Improved Lattice-Based Threshold Ring Signature Scheme

Slim Bettaieb [1] Julien Schrek[1]

[1] XLIM-DMI, Université de Limoges, (France)

PQCrypto - 5 June 2013

Outline

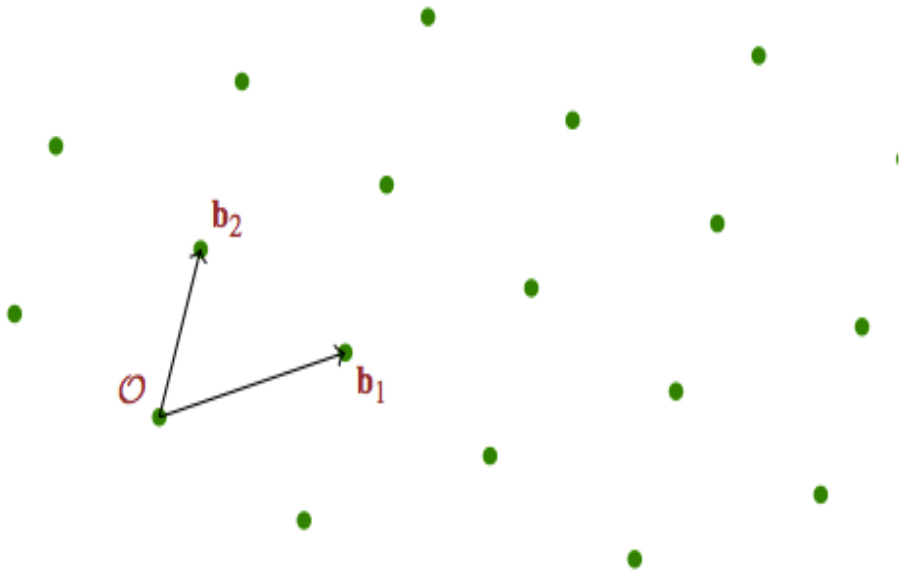
Lattices

Lattice

- A lattice is a discrete subgroup of $\mathbb{R}^n$ which spans $\mathbb{R}^n$
- Let $b_1, b_2, \ldots, b_n \in \mathbb{R}^n$, n linearly independant vectors, the lattice generated by them is

$$\mathcal{L} := \{\sum_i x_i b_i \mid x_i \in \mathbb{Z}\}.$$

A lattice in $\mathbb{R}^2$



Lattice-based Cryptography

- 90s : Strong security reductions
- Belived to resist quantum computer attacks

Lattice Hard Problem

$\mathrm{ISIS}_{q,n,m,\alpha}$

Given a random matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ a vector $\mathbf{s} \in \mathbb{Z}_q^n$ and a real α find a vector $\mathbf{v} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{v}^T = \mathbf{s} \bmod q$ and $\|\mathbf{v}\|_2 \leq \alpha$.

