Double Validation Multi Level Proxy Blind Signature Scheme Key Management

Wang Jin-feng¹

¹Chongqing College of Electronic Engineering, Chongqing, 401331, China
E-mail: 77011405@qq.com

Abstract

Identity-based signature (IBS) scheme can be widely used in resource-limited situations such as mobile e-commerce. In this paper, a lattice-based IBS scheme is first established by using trapdoor generation algorithm GenTrap, preimage sample algorithm SampleD and trapdoor delegated algorithm DelTrap put forward by Micciancio and Peikert in Eurocrypt'12; then the proposed scheme is proven to satisfy strong unforgeability against selective ID and static chosen message attack in the standard model based on small integer solutions (SIS); and finally the proposed scheme is compared with the existing similar scheme in computing performance. The results show that the scheme presented in this paper enjoys the highest efficiency.

Keywords: Signature; Identity based; Strong unforgeability; Lattice

1. Introduction

Identity-based cryptography (IBC) system [1] can be widely used in a variety of resource-limited situations. At present, people have designed a large number of identity-based cryptography schemes by using bilinear pairings, such as identity-based encryption scheme [2], identity-based signature (IBS) scheme [3]. However, due to low efficiency of bilinear pairings, people have always tried to seek other ways to build IBC scheme and the lattice-based cryptography system is one of a few anti-quantum computing classic key cryptosystems. As the advent of quantum computer is only a matter of time, the lattice-based cryptography system has raised widespread public attention. Especially, design and analysis of the lattice-based IBC scheme have attracted much more attention.

Ajtai [4] defined small integer solutions (SIS) in STOC'96 and creatively proved that this question is difficult in the average situation. In 1999, Ajtai [5] proposed a trapdoor generation algorithm, which was improved by Alwen and Peikert [6] in 2009[5]. Gentry and Peikert [7] put forward a preimage sample containing trapdoor one-way function based on SIS in STOC'08, and established a lattice-based signature scheme accordingly, which is unforgeable in the random oracle model. Based on the preimage sample trapdoor function[7] of Gentry *et. al.*, Cash and Hofheinz [8] proposed a lattice-based delegation technology in Eurocrypt'10, and established a lattice-based signature scheme accordingly, which is existential unforgeable in the standard model. By defining a new trapdoor concept, Micciancio and Peikert [9] designed a simple but efficient trapdoor generation algorithm GenTrap, preimage sample algorithm SampleD and trapdoor delegated algorithm DelTrap in Eurocrypt'12, and established an efficient lattice-based signature scheme accordingly, which is unforgeable in the standard model.

Recently, using the preimage sample trapdoor function proposed by Gentry *et. al.*, Xia and Yang [10] have established a lattice-based IBS scheme and proven that this scheme is existential unforgeable in the random oracle model; based on the lattice-based delegation technology presented by Cash, *et. al.*, [8], Liu and Hu [11] have

established a lattice-based IBS scheme and proven that this scheme is unforgeable in the standard model. In this paper, according to the algorithms given by Micciancio, *et. al.*, [10], an efficient lattice-based IBS scheme is established and the proposed IBS scheme is proven to be unforgeable in the standard model. Compared with other existing similar IBS schemes, the scheme presented by this paper is much more highly effective.

2. Pre-requisites

2.1. Lattice

Definition 1 Let $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m \in \mathbf{R}^m$ be a set of linear independent vectors, the $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m] \in \mathbf{R}^{m \times m}$ based lattice Λ and its dual lattice Λ^* are defined as

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

$$\Lambda^* = \left\{ \mathbf{z} \in \mathbf{R}^m : \forall \mathbf{y} \in \Lambda, \mathbf{z}'\mathbf{y} = \langle \mathbf{z}, \mathbf{y} \rangle \in \mathbf{Z} \right\}.$$

Definition 2 For integer q and matrix $\mathbf{A} \in \mathbf{Z}_q^{n \times m}$, two integer lattices are defined as

$$\Lambda^\perp(\mathbf{A}) = \left\{ \mathbf{e} \in \mathbf{Z}^m : \mathbf{A}\mathbf{e} = \mathbf{0} \bmod q \right\},$$

$$\Lambda(\mathbf{A}) = \left\{ \mathbf{y} \in \mathbf{Z}^m : \exists \mathbf{s} \in \mathbf{Z}^n, \mathbf{y} = \mathbf{A}'\mathbf{s} \bmod q \right\}.$$

These two defined are in dual relationship, namely $\Lambda^\perp(\mathbf{A}) = q\Lambda(\mathbf{A})^*$, $\Lambda(\mathbf{A}) = q\Lambda^\perp(\mathbf{A})^*$.

