcal{L})$ the successive minima which is the smallest values $\lambda_i(\mathcal{L})$ such that the sphere of radius $\lambda_i(\mathcal{L})$ of center the origin contains at least i linearly independent lattice vectors.

Definition 2 (SIS$_{q,n,m,\alpha}$ problem). *Given a random matrix $\mathbf{A} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m}$ find a non zero vector $\mathbf{v} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{v}^T = 0$ and $\|\mathbf{v}\| \leq \alpha$.*

Definition 3 (ISIS$_{q,n,m,\alpha}$ problem). *Given a random matrix $\mathbf{A} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m}$ a vector $\mathbf{v} \in \mathbb{Z}_q^n$ and a real α find a vector $\mathbf{s} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{s}^T = \mathbf{v} \bmod q$ and $\|\mathbf{s}\| \leq \alpha$.*

Definition 4 (SIVP$_\gamma$ problem). *Given an n dimensional lattice $\mathcal{L}$, find n linearly independent lattice vectors of length at most $\gamma \cdot \lambda_n(\mathcal{L})$.*

In [15], Gentry *et al.* proved that the worst-case hardness of SIVP is reduced to the average-case hardness of SIS or ISIS problem. Their result is in the following theorem.

Theorem 1 ([15]). *Let $m, \alpha = poly(n)$ and for any prime $q \geq \alpha \cdot \omega(\sqrt{n \log n})$. There is a probabilistic polynomial time reduction from solving $SIVP_\gamma$ for $\gamma = \alpha \cdot \tilde{O}(\sqrt{n})$ in the worst case to solving $SIS_{q,n,m,\alpha}$ and $ISIS_{q,n,m,\alpha}$ on average with non negligible probability.*

In [16], Kawachi, Tanaka and Xagawa introduced a lattice-based commitment scheme COM. The proposed scheme satisfies the essential security properties, namely, the statistically-hiding and computationally-binding properties. Let $\mathsf{COM}(\mu, \rho)$ be a commitment scheme.

- COM is said to be a statistically hiding scheme if for any messages μ_1, μ_2, any attacker cannot distinguish between $\mathsf{COM}(\mu_1, \rho_1)$ and $\mathsf{COM}(\mu_2, \rho_2)$.
- The computational binding property ensure that no polynomial time attacker can change the committed message to another one.

2.2 Ring Signature

In this subsection we review some definitions and properties about ring signatures that will be used in the following sections.

Ring signature We use the same definition as in [17]. A ring signature is a digital signature where the signer is not known, however his membership of a particular set can be verified.

Definition 5 (Ring Signature Scheme). *A ring signature scheme consists of the three following algorithms:*

- $\mathsf{R.KeyGen}$: *A probabilistic polynomial time algorithm that takes as input a security parameter and outputs a key pair formed by a public key PK and a secret key SK.*
- $\mathsf{R.Sign}$: *A probabilistic polynomial time algorithm that takes as input a set of public keys $PK_1, \ldots, PK_N$, a message μ, and a signing key. The output is a ring signature of the message μ.*
- $\mathsf{R.Verify}$: *A deterministic algorithm that takes as input a ring signature, a message μ and the list of public keys of the users of the ring. The output of this algorithm is* accept *if the ring signature is valid or* reject *otherwise.*

Threshold Ring Signature In 2002, Bresson, Stern and Szydlo introduced the concept of threshold ring signatures [6]. In such a scheme, a set of t users wants to collaborate to produce a signature while preserving the anonymity of the participating signers. We give a formal definition of t-out-of-N threshold ring signature scheme. We denote the set of users by $U' = \{1, \ldots, N\}$ and by S' the set of signers with $S' \subset U'$. Each user i in U' has a public/secret key pair (PK_i, SK_i).

Definition 6 (Threshold Ring Signature Scheme). *A threshold ring signature scheme consists of the three following algorithms:*

- $\mathsf{T.KeyGen}$: *outputs a public key PK and a secret key SK.*
- $\mathsf{T.Sign}(\mu, U', S')$: *an interactive protocol between t users that take on input a set of public keys correponding to users in U' a set of t secret keys corresponding to users in S' and a message μ. The output is a t-out-of-N-threshold ring signature σ on μ.*

- $\mathsf{T.Verify}(\mu, \sigma, t, U')$: *deterministic algorithm that takes as input a value t, a set of public keys corresponding to users in U', a message-signature pair (μ, σ), and outputs* accept *or* reject*.*

A t-out-of-N threshold ring signature scheme is said to be secure if it is source hiding and unforgeable.

Anonymity. The source hiding definition described in [17] and [11] does not fit with threshold ring signature schemes obtained using the Fiat-Shamir transform. Indeed, the one-way functions used during the commitments do not allow to build two identical signatures for different set of signers. Moreover, this remains almost impossible even if two sets of signers have the same secret keys. We introduce a new definition generalised from the anonymity property for ring signatures see Definition 4 in [18]. With this definition we introduce the notion of indistinguishability.

Definition 7 (Indistinguishable source hiding). *Given a t-out-of-N threshold ring signature and a probabilistic polynomial time adversary $\mathcal{A}$, consider the following game*

1. *For $i = 1$ to N, generate (PK_i, SK_i). Give to $\mathcal{A}$ the set of public keys $P = \{PK_1, \ldots, PK_N\}$. The adversary $\mathcal{A}$ is also given access to a signing oracle $\mathsf{OT.Sign}(\cdot,\cdot,\cdot)$, that returns $\sigma = \mathsf{T.Sign}(\mu, P, S)$ on input (μ, P, S) with S a set signers.*
2. *$\mathcal{A}$ outputs a message μ, distinct sets $\{i_{1,0}, \ldots, i_{t,0}\}$, $\{i_{1,1}, \ldots, i_{t,1}\}$ and a ring P for which $PK_{i_{l,j}} \in P$ for $l \in \{0, 1\}$ and $j \in \{1, \ldots, t\}$. Adversary $\mathcal{A}$ is given $\{SK_1, \ldots, SK_N\} \backslash \{SK_{i_{1,0}}, \ldots, SK_{i_{t,0}}\}$. Furthermore, a random bit b is chosen and $\mathcal{A}$ is given $\sigma \leftarrow \mathsf{T.Sign}(\mu, P, \{SK_{i_{1,b}}, \ldots, SK_{i_{t,b}}\})$.*
3. *The adversary outputs a bit b', and succeeds if $b' = b$.*

Unforgeability. We give a formal definition of existential unforgeability under chosen message attacks in the setting of t-out-of-N threshold ring signature. The definition is described using a game between an existential forger $\mathcal{F}$ and a challenger $\mathcal{C}$, and it is similar to one used in [17] and [11].

Definition 8 (Existensial Unforgeability). *A threshold ring signature scheme is existentially unforgeable under a chosen message attack if for any probabilistic polynomial time $\mathcal{F}$, the probability that $\mathcal{F}$ succeeds in the following game is negligible:*

1. *The challenger $\mathcal{C}$ generates key pairs $\{PK_i, SK_i\}_{i=1}^{N}$, and gives the set of public keys $P = \{PK_i\}_{i=1}^{N}$ to $\mathcal{F}$.*
2. *$\mathcal{F}$ is given access to a signing oracle as in Definition 7.*
3. *$\mathcal{F}$ is also given access to a key exposure oracle $\mathsf{OExp}(\cdot)$, that returns a secret key SK_i on input i.*
4. *$\mathcal{F}$ outputs a t-out-of-N threshold ring signature $\sigma^\star$ for a new message $\mu^\star$.*

The adversary $\mathcal{F}$ succeeds if the verification $\mathsf{T.Verify}(\mu^\star, \sigma^\star, t, P) = 1$, $\mu^\star$ has not been asked by $\mathcal{F}$ in a signing query in step 2 of the game and the number of key exposure queries is strictly less than t.

2.3 CLRS identification scheme

CLRS is an identification scheme proposed by Cayrel, Lindner, Rückert and Silva [12]. It is a lattice-based version of a generalisation of the Stern code-based identification scheme presented in [19].

The Stern protocol was introduced in 1993, it was the first efficient code-based identification scheme. It has the specific property to be zero-knowledge, indeed nobody can give any information about the involved secret from the transcripts of the interactions between a prover and a verifier. The zero-knowledge property allows to obtain a digital signature scheme by applying the Fiat-Shamir transform. Stern's scheme uses challenges and answers to establish the authentication of the user. There is only one challenge by round, we call it a three-pass protocol. A generalisation of that scheme was presented in [20] by using two challenges for each round. Hence, the digital signatures obtained from this five-pass protocol have a smaller size. The CLRS identification scheme is a lattice-based version of this protocol.

We use a variation of the CLRS identification scheme in our construction, as well as it was done in [11].

The scheme In Figure 2, we have an identification between a prover P and a verifier V. The prover's secret key is a vector $\mathbf{x}$ of Hamming weight $m/2$. The public key $\mathbf{y}$ is related to $\mathbf{x}$ by the equation $\mathbf{y} = \mathbf{A}\mathbf{x}^T \bmod q$.

```
Input: $n, m, q$
        $\mathbf{x} \overset{\$}{\leftarrow} \{0,1\}^m$, with $wh(\mathbf{x}) = m/2$
        $\mathbf{A} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n \times m}$
        $\mathbf{y} \leftarrow \mathbf{A}\mathbf{x}^T \bmod q$
        $\mathsf{COM} \overset{\$}{\leftarrow} \mathcal{F}$, a suitable family of commitment functions.
Output: $(SK, PK) = (\mathbf{x}, (\mathbf{y}, \mathbf{A}, \mathsf{COM}))$
```

Fig. 1. Key generation algorithm

```
$P$ chooses $\sigma \overset{\$}{\leftarrow} S_m$, $\mathbf{u} \overset{\$}{\leftarrow} \mathbb{Z}_q^m$, $\mathbf{r}_0 \overset{\$}{\leftarrow} \{0,1\}^n$ and $\mathbf{r}_1 \overset{\$}{\leftarrow} \{0,1\}^n$.
$P$ computes $c_0 \leftarrow \mathsf{COM}(\sigma || \mathbf{A}\mathbf{u} || \mathbf{r}_0)$ and $c_1 \leftarrow \mathsf{COM}(\sigma(\mathbf{u}) || \sigma(\mathbf{x}) || \mathbf{r}_1)$.

 1. [first commitment] $P$ sends $c_0$ and $c_1$ to $V$.
 2. [first challenge] $V$ sends $\alpha \overset{\$}{\leftarrow} \mathbb{Z}_q$ to $P$.
 3. [second commitment] $P$ sets $\beta = \sigma(\mathbf{u} + \alpha\mathbf{x})$ and sends $\beta$ to $V$.
 4. [second challenge] $V$ sends $b \overset{\$}{\leftarrow} \{0,1\}$, to $P$.
 5. [final answer]
    If $b = 0$ then
        $P$ sends $\sigma$ and $\mathbf{r}_0$ to $V$.
    If $b = 1$ then
        $P$ sends $\sigma(\mathbf{x})$ and $r_1$ to $V$.

Verification:
If $b = 0$ then $V$ checks if
        $c_0 \overset{?}{=} \mathsf{COM}(\sigma \| \mathbf{A}\sigma^{-1}(\beta)^T - \alpha\mathbf{y} \| \mathbf{r}_0)$
If $b = 1$ then $V$ checks, $wh(\sigma(\mathbf{x})) \overset{?}{=} m/2$ and
        $c_1 \overset{?}{=} \mathsf{COM}(\beta - \alpha\sigma(\mathbf{x}) \| \sigma(\mathbf{x}) \| \mathbf{r}_1)$
```

Fig. 2. CLRS Identification protocol

High level description The protocol is made with challenges and answers. The verifier asks some challenges to the prover who needs to answer correctly. The challenges focus on the secret value $\mathbf{x}$. The vector $\mathbf{x}$ has an Hamming weight of $m/2$ and verify $\mathbf{A}\mathbf{x}^T = \mathbf{y}$. We can see that two different properties are required to identify the secret. It is a fundamental observation to understand the scheme. Indeed, the verifer will either ask to verify the Hamming weight of $\mathbf{x}$ or verify the relation $\mathbf{A}\mathbf{x}^T = \mathbf{y}$.

