Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
June 2016, 23(3): 11–17
www.sciencedirect.com/science/journal/10058885
The Journal of China Universities of Posts and Telecommunications
http://jcupt.bupt.edu.cn

Improved lattice-based ring signature schemes from basis delegation

Gao Wen (✉), Hu Yupu, Wang Baocang, Xie Jia

State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China

Abstract

Ring signature enables the members to sign anonymously without a manager, it has many online applications, such as e-voting, e-money, whistle blowing etc. As a promising post-quantum candidate, lattice-based cryptography attracts much attention recently. Several efficient lattice-based ring signatures have been naturally constructed from lattice basis delegation, but all of them have large verification key sizes. Our observation finds that a new concept called the split- small integer solution (SIS) problem introduced by Nguyen et al. at PKC'15 is excellent in reducing the public key sizes of lattice-based ring signature schemes from basis delegation. In this research, we first define an extended concept called the extended split-SIS problem, and then prove that the hardness of the extended problem is as hard as the approximating shortest independent vectors problem (SIVP) problem within certain polynomial factor. Moreover, we present an improved ring signature and prove that it is anonymous and unforgeable against the insider corruption. Finally, we give two other improved existing ring signature schemes from lattices. In the end, we show the comparison with the original scheme in terms of the verification key sizes. Our research data illustrate that the public key sizes of the proposed schemes are reduced significantly.

Keywords lattice-based, ring signature scheme, anonymous, unforgeable

1 Introduction

1.1 Backgrounds

A ring signature scheme enables a signer to generate a message anonymously in the name of others. The verifier checks only the validity of the signature, but can not tell the real signer apart. Ring signature schemes have several practical functionalities, such as the anonymity, equal rights and dynamics choices of all signers. They are widely employed in many online applications: e-voting, anonymous disclosing systems, online criminal detection systems et al.

Previous digital signature schemes are mainly constructed based on number theoretic assumptions [1–4]. Cryptographic researchers turned to find new cryptosystems to resist quantum attacks, since the cryptography schemes based on the large integer factorization and discrete logarithm problems can be solved in polynomial time by Shor's quantum algorithms [5].

Lattice-based cryptography is considered as the most promising primitive among the post quantum alternatives. So far, most of the existing lattice-based ring signatures [6–8] are constructed from lattice basis delegation [9]. A common disadvantage of them is the large verification key size, and this leads to expensive costs when implemented. Therefore, it is badly in need of a technique which can notably reduce the verification key sizes of lattice-based ring signatures.

1.2 Contributions

We find that the split-SIS problem introduced by Nguyen et al. [10] is applicable to reduce the public key size of ring signature schemes. Based on the split-SIS problem, we define an extended concept called the extended split-SIS problem, and then prove the hardness of the proposed problem. An improved ring signature scheme is proposed and proved to be anonymous and unforgeable against the insider corruption. Next, we give two other

Received date: 14-12-2015
Corresponding author: Gao Wen, E-mail: janegw@163.com
DOI: 10.1016/S1005-8885(16)60027-4

improved existing ring signature schemes from lattices. The comparison in terms of the verification key sizes is shown in Table.1 in Sect. 6.

1.3 Related works

In 2010, Brakerski and Kalai et al. [6] constructed the first lattice-based ring signature schemes based on the SIS problem by the hash-and-sign [9,11] approach. Wang et al. [7] proposed a lattice-based ring signature scheme in the standard model by a similar method. Then, Wang et al. [8] put forward two ring signature schemes at ICICS'11. In 2013, two lattice-based ring signatures with the technique from Lyubashevsky [12] were proposed by Ref. [13] and Ref. [14], respectively.

A common disadvantage in these schemes in Refs. [6–8, 14] is that the dimension of the new bonsai tree should be much larger than the bonsai tree in the original signature, because the ring members need to join other members' public keys. These ring signature schemes therefore have larger verification key sizes and higher storage costs.

2 Preliminaries

2.1 Notations

We use $\mathbb{R}$ ($\mathbb{Z}$) to denote the set of real numbers (integers), and $\leftarrow_R$ to represent randomly elements chosen from a distribution. Variable x that obeying distribution D is denoted by $x \sim D$. For positive integer d, $[d]$ denotes the set $\{1,2,\ldots,d\}$. Vectors are written in column form by bold lower-case letters, and $\|\cdot\|$ denotes the l_2 norm of vectors. For vectors $\boldsymbol{a} \in \mathbb{R}^s$ and $\boldsymbol{b} \in \mathbb{R}^t$, the connection of $\boldsymbol{a}$ followed by $\boldsymbol{b}$ is denoted by $(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{R}^{s+t}$, and $<\boldsymbol{a},\boldsymbol{b}>$ represents the inner product of $\boldsymbol{a}$ and $\boldsymbol{b}$ when $s=t$. For matrix $\boldsymbol{B} \in \mathbb{R}^{n\times m'}$, the connection of the columns of $\boldsymbol{A}$ and $\boldsymbol{B}$ is denoted by $[\boldsymbol{A} \| \boldsymbol{B}] \in \mathbb{R}^{n\times(m+m')}$.