2.2. SIS

Definition 3 If integer q , matrix $\mathbf{A} \in \mathbf{Z}_q^{n \times m}$ and real number β are given to solve a nonzero integer vector $\mathbf{v} \in \mathbf{Z}^m$, where $\|\mathbf{v}\| \leq \beta$, $\mathbf{A}\mathbf{v} = \mathbf{0} \bmod q$, namely $\mathbf{v} \in \Lambda^\perp(\mathbf{A})$, the this question is of SIS.

2.3. Discrete Gaussian Distribution

Definition 4 For any vector $\mathbf{c} \in \mathbf{R}^n$, real number $s > 0$ and n -dimension lattice Λ , the Gaussian distribution of $\mathbf{R}^n$ is defined as $\forall \mathbf{x} \in \mathbf{R}^n$, $\rho_{s,\mathbf{c}}(\mathbf{x}) = \exp(-\pi \|\mathbf{x} - \mathbf{c}\|^2 / s^2)$, where $\mathbf{c}$ is the center and s is the standard deviation. When subscripts s and $\mathbf{c}$ are 1 and $\mathbf{0}$ respectively, they can be omitted.

Definition 5 For any vector $\mathbf{c} \in \mathbf{R}^n$, real number $s > 0$ and n -dimension lattice Λ , discrete Gaussian distribution of Λ is defined as $\forall \mathbf{x} \in \Lambda$, $D_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \rho_{s,\mathbf{c}}(\mathbf{x}) / \rho_{s,\mathbf{c}}(\Lambda)$, where $\rho_{s,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x} \in \Lambda} \rho_{s,\mathbf{c}}(\mathbf{x})$. The same as the case above, subscripts s and $\mathbf{c}$ can also be omitted.

Definition 6 For any n -dimension lattice Λ and real number $\varepsilon > 0$, if the smooth parameter $\eta_\varepsilon(\Lambda)$ is the smallest real number $s > 0$, $\sum_{\mathbf{0} \neq \mathbf{x} \in \Lambda} \rho_{1/s}(\mathbf{x}) \leq \varepsilon$. Popularly speaking, the smooth parameter $\eta_\varepsilon(\Lambda)$ refers to magnitude of Gaussian noise size $s > 0$ that must be added in order to get uniform on Λ .

2.4. Important Conclusions

Lemma 7 (Literature [7]) For any n -dimension lattice Λ and real number $\varepsilon > 0$,

$$\eta_\varepsilon(\Lambda) \leq bl(\Lambda) \cdot \sqrt{\log(2n(1+1/\varepsilon)) / \pi}$$

So for any function $\omega(\sqrt{\log n})$, there is negligible $\varepsilon(n)$ allowing $\eta_\varepsilon(\Lambda) \leq bl(\Lambda) \cdot \omega(\sqrt{\log n})$, where $bl(\Lambda) = \min_{\mathbf{B}} \|\mathbf{B}\| = \min_{\mathbf{B}} \max_{i \in [n]} \|\mathbf{b}_i\|$.

Lemma 8 (Literature [7]) There is a probabilistic polynomial time algorithm inputting the base $\mathbf{B}$ of n -dimension lattice Λ , real number $s \geq \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$ and vector $\mathbf{c} \in \mathbb{R}^n$ to output samples depending on distribution $D_{\Lambda, s, \mathbf{c}}$.

