Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 307637, 6 pages
http://dx.doi.org/10.1155/2014/307637

Research Article

A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model

Lili Zhang and Yanqin Ma

Institute of Information Engineering and Huanghe Science and Technology College, Zhengzhou 450063, China

Correspondence should be addressed to Lili Zhang; 312495261@qq.com

Received 25 April 2014; Revised 15 August 2014; Accepted 17 August 2014; Published 25 September 2014

Academic Editor: Yan-Wu Wang

A proxy blind signature scheme is a special form of blind signature which allowed a designated person called proxy signer to sign on behalf of original signers without knowing the content of the message. It combines the advantages of proxy signature and blind signature. Up to date, most proxy blind signature schemes rely on hard number theory problems, discrete logarithm, and bilinear pairings. Unfortunately, the above underlying number theory problems will be solvable in the postquantum era. Lattice-based cryptography is enjoying great interest these days, due to implementation simplicity and provable security reductions. Moreover, lattice-based cryptography is believed to be hard even for quantum computers. In this paper, we present a new identity-based proxy blind signature scheme from lattices without random oracles. The new scheme is proven to be strongly unforgeable under the standard hardness assumption of the short integer solution problem (SIS) and the inhomogeneous small integer solution problem (ISIS). Furthermore, the secret key size and the signature length of our scheme are invariant and much shorter than those of the previous lattice-based proxy blind signature schemes. To the best of our knowledge, our construction is the first short lattice-based identity-based proxy blind signature scheme in the standard model.

1. Introduction

Digital signature schemes are the cornerstone of e-business, e-government, software security, and many more applications. The importance of these schemes is likely to grow in the future as more and more everyday tasks and processes are computerized.

The concept of blind signature was first proposed in 1982 by Chaum [1]: user A could obtain the signature of B on any given message, without any information about the message or its signature revealed, and any receiver could verify the signature that is signed by signer B.

In 1996, Mambo et al. introduced the concept of proxy signature [2]: an original signer delegates his signing authority to another signer, who is called a proxy signer. At last, the proxy signer can sign any message on behalf of the original signer and the verifier can verify and distinguish between normal signature and proxy signature.

In 1985, Shamir introduced the concept of identity-based (ID-based) cryptography and presented an ID-based signature (IBS) scheme [3]. In an IBS scheme, a public key can be derived from the identity of the user, and a corresponding secret key can be generated by a private key generator (PKG). Of course, the IBS scheme can simplify key management procedures in certificate-based public key systems, so it can be an alternative for certificate-based public key systems in some occasions, especially, when efficient key management and moderate security are required.

In 2000, Lin and Jan [4] introduced the concept of proxy blind signature. Proxy blind signatures are actually the combination of both proxy signature and blind signature. It plays an important role in the following scenario: in e-cash system, the user makes the bank blindly sign a coin using blind signature schemes. Whenever a user goes through a valid branch to withdraw a coin, he/she needs the branch to make proxy blind signature on behalf of the signee bank.

Tan et al.'s scheme is a proxy blind signature scheme which is based on Schnorr blind signature. But Awasthi and der Lal [5] showed a forgery attack on Tan et al.'s scheme and proposed a more secure proxy blind signature scheme. Recently Sun et al. [6] pointed out that neither Tan et al.'s scheme nor Awasthi and der Lal's scheme satisfies the unlinkability property of the proxy blind signature scheme. But they did not give an improved scheme to overcome the insecurity. For the first time, Zhang et al. [7] proposed a proxy blind signature scheme from bilinear pairings. In 2004, Zheng et al. [8] proposed an ID-based proxy blind signature scheme which uses bilinear pairings of elliptic curves or hyperelliptic curves. Since then, many identity-based proxy blind signature schemes have been proposed, for example, [9–11].

Up to date, most of proposed identity-based proxy blind signature schemes rely on hard number theory problems such as integer factorization, discrete logarithm, and bilinear pairings with the Diffie-Hellman problem. However, the above underlying number theory problems will be solvable if practical quantum computers become reality, so it implies a potential security threat to these identity-based proxy blind schemes. Thus, a natural question one can ask is how to design identity-based proxy blind signature schemes that are secure in the quantum environment.

In recent years, lattices have emerged as a possible alternative to number theories. Lattice-based cryptography began with the seminal work of Ajtai [12], who showed that it is possible to construct families of cryptographic functions. Moreover, lattice-based cryptography is believed to be hard even for quantum computers [13]. Several lattice-based signature schemes [14–18] have been proposed so far. Among them, Jiang et al. [18] presented the first proxy signature scheme from lattices. Unfortunately, Tian and Huang [19] pointed that an original signer is able to forge a proxy signature on any message in the scheme. In 2010, Cash et al. put forward a new cryptographic notion called a bonsai tree based on hard lattice [20]. Since then, many proxy signatures [21, 22] were presented in bonsai tree model based on the bonsai tree signature scheme. However, both the private keys and the signatures in these schemes become dramatically longer than general signature. Therefore, they may not be practical for large communities.