The masks used to protect the secret properties are from two different kinds. A permutation σ allows to mask which of the vectors of some given Hamming weight is used. The random vector $\mathbf{u}$ allows to mask which one of the vector verifying $\mathbf{A}\mathbf{x} = \mathbf{y}$ is used. After masking the secret twice (with each

mask), the prover can unmask the masked secret with the permutation σ or the additional random vector to prove either that the secret is a vector of given Hamming weight or that it verify $\mathbf{Ax} = \mathbf{y}$. We can identify 5 steps in the scheme: first commitment step, first challenge, second commitment, second challenge and final answer. The first commitment aims to set the random permutation and the random vector. The first challenge α is here to prevent replay attacks. The second commitment β is the secret masked two times. The second challenge b consists on asking to reveal either the weight of the secret ($b = 1$) or a way to compute $\mathbf{Ax}^T$ ($b = 0$).
This protocol is a probabilistic protocol in the fact that it is possible to anticipate the challenges and respond correctly without knowing the secret key. The soundness is close to 1/2. Therefore, to reduce the cheating probability, the protocol has to be repeated many times.

2.4 Fiat-Shamir transform

To build signature schemes from canonical identification schemes, one can use the Fiat-Shamir transform.

The challenges of the scheme are built with a random oracle H instead of an honest verifier. They are generated randomly at uniform from the message and commitments. In this way, a malicious prover cannot anticipate challenges one at a time and needs to anticipate them at once. The cheating probability remains the same as in the authentication protocol. Pointcheval and Stern [21] proved that an unforgeable signature scheme can be obtained when applying the Fiat-Shamir transform.

Recently Cayrel et al [22] proved that the Fiat-Shamir transform can be extended to fit with the $(2n + 1)$-pass identification schemes (n is an integer in our case $n = 2$). We briefly review this transformation. In order to transform a five-pass identification scheme to a signature scheme, the signer proceeds as follows. He uses two random oracle $\mathcal{O}_1$ and $\mathcal{O}_2$ to generate the challenges C_1 and C_2 given by the verifier in the identification scheme. Let μ be a message, the signature σ of μ is formed by R_1, C_1, R_2, C_2 and RSP, where R_1, R_2 and RSP are the values calculated by the prover in the identification scheme.

3 Ring signature

A ring signature is a digital signature where the signer is not known, however his membership of a particular set can be verified. In the following we explain the idea described in [10] and [11], then we show the differences with our scheme. In this section we consider U as a set of N users.

3.1 Description of CLRS ring signature scheme

The ring signature scheme in [11] is obtained by applying the Fiat-Shamir transform to a ring identification scheme. The idea is to construct, for each user i, a secret key $\mathbf{x}_i$ with the same property $\mathbf{Ax}_i^T = 0$. Hence, we cannot distinguish two users from their public keys. The problem is to construct several such secret keys. In fact, statistically, there is only one vector $\mathbf{v}$ of small enough weight w such that $\mathbf{Av}^T = 0$. The construction consists on changing the matrix $\mathbf{A}$ for each user. Now they are identified by their public matrix $\mathbf{A}_i$ instead of their public value $\mathbf{A}_i\mathbf{x}_i^T$. To generate a ring identification, N identifications are done, one for each user. The real signer uses his secret key $\mathbf{x}_i$ for only one identification and the null vector for the others. The anonymity is obtained with a permutation of the users' commitments.

3.2 Our ring signature scheme

This scheme uses the same key generation algorithm as the CLRS scheme presented in section 2.3. On the other hand, a matrix $\mathbf{M}$ is added to the public values. The matrix $\mathbf{M}$ is composed of all public elements $\mathbf{y}_1, \ldots, \mathbf{y}_N$ with $\mathbf{A}\mathbf{x_i}^T = \mathbf{y}_i$ for $i \in \{1, \ldots, N\}$.

The ring signature scheme can be obtained from the ring identification scheme in Figure 3 by applying the Fiat-Shamir transform. This scheme is very similar to the CLRS identification scheme described in section 2.3. As it is detailed in Figure 3, a new commitment β' and two masks $\mathbf{u}'$ and Σ were added as well as a secret value δ_j. Those new elements were designed to guarantee the anonymity of the real signer. The idea is to use δ_j as the secret identifying the real signer and to mask it in the same way as the secret key $\mathbf{x}_i$.
In this scheme, the $\mathbf{y}_j$ which defines the signer and which is used to compute the first commitment is masked in β'. Indeed, we have $\mathbf{y}_j = \mathbf{M}\delta_j^T$ with δ_j masked by Σ and $\mathbf{u}'$. The first commitment can be computed in the same way for each signer as far as $\mathbf{A}(\mathbf{x}_i + \mathbf{u})^T - \mathbf{M}(\delta_i + \mathbf{u}')^T$ is equal for each signer i. We use the same construction to mask $\mathbf{x}_i$ and δ_i because both values are identified by their weight and their image by a particular matrix ($\mathbf{A}$ or $\mathbf{M}$).
The fact that $wh(\Sigma(\delta_j)) = 1$ with Σ a permutation guarantees that one user in the ring U' is the real signer.

Let $U' = \{\text{users}\}$. Let $\mathbf{M}$ the matrix of all public elements $\mathbf{y}_1, \ldots, \mathbf{y}_N$ of users in U'.

$$\mathbf{M} = \begin{pmatrix} | & | & \cdots & | \\ \mathbf{y}_1 & \mathbf{y}_2 & \cdots & \mathbf{y}_N \\ | & | & \cdots & | \end{pmatrix}, \text{ with } \mathbf{y}_i = \mathbf{A}\mathbf{x}_i^T \text{ for all } i \in \{1, \ldots, N\}.$$

The user S with index j in $\{1, \ldots, N\}$, do the following:
He sets $\delta_j \in \{0,1\}^N$ with 1 in the j-th position and 0 elsewhere. He chooses a random permutation Σ of $\{1, \ldots, N\}$, $\mathbf{u}' \xleftarrow{\$} \mathbb{Z}_q^N$, $\sigma \xleftarrow{\$} S_m$, $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m$, $\mathbf{r}_0 \xleftarrow{\$} \{0,1\}^n$ and $\mathbf{r}_1 \xleftarrow{\$} \{0,1\}^n$.
He computes

$$c_0 \leftarrow \mathsf{COM}(\sigma || \Sigma || \mathbf{A}\mathbf{u}^T - \mathbf{M}\mathbf{u}'^T || \mathbf{r}_0) \text{ and } c_1 \leftarrow \mathsf{COM}(\sigma(\mathbf{u}) || \Sigma(\mathbf{u}') || \sigma(\mathbf{x}_j) || \Sigma(\delta_j) \| \mathbf{r}_1).$$