Lemma 9 (Literature [12]) For any n -dimension lattice Λ , vector $\mathbf{c} \in \mathbb{R}^n$ and real number $0 < \varepsilon < 1$ and $s \geq \eta_\varepsilon(\Lambda)$,

$$\Pr_{\mathbf{x} \sim D_{\Lambda, s, \mathbf{c}}} [\|\mathbf{x} - \mathbf{c}\| > s\sqrt{n}] \leq \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n}$$

Lemma 10 (Literature [9]) Suppose $\mathbf{X} \in \mathbb{R}^{n \times m}$ is sub-Gaussian random matrix δ and know its parameter s , there is a universal constant $C > 0$ allowing singular value $s_1(\mathbf{X}) \leq C \cdot s \cdot (\sqrt{m} + \sqrt{n} + t)$ of matrix $\mathbf{X}$ for any $t \geq 0$, but the probability for this formula to be false is $2 \exp(\delta) \exp(-\pi t^2)$ at most.

Lemma 11 (Literature [9]) Let $\mathbf{S} \in \mathbb{Z}^{w \times w}$ be the base of $\Lambda^\perp(\mathbf{G})$, $\mathbf{R} \in \mathbb{Z}^{(m-w) \times w}$ be the trapdoor of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and its mark be $\mathbf{H} \in \mathbb{Z}_q^{n \times m}$, the lattice $\Lambda^\perp(\mathbf{A})$ can be got from $\mathbf{S}_\mathbf{A} = \begin{bmatrix} \mathbf{I} & \mathbf{R} \\ \mathbf{0} & \mathbf{I} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{W} & \mathbf{S} \end{bmatrix}$, where $\mathbf{W} \in \mathbb{Z}^{w \times m}$ is any solution to $\mathbf{G}\mathbf{W} = -\mathbf{H}^{-1}\mathbf{A}[\mathbf{I}|\mathbf{0}]^T \pmod{q}$. And when $\mathbf{S}_\mathbf{A}$ is in proper order, $\mathbf{S}_\mathbf{A}$ satisfies $\|\mathbf{S}_\mathbf{A}\| \leq s_1 \left(\begin{bmatrix} \mathbf{I} & \mathbf{R} \\ \mathbf{0} & \mathbf{I} \end{bmatrix} \right) \cdot \|\tilde{\mathbf{S}}\| \leq (s_1(\mathbf{R}) + 1) \cdot \|\tilde{\mathbf{S}}\|$.

3. Formalized Definition and Security Model of IBS Schemes

3.1. Formalized Definition

An IBS scheme is composed of 4 algorithms including system parameter generation algorithm Setup, private key extraction algorithm Extract, signature algorithm Sign and signature verification algorithm Verify. $\text{Setup}(1^n)$ outputs system parameter PP and master key MK ; $\text{Extract}(\text{MK}, id)$ outputs private key SK_{id} to user id ; $\text{Sign}(\text{SK}_{id}, \mu)$ outputs signature σ of user id to message μ ; $\text{Verify}(id, \mu, \sigma)$ outputs 1 if and only if σ is the effective signature of user id to message μ .

3.2. Security Model

According to safety concepts of selective identity proposed in literature [13] and static chosen message proposed in literature [14], we can define strong unforgeability of IBS scheme against selective ID and static chosen message attack (SU-SMA-SelectiveID). This security concept may be defined through the game between the rival $\mathbf{A}$ and the challenger $\mathbf{C}$.

Preliminary stage: $\mathbf{A}$ sends $(id^*, \mu^{(1)}, \dots, \mu^{(Q)})$ to $\mathbf{C}$, where id^* is the target identity.

Static signature reply: First $\mathbf{C}$ runs $\text{Setup}(1^n)$ to output PP and MK , then runs $\text{Extract}(\text{MK}, id^*)$ to output SK_{id^*} , runs $\text{Sign}(\text{SK}_{id^*}, \mu^{(i)})(i \in [Q])$ to output $\sigma^{(i)}$, and finally sends PP and signature $(id^*, \mu^{(i)}, \sigma^{(i)})(i = 1, \dots, Q)$ to $\mathbf{A}$.

Private key extraction inquiry: $\mathbf{A}$ outputs $id(id \neq id^*)$, $\mathbf{C}$ runs $\text{Extract}(\text{MK}, id)$ to output SK_{id} and sends private key SK_{id} to $\mathbf{A}$.