Recently, Agrawal et al. [23] presented a basis delegation algorithm which keeps the dimension of the lattices involved constant. Based on the algorithm, the first lattice-based hierarchical identity-based encryption scheme with short ciphertexts in the standard model was proposed in [23]. Still, there is no identity-based proxy blind signature scheme from lattices in the standard model.

Following the above discussion, in this paper, we will construct a new identity-based proxy blind signature scheme from lattices in the standard model, which is obtained from Agrawal et al.'s basis delegation algorithm [23]. The new scheme is provably secure against strong forgery under hard problems on lattices, and the size of secret keys and the signature length of our scheme are much shorter than those of signature schemes [21, 22].

The rest of the paper is organized as follows: the next section gives the introduction of lattices, Section 3 explains briefly the definition of proxy blind signature, and Section 4 gives a detailed description of our identity-based proxy blind signature from lattice basis delegation. In Section 5, an analysis about our scheme is presented. Section 6 concludes this paper.

2. Preliminaries

2.1. Lattice. Let $B = [b_1, b_2, \ldots, b_n]$ and let $b_1, b_2, \ldots, b_n$ be n linearly independent vectors in R^n; the n-dimensional lattice Λ generated by the basis B is

$$\Lambda(B) = \left\{ Bc = \sum_{i=1}^{n} b_i c_i \mid c \in Z^n \right\}, \tag{1}$$

here B is called a basis of the lattice $\Lambda^{\perp}(B)$. For a basis $B = [b_1, b_2, \ldots, b_n]$, let $\widetilde{B}$ denote its Gram-Schmidt orthogonalization, defined iteratively as follows: $\widetilde{b_1} = b_1$, and for $i = 2, 3, \ldots, n$, $\widetilde{b_i}$ is the component of b_i orthogonal to span $(b_1, b_2, \ldots, b_{i-1})$.

The minimum distance λ_1 of the lattice is the length l_2 (in the Euclidean norm, unless otherwise indicated) of its shortest nonzero vector:

$$\lambda_1(\Lambda) = \min_{x \in \Lambda} \|x\|. \tag{2}$$

We define the orthogonal lattice $\Lambda^{\perp}(B)$ as

$$\Lambda^{\perp}(B) = \left\{ e \in R_m \mid Be = 0 \bmod q, B \in R_q^{n\times m} \right\}. \tag{3}$$

2.2. Hard Problems on Lattices. Security of our signature scheme rests on the hardness assumption of the short integer solution (SIS) problem and the inhomogeneous small integer solution problem [14].

Definition 1 (the small integer solution problem (SIS) (in the Euclidean l_2 norm)). Given an integer q, a matrix $A \in R_q^{n\times m}$, and a real β, the goal of the short integer solution problem $\mathrm{SIS}_{q,m,\beta}$ is to find a nonzero integer vector $e \in Z_q^m$, such that $Ae = 0 \bmod q$ and $\|e\|_2 \le \beta$.

Definition 2 (the inhomogeneous small integer solution problem (ISIS) (in the Euclidean l_2 norm)). Give an integer q, a matrix $A \in R_q^{n\times m}$, a syndrome $y \in Z_q^n$, and a real β, to find an integer vector $e \in Z_q^m$, such that $Ae = y \bmod q$ and $\|e\|_2 \le \beta$.

2.3. Trapdoor and Basis Delegation Functions for Lattices. It was shown in [14] that if $\mathrm{SIS}_{q,m,\beta}$ is hard, $A \in R_q^{n\times m}$ defines a one-way function $f_A : D_n \to R_n$, with $f_A(e) = Ae$, where $D_n = \{e \in Z^m \mid \|e\| \le rm\}$ and $R_n = Z_q^n$. The input distribution is $D_{Z^m,r}$, and a short basis for $\Lambda^{\perp}(A)$ can be used as a trapdoor to sample from $f_A^{-1}(y)$.

Here we briefly introduce some enhanced variants of trapdoor functions [14] with preimage sampling, which are given by a tuple of probabilistic polynomial-time algorithms (*TrapGen*, *SampleD*, and *SamplePre*), which will be used as building blocks in our signature scheme.

The following functions take the Gaussian smoothing parameter $r \ge \|\widetilde{B}\| \cdot \omega(\sqrt{lgm})$ as a parameter.

TrapGen(1^n). Let n, q, and m be integers with $q \ge 2$, $m \ge 2nlgq$; TrapGen(1^n) outputs a pair (A, T), where A

is statistically close to uniform on $Z_q^{n\times m}$ and T is a good basis of $\Lambda^{\perp}(A)$, such that $\|\widetilde{B}\| \leq m\sqrt{lgm}$.

SampleD(A, r). Sample an e from distribution $D_{Z^m,r}$, for which the distribution of Ae is uniform over Z_q^n.

SamplePre(A, T, y, r). On input of $A \in Z_q^{n\times m}$, a good basis T for $\Lambda^{\perp}(A)$ as the trapdoor, a vector $y \in Z_q^n$, and r, the conditional distribution of the output e is within negligible statistical distance of $D_{\Lambda_y^{\perp},r}$.

At CRYPTO 2010, Agrawal et al. [23] presented a new short lattice basis delegation algorithm that keeps the lattice dimension unchanged. Now, we briefly recall the main results in [23].

Definition 3. Let q be a prime, let $m \geq 6nlgq$, let and $\sigma > \sqrt{m}\omega(\sqrt{lgm})$; $D_{m\times m}$ is defined as the distribution on full rank matrices $\{A_i = [a_{i1}, a_{i2}, \ldots, a_{im}]\} \in Z_q^{m\times m}$, where $a_{ij} \sim D_{Z^m,\sigma,0}$ for all $j \in [m]$.

BasisDel (A, R, S_A, σ). Let $q > 2$, $A \in R_q^{n\times m}$, R a matrix (or a product of d matrices) sampled from $D_{m\times m}$, and S_A a basis of $\Lambda^{\perp}(A)$; the algorithm BasisDel (A, R, S_A, σ) outputs a random basis B for $\Lambda^{\perp}(AR^{-1})$, such that $\|\widetilde{B}\| \leq \sigma\sqrt{m}$, where $\sigma \geq \|\widetilde{S_A}\| m^d \omega(lg^{d+1}(m))$.

SampleRwithBasis (A). For $q > 2$, $m > 5nlgq$, and $A \in R_q^{n\times m}$, the algorithm SampleRwithBasis (A) outputs a random matrix $R \sim D_{m\times m}$ and a basis B for $\Lambda^{\perp}(AR^{-1})$, such that $\|\widetilde{B}\| \leq \sqrt{m}$.

3. Proxy Blind Signature

A proxy blind signature [4, 9–11] is considered to be the combination of proxy signature and blind signature. It consists of four participants: an original signer, a proxy blind signer, a user, and a verifier and the following four algorithms: keygen, generation of the proxy key, proxy signature generation, and verification. A proxy blind signature scheme should satisfy the following requirements.

Distinguishability. Proxy signatures are distinguishable from normal signatures by everyone.

Verifiability. From the proxy signature, the verifier can be convinced of the original signers agreement on the signed message.

Strong Nonforgeability. A designated proxy signer can create a valid proxy signature for the original signer. But the original signer and other third parties who are not designated as a proxy signer cannot create a valid proxy signature.

Strong Identifiability. Anyone can determine the identity of the corresponding proxy signer from the proxy signature.

Strong Nondeniability. Once a proxy signer creates a valid proxy signature of an original signer, he/she cannot repudiate the signature creation.

Prevention of Misuse. The proxy signer cannot use the proxy key for purposes other than generating a valid proxy signature. That is, he/she cannot sign messages that have not been authorized by the original signer.

Blindness Property. A signer cannot distinguish, except with negligible probability, the order in which he/she issued signatures.

4. A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model

We introduce our lattice-based identity-based proxy blind signature scheme in the standard model in this section which needs the following parameters.

Let n be a prime number, and $m \geq 2nlgq$, $q \geq \beta\omega(lgn)$, and $\beta = poly(n)$. A bound $\widetilde{L} = O(nlgq)$, the Gaussian parameter $\sigma = \widetilde{L}\omega(lgn)$, and a hash function H that outputs matrices in $Z_q^{m\times m}$ is

$$H : \{0,1\}^* \longrightarrow Z_q^{m\times m}, \quad H(\mathrm{ID}) \sim D_{m\times m}. \tag{4}$$

The original signer A and the proxy blind signer B have the identity ID_1 and the identity ID_2, respectively, and the details are described as follows.

Setup. Given the security parameter n, the PKG runs TrapGen(1^n) to generate a matrix $A_0 \in Z_q^{n\times m}$ and a corresponding short basis S_0 of $\Lambda^{\perp}(A_0)$. Let S_0 be the master secret key and let A_0 be the master public key. The following construction assumes that messages M are arbitrary d-bit strings in $\{0,1\}^d$, choosing d independent matrices $C_1, C_2, \ldots, C_d \in Z_q^n$. Publish the system public parameters $PK = \langle A_0, C_1, C_2, \ldots, C_d\rangle$ and keep the master key S_0 secret.

KeyGen. On input of an identity ID_i $(i = 1, 2)$, the PKG runs BasisDel $(A_0, H(\mathrm{ID}_i), S_0, \sigma)$ to generate a private key S_i for ID_i $(i = 1, 2)$, where S_i is a random basis for $\Lambda^{\perp}(A_0(H(\mathrm{ID}_i))^{-1})$ and $\|\widetilde{S_i}\| \leq \sigma\sqrt{m}$.

Generation of the Proxy Key. The original signer A chooses the identity ID_2 of the proxy signer B and then runs BasisDel $(A_0(H(\mathrm{ID}_1))^{-1}, H(\mathrm{ID}_2), S_1, \sigma)$ to generate S_δ, where S_δ is a random basis for $\Lambda^{\perp}(A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1})$ and $\|\widetilde{S_\sigma}\| \leq \sigma\sqrt{m}$. Then the original signer A sends S_δ to the proxy signer B as the proxy key.

Proxy Blind Signature. Suppose that M is the message to be signed, and the proxy signer B and the user C compute the signature as follows.

(1) Blinding: the user C chooses uniformly $t \in D = \{t \in R \mid \|t\| \geq 1/\sigma\}$ and samples $t_1, t_2 \sim D_{Z^m,\sigma}$ using *SampleD*, where the distribution of

$A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}t_1$ and $A_0(H(\mathrm{ID}_2))^{-1}t_2$ is uniform over Z_q^n. Then computes

$$\mu_1 = t\sum_{i=1}^{d}(-1)^{M[i]}C_i + A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}t_1; \quad (5)$$

$$\mu_2 = t\sum_{i=1}^{d}(-1)^{M[i]}C_i + A_0(H(\mathrm{ID}_2))^{-1}t_2. \quad (6)$$

At last, he/she sends (μ_1, μ_2) to the proxy signer B.

(2) Signing: if $(\mu_1, \mu_2, e'_1, e'_2)$ is in the local storage, B outputs (e'_1, e'_2); otherwise, B chooses nonzero vectors as follows:

$$\begin{gathered} e'_1 \longleftarrow \text{SamplePre}\left(A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}, S_\delta, \mu_1, \sigma\right), \\ e'_2 \longleftarrow \text{SamplePre}\left(A_0(H(\mathrm{ID}_2))^{-1}, S_2, \mu_2, \sigma\right), \end{gathered} \quad (7)$$

and then checks up $\|e'_1\| \le \sigma\sqrt{m}$ and $\|e'_2\| \le \sigma\sqrt{m}$, and if not, B chooses e'_1 and e'_2 again, stores $(\mu_1, \mu_2, e'_1, e'_2)$ in the local storage, and sends (e'_1, e'_2) to C.

(3) Unblinding: after receiving (e'_1, e'_2), the user C computes

$$\begin{gathered} e_1 = t^{-1}\left(e'_1 - t_1\right), \\ e_2 = t^{-1}\left(e'_2 - t_2\right), \end{gathered} \quad (8)$$

and then he/she outputs (M, e_1, e_2).

Verification. A verifier can accept the proxy blind signature (M, e_1, e_2) if and only if:

(1) $e_1 \ne 0$, and $\|e_1\| \le 2\sigma^2\sqrt{m}$;

(2) $e_2 \ne 0$, and $\|e_2\| \le 2\sigma^2\sqrt{m}$;

(3) $A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}e_1 = \sum_{i=1}^{d}(-1)^{M[i]}C_i$;

(4) $A_0(H(\mathrm{ID}_2))^{-1}e_2 = \sum_{i=1}^{d}(-1)^{M[i]}C_i$.

5. Analysis of the Proposed Scheme

5.1. Completeness. For the proxy blind signature (M, e_1, e_2), we have

(1)

$$\begin{aligned} \|e_1\| &= \left\|t^{-1}\left(e'_1 - t_1\right)\right\| = \left(\frac{1}{|t|}\right)\left\|\left(e'_1 - t_1\right)\right\| \\ &\le \sigma\left(\left\|e'_1\right\| + \left\|t_1\right\|\right) \le \sigma \times (2\sigma\sqrt{m}) = 2\sigma^2\sqrt{m}, \end{aligned} \quad (9)$$

(2)

$$\begin{aligned} \|e_2\| &= \left\|t^{-1}\left(e'_2 - t_2\right)\right\| = \left(\frac{1}{|t|}\right)\left\|\left(e'_2 - t_2\right)\right\| \\ &\le \sigma\left(\left\|e'_2\right\| + \left\|t_2\right\|\right) \le \sigma \times (2\sigma\sqrt{m}) = 2\sigma^2\sqrt{m}, \end{aligned} \quad (10)$$

(3)

$$\begin{aligned} &A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}e_1 \\ &\quad = A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}\left[t^{-1}\left(e'_1 - t_1\right)\right] \\ &\quad = t^{-1}A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}\left(e'_1 - t_1\right) \\ &\quad = t^{-1}\left[\mu_1 - A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}t_1\right] \\ &\quad = t^{-1}\left[t\sum_{i=1}^{d}(-1)^{M[i]}C_i\right] = \sum_{i=1}^{d}(-1)^{M[i]}C_i, \end{aligned} \quad (11)$$

(4)

$$\begin{aligned} &A_0(H(\mathrm{ID}_2))^{-1}e_2 \\ &\quad = A_0(H(\mathrm{ID}_2))^{-1}\left[t^{-1}\left(e'_2 - t_2\right)\right] \\ &\quad = t^{-1}A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}\left(e'_2 - t_2\right) \\ &\quad = t^{-1}\left[\mu_2 - A_0(H(\mathrm{ID}_2))^{-1}t_2\right] \\ &\quad = t^{-1}\left[t\sum_{i=1}^{d}(-1)^{M[i]}C_i\right] = \sum_{i=1}^{d}(-1)^{M[i]}C_i. \end{aligned} \quad (12)$$

5.2. Analysis of Security. Our proxy blind signature scheme satisfies all the requirements stated in Section 3 based on the hardness assumption of SIS problem and ISIS problem. We proof only blindness property and strong nonforgeability.

Theorem 4 (blindness). *The proxy blind signature scheme above is* $(\infty, 0)$*-blind [15].*

Proof. The proxy signer cannot relate the message M and blinded message (μ_1, μ_2) by definition; the statistical distance is

$$\begin{aligned} &\Delta\left(\sum_{i=1}^{d}(-1)^{M[i]}C_i, \mu_1\right) \\ &\quad = \frac{1}{2}\sum_{c \in Z_q^n}\left|\text{prob}\left(\sum_{i=1}^{d}(-1)^{M[i]}C_i = c\right) - \text{prob}\left(\mu_1 = c\right)\right|, \end{aligned} \quad (13)$$

because $C_1, C_2, \ldots, C_d \in Z_q^n$ is uniformly random chosen from Z_q^n, so $\text{prob}(\sum_{i=1}^{d}(-1)^{M[i]}C_i = c)$ is $(1/2)^n$. Because $\mu_1 = t\sum_{i=1}^{d}(-1)^{M[i]}C_i + A_0(H(\mathrm{ID}_1))^{-1}(H(\mathrm{ID}_2))^{-1}t_1$ and $t_1 \sim D_{Z^m,\sigma}$, $\text{prob}(\mu_1 = c)$ is close to $(1/2)^n$. Thus, $\Delta(\sum_{i=1}^{d}(-1)^{M[i]}C_i, \mu_1)$ is close to 0. Similarly, $\Delta(\sum_{i=1}^{d}(-1)^{M[i]}C_i, \mu_2)$ is close to 0. So the proxy signer cannot relate the message M and blinded message (μ_1, μ_2). □

Theorem 5. *The proxy blind signature scheme in this paper is existentially unforgeable under chosen-message attack.*

Proof. If an adversary F breaks existentially unforgeability under chosen-message attack of the proxy blind signature scheme in this paper with probability ε, makes at most q_e ($q_e > 2$) extraction queries and q_s signature queries, then there is a *PPT* algorithm T attacking the SIS problem with probability negligibly close to

$$\left(1-2^{-\omega(lgm)}\right)\left(1-\frac{1}{A_{q_e}^{2}}\right)\varepsilon. \tag{14}$$

□

Setup. At first, algorithm T chooses randomly a matrix B in $Z_q^{n\times m}$ and generates

$$\left(R_1,T_1\right) \longleftarrow \text{SampleRwithBasis}\,(B)\,, \tag{15}$$

where $R_1 \sim D_{m\times m}$, T_1 is a basis for $\Lambda^{\perp}(BR_1^{-1})$, and $\|\widetilde{T_1}\| \le \sqrt{m}$. Then, choose $R_2 \sim D_{m\times m}$ and run BasisDel $(BR_1^{-1},R_2,T_1,\sigma)$ to generate S_0, where S_0 is a random basis for $\Lambda^{\perp}(BR_1^{-1}R_2^{-1})$. Set $A_0 = BR_1^{-1}R_2^{-1}$, and then let S_0 be the master secret key and let A_0 be the master public key. Next, sample d nonzero vectors $E_1,E_2,\ldots,E_d \sim D_{Z^m,\sigma^2/d,0}$, using SampleD($1^m$) (if $\|E_i\| > (\sigma^2\sqrt{m})/d$, choose E_i again for $i = 1,2,\ldots,d$) and choose $q_e - 2$ independent nonsingular matrices $R_3,R_4,\ldots,R_{q_e} \sim D_{m\times m}$ in $Z_q^{m\times m}$. Finally, let $C_i = BE_i$ for $i=1,2,\ldots,d$. We know that C_i is statistically close to uniform over Z_q^n.

Algorithm T sends the system parameters

$$PK = \left\langle A_0, C_1, C_2, \ldots, C_d \right\rangle \tag{16}$$

to adversary F and keeps the master key S_0 secret.

Extraction Queries. When the secret key of the identity ID_i is queried for $i = 1,2,\ldots,q_e$, algorithm T lets $H(\mathrm{ID}_i) = R_i^{-1}$, runs BasisDel $(A_0, H(\mathrm{ID}_i), S_0, \sigma)$ to generate S_i, and stores (ID_i, S_i) and sends S_i to the adversary F. (If the secret key was previously queried on ID_i, T looks up (ID_i, S_i) in its local storage and returns S_i to F.)

Proxy Key Queries. After receiving $(\mathrm{ID}_i, \mathrm{ID}_j)$, where ID_i is the identity of the original signer and ID_j is the identity of the proxy signer, algorithm T returns

$$S_{\delta}^{i,j} \longleftarrow \text{BasisDel}\left(A_0\left(H\left(\mathrm{ID}_i\right)\right)^{-1},\left(H\left(\mathrm{ID}_j\right)\right),S_i,\sigma\right) \tag{17}$$

to F. Of course, $S_{\delta}^{i,j}$ is a random basis for

$$\Lambda^{\perp}\left(A_0\left(H\left(\mathrm{ID}_1\right)\right)^{-1}\left(H\left(\mathrm{ID}_2\right)\right)^{-1}\right) = \Lambda^{\perp}\left(A_0R_iR_j\right). \tag{18}$$

Signature Queries. When algorithm T receives $(\mathrm{ID}_i, \mathrm{ID}_j, \mu_{1,M}, \mu_{2,M})$, where ID_i is the identity of the original signer, ID_j is the identity of the proxy signer, and $(\mu_{1,M}, \mu_{2,M})$ is the blinded message of M, he/she generates blinded signature $(e'_{1,M}, e'_{2,M})$ for $(\mu_{1,M}, \mu_{2,M})$ (blinded message of M) as follows.

If $(\mathrm{ID}_i, \mathrm{ID}_j, \mu_{1,M}, \mu_{2,M})$ was queried previously, T looks up $(\mathrm{ID}_i, \mathrm{ID}_j, \mu_{1,M}, \mu_{2,M}, e'_{1,M}, e'_{2,M})$ in its local storage and returns $(e'_{1,M}, e'_{2,M})$ as the proxy signature to F; otherwise, T chooses nonzero vectors

$$\begin{aligned} e'_{1,M} &\longleftarrow \text{SamplePre}\left(A_0H\left(\mathrm{ID}_i\right)^{-1}H\left(\mathrm{ID}_j\right)^{-1}, S_{\delta}^{i,j}, \mu_{1,M}, \sigma\right), \\ e'_{2,M} &\longleftarrow \text{SamplePre}\left(A_0H\left(\mathrm{ID}_j\right)^{-1}, S_j, \mu_{2,M}, \sigma\right). \end{aligned} \tag{19}$$

Then T checks up $\|e'_{1,M}\| \le \sigma\sqrt{m}$ and $\|e'_{2,M}\| \le \sigma\sqrt{m}$, and if not, it chooses $e'_{1,M}$ and $e'_{2,M}$ again and then stores $(\mathrm{ID}_i, \mathrm{ID}_j, \mu_{1,M}, \mu_{2,M}, e'_{1,M}, e'_{2,M})$ in the local storage and sends $(e'_{1,M}, e'_{2,M})$ to adversary F.

After receiving $(e'_{1,M}, e'_{2,M})$, adversary F removes the blind factor to get the proxy blind signature $(\mathrm{ID}_i, \mathrm{ID}_j, M, e_{1,M}, e_{2,M})$.

Forgery. Finally, if the adversary F outputs a valid forgery $(\mathrm{ID}_i, \mathrm{ID}_j, \mathrm{M}, e_{1,M}, e_{2,M})$ with probability ε, we have

(1) $e_{1,M} \neq 0$, and $\|e_{1,M}\| \le 2\sigma^2\sqrt{m}$;

(2) $e_{2,M} \neq 0$, and $\|e_{2,M}\| \le 2\sigma^2\sqrt{m}$;

(3) $A_0(H(\mathrm{ID}_i))^{-1}(H(\mathrm{ID}_j))^{-1}e_{1,M} = \sum_{i=1}^{d}(-1)^{M[i]}C_i$;

(4) $A_0(H(\mathrm{ID}_j))^{-1}e_{2,M} = \sum_{i=1}^{d}(-1)^{M[i]}C_i$.

If $i \neq 2$ or $j \neq 1$, we abort. Otherwise, if $i = 2$ and $j = 1$, we have

$$A_0\left(H\left(\mathrm{ID}_i\right)\right)^{-1}\left(H\left(\mathrm{ID}_j\right)\right)^{-1} = BR_1^{-1}R_2^{-1}R_2R_1 = B. \tag{20}$$

Because

$$A_0\left(H\left(\mathrm{ID}_i\right)\right)^{-1}\left(H\left(\mathrm{ID}_j\right)\right)^{-1}e_{1,M} = \sum_{i=1}^{d}(-1)^{M[i]}C_i \tag{21}$$

and $C_i = BE_i$, we can get $Be_{1,M} = \sum_{i=1}^{d}(-1)^{M[i]}C_i = \sum_{i=1}^{d}(-1)^{M[i]}BE_i = B\sum_{i=1}^{d}(-1)^{M[i]}E_i$. Let $E_M = \sum_{i=1}^{d}(-1)^{M[i]}E_i$, and then $Be_{1,M} = BE_M$ and $\|E_M\| \le \sum_{i=1}^{d}\|E_i\| \le d\times(\sigma^2\sqrt{m})/d = \sigma^2\sqrt{m}$, so

$$\begin{aligned} B\left(e_{1,M}-E_M\right) &= 0 \mod q, \\ \left\|e_{1,M}-E_M\right\| &\le \left\|e_{1,M}\right\| + \left\|E_M\right\| \\ &\le 2\sigma^2\sqrt{m} + \sigma^2\sqrt{m} = 3\sigma^2\sqrt{m}. \end{aligned} \tag{22}$$

Thus, T outputs $e_{1,M} - E_M$ as a solution to the SIS problem with $(q, m, 3\sigma^2\sqrt{m}, B)$.

We now analyze the reduction: by the preimage min-entropy property of the hash family, thus the signature $e_{1,M} = E_M$ with negligible probability $2^{-\omega(lgm)}$. The adversary F outputs the valid forgery $(\mathrm{ID}_i, \mathrm{ID}_j, M, e_{1,M}, e_{2,M})$ with probability ε, and prob$(i = 2, j = 1) = 1/A_{q_e}^2$, so $e_{1,M} - E_M$ is a solution to the SIS problem with $(q, m, 3\sigma^2\sqrt{m}, B)$ with probability negligibly close to

$$\left(1-2^{-\omega(lgm)}\right)\left(1-\frac{1}{A_{q_e}^{2}}\right)\varepsilon. \tag{23}$$

Table 1: Comparison between schemes [21, 22] and our scheme.

Schemes	[21]	[22]	This work
The length of public keys	3 mn	3 mn	mn + dm
The length of secret keys	5 m^2	5 m^2	m^2
The length of signature	2 m	6 m	2 m

5.3. Efficiency Analysis. The efficiency of signature scheme is mainly considered to include the length of public keys, secret keys, and signatures. The lattice-based special signature scheme [21, 22] is also provably secure; however, the private keys and the signatures in these schemes are dependent on the identity length of the signer. In contrast, the size of private keys and the size of signature in our scheme are both unchanged and much shorter. Therefore, our scheme is more practical. Table 1 shows the comparison of the schemes.

6. Conclusions

In this paper, we have constructed a new lattice-based proxy blind signature scheme with short secret keys and short signatures in the standard model. Our signature scheme is more efficient than other current proxy blind signature schemes, and the security mainly depends on hard problems on lattices, so this scheme in this paper is still secure in quantum computing environment.

Conflict of Interests

The authors declared that they have no conflict of interests regarding this work.

Acknowledgments

This work was supported by Scientific Research Project Fund of Science and Technology Bureau of Zhengzhou (no. 20140713) and the project of science and technology office of Henan province (no. 142300410342). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] D. Chaum, “Blind signat ures for untraceable payments,” in *Proceedings of CRYPTO 82*, pp. 199–203, 1982.

[2] M. Mambo, K. Usuda, and E. Okamoto, “Proxy signatures for delegating signing operation,” in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pp. 48–56, ACM Press, March 1996.

[3] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Advances in Cryptology*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, Springer, Berlin, Germany, 1985.

[4] W. D. Lin and J. K. Jan, “A security personal learning tools using a proxy blind signature scheme,” in *Proceedings of International Conference on Chinese Language Computing*, pp. 273–277, Chicago, Ill, USA, 2000.

[5] A. K. Awasthi and S. Lal, “Proxy blind signature scheme,” *Transaction on Cryptology*, vol. 2, no. 1, pp. 5–11, 2005.

[6] H. M. Sun, B. T. Hsieh, and S. M. Tseng, “On the security of some proxy blind signature schemes,” *Journal of Systems and Software*, vol. 74, no. 3, pp. 297–302, 2005.

[7] F. Zhang, R. Safavi-Naini, and C.-Y. Lin, “New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairing,” Cryptology ePrint Archive, 2003, http://eprint.iacr.org/2003/104.

[8] D. Zheng, Z. Huang, K. Chen, and W. D. Kou, “Id-based proxy blind signature,” in *Proceedings of the 18th International Conference on Advanced Information and Applications*, vol. 74, pp. 380–383, IEEE Computer Society, 2004.

[9] W. Lang, Z. Yang, and Y. Tang, “An identity-bas ed proxy blind signature scheme from bilinear pairings,” *Asian Journal of Information Technology*, vol. 3, no. 10, pp. 839–842, 2004.

[10] Q. Zhang, Q. Wen, and G. Chen, “Efficient ID-based proxy blind signature scheme,” *Wuhan University Journal of Natural Sciences*, vol. 12, no. 1, pp. 105–108, 2007.

[11] M. Yang and Y. Wang, “A new efficient ID-based proxy blind signature scheme,” *Journal of Electronics*, vol. 25, no. 2, pp. 226–231, 2008.

[12] M. Ajtai, “Generating hard instances of lattice problems,” in *Proceedings of the STOC*, pp. 99–108, New York, NY, USA, 1996.

[13] O. Regev, “Lattice-based cryptography,” in *Advances in Cryptology (CRYPTO ’06)*, vol. 4117 of *Lecture Notes in Computer Science*, pp. 131–141, 2006.

[14] G. Craig, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” in *Proceedings of the S-TOC*, pp. 197–206, 2008.

[15] M. Rückert, “Lattice-based blind signatures,” in *Advances in Cryptology—ASIACRYPT 2010*, vol. 6477 of *Lecture Notes in Computer Science*, pp. 413–430, Springer, Berlin, Germany, 2010.

[16] S. D. Gordon, J. Katz, and V. Vaikuntanathan, “A group signature scheme from lattice assumptions,” in *Advances in Cryptology—ASIACRYPT 2010*, vol. 6477 of *Lecture Notes in Computer Science*, pp. 395–412, Springer, Berlin, Germany, 2010.

[17] M. Rückert, “Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles,” in *Post-Quantum Cryptography*, vol. 6061 of *Lecture Notes in Computer Science*, pp. 182–200, Springer, Berlin, Germany, 2010.

[18] Y. Jiang, F. Kong, and X. Ju, “Lattice-based proxy signature,” in *Proceeding of the International Conference on Computational Intelligence and Security (CIS '10)*, pp. 382–385, Nanning, China, December 2010.

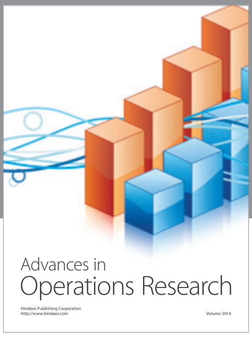
[19] M. Tian and L. Huang, “Breaking a proxy signature scheme from lattices,” *International Journal of Network Security*, vol. 14, no. 6, pp. 320–323, 2012.

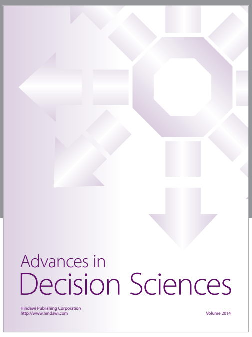
[20] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, “Bonsai trees, or how to delegate a lattice basis,” in *Advances in Cryptology—EUROCRYPT 2010LNCS*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 523–552, 2010.

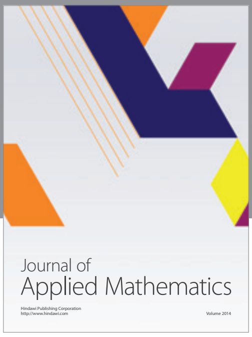
[21] L. L. Zhang and Y. Sang, “A lattice-based identity-based proxy signature from bonsai trees,” *International Journal of Advancements in Computing Technology*, vol. 4, no. 20, pp. 99–104, 2012.

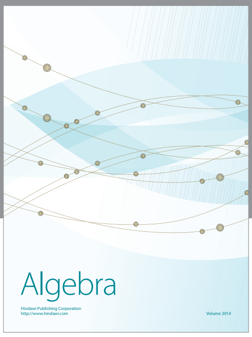
[22] F. Xia, B. Yang, S. Ma, H. Sun, and M. Zhang, “Lattice-based proxy signature scheme,” *Journal of Hunan University*, vol. 38, no. 6, pp. 84–88, 2011.

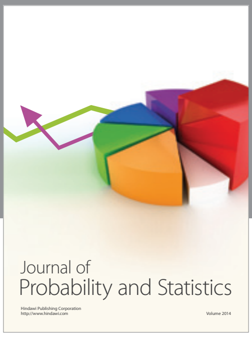
[23] S. Agrawal, D. Boneh, and X. Boyen, “Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE,” in *Advances in Cryptology—CRYPTO 2010*, vol. 6223 of *Lecture Notes in Computer Science*, pp. 98–115, Springer, Berlin, Germany, 2010.


Advances in
Operations Research

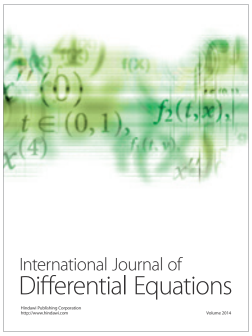

Advances in
Decision Sciences


Journal of
Applied Mathematics

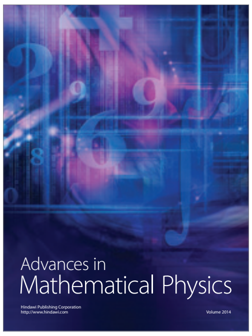

Algebra

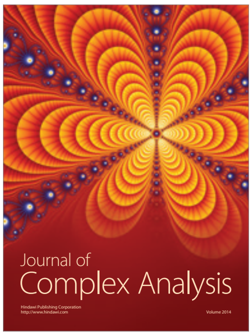

Journal of
Probability and Statistics

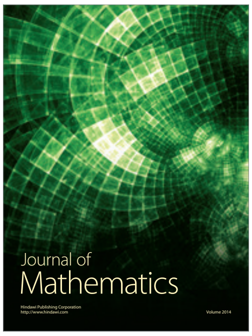
The Scientific
World Journal

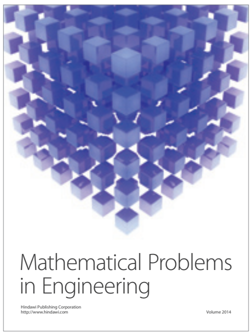

International Journal of
Differential Equations

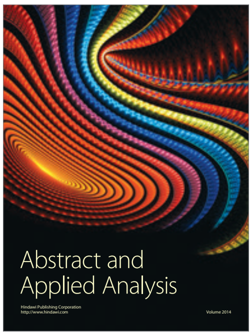
International Journal of
Combinatorics

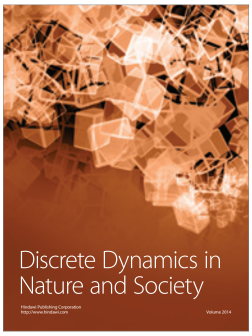

Advances in
Mathematical Physics

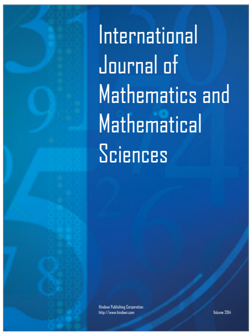

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

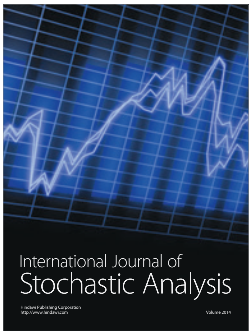

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization