Information Processing Letters 116 (2016) 497–502

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Efficient multi-party concurrent signature from lattices

Xinyin Xiang [a,b,*], Hui Li [a,*], Mingyu Wang [b,*], Xingwen Zhao [a,*]

[a] State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, China
[b] School of Information, Xi'an University of Finance and Economics, Xi'an, 710100, China

ARTICLE INFO

Article history:
Received 12 March 2015
Received in revised form 19 November 2015
Accepted 22 February 2016
Available online 3 March 2016
Communicated by S.M. Yiu

Keywords:
Concurrent signature
Multi-party
Lattice
SIS
Cryptography

ABSTRACT

Concurrent signature is a novel paradigm, which can achieve fair exchange of signatures between users. Since its appearance, the topic has been widely concerned, while the study of concurrent signature in multi-user setting suffers from some criticism. Almost all known multi-user concurrent signature schemes rely on the hardness assumptions that is insecure against quantum analysis. Furthermore, most of multi-party concurrent signature (MCS) schemes are lacking of formal security models. In the paper, in the random oracle model, we propose a construction of lattice-based MCS scheme and prove its security under the hardness of the small integer solution (SIS) problem. Since our proposed scheme is based on the lattice assumptions, which is believed to be quantum-resistant, the mathematical properties make our scheme simpler and more flexible.

1. Introduction

The notion of concurrent signature [1] is firstly proposed by Chen et al., which provides a valid approach for achieving fair exchange of signatures. In the scheme, it usually includes two users and permits any untrusted users to perform the exchange of signatures, the signature is produced with ambiguous manner so that other outsiders cannot distinguish who is indeed signer until a keystone is released by one of the users. After all the keystones are released, the signature will be concurrently bound to their signers and can be verified by anyone. Owing to the feature, concurrent signature schemes are useful in some actual settings including contract signing.

Along with the work of Chen et al., some related researches are proposed in recent years [2–12], the above work mainly consists of two-user setting or multi-user setting. Mu et al. [2] and Chow et al. [3] proposed two perfect concurrent signature schemes. Unfortunately, Wang et al. [4] pointed out that both of them were insecure. Later, Susilo et al. [5] gave a three-party concurrent signature scheme that the signature was generated by one of the parties or other two parties jointly, but their schemes only satisfied weak ambiguity. Tonien et al. [6] first presented a new concurrent signature scheme in the multi-user setting, Tonien et al. also claimed that their schemes satisfied the property of unforgeability, ambiguity and fairness. However, Shieh [7] indicated Tonien et al.'s schemes could not indeed achieve concurrent signature and did not satisfy unforgeability and ambiguity, Shieh also proposed a new MCS scheme. Tan et al. [8] pointed out that Shieh et al.'s schemes only supported weak unforgeability and ambiguity. Recently, Xu et al. [9] proposed a new MCS scheme, but their schemes lack reasonable security definition of the MCS schemes. Liu et al. [10] proposed a MCS scheme with enhanced security. Unfortunately, Mao et al. [11] pointed out that their schemes were insecure because the generated signature could be forged by an inside adversary.

It is worth mentioning that the designs of previous concurrent signature schemes mainly rely on the hardness of the discrete logarithm or factorization, these schemes will be fragile once quantum era come into a reality, the only alternative of these primitives is concurrent signature

* Corresponding authors.
E-mail addresses: xiangxinyin@163.com (X. Xiang), lihui@mail.xidian.edu.cn (H. Li), wmyufe@163.com (M. Wang), xwzhao@xidian.edu.cn (X. Zhao).

http://dx.doi.org/10.1016/j.ipl.2016.02.007
0020-0190/© 2016 Elsevier B.V. All rights reserved.

schemes based on lattice assumptions. Hence, designing an efficient multi-party concurrent signature scheme which can be resistant against quantum computers, will be an interesting open question.

Our contribution: To tackle the previous challenges, we try to reply to these open questions. More precisely, based on the recent result by Tan et al., we further present an efficient multi-party concurrent signature scheme from lattices that overcomes the security flaws of the existing schemes. Additionally, in the random oracle model, we prove the security of the scheme under the hardness of the small integer solution (SIS) problem.

Organization: In Section 2, we review the preliminaries that are used throughout this paper. In Section 3, we propose the architecture for multi-party concurrent signature scheme. In Section 4, a lattice-based multi-party concurrent signature scheme is described, and we analyze security of our proposed scheme. Finally, we conclude our work in Section 5.

2. Preliminaries

2.1. Notation

Throughout the paper, we use $\mathbb{R}$ and $\mathbb{Z}$ to denote the real numbers and integers respectively. $\parallel v \parallel_p$ means l_p norm of a vector v, vectors are in column form and lower-case letters (e.g. x) is used to denote them. Matrices are denoted by upper-case letters (e.g. A). For any integer k, $[k]$ is denoted the set $\{1, \dots, k\}$. If a function is negligible, we use $\mathrm{negl}(n)$ to denote the function. The statistical distance between two distributions X, Y over a finite or countable set D is $\triangle(X, Y) = \frac{1}{2}\sum_{\omega \in D} \mid X(\omega) - Y(\omega) \mid$. Let $\{X_n\}$ and $\{Y_n\}$ be ensembles of random variables indexed by the security parameter n. We say that X and Y are statistically close if $\triangle(X_n, Y_n) = \mathrm{negl}(n)$.

