Available online at www.sciencedirect.com
ScienceDirect

ELSEVIER

August 2016, 23(4): 83–90
www.sciencedirect.com/science/journal/10058885

The Journal of China Universities of Posts and Telecommunications

http://jcupt.bupt.edu.cn

Attribute-based signatures on lattices

Xie Jia[1] (✉), Hu Yupu[1], Gao Juntao[1], Gao Wen[1], Li Xuelian[2]

1. The State Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, China
2. School of Mathematics and Statistics, Xidian University, Xi'an 710071, China

Abstract

Because of its wide application in anonymous authentication and attribute-based messaging, the attribute-based signature scheme has attracted the public attention since it was proposed in 2008. However, most of the existing attribute-based signature schemes are no longer secure in quantum era. Fortunately, lattice-based cryptography offers the hope of withstanding quantum computers. And lattices has elevated it to the status of a promising potential alternative to cryptography based on discrete log and factoring, owing to implementation simplicity, provable security reductions and quantum-immune. In this paper, the first lattice attribute-based signature scheme in random oracle model is proposed, which is proved existential unforgeability and perfect privacy. Compared with the current attribute-based signature schemes, our new attribute-based signature scheme can resist quantum attacks and has much shorter public-key size and signature size. Furthermore, this scheme is extended into an attribute-based signature scheme on number theory research unit (NTRU) lattice, which is also secure even in quantum era and has much higher efficiency than the former.

Keywords attribute, signature, lattice, unforgeability, perfect privacy

1 Introduction

The concept of attribute-based signature (ABS) scheme was first introduced in Ref. [1] as an extension of the identity-based signature. Generally speaking, in the ABS scheme a user obtains his private key for a set of attributes, instead of just the identity, from the attribute authority. The ABS breaks the one to one restriction in the traditional public key cryptography. That is to say, one can distribute a message to a specific set of users and sign it under just one common public key. Because of its perfect privacy and good expression ability, the ABS scheme has widely cryptographic application, such as anonymous authentication and attribute-based messaging.

Since the first ABS scheme emerged, several beautiful ABS constructions had been proposed [1–9]. Escala et al proposed the first ABS scheme satisfying proven secure against fully adaptive adversaries in Ref. [2]. Li et al. constructed two ABS schemes supporting flexible threshold predicates in Ref. [3], where the length of the signature depends on the largest size of attribute set. Two ABS constructions with constant signature size were proposed in Ref. [4]. And they are proven secure against selective predicate and adaptive message attacks. Zeng et al. proposed an ABS scheme with constant signature size in Ref. [5], which is not only unforgeable but also unconditionally anonymous. Okamoto and Takashima respectively proposed a fully secure ABS scheme in the standard model in Ref. [6] and the first decentralized multi-authority ABS scheme in Ref. [7]. The later no longer need the trusted setup and central authority.

However, most of the ABS schemes above are based on the discrete logarithm problem, which have high efficiency but are no longer intractable when quantum computer comes into reality according to Ref. [10]. Fortunately, Bernstein has conjectured in Ref. [11] that lattice-based cryptographic schemes can withstand quantum attacks. What is more, lattice-based cryptographic schemes are also easy to implement because typical computations involved in them are only integer matrix–vector multiplication and modular addition operations (Ref. [12], for an overview on

Received date: 25-11-2015
Corresponding author: Xie Jia, E-mail: xiejia199325@163.com
DOI: 10.1016/S1005-8885(16)60049-3

lattice-based cryptography). And lattice-based cryptographic schemes are supported by the worst-case to average-case security guarantees. Considering these three advantages, lattice-based cryptography enters a rapid development period and in the last ten years it have got many achievements, such as cryptographic primitive [13–18], encryption scheme (public key encryption [19–24], fully homomorphic encryption schemes [25–28]), signature schemes [14,29–35], multilinear maps [36–38]. So far, there have been three lattice-based ABS schemes which were respectively proposed in Refs. [39–41]. Even though all of them are proven secure even in quantum era, they are the attribute-based signatures in standard model and their efficiency is low. So how to construct ABS schemes, which are quantum-immune, in random oracle model and with high efficiency, may be the urgent issue in the coming years.