1. [**first commitment**] S sends c_0 and c_1 to the verifier V.
2. [**first challenge**] V sends $\alpha \xleftarrow{\$} \mathbb{Z}_q$ to S.
3. [**second commitment**] S sends β and β' to V, with
$$\beta = \sigma(\mathbf{u} + \alpha\mathbf{x}_j) \text{ and } \beta' = \Sigma(\mathbf{u}' + \alpha\delta_j).$$
4. [**second challenge**] V sends $b \xleftarrow{\$} \{0,1\}$ to S.
5. [**final answer**]
   If $b = 0$ then
      S sends $\phi = \Sigma, \psi = \sigma$, and $\mathbf{a} = \mathbf{r}_0$ to V.
   If $b = 1$ then
      S sends $\chi = \Sigma(\delta_j), \mathbf{d} = \sigma(\mathbf{x}_j)$ and $\mathbf{e} = \mathbf{r}_1$ to V.

Verification :

If $b = 0$ then V checks if
$$c_0 \stackrel{?}{=} \mathsf{COM}(\psi \| \phi \| \mathbf{A}\psi^{-1}(\beta)^T - \mathbf{M}\phi^{-1}(\beta')^T \| \mathbf{a})$$
If $b = 1$ then V checks if
$$c_1 \stackrel{?}{=} \mathsf{COM}((\beta - \alpha\mathbf{d}) \| (\beta' - \alpha\chi) \| \mathbf{d} \| \chi \| \mathbf{e})$$
$$\mathbf{d} \stackrel{?}{\in} \{0,1\}^m \text{ , } wh(\mathbf{d}) \stackrel{?}{=} m/2 \text{ and } wh(\chi) \stackrel{?}{=} 1.$$

Fig. 3. Ring identification scheme

3.3 Features of the scheme

This scheme, without β', u' and Σ, is the same as the identification scheme CLRS. We do not need to send N identifications to obtain anonymity like it was done in previous ring signature schemes. Therefore, a significant reduction of signature size is obtained for reasonable values of N and t.
An other notable property is the use of a unique random matrix $\mathbf{A}$ instead of N public matrices $\mathbf{A}_i$ in [11]. A consequence is a reduction of the size of the public keys.

4 Threshold ring signature

The threshold ring signature is a generalisation of the ring signature. The threshold ring signature is made by many signers instead of only one for the ring signature.

The authors of [6] and [10] claim that a threshold ring signature is not a repetition of several ring signatures. The reason is that we have to prove that at least t signer has been involved in the process. For example, a signer alone should not be able to sign twice in the same signature and produce a valid signature.
In our case, the threshold ring signature is more like t different ring signatures. That is why the signature size is close to t signatures instead of N for other schemes [10, 11].

4.1 From ring signature to threshold ring signature

In this subsection we explain how to prove that t different users can make a threshold ring signature with our scheme. The threshold ring signature scheme is obtained by applying the Fiat-Shamir transform on the threshold ring identification scheme given in Figure 4. The idea is very simple, each δ_i represents a different user, which can be identified with the matrix $\mathbf{M}$. We only have to show that the δ_i, used in the identification, are different. We prove that point by verifying that the $\Sigma(\delta_i)$ are different because if $\Sigma(\delta_i) \neq \Sigma(\delta_j)$ then $\delta_i \neq \delta_j$, with Σ a permutation.
From security perspective, Σ is known by all the signers, and this does not affect the unforgeability because Σ only masks δ_i which defines the identity of the signer. Moreover, no information about $\mathbf{x}_i$ is revealed. The anonymity property remains unchanged because signers are supposed to know each other when they produce the signature.
During the verification, when $b = 0$, we have just to verify that each $\Sigma(\delta_i)$ is different from the others. Thus, this proves that t different signers have cooperated to generate the threshold ring signature.

4.2 Lattice-Based Threshold Identification Scheme

In this subsection we present our threshold identification scheme. The scheme is in Figure 4, the verification algorithm is given in Figure 5.

Let $\mathbf{M}$ the matrix of all public elements $\mathbf{y}_1, \ldots, \mathbf{y}_N$ of users in U'.

$$\mathbf{M} = \begin{pmatrix} | & | & \cdots & | \\ \mathbf{y}_1 & \mathbf{y}_2 & \cdots & \mathbf{y}_N \\ | & | & \cdots & | \end{pmatrix}, \text{ with } \mathbf{y}_i = \mathbf{A}\mathbf{x}_i^T \text{ for all } i \in \{1, \ldots, N\}.$$

$\delta_i \in \{0,1\}^N$ the vector with 1 on the i-th position and 0 elsewhere else.
U' ={users} and S' ={signers}, with $S' \subset U'$, $|S'| = t$ and $|U'| = N$.
L the leader, with $L \in S'$ and V the verifier.

1. [**first commitment**]

```
$L$ construct at random $\Sigma$ a permutation of $\{1, \ldots, N\}$.

for $i$ from 1 to $t$ do
        $L$ choose the i-th signer $\mathcal{S}_j$
        $S_j$ receives $\Sigma$ from $L$.
        $S_j$ constructs $\sigma_i \xleftarrow{\$} S_m$, $\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^m$, $\mathbf{u}'_i \xleftarrow{\$} \mathbb{Z}_q^N$, $\mathbf{r}_{0,i} \xleftarrow{\$} \{0,1\}^n$ and $\mathbf{r}_{1,i} \xleftarrow{\$} \{0,1\}^n$
        $S_j$ computes : $c_{0,i} \leftarrow \mathsf{COM}(\sigma_i || \Sigma \| \mathbf{A}\mathbf{u}_i^T - \mathbf{M}\mathbf{u}_i'^T || \mathbf{r}_{0,i})$
                         $c_{1,i} \leftarrow \mathsf{COM}(\sigma_i(\mathbf{u}_i) || \Sigma(\mathbf{u}'_i) \| \sigma_i(\mathbf{x}_j) || \Sigma(\delta_j) \| \mathbf{r}_{1,i})$
        $S_j$ sends $c_{0,i}$ and $c_{1,i}$ to $L$.
end for

$L$ computes $\mathbf{r}_0 \xleftarrow{\$} \{0,1\}^n$ and $\mathbf{r}_1 \xleftarrow{\$} \{0,1\}^n$.
$L$ computes the master commitments :
$C_0 = \mathsf{COM}(c_{0,1} || \ldots || c_{0,t} \| \mathbf{r}_0)$ and $C_1 = \mathsf{COM}(c_{1,1} || \ldots || c_{1,t} \| \mathbf{r}_1)$
```

   L sends C_0 and C_1 to V.