2.2. Lattices

Given m linearly independent vectors $B = \{b_1, b_2, \dots, b_m\}$, an m-dimensional lattice generated by B is defined as $\Lambda = \mathcal{L}(B) = Bc = \{\sum_{i=1}^{m} \cdot b_i c_i : c \in \mathbb{Z}^m\}$, where $\Lambda = \mathcal{L}(B)$ is a basis of B. Next, the integer lattices called q-ary lattices is very important in the lattice-based schemes.

For $m \geq n \geq 1$ and $q \geq 2$, given a matrix $A \in \mathbb{Z}_q^{m \times n}$, we define the lattice $\Lambda_q^{\perp}(A) = \{e \in \mathbb{Z}^m : Ae = 0 \mod q\}$ and $\Lambda_q^u(A) = \{e \in \mathbb{Z}^m : Ae = u \mod q\}$. Thus, $\Lambda_q^u(A)$ is obviously a coset of $\Lambda_q^{\perp}(A)$; namely, $\Lambda_q^u(A) = t + \Lambda^{\perp}(A)$, where t is an arbitrary solution (over $\mathbb{Z}_q^m$) of the equation $At = u \mod q$.

2.3. Discrete Gaussians over lattices

Let L be a subset of $\mathbb{Z}^m$. For any vector $c \in \mathbb{R}^m$ and any positive parameter $\delta \in \mathbb{R} > 0$, let $\rho_{\delta,c}(x) = exp(\frac{-\pi \|x-c\|^2}{\delta^2})$ be a Gaussian-shaped function on $\mathbb{R}^m$ with center c and parameter δ. Next, for every $x \in L$, we set $\rho_{\delta,c}(L) = \sum_{x \in L} \rho_{\delta,c}(x)$ be the sum of $\rho_{\delta,c}(x)$ over L with parameters (δ, c) and $\mathcal{D}_{L,\delta,c}(x) = \frac{\rho_{\delta,c}(x)}{\rho_{\delta,c}(L)}$. For simplicity, $\rho_{\delta,0}$ and $\mathcal{D}_{L,\delta,0}$ are abbreviated as ρ_δ and $\mathcal{D}_{L,\delta}$, respectively.

Definition 1 *(Discrete normal distribution).* For any standard deviation $\sigma > 0$ and a vector $v \in \mathbb{Z}^m$, define the function as follows:

$$\rho_{\sigma,v}^m(x) = (2\pi\sigma^2)^{-m/2} exp(\frac{\parallel x - v \parallel^2}{-2\sigma^2})$$

Next, let the quantity $\rho_\sigma^m(\mathbb{Z})$ be the sum on $\rho_\sigma^m(z)$. For any $\sigma > 0$, the discrete normal distribution over $\mathbb{Z}$ centered on vector $v \in \mathbb{Z}^m$ is defined as $D_{v,\sigma}^m(x) = \rho_{v,\sigma}^m(x)/\rho_\sigma^m(\mathbb{Z}^m)$. When $v = 0$, let $\rho_{v,\sigma}^m(x)$ be $\rho_\sigma^m(x)$.

Lemma 1. *(See [13].) For any $\sigma > 0$, where*

(1) $Pr[\mid y \mid > 10\sigma, y \leftarrow D_\sigma^1] \leq 2e^{-100}$.
(2) $Pr[y \leftarrow D_\sigma^m, \sigma \geq 3/\sqrt{2\pi}] \leq 2^{-m}$.

The below lemma shows that it is interesting in the event of rejection sampling algorithm.

Lemma 2. *(See [13].) For any positive α and $v \in \mathbb{Z}^m$, if $\sigma = \omega(\parallel y \parallel \sqrt{\log m})$, we have*

$$Pr[y \leftarrow D_\sigma^m : D_\sigma^m(y)/D_{v,\sigma}^m(y) = O(1)] = 1 - 2^{-\omega(\log m)}$$

therefore, this means

$$Pr[y \leftarrow D_\sigma^m : D_\sigma^m(y)/D_{v,\sigma}^m(y) < e^{12/\alpha + 1/(2\alpha^2)}]$$
$$= 1 - 2^{-100}$$

2.4. Hard problems for q-ary lattices

We describe definitions of the small integer solution (SIS) problem, the security of our proposed scheme rests on the hardness of the below problems that cannot be solved in polynomial time with non-negligible advantage. The related problem is defined as follows.

Definition 2 *(SIS).* Given (m, q, β) and $A \in \mathbb{Z}_q^{n \times m}$, its goal is to calculate a non-zero vector $x \in \mathbb{Z}^m$ such that $Ax = 0 \mod q$ with $\parallel x \parallel \leq \beta$.

Ajtai [14] first described that the SIS problem was hard. Later, Micciancio et al. [15] formalized its notion and claimed that the SIS problem was seen as the worst-case hard lattice problems.

3. Framework of multi-party concurrent signature scheme

In a MCS scheme, we consider the following setting: each party picks a keystone and independently generates a keystone fix, the appearance of concurrent binding will occur once all the keystones are released. Furthermore, we utilize a new technique in the exchange of MCS such that each user can generate a priori keystone fix by using a keystone fix.