1.1 Our contributions

We propose the first lattice-based ABS scheme in random oracle model. And the scheme is proved existentially unforgeable against adaptively chosen message and selective access structure attacks, based on the hardness of small integer solution (SIS) problem. What's more, the efficiency of our new scheme is much higher than the existed lattice-based ABS schemes in Refs. [39–41]. Furthermore, we extend our scheme into the ABS scheme on NTRU lattice, which can improve the efficiency in large amplitude, and its security depends on the hardness of the ring small integer solution (R-SIS) problem, it means the ABS scheme over NTRU lattice is also security even in quantum era.

1.2 Paper organization

The remainder of this paper is organized as follows. Sect. 2 presents some preliminaries. Sect. 3 gives the syntax and security model for ABS schemes. The first lattice-based ABS scheme in random oracle model is provided in Sect. 4. The extensional ABS scheme from NTRU lattices is proposed in Sect. 5. Finally, Sect. 6 concludes this paper.

2 Preliminaries

2.1 Notation

The security parameter in this paper is a positive integer n. $\mathbb{R}$ and $\mathbb{Z}$ respectively denote the real space and integer space. Ring $R=\mathbb{Z}[x]/(x^n+1)$ and ring $R_q=\mathbb{Z}_q[x]/(x^n+1)$ will be used. $[k]$ is the set $\{1,2,\ldots,k\}$, where k is a positive integer. Vectors and matrixes are respectively denoted as bold low-case letters and bold upper-case letters in italic. $\tilde{\boldsymbol{A}}$ denotes the Gram-Schmidt orthogonalization of the matrix $\boldsymbol{A}$. And $\|\boldsymbol{v}\|$ denotes the Euclid norm of vector $\boldsymbol{v}$.

Let $f=\sum_{i=0}^{n-1} f_i x^i$ and $g=\sum_{i=0}^{n-1} g_i x^i$ be polynomials in R.

Notation: fg denotes polynomial multiplication in R, while $f*g=fg \bmod (x^n+1)$.

(f) is the vector whose coordinates are respectively $f_0,\ldots,f_{n-1}$. $(f,g)\in\mathbb{R}^{2n}=R^{1\times 2}$ is the concatenation of (f) and $\boldsymbol{G}$.

Definition 1 Anticirculant matrices An n dimensional anticirculant matrix of f is the following Toeplitz matrix:

$$\boldsymbol{C}_n\boldsymbol{F}=\begin{pmatrix} f_0 & f_1 & f_2 & \cdots & f_{n-1} \\ -f_{n-1} & f_0 & f_1 & \cdots & f_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ -f_1 & -f_2 & \cdots & \cdots & f_0 \end{pmatrix}=\begin{pmatrix} (f) \\ (xf) \\ \vdots \\ (x^{n-1}f) \end{pmatrix}$$

When it is clear from context, we will drop the subscript n, and just write $\boldsymbol{C}(f)$.

2.2 Lattices

Definition 2 $\boldsymbol{B}=[\boldsymbol{b}_1,\ldots,\boldsymbol{b}_m]\in\mathbb{R}^{m\times m}$ is a matrix, where the column vectors $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_m\in\mathbb{R}^m$ are linearly independent [29]. The m dimensional lattice $\varLambda$ generated by the basis $\boldsymbol{B}$ is the set,

$$\varLambda=L(\boldsymbol{B})=\left\{\boldsymbol{y}\in\mathbb{R}^m:\exists\boldsymbol{s}\in\mathbb{Z}^m,\ \boldsymbol{y}=\boldsymbol{B}\boldsymbol{s}=\sum_{i'=1}^{m}s_i\boldsymbol{b}_i\right\}$$

Definition 3 For a prime q, a matrix $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ and a vector $\boldsymbol{y}\in\mathbb{Z}_q^n$, we define two common cosets as follows [29]

$$\varLambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{e}=\boldsymbol{0}(\bmod q)\},$$

$$\varLambda^{y}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{e}=\boldsymbol{y}(\bmod q)\}.$$

Definition 4 NTRU lattice. Let q be the prime bigger than 5 and n be a power of 2. And f, $g\in R_q$ (f is invertible modulo q). Let $h=g*f^{-1} \bmod q$. The NTRU lattice associated to h and q is $\varLambda_{h,q}=\{(u,v)\in R^2 \mid u+v*h=0 \bmod q\}$. Here $\varLambda_{h,q}$ is a full-rank lattice of $\mathbb{R}^{2n}$ generated by the row of