2. [**first challenge**] V sends α, such as $\alpha \xleftarrow{\$} \mathbb{Z}_q$.

3. [**second commitment**]

```
We denote $\bar{\mathbf{x}}_i$ (respectively $\bar{\delta}_i$) the $\mathbf{x}_j$ (respectively $\delta_j$) corresponding to the $i$-th signer $\mathcal{S}_j$.
for $i$ from 1 to $t$ do
        $L$ choose the i-th signer $\mathcal{S}_j$
        $S_j$ computes $\beta_i \leftarrow \sigma_i(\mathbf{u}_i + \alpha\bar{\mathbf{x}}_i)$
        $S_j$ computes $\beta'_i \leftarrow \Sigma(\mathbf{u}'_i + \alpha\bar{\delta}_i)$
        $S_j$ sends $\beta_i, \beta'_i$ to $L$.
end for
```

   L sends $\mathbf{v}_1 = \beta_1, \ldots, \mathbf{v}_t = \beta_t$ and $\mathbf{w}_1 = \beta'_1, \ldots, \mathbf{w}_t = \beta'_t$ to V.

4. [**second challenge**] V sends $b = 0$ or $b = 1$ to L.

5. [**final answer**]

```
if $b = 0$ then
        for $i$ from 1 to $t$ do
                $L$ choose the i-th signer $\mathcal{S}_j$
                $S_j$ sends $\sigma_i, \mathbf{r}_{0,i}$ to $L$
        end for
if $b = 1$ then
        for $i$ from 1 to $t$ do
                $L$ choose the i-th signer $\mathcal{S}_j$
                $S_j$ sends $\mathbf{u}_i, \mathbf{u}'_i$ and $\mathbf{r}_{1,i}$ to $L$
        end for
```

   if $b = 0$ then
      L sends $\phi = \Sigma$, $\psi_1 = \sigma_1, \ldots, \psi_t = \sigma_t$, $\mathbf{a}_1 = \mathbf{r}_{0,1}, \ldots, \mathbf{a}_t = \mathbf{r}_{0,t}$ and $\rho = \mathbf{r}_0$ to V.
   if $b = 1$ then
      L sends $\chi_1 = \Sigma(\bar{\delta}_1), \ldots \chi_t = \Sigma(\bar{\delta}_t)$, $\mathbf{d}_1 = \sigma_1(\bar{\mathbf{x}}_1), \ldots, \mathbf{d}_t = \sigma_t(\bar{\mathbf{x}}_t)$, $\mathbf{e}_1 = \mathbf{r}_{1,1}, \ldots, \mathbf{e}_t = \mathbf{r}_{1,t}$
        and $\varrho = \mathbf{r}_1$ to V.

Fig. 4. Threshold ring identification scheme

```
if $b = 0$ then
    for $i$ from 1 to $t$
        Set $c_i = \mathsf{COM}(\psi_i \| \phi \| \mathbf{A}\psi_i^{-1}(\mathbf{v}_i)^T - \mathbf{M}\phi^{-1}(\mathbf{w}_i)^T \| \mathbf{a}_i)$
    end for
    $V$ checks that $C_0 \overset{?}{=} \mathsf{COM}(c_1 \| \dots \| c_t \| \rho)$
if $b = 1$ then
    for $i$ from 1 to $t$
        Set $c_i = \mathsf{COM}(\mathbf{v}_i - \alpha \mathbf{d}_i \| \mathbf{w}_i - \alpha \chi_i \| \mathbf{d}_i \| \chi_i \| \mathbf{e}_i)$

        $V$ checks that $wh(\mathbf{d}_i) = m/2$ and $\mathbf{d}_i \in \{0,1\}^m$

        $V$ checks that $wh(\chi_i) = 1$
    end for
    $V$ checks that $\sum_{i=1}^{t} wh(\chi_i) = t$ and $\chi_i \in \{0,1\}^N$
    $V$ checks that $C_1 \overset{?}{=} \mathsf{COM}(c_1 \| \dots \| c_t \| \varrho)$
```

Fig. 5. Verification algorithm

5 Security analysis

In this section we prove the security of our scheme. A threshold ring signature scheme must satisfy two properties. The source hiding, which ensures the anonymity of the users and the existential unforgeability, which is common to every digital signature.

5.1 Source hiding

Lemma 1. *For any transcript τ of the threshold identification scheme in Figure 4 performed by a set S of t signers we have that:*
For any set S' of t signers there exists a transcript σ' performed by S' such that the differences between τ and τ' are in the commitment values.

Proof. We will prove the lemma for one round of the threshold identification scheme. Let τ be the transcript of the threshold identification, it is easy to see that τ consists of $((C_0, C_1), \alpha, (\beta_i, \beta_i'; i \in \{1, \dots, t\}), b, RSP)$ where RSP is the response sent by the leader L to the verifier V.

Let $(\mathbf{x}_i, \delta_i; i \in \{1, \dots, t\})$, be the secrets used by the signers in S and $(\mathbf{x}_i', \delta_i'; i \in \{1, \dots, t\})$, be the secrets used by the signers in S'. We will show how to choose $(\mathbf{u}_i, \mathbf{u}_i', \sigma_i, \Sigma)$ such that the transcript does not change except C_0 and C_1 when the secret keys $(\mathbf{x}_i, \delta_i; i \in \{1, \dots, t\})$ are replaced by $(\mathbf{x}_i', \delta_i'; i \in \{1, \dots, t\})$.

If $b = 0$, we set $U_i = \mathbf{u}_i + \alpha \mathbf{x}_i - \alpha \mathbf{x}_i'$ and $U_i' = \mathbf{u}_i' + \alpha \delta_i - \alpha \delta_i'$. Therefore, when we replace $(\mathbf{x}_i, \mathbf{u}_i, \mathbf{u}_i', \delta_i; i \in \{1, \dots, t\})$ by $(\mathbf{x}_i', U_i, U_i', \delta_i'; i \in \{1, \dots, t\})$, we obtain that β_i and β_i' keep the same values. Since $\mathbf{u}_i$ and $\mathbf{u}_i'$ do not appears in RSP, then the only thing that change in the transcript are the values C_0 and C_1.

If $b = 1$, we choose π_i and Π such that $\pi_i(\mathbf{x}_i') = \mathbf{x}_i$ and $\Pi(\delta_i') = \delta_i$ and we set $U_i = \pi^{-1}(\mathbf{u}_i)$ and $U_i' = \Pi^{-1}(\mathbf{u}_i')$. Therefore, when we replace $(\sigma_i, \mathbf{u}_i, \Sigma, \mathbf{u}_i')$ by $(\sigma_i \circ \pi_i, U_i, \Sigma \circ \Pi, U_i')$, we obtain that β_i and β_i' keep the same values as well as in RSP. Then, the only thing that change in the transcript are the values C_0 and C_1.

Applying this construction for all the rounds finishes the proof.

Lemma 2. *Let n, q be the parameters of the commitment scheme* COM *and rd the number of rounds of the threshold identification scheme. For any message μ and any threshold signature σ generated by a set S of t signers, we have : For any set S' of t signers there exists a signature σ' with probability*

$$p = 1 - \left(1 - \frac{1}{(2q)^{rd}}\right)^{2^{n \times rd}}$$

performed by S' such that the difference between σ and σ' are in the commitment values.

Proof. Using the Fiat-Shamir transform we can see the threshold signature as $(R_1, CH_1, R_2, CH_2, RSP)$ with R_1 is the concatenation of C_0 and C_1 of all the rounds, R_2 is the concatenation of all β_i and β_i' of all the rounds and RSP is the concatenation of final answers of all the rounds. The values of CH_1 and CH_2 are computed by two random oracle $\mathcal{O}_1$ and $\mathcal{O}_2$ such that $CH_1 = \mathcal{O}_1(\mu, R_1)$ with μ the message and $CH_2 = \mathcal{O}_2(\mu, CH_1, R_2)$. The Lemma 1 states the existence of another transcript equal to the signature except the values of C_0 and C_1. Those commitments are computed using the commitment scheme COM with random values $\mathbf{r}_0$ and $\mathbf{r}_1$. For each round of the transcript we can take an other $\mathbf{r}_0$ or $\mathbf{r}_1$ and we get another transcript equal to the signature except the values of C_0 and C_1. To finish the proof we compute the probability that one of those transcripts corresponds to a signature of μ. Most of the time the transcript is not a signature because the challenges are different than $\mathcal{O}_1(\mu, R_1)$ and $\mathcal{O}_2(\mu, CH_1, R_2)$. The probability that the transcript corresponds to a signature of μ can be computed by a Bernoulli distribution with parameters $p_B = \frac{1}{(2q)^{rd}}$ and $n_B = 2^{n \times rd}$. The parameter p_B corresponds to the probability to obtain a particular challenge and n_B correspond to the number of transcript. Then, the probability to obtain a signature is

$$1 - \left(1 - \frac{1}{(2q)^{rd}}\right)^{2^{n \times rd}}.$$

Theorem 2. *If there is a probabilistic polynomial time attacker $\mathcal{A}$ that can win the game of source hiding, then $\mathcal{A}$ can break the statistically hiding property of the commitment scheme* COM*.*

Proof. Let S_0 and S_1 be two sets of t signers. In the game described in Definition 7, the attacker is given as a challenge a threshold ring signature generated by S_b (with $b \in \{0, 1\}$) and he has to guess with non negligible probability b' such that $b' = b$.

We consider that the attacker has access to the set of all the secret keys and chooses two sets of t signers S_0 and S_1. Then, he chooses a message μ and requests a challenge. After receiving the threshold ring signature σ of μ signed under S_b, the attacker has to guess the set which generated it.

By lemma 2, we obtain that there exists a signature σ' generated by $S_{\bar{b}}$ with probability p such that the difference between σ and σ' are in the commitments calculated by COM. In the parameters of the commitment scheme COM, q is polynomial on n, therefore the probability p is not negligible. If the attacker $\mathcal{A}$ wins the source hiding game, then $\mathcal{A}$ can distinguish between two outputs of the commitment scheme COM with non negligible probability.

5.2 Unforgeability

In this subsection we prove that if a forger can win the game in Definition 8, then a polynomial time algorithm can be built to solve a standard lattice problem. The proof of unforgeability is given in Theorem 3. We start by giving the following lemma which is used in the proof of unforgeability.

Lemma 3. *If there exist a probabilistic polynomial time algorithm $\mathcal{A}$ that is able to produce a t-out-of-N threshold signature scheme with probability greater than $\left(\frac{q+2}{2q}\right)^{rd}$, than either he can produce t values which can be used as secret keys or he can find a collision in the commitment scheme* COM*.*

Proof. If $\mathcal{A}$ produces a t-out-of-N threshold signature with probability greater than $\left(\frac{q+2}{2q}\right)^{rd}$, then he succeeds, in the corresponding threshold identification scheme, in at least one round with probability greater than $\frac{q+2}{2q}$. In each round there are $2q$ possible challenges, q possibilities for the first challenge step and 2 possibilities for the second challenge step. By the pigeon-hole principle we deduce that $\mathcal{A}$ can answer correctly with a particular commitment for two different challenges α, β in the first challenge step and any possible challenge in the second challenge step. Therefore, he can build the following transcript:

$$((C_0, C_1), \alpha, (\mathbf{v}_i, \mathbf{w}_i), 0, (\phi, \psi_i, \mathbf{a}_i, \rho))\,, \quad i \in \{1, \dots, t\}$$

$$((C_0, C_1), \alpha, (\mathbf{v}_i, \mathbf{w}_i), 1, (\chi_i, \mathbf{d}_i, \mathbf{e}_i, \varrho))\,, \quad i \in \{1, \dots, t\}$$

$$((C_0, C_1), \beta, (\mathbf{v}'_i, \mathbf{w}'_i), 0, (\phi', \psi'_i, \mathbf{a}'_i, \rho'))\,, \quad i \in \{1, \dots, t\}$$

$$((C_0, C_1), \beta, (\mathbf{v}'_i, \mathbf{w}'_i), 1, (\chi_i, \mathbf{d}_i, \mathbf{e}_i, \varrho))\,, \quad i \in \{1, \dots, t\}$$

such that all those transcript succeeds in the verification protocol for that round. We have that either $\mathcal{A}$ can find a collision in COM or we obtain the following equations from the verification protocol.

1. $\psi_i = \psi'_i$, $\phi = \phi'$, $\mathbf{A}\psi_i^{-1}(\mathbf{v}_i)^T - \mathbf{M}\phi^{-1}(\mathbf{w}_i)^T = \mathbf{A}\psi_i'^{-1}(\mathbf{v}'_i)^T - \mathbf{M}\phi'^{-1}(\mathbf{w}'_i)^T$, $\mathbf{a}_i = \mathbf{a}'_i$ for $i \in \{1, \dots, t\}$.
2. $\mathbf{v}_i - \alpha\mathbf{d}_i = \mathbf{v}'_i - \beta\mathbf{d}'_i$, $\mathbf{w}_i - \alpha\chi_i = \mathbf{w}'_i - \beta\chi'_i$, $\mathbf{d}_i = \mathbf{d}'_i$, $\chi_i = \chi'_i$, $\mathbf{e}_i = \mathbf{e}'_i$ for $i \in \{1, \dots, t\}$.
3. $wh(\mathbf{d}_i) = wh(\mathbf{d}'_i) = m/2$, $\mathbf{d}_i \in \{0,1\}^m$, $\mathbf{d}'_i \in \{0,1\}^m$ for $i \in \{1, \dots, t\}$.
4. $\sum_{i=1}^t wh(\chi_i) = t$, $\sum_{i=1}^t wh(\chi'_i) = t$, $\chi_i \in \{0,1\}^N$, $\chi'_i \in \{0,1\}^N$ for $i \in \{1, \dots, t\}$.

From the equations in 2, we have that $\mathbf{v}'_i = \mathbf{v}_i - \alpha\mathbf{d}_i + \beta\mathbf{d}'_i$ and $\mathbf{w}'_i = \mathbf{w}_i - \alpha\chi_i + \beta\chi'_i$. When we replace $\mathbf{v}'_i$ and $\mathbf{w}'_i$ in the third equation in 1, we obtain:

$$\mathbf{A}\psi_i^{-1}(\mathbf{v}_i)^T - \mathbf{M}\phi^{-1}(\mathbf{w}_i)^T = \mathbf{A}\psi_i^{-1}(\mathbf{v}_i - \alpha\mathbf{d}_i + \beta\mathbf{d}_i)^T - \mathbf{M}\phi^{-1}(\mathbf{w}_i - \alpha\chi_i + \beta\chi_i)^T$$

$$0 = (\beta - \alpha)(\mathbf{A}\psi_i^{-1}(\mathbf{d}_i)^T - \mathbf{M}\phi^{-1}(\chi_i)^T)$$

Since $\alpha \neq \beta$ we have that $\mathbf{A}\psi_i^{-1}(\mathbf{d}_i)^T = \mathbf{M}\phi^{-1}(\chi_i)^T$. From the equation in 4, we have that $\mathbf{M}\phi^{-1}(\chi_i)^T$ correspond to t different public keys and $\psi_i^{-1}(\mathbf{d}_i)$ can be used to simulate t different secret keys. □

In the following theorem we prove the unforgeability of the threshold signature scheme.

Theorem 3 (Unforgeability). *If a forger wins the game in Definition 8 with probability p' in polynomial time, then the forger can solve an ISIS$_{q,n,m,\sqrt{m}}$ instance in polynomial time with probability $p'p\frac{1}{N^2}$ or find a collision in the commitment scheme* COM.

Proof. The challenger $\mathcal{C}$ is given an ISIS instance $(\mathbf{A}, \mathbf{y})$. Then, $\mathcal{C}$ chooses $k \in \{1 \dots N\}$ and sets $\mathbf{x}_k := 0$, $\mathbf{y}_k := \mathbf{y}$. $\mathcal{C}$ generates $N-1$ keys $(\mathbf{x}_i, \mathbf{y}_i)$ with $i \in \{1 \dots N\}$ and $i \neq k$.

We start the game in Definition 8 with the forger $\mathcal{F}$ and the pairs $(\mathbf{x}_i, \mathbf{y}_i)$ with $i \in \{1 \dots N\}$, as key pairs. We notice that only the key pair $(\mathbf{x}_k, \mathbf{y}_k)$ is not generated as a valid key pair and since $\mathbf{x}_k$ is not revealed, the set of key pairs $(\mathbf{x}_i, \mathbf{y}_i)$ is indistinguishable from a valid set of key pairs.

The challenger $\mathcal{C}$ simulates the signing oracle $\mathsf{OT.Sign}$. When $\mathcal{F}$ requests the signing oracle, he send a query to the challenger $\mathcal{C}$ involving the public keys $\mathbf{y}_i$, $i \in I$ and $I \subseteq N$. If k is not in the set I, the challenger $\mathcal{C}$ is able to produce the corresponding signature. Otherwise the challenger produces a signature σ by replacing $\mathbf{x}_k$ by $\mathbf{x}_j$ with $j \notin I$. By Lemma 2, with probability p there exist a signature σ' such that σ' could be produced using the secret key corresponding to $\mathbf{y}_i$.

The challenger $\mathcal{C}$ also simulates the oracle OExp. If the forger $\mathcal{F}$ asks for the value of $\mathbf{x}_k$, the game ends without a forged signature. Since the forger do not ask for all the secret keys, the probability that he ask for $\mathbf{x}_k$ is less than $\frac{N-1}{N}$. Otherwise, the forger $\mathcal{F}$ wins the game and outputs a valid signature in polynomial time with probability p'.

According to Lemma 3, $\mathcal{F}$ can either simulate t different secret keys or find a collision on the commitment scheme COM. If he succeeds to simulate t secret keys, at least one of them, $\mathbf{x}_l$, was not a query for the key exposure oracle. The vector $\mathbf{x}_l$ is such that $wh(\mathbf{x}_l) = m/2$ and $\mathbf{A}\mathbf{x}_l^T = \mathbf{y}_l$. Since k was chosen randomly at uniform in $\{1, \ldots, N\}$, then the probability that k is equal to l is $1/N$. If l is equal to k, then $\mathbf{x}_l$ is a solution of the $\mathrm{ISIS}_{q,n,m,\sqrt{m}}$ instance $(\mathbf{A}, \mathbf{y})$.