Let n be the system security parameter, other parameters are implicitly determined by n. We use the notations of O, ω to represent the growth of functions. By using poly(n) we denote some arbitrary $f(n)=O(n^c)$ for some c. $f(n)$ is negligible if $f(n)<n^{-c}$ holds for all positive c and sufficiently large n, such $f(n)$ is denoted by negl(n). A probability is overwhelming if it is $1-\text{negl}(n)$.

2.2 Lattices

Let $\boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n\} \in \mathbb{R}^n$ consist of n linearly independent vectors, an n-dimensional lattice generated by $\boldsymbol{B}$ is defined as $\Lambda = L(\boldsymbol{B}) = \{\boldsymbol{Bc} : \boldsymbol{c} \in \mathbb{Z}^n\}$. $\boldsymbol{B}$ is called a *basis* of the lattice $\Lambda=L(\boldsymbol{B})$. We use $\tilde{\boldsymbol{B}}=\{\tilde{\boldsymbol{b}}_1,\tilde{\boldsymbol{b}}_2,\ldots,\tilde{\boldsymbol{b}}_n\}$ to denote the Gram-Schmidt orthogonalization of $\boldsymbol{B}$, and it is defined as: $\tilde{\boldsymbol{b}}_1=\boldsymbol{b}_1$, and $\tilde{\boldsymbol{b}}_i=\boldsymbol{b}_i-\sum_{j=1}^{i-1}\mu_{ij}\tilde{\boldsymbol{b}}_j$ for $i=2,\ldots,n$, where $\mu_{ij}=<\boldsymbol{b}_i,\tilde{\boldsymbol{b}}_j>/<\tilde{\boldsymbol{b}}_j,\tilde{\boldsymbol{b}}_j>$ and $\tilde{\boldsymbol{b}}_i$ is the component of $\boldsymbol{b}_i$ orthogonal to $\text{span}(\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_{i-1})$.

Proposition 1 ([11]) For any polynomial m, $\beta=poly(n)$ and prime $q \geqslant \beta\omega(\sqrt{n\log n})$, the average case problems $\text{SIS}_{q,2m,\beta}$ and $\text{ISIS}_{q,2m,\beta}$ are as hard as approximating SIVP in the worst case to within certain $\gamma=\beta O(\sqrt{n})$ factors.

2.3 Split-SIS problem

The split- inhomogeneacls small integer solution (ISIS) problem is firstly introduced by Nguyen et al. in Ref. [10]. Given uniformly random matrices $\boldsymbol{A}_1,\boldsymbol{A}_2 \in \mathbb{Z}_q^{n\times m}$, integer $N=N(n)$ and $\beta=\beta(n)$, the target of the split-$\text{SIS}_{q,m,\beta,N}$ problem is to find a tuple $(\boldsymbol{x}=(\boldsymbol{x}_1,\boldsymbol{x}_2),h) \in \mathbb{Z}^{2m}\times\mathbb{Z}$ such that

$-\boldsymbol{x}_1 \neq \boldsymbol{0} \mod q$ or $h\boldsymbol{x}_2 \neq \boldsymbol{0} \mod q$;

$-\|\boldsymbol{x}\| \leqslant \beta$, $h \in [N]$, and $\boldsymbol{A}_1\boldsymbol{x}_1 + h\boldsymbol{A}_2\boldsymbol{x}_2 = \boldsymbol{0} \mod q$.

3 Extended split-SIS problem

We define the extended split-SIS problem and prove its hardness in this section. Take uniformly random matrices $\boldsymbol{A}_0,\boldsymbol{A}_1,\boldsymbol{A}_2 \in \mathbb{Z}_q^{n\times m}$, integer $N=N(n) \geqslant 1$ and $\beta=\beta(n)$ as inputs, the target of the extended split-$\text{SIS}_{q,m,\beta,N}$ problem is to find a vector $\boldsymbol{x}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N) \in \mathbb{Z}^{(N+1)m}$ that satisfies the following two conditions.

1) $\boldsymbol{x} \neq 0 \bmod q$ and $j\boldsymbol{x}_j \neq 0 \bmod q$ for $j \in [N]$.

2) $\|\boldsymbol{x}\| \leqslant \beta$, and $\boldsymbol{A}_0\boldsymbol{x}_0 + \sum_{j\in[N]}(\boldsymbol{A}_1 + j\boldsymbol{A}_2)\boldsymbol{x}_j = \boldsymbol{0} \bmod q$.

Theorem 1 (hardness of extended split-SIS problems) For any polynomial bounded $m=m(n)$, $\beta=\text{poly}(n)$ and prime $q \geqslant \beta\omega(\sqrt{n\log n}) > (N^2+N)/2$, the extended split-$\text{SIS}_{q,m,\beta,N}$ problem is polynomial equivalent to $\text{SIS}_{q,3m,\delta}$ problem with $\eta=N\beta$. In particular, the average case extended split-$\text{SIS}_{q,m,\beta,N}$ problem is at least as hard as approximating SIVP in the worst case to within certain $\gamma=\delta\tilde{O}(\sqrt{n})$ factors.