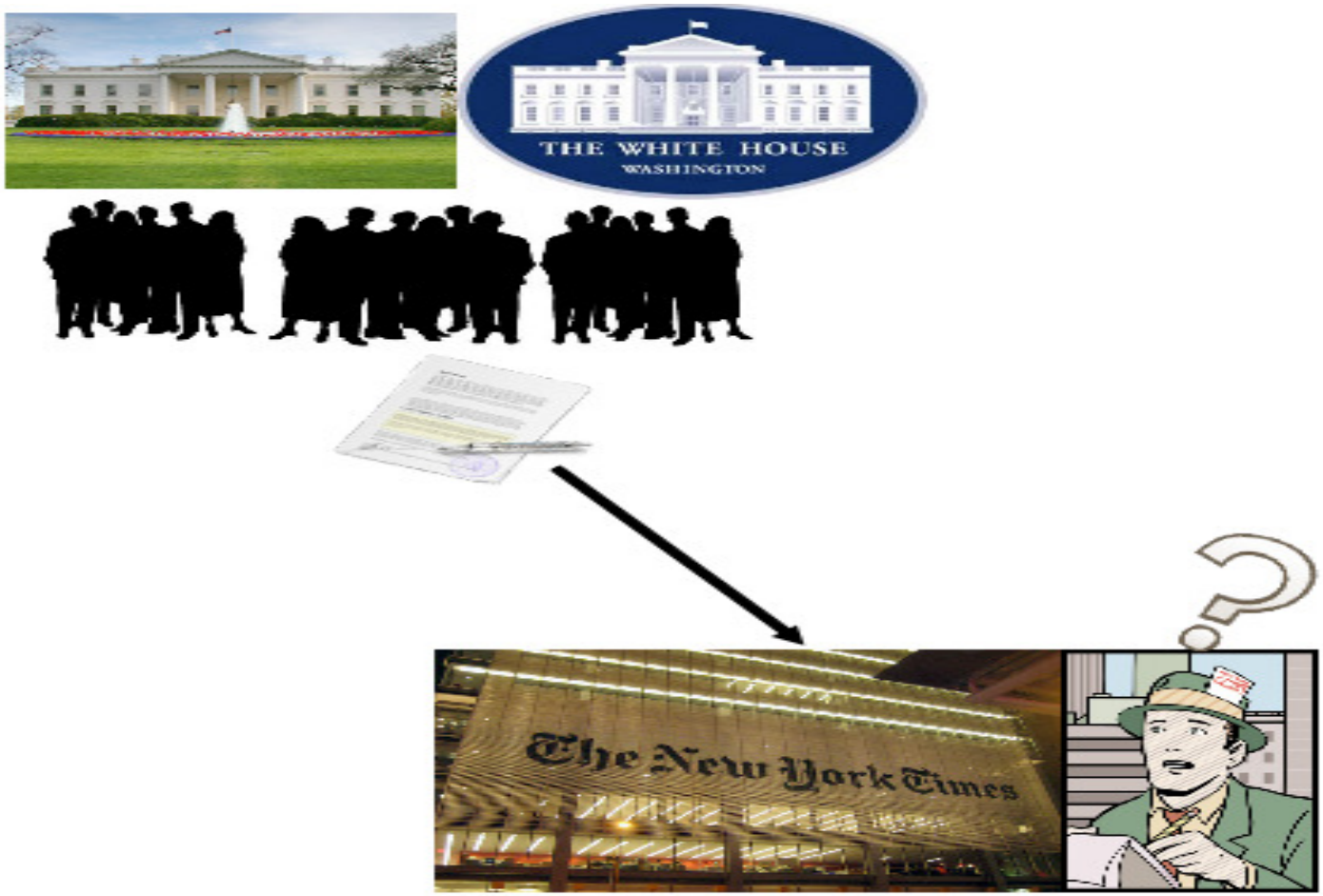
[GPV08] Reduction to a standard lattice problem SIVP_γ (NP-complet)

SIVP_γ

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

Motivation

How to leak a secret [RST01] : A ring signature could be used to provide an anonymous signature from "a high-ranking White House official", without revealing which official signed the message .



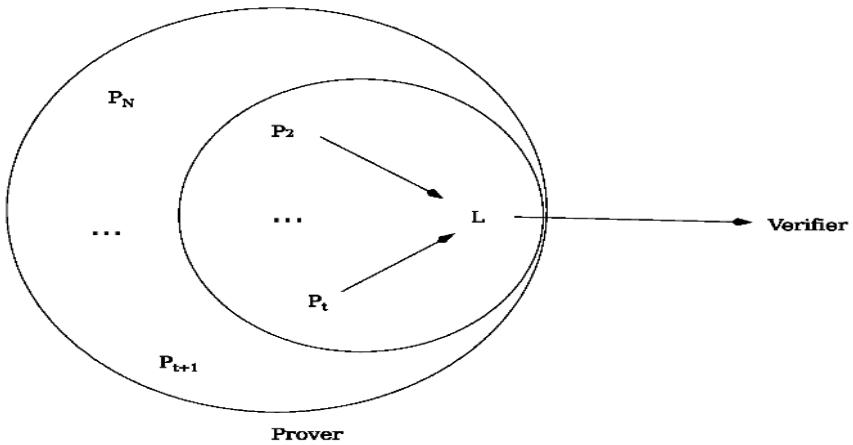
Definitions

Ring Signature

One person signs anonymously among N users.