With the interaction of the challenger and the forger, we can build a probabilistic polynomial time algorithm that can solve an $\mathrm{ISIS}_{q,n,m,\sqrt{m}}$ instance with probability greater than $pp'\frac{1}{N^2}$. □

It was shown in [16] that the security of the commitment scheme COM is based on the average hardness of $\mathrm{ISIS}_{q,n,m,\sqrt{m}}$. By Theorem 1 we have that there exist average-case/worst-case reduction from SIVP_γ to $\mathrm{ISIS}_{q,n,m,\alpha}$ with an approximation factor $\gamma = \alpha \cdot \tilde{O}(\sqrt{n})$. Therefore, we have that for a prime $q = \tilde{O}(n)$, $m = O(n \log q)$ and $\alpha = \sqrt{m}$, the unforageability of our threshold ring signature scheme is based on $\mathrm{SIVP}_{\tilde{O}(n)}$.

6 Parameters

In this section we compare our threshold ring signature and our ring signature to the CLRS ring and threshold ring signature in [11]. The comparison is only made with this scheme because others schemes in [13, 14] don't give instantiation parameters.

6.1 Parameters assumption

We use the same parameters used in [11] (subsection 5.1) to compare the performance of the schemes. The parameters are $n = 64, m = 2048, q = 257$ and the length of the commitment of COM is 224 bits for bit-security equal to 111. To compute the size of the signature, we use a seed to represent each random permutation σ_i and Σ. In fact, the signer only has to send a seed from which the verifier can obtain the desired element and thus reduce the communication cost. The vector $\sigma_i(\mathbf{x}_i)$ is a vector in $\{0,1\}^m$, its length is so m-bits instead of $\log_2 q \times m$ bits.

6.2 Ring signature

In the following table we can see the significant reduction obtained with our ring signature scheme. Our scheme stay reasonable even for huge size of ring. The number of member of the ring is given by N.

N	100	1000	5000	10000	100000
CLRS ring	24.43	244.24	1221.21	2442.42	24424.20
Scheme in Figure 3	0.26	0.37	0.84	1.43	12.05

Table 1. Comparison of lattice-based ring signature schemes in Mbytes.

6.3 Threshold ring signature

In the following table we can see different signature sizes for some values of t and N.

N	100	100	100	100	100	100	200	200	200	1000	1000	1000
t	2	10	30	50	70	100	2	10	50	2	10	50
CLRS threshold ring	24.43	24.43	24.43	24.43	24.43	24.43	48.85	48.85	48.85	244.24	244.24	244.24
Scheme in Figure 4	0.52	2.56	7.68	12.80	17.92	25.60	0.54	2.68	13.39	0.73	3.63	18.11

Table 2. Comparison of lattice-based threshold ring signature schemes in Mbytes.

We see that our threshold scheme has a size close to t ring signatures and do not depend so much on the parameter N for the given parameters.

Acknowledgement

We deeply thank one of the anonymous reviewer of the conference which comments and suggestions were very helpful.

References

1. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen **261**(4) (1982) 515–534
2. Coppersmith, D.: Finding small solutions to small degree polynomials. In: Cryptography and lattices. Springer (2001) 20–31
3. Ajtai, M.: Generating hard instances of lattice problems. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, ACM (1996) 99–108
4. Chaum, D., Van Heyst, E.: Group signatures. In: Advances in Cryptology-EUROCRYPT'91, Springer (1991) 257–265
5. Rivest, R., Shamir, A., Tauman, Y.: How to leak a secret. Advances in Cryptology-ASIACRYPT 2001 (2001) 552–565
6. Bresson, E., Stern, J., Szydlo, M.: Threshold ring signatures and applications to ad-hoc groups. In: Advances in CryptologyÑCrypto 2002. Springer (2002) 465–480
7. Liu, J., Wei, V., Wong, D.: A separable threshold ring signature scheme. Information Security and Cryptology-ICISC 2003 (2004) 12–26
8. Dallot, L., Vergnaud, D.: Provably secure code-based threshold ring signatures. In: Cryptography and Coding. Springer (2009) 222–235
9. Zheng, D., Li, X., Chen, K.: Code-based ring signature scheme. IJ Network Security **5**(2) (2007) 154–157
10. Melchor, C.A., Cayrel, P.L., Gaborit, P.: A new efficient threshold ring signature scheme based on coding theory. In: Post-Quantum Cryptography. Springer (2008) 1–16
11. Cayrel, P.L., Lindner, R., Rückert, M., Silva, R.: A lattice-based threshold ring signature scheme. In: Progress in Cryptology–LATINCRYPT 2010. Springer (2010) 255–272
12. Cayrel, P.L., Lindner, R., Rückert, M., Silva, R.: Improved zero-knowledge identification with lattices. In: Provable Security. Springer (2010) 1–17
13. Wang, J., Sun, B.: Ring signature schemes from lattice basis delegation. In: Information and Communications Security. Springer (2011) 15–28
14. Brakerski, Z., Kalai, Y.: A framework for efficient signatures, ring signatures and identity based encryption in the standard model. Technical report, Cryptology ePrint Archive, Report 2010/086 (2010)
15. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th annual ACM symposium on Theory of computing, ACM (2008) 197–206
16. Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently secure identification schemes based on the worst-case hardness of lattice problems. Advances in Cryptology-ASIACRYPT 2008 (2008) 372–389
17. Aguilar Melchor, C., Cayrel, P., Gaborit, P., Laguillaumie, F.: A new efficient threshold ring signature scheme based on coding theory. Information Theory, IEEE Transactions on **57**(7) (2011) 4833–4842

18. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. In: Theory of Cryptography. Springer (2006) 60–79
19. Stern, J.: A new identification scheme based on syndrome decoding. In: Advances in Cryptology-CRYPTO'93, Springer (1994) 13–21
20. Cayrel, P.L., Veron, P.: Improved code-based identification scheme. arXiv preprint arXiv:1001.3017 (2010)
21. Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: Advances in Cryptology-EUROCRYPT'96, Springer (1996) 387–398
22. Alaoui, S.M.E.Y., Dagdelen, Ö., Véron, P., Galindo, D., Cayrel, P.L.: Extended security arguments for signature schemes. In: Progress in Cryptology-AFRICACRYPT 2012. Springer (2012) 19–34