Other signature inquiry: $\mathbf{A}$ outputs $(id, \mu)(id \neq id^*)$, $\mathbf{C}$ runs $\text{Extract}(\text{MK}, id)$ to output SK_{id} , runs $\text{Sign}(\text{SK}_{id}, \mu)$ to output σ and sends signature (id, μ, σ) to $\mathbf{A}$.

Forge stage: $\mathbf{A}$ outputs (id^*, μ^*, σ^*) . If $\text{Verify}(id^*, \mu^*, \sigma^*) = 1$ and (id^*, μ^*, σ^*) is not the inquiry result of a signature, $\mathbf{A}$ is considered to win the game.

We define the rival A 's advantage $\text{Adv}_{A, \text{IBS}}^{\text{SU-SMA-SelectiveID}}$ as the probability of winning the above game.

Definition 12 In the above game, if there is no such rival A that its advantage is δ at least, the running time is δ at most, the number of private key extraction inquiry times is q_E at most, and the number of signature inquiry times is q_S at most, we can say that this IBS scheme is secure for (t, q_E, q_S, δ) in the SU-SMA-SelectiveID model.

4. A New Lattice-based IBS Scheme

Setup algorithm: if security parameter n and the exiting matrix $G \in \mathbb{Z}_q^{n \times nk}$ are known, Literature [9] can be referred to for its structure. Let $q = \text{poly}(n)$, $k = \lceil \log q \rceil = O(\log n)$, $\bar{m} = O(nk)$, distribution $D = D_{\mathbb{Z}, \omega(\sqrt{\log n})}^{\bar{m} \times nk}$, choice matrix $\bar{A} \leftarrow \mathbb{Z}_q^{n \times \bar{m}}$, run trapdoor generation algorithm GenTrap to output matrix $A \in \mathbb{Z}_q^{n \times (\bar{m} + nk)}$ and trapdoor $R \in \mathbb{Z}_q^{\bar{m} \times nk}$. Select any matrixes $A_i \leftarrow \mathbb{Z}_q^{n \times nk}$ ($0 \leq i \leq l$) and $B_j \leftarrow \mathbb{Z}_q^{n \times nk}$ ($0 \leq j \leq d$), where l is the length of user ID, d is the length of the message, and selection vector $u \leftarrow \mathbb{Z}_q^n$. System parameter $\text{PP} = \{A, A_0, \dots, A_l, B_0, \dots, B_d, u\}$ and the master key $\text{MK} = R$.

Extract algorithm: Suppose user $id = (b_1 b_2 \dots b_l) \in \{0, 1\}^l$, and let $A_{id} = [A | A_0 + \sum_{i=1}^l b_i A_i] \in \mathbb{Z}_q^{n \times (\bar{m} + 2nk)}$, $s' = O(\sqrt{lnk}) \cdot \omega(\sqrt{\log n})^2$, if trapdoor R of matrix A can run trapdoor delegation algorithm DelTrap to output trapdoor $R' \in \mathbb{Z}_q^{(\bar{m} + nk) \times nk}$ of matrix A_{id} , namely private key SK_{id} of id .

Sign algorithm: Suppose user $id = (b_1 b_2 \dots b_l) \in \{0, 1\}^l$, message $\mu = (\mu_1 \mu_2 \dots \mu_d) \in \{0, 1\}^d$, let $A_\mu = [A_{id} | B_0 + \sum_{j=1}^d \mu_j B_j] \in \mathbb{Z}_q^{n \times (\bar{m} + 3nk)}$, and $s = O(\sqrt{l + d}nk) \cdot \omega(\sqrt{\log n})^3$, as the trapdoor of matrix A_μ can be obtained from trapdoor of matrix A_{id} by adding zero lines, running preimage sample algorithm SampleD according to trapdoor SK_{id} of matrix A_{id} can output sample $v \in \mathbb{Z}^{\bar{m} + 3nk}$ on distribution $D_{\Lambda_{\bar{A}}^{\perp}(A_\mu), s}$, namely the signature of user id to message μ .

Verify algorithm: For signature v of user id to message μ , if $\|v\| \leq s \cdot \sqrt{\bar{m} + 3nk}$ and $A_\mu \cdot v = u$, where the definition of matrix A_μ is as stated above, the signature v is valid, otherwise, invalid.

5. Scheme Analysis

5.1. Correct

Theorem 13 the IBS scheme presented in this paper is correct.

Proof: Because $R \leftarrow D$, but $D = D_{\mathbb{Z}, \omega(\sqrt{\log n})}^{\bar{m} \times nk}$, we can know $s_1(R) \leq O(\sqrt{\bar{m}} + \sqrt{nk}) \cdot \omega(\sqrt{\log n}) = O(\sqrt{nk}) \cdot \omega(\sqrt{\log n})$ according to Lemma 10. According to Lemma 11, we can know $\|S_A\| \leq O(\sqrt{nk}) \cdot \omega(\sqrt{\log n})$, and according to Lemma 7, we can know $\eta_e(\Lambda^\perp(A)) \leq O(\sqrt{nk}) \cdot \omega(\sqrt{\log n})^2$. Besides, $s' = O(\sqrt{lnk}) \cdot \omega(\sqrt{\log n})^2$, so $s' \geq \eta_e(\Lambda^\perp(A))$, Extract algorithm is proven to be performed correctly according to Lemma 8, and according to Lemma 10 we know $s_1(R') \leq s' \cdot O(\sqrt{\bar{m} + nk} + \sqrt{nk}) = O(\sqrt{lnk}) \cdot \omega(\sqrt{\log n})^2$. As a result, $\eta_e(\Lambda^\perp(A_\mu)) \leq O(\sqrt{lnk}) \cdot \omega(\sqrt{\log n})^3$, also for $s = O(\sqrt{l + d}nk) \cdot \omega(\sqrt{\log n})^3$, $s \geq \eta_e(\Lambda^\perp(A_\mu))$ and Sign algorithm is proven to be performed correctly with $A_\mu \cdot v = u$. In addition, according to Lemma 9, we can know $\|v\| \leq s \cdot \sqrt{\bar{m} + 3nk}$. Therefore, the above IBS scheme is correct.

5.2. Secure

Theorem 14 Suppose (q, β) -SIS is difficult for (t', δ') , where $\beta = O((l+d)(nk)^2) \cdot \omega(\sqrt{\log n})^4$, the IBS scheme presented in this paper is secure for (t, q_E, q_S, δ) in the SU-SMA-SelectiveID model, where $\delta' \geq \delta/(2(d-1)q_S + 2) - \text{negl}(n)$, q_E and q_S represents the number of private key extraction inquiry times and signature inquiry times, respectively.

Proof: Suppose the rival A can break through the IBS scheme presented in this paper in the SU-SMA-SelectiveID model and enjoys advantage of δ at least, a polynomial time algorithm B can be set up for solving SIS. A can be divide into two types, one outputting forge on the message never inquiring signature and the other one outputting forge on the message inquiring signature. It is obvious that A has the probability of $\delta/2$ at least to output effective forge in any situation. The input matrix of B is $A_{\text{SIS}} = [A|u] = [\bar{A}|B|u'] \in \mathbb{Z}_q^{n \times (\bar{m} + nk + 1)}$, namely an example of SIS. In order to use A to solve this SIS example, B must simulate challenger C of A .

The process where B interacts with the rival of the first type is as follows:

Preliminary stage: B receives $(id^*, \mu^{(1)}, \dots, \mu^{(l)})$ output by A , where $id^* = (b_1^* b_2^* \dots b_l^*)$ is the target identity.

Static signature reply: B first produces public parameters $A_0, A_1, \dots, A_l$ according to the target identity id^* . For $i = 0, 1, \dots, l$, $R_i \leftarrow D$ is taken, let $A_i = H_i G - \bar{A} R_i$, where

$$H_i = \begin{cases} (-1)^{b_i^*} \cdot h(u_i) & i \in [l] \\ -\sum_{j \in [l]} b_j^* \cdot H_j & i = 0 \end{cases}.$$

For definition of ring homomorphism $h: \mathbf{R} \rightarrow \mathbb{Z}_q^{n \times n}$, Literature (9) can be referred to. It is easy to see that, if $id = id^*$, $H_0 + \sum_{i \in [l]} b_i^* H_i = \mathbf{0}$; if $id \neq id^*$, $H_0 + \sum_{i \in [l]} b_i H_i = \sum_{i \in [l]} (b_i - b_i^*) \cdot H_i = \sum_{i \in [l], b_i \neq b_i^*} (-1)^{b_i^*} \cdot H_i = h\left(\sum_{i \in [l], b_i \neq b_i^*} u_i\right)$, so if $id \neq id^*$, $H_0 + \sum_{i \in [l]} b_i H_i$ is reversible. Then message $\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(l)}$ is used to produce $B_0, B_1, \dots, B_d$. The computation string $p \in \{0, 1\}^{\leq d}$ set of B is P , but P is not a prefix of any message $\mu^{(i)} \in \{\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(l)}\}$, and P is the shortest string that satisfy these conditions. It is not hard to solve the set P , literatures can be referred to for computation with $|P| = (d-1)Q + 1$. Arbitrarily choose $p \in P$ and record $\tau = |p| \leq d$, for $i = 0, 1, \dots, d$, take $T_i \leftarrow D$, let $B_i = E_i G - \bar{A} T_i$, where

$$E_i = \begin{cases} h(0) = \mathbf{0} & i > \tau \\ (-1)^{p_i} \cdot h(w_i) & i \in [\tau] \\ -\sum_{j \in [\tau]} p_j \cdot E_j & i = 0 \end{cases}.$$

We can see that for any message μ , if μ is the prefix of p , $E_0 + \sum_{i \in [d]} \mu_i E_i = \mathbf{0}$; if μ takes r instead of p as its prefix at the position τ , $E_0 + \sum_{i \in [d]} \mu_i E_i = \sum_{i \in [\tau]} (r_i - p_i) \cdot E_i = \sum_{i \in [\tau], r_i \neq p_i} (-1)^{p_i} \cdot E_i = h\left(\sum_{i \in [\tau], r_i \neq p_i} w_i\right)$, so $E_0 + \sum_{i \in [d]} \mu_i E_i$ is reversible if μ does not take p as its prefix. B will send the produced system parameter $PP = \{A, A_0, \dots, A_l, B_0, \dots, B_d, u = u'\}$ to A .

In order to produce signature of id^* on $\mu \in \{\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(l)}\}$, B computes

$$\begin{aligned}
 \mathbf{A}_\mu &= \left[\mathbf{A}_{id^*} \middle| \mathbf{B}_0 + \sum_{i \in [d]} \mu_i \mathbf{B}_i \right] \\
 &= \left[\bar{\mathbf{A}} \mathbf{B} \middle| \mathbf{A}_0 + \sum_{i \in [l]} b_i^* \mathbf{A}_i \left(\mathbf{E}_0 + \sum_{i \in [d]} \mu_i \mathbf{E}_i \right) \mathbf{G} - \bar{\mathbf{A}} \left(\mathbf{T}_0 + \sum_{i \in [d]} \mu_i \mathbf{T}_i \right) \right] \\
 &= \left[\bar{\mathbf{A}} \mathbf{B} \middle| -\bar{\mathbf{A}} \left(\mathbf{R}_0 + \sum_{i \in [l]} b_i^* \mathbf{R}_i \right) \mathbf{E}_\mu \mathbf{G} - \bar{\mathbf{A}} \mathbf{T}_\mu \right] \\
 &= \left[\bar{\mathbf{A}} \mathbf{B} \middle| -\bar{\mathbf{A}} \mathbf{R}_{id^*} \mathbf{E}_\mu \mathbf{G} - \bar{\mathbf{A}} \mathbf{T}_\mu \right]
 \end{aligned}$$

Because the prefix of μ at the position τ is not p , $\mathbf{E}_\mu = \mathbf{E}_0 + \sum_{i \in [d]} \mu_i \mathbf{E}_i$ is reversible, $\mathbf{T}_\mu = \mathbf{T}_0 + \sum_{i \in [d]} \mu_i \mathbf{T}_i$ is the trapdoor that $\mathbf{A}_\mu$ corresponds to and $s_1(\mathbf{T}_\mu) \leq \sqrt{d+1} \cdot O(\sqrt{m} + \sqrt{nk}) \cdot \omega(\sqrt{\log n}) = O(\sqrt{dnk}) \cdot \omega(\sqrt{\log n})$. Besides, $s = O(\sqrt{l+dnk}) \cdot \omega(\sqrt{\log n})^3$, so $\mathbf{B}$ can use SampleD algorithm to produce $\mathbf{v}_\mu \leftarrow D_{\Lambda_u^+(\mathbf{A}_\mu), s}$, namely signature of user id^* on the message μ . $\mathbf{B}$ sends the produced signature $(id^*, \mu^{(i)}, \mathbf{v}_{\mu^{(i)}}) (i=1, \dots, Q)$ to $\mathbf{A}$.

Private key extraction inquiry: When the rival $\mathbf{A}$ inquires the private key to user id ($id \neq id^*$), $\mathbf{B}$ computes

$$\begin{aligned}
 \mathbf{A}_{id} &= \left[\mathbf{A} \middle| \mathbf{A}_0 + \sum_{i \in [l]} b_i \mathbf{A}_i \right] \\
 &= \left[\bar{\mathbf{A}} \mathbf{B} \middle| \left(\mathbf{H}_0 + \sum_{i \in [l]} b_i \mathbf{H}_i \right) \mathbf{G} - \bar{\mathbf{A}} \left(\mathbf{R}_0 + \sum_{i \in [l]} b_i \mathbf{R}_i \right) \right] \\
 &= \left[\bar{\mathbf{A}} \mathbf{B} \middle| \mathbf{H}_{id} \mathbf{G} - \bar{\mathbf{A}} \mathbf{R}_{id} \right]
 \end{aligned}$$

Because $\mathbf{H}_{id} = \mathbf{H}_0 + \sum_{i \in [l]} b_i \mathbf{H}_i$ is reversible, $\mathbf{R}_{id} = \mathbf{R}_0 + \sum_{i \in [l]} b_i \mathbf{R}_i$ is the trapdoor that $\mathbf{A}' = [\bar{\mathbf{A}} \mathbf{H}_{id} \mathbf{G} - \bar{\mathbf{A}} \mathbf{R}_{id}]$ corresponds to, and $s_1(\mathbf{R}_{id}) \leq \sqrt{l+1} \cdot O(\sqrt{m} + \sqrt{nk}) \cdot \omega(\sqrt{\log n}) = O(\sqrt{lnk}) \cdot \omega(\sqrt{\log n})$. Besides $s' = O(\sqrt{lnk}) \cdot \omega(\sqrt{\log n})^2$, so $\mathbf{B}$ can use DelTrap to produce the private key $\mathbf{SK}_{id}$ to user id .

Other signature inquiry: $\mathbf{A}$ inquiries signature of user $id \neq id^*$ on the message μ without loss of generality; suppose $\mathbf{A}$ has not inquired the private key to id , $\mathbf{B}$ first produces a private key just like private key extraction inquiry, and then produces signature of user id on the message μ according to Sign.

Forge stage: $\mathbf{A}$ outputs forge $(id^*, \mu^*, \mathbf{v}^*)$, and $\mu^* \notin \{\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(Q)}\}$. If limited μ^* must take p as its prefix, the probability for a rival to forge effective signature is $\delta / (2(d-1)Q+2) \geq \delta / (2(d-1)q_s+2)$ at least. In this case, $\mathbf{B}$ can solve its SIS challenge example, namely

$$\begin{aligned}
 \mathbf{A}_{\mu^*} &= \left[\mathbf{A}_{id^*} \middle| \mathbf{B}_0 + \sum_{i \in [d]} \mu_i^* \mathbf{B}_i \right] \\
 &= \left[\mathbf{A} \middle| \mathbf{A}_0 + \sum_{i \in [l]} b_i^* \mathbf{A}_i \left(\mathbf{T}_0 + \sum_{i \in [d]} \mu_i^* \mathbf{T}_i \right) \right] \\
 &= \left[\bar{\mathbf{A}} \mathbf{B} \middle| -\bar{\mathbf{A}} \mathbf{R}_{id^*} \mathbf{E}_{\mu^*} \mathbf{G} - \bar{\mathbf{A}} \mathbf{T}_{\mu^*} \right]
 \end{aligned}$$

Therefore,
$$[\bar{\mathbf{A}} \mathbf{B}] \cdot \begin{bmatrix} \mathbf{I}_m & -\mathbf{R}_{id^*} & -\mathbf{T}_{\mu^*} \\ & \mathbf{I}_{nk} & \end{bmatrix} \mathbf{v}^* = \mathbf{u} \bmod q$$
, let
$$\mathbf{z} = \begin{bmatrix} \mathbf{I}_m & -\mathbf{R}_{id^*} & -\mathbf{T}_{\mu^*} \\ & \mathbf{I}_{nk} & \end{bmatrix} \mathbf{v}^*$$
, then
$$\mathbf{A} \cdot \mathbf{z} = \mathbf{u} \bmod q, \quad \mathbf{A}_{\text{SIS}} \cdot \begin{bmatrix} \mathbf{z} \\ -1 \end{bmatrix} = \mathbf{0} \bmod q$$
. Since
$$\|\mathbf{v}^*\| \leq s \cdot \sqrt{m+3nk} = O(\sqrt{l+dnk})^{3/2} \cdot \omega(\sqrt{\log n})^3$$

$$\begin{aligned}\|z\| &\leq (s_1(\mathbf{R}_{id^*}) + s_1(\mathbf{T}_{\mu^*})) \cdot \|\mathbf{v}^*\| \\ &\leq (O(\sqrt{lnk}) + O(\sqrt{dnk})) \cdot O(\sqrt{l+d}(nk)^{3/2}) \cdot \omega(\sqrt{\log n})^4 \\ &\leq O((l+d)(nk)^2) \cdot \omega(\sqrt{\log n})^4\end{aligned}$$

The largest is $\beta-1$, then $z' = \begin{bmatrix} z \\ -1 \end{bmatrix}$, which is a solution to the given SIS example.

The process where B interacts with the rival of the second type is as follows:

B receives $(id^*, \mu^{(1)}, \dots, \mu^{(e)})$ output by A and arbitrarily selects a message $\mu = \mu^{(i)}$ from the received messages. B produces $A_0, A_1, \dots, A_l$ according to the target identity id^* . Let $p = \mu$ and use p to produce $B_0, B_1, \dots, B_d$. Select $\mathbf{v} \leftarrow D_{\mathbf{z}^{B_0+B_1+\dots+B_d}, s}$, and compute $\mathbf{u} = A_\mu \cdot \mathbf{v}$. B sets signature $\mathbf{v}$ of the message μ and uses the above method to produce signatures of other messages. Moreover, regarding the private key extraction inquiry and other signature inquiry, B can use the above method to make the corresponding reply. In the forge stage, A outputs forge $(id^*, \mu^*, \mathbf{v}^*)$, where $\mu^* \in \{\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(e)}\}$. If limited $\mu^* = \mu$, the probability for the rival to forge effective signature is $\delta/(2Q) \geq \delta/(2q_s)$ at least. In such case, $A_{\mu^*} = \begin{bmatrix} \bar{A}B & -\bar{A}R_{id^*} & -\bar{A}T_{\mu^*} \end{bmatrix}$, so $\begin{bmatrix} \bar{A}B \\ \mathbf{I}_{nk} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{I}_{\bar{m}} & -\mathbf{R}_{id^*} & -\mathbf{T}_{\mu^*} \end{bmatrix} (\mathbf{v}^* - \mathbf{v}) = \mathbf{0} \bmod q$, let $\mathbf{z} = \begin{bmatrix} \mathbf{I}_{\bar{m}} & -\mathbf{R}_{id^*} & -\mathbf{T}_{\mu^*} \\ \mathbf{I}_{nk} \end{bmatrix} (\mathbf{v}^* - \mathbf{v})$, then $A \cdot \mathbf{z} = \mathbf{0} \bmod q$, $A_{\text{SIS}} \cdot \begin{bmatrix} \mathbf{z} \\ 0 \end{bmatrix} = \mathbf{0