Threshold Ring Signature

t users signs anonymously among N users.



Signature

- link an identity to a message

Anonymity

- No information about the identity

Features

Ring Signatures

- Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

Threshold Ring Signatures

- In 2002, Ring Signature was extended to threshold ring signatures.
- t-out-of-N users interacts together in order to produce a signature.
- No information is leaked about the set of signers.

Related Work

Brakerski-Kalai (eprint 2010/086) [Ring Signature]

- Hash-and-sign / bonsai-tree approach

Wang-Sun (ICICS '11)[Ring Signature]

- Hash-and-sign / bonsai-tree approach

Aguilar Melchor-Bettaieb-Boyen-Fousse-Gaborit (Africacrypt '13)[Ring Signature]

- Lyubashevsky's signatures 2009 and 2013

Cayrel-Linder-R*ü*ckert-Silva (Latincrypt '10)[Threshold Ring Signature]

- Threshold ring signature scheme (hard feature to obtain)
- Zero knowledge construction

T-CLRS (Cayrel-Lindner-Ruckert-Silva)

Main strengths

- Threshold property
- Fast (mostly linear operations)
- Based on lattice hard problems SIVP

Weakness

- The size of signatures (24.43 Megabytes for a ring of 100 users)

- Obtained from identification scheme.
- Generalizes the zero knowledge identification scheme CLRS ’10

ZK Identification Scheme : CLRS

CLRS - Key Generation

Secret key : a vector $\mathbf{x} \in \{0,1\}^m$ with Hamming weight m/2.
Public key : $\mathbf{y} \in \mathbb{Z}_q^m$ such that $\mathbf{y} = \mathbf{A}\mathbf{x}^T \mod q$

- Commitment / Challenges / Answers (5 rounds)

Idea :

Two masks : a permutation σ and a random vector $\mathbf{u}$
Masked secret : $\sigma(\mathbf{u} + \alpha\mathbf{x})$
$\longrightarrow$ Unmask one of the two masks (σ or $\mathbf{u}$) to verify one of the property of $\mathbf{x}$

- The verifier chooses randomly the property of $\mathbf{x}$ to be verified (challenge).
- A malicious prover can anticipate one property of $\mathbf{x}$.
- A malicious prover can not anticipate the two properties of $\mathbf{x}$.
- Revealing only one mask does not leak any information about $\mathbf{x}$.

CLRS Identification Scheme

P chooses $\sigma \xleftarrow{\$} S_m$, $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m$, $\mathbf{r}_0 \xleftarrow{\$} \{0,1\}^n$ and $\mathbf{r}_1 \xleftarrow{\$} \{0,1\}^n$.
P computes $c_0 \leftarrow \mathsf{COM}(\sigma||\mathbf{Au}||\mathbf{r}_0)$ 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 $\alpha \xleftarrow{\$} \mathbb{Z}_q$ to P.
3. [**second commitment**] P sets $\beta = \sigma(\mathbf{u} + \alpha\mathbf{x})$ and sends β to V.
4. [**second challenge**] V sends $b \xleftarrow{\$} \{0,1\}$, to P.
5. [**final answer**]
   If $b = 0$ then
   P sends σ 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

$$c_0 \stackrel{?}{=} \mathsf{COM}(\sigma\|\mathbf{A}\sigma^{-1}(\beta)^T - \alpha\mathbf{y}\|\mathbf{r}_0)$$

If $b = 1$ then V checks, $wh(\sigma(\mathbf{x})) \stackrel{?}{=} m/2$ and

$$c_1 \stackrel{?}{=} \mathsf{COM}(\beta - \alpha\sigma(\mathbf{x})\|\sigma(\mathbf{x})\|\mathbf{r}_1)$$

Signature from CLRS Identification Scheme

Fiat-Shamir transform

A 3 rounds ZK identification sheme can be turned into a digital signature by simulating the challenge with the hash values of the message.

- In 2012, Alaoui et al. extended the Fiat-Shamir transform to fit with 5 rounds identification schemes.
- This transformation is proved in the random oracle model

T-CLRS '10

- Let S a set N users
- Secret keys : $x_i \in \{0,1\}^m$ such that $wh(x_i) = m/2$ for $1 \leq i \leq N$
- Public keys : A_i such that $A_i x_i^T = 0$ for $1 \leq i \leq N$.

Idea :

- N identifications simultaneously (using all the public keys)
- The t signers use their secret keys and the other are simulated with 0 as secret key.

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_N \end{bmatrix} \quad x = \underbrace{\begin{bmatrix} x_1, & 0, & 0, & \cdots, & x_i, & 0, & 0, & \cdots, & x_N \end{bmatrix}}_{\text{t secret keys}}$$

T-CLRS '10

In CLRS, the secret x is masked by a permutation $\sigma \in S_m$ and a random word u.
In T-CLRS, σ is N permutations $(\sigma_1, \cdots, \sigma_N) \in S_m^N$.

t-out-of-N signers

The number of signer is verified by cheking the number of non zero block in $\sigma(x)$

Anonymity

An additional block permutation Σ is used to dissociate the $\sigma_i(x_i)$ and the public key A_i

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_N \end{bmatrix} \quad x = \underbrace{[x_1, \quad 0, \quad 0, \quad \cdots, \quad x_i, \quad 0, \quad 0, \quad \cdots, \quad x_N]}_{\text{t secret keys}}$$

T-CLRS

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_N \end{bmatrix} \quad x = \underbrace{[x_1, \ 0, \ 0, \ \cdots, \ x_i, \ 0, \ 0, \ \cdots, \ x_N]}_{\text{t secret keys}}$$

- N CLRS schemes simultaneously
- Block permutation Σ to achieve anonymity

Problem :

The size of the signature is about N times the size of the CLRS signature.

Our Scheme

- Let S a set N users
- Secret keys : $x_i \in \{0,1\}^m$ such that $wh(x_i) = m/2$ for $1 \leq i \leq N$
- Public keys : A such that $Ax_i^T = y_i$ for $1 \leq i \leq N$.

Idea :

- We use a matrix M of all the y_i, $1 \leq i \leq N$.
- The t signers make t CLRS signatures with the matrix $(A|M)$.
- The secret key in each CLRS scheme is (x_i, δ_i) with $\delta_i = \underbrace{(0, \cdots, 1, \cdots, 0)}_{\text{1 in the ith position}}$

Anonymity

We apply a permutation Σ to the δ_i

t-out-of-N signers

We use the same permutation Σ for the t δ_i to make sure that they are different.

$$\Sigma(\delta_i) \neq \Sigma(\delta_j) \Rightarrow \delta_i \neq \delta_j$$

Scheme

Let L be the leader.

1. L chooses randomly $\Sigma \in S_N$. Each signer build their own commitments with Σ.
2. The first challenge α is sent by the verifier.
3. The masked secret is sent :
$$\sigma_i(\mathbf{u}_i + \alpha \mathbf{x}_i)$$
$$\Sigma(\mathbf{u}'_i + \alpha \delta_i)$$
4. The second challenge $b \in \{0,1\}$ is sent
5. - If $b = 0$, σ_i and Σ are reveald $\rightarrow$ verification that $Ax_i^T = M\delta_i^T$
   - If $b = 1$, $\mathbf{u}_i$ and $\mathbf{u}'_i$ are reveald $\rightarrow$ verification that $x_i \in \{0,1\}^m$, $wh(x_i) = m/2$, $\sum_i^t wh(\Sigma(\delta_i)) = t$ and $wh(\delta_i) = 1$.

- Size(our scheme) $\simeq t\times$ Size(CLRS) + $t\times$ Size($\Sigma(\mathbf{u}'_i + \alpha\delta_i)$)
- Size(T-CLRS) $\simeq N\times$ Size(CLRS)

Results

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

TABLE: Comparison of lattice-based ring signature schemes in Mbytes.

N	100	100	100	100	100	100
t	2	10	30	50	70	100
CLRS threshold ring	24.43	24.43	24.43	24.43	24.43	24.43
Our Scheme	0.52	2.56	7.68	12.80	17.92	25.60

TABLE: Comparison of lattice-based threshold ring signature schemes in Mbytes.

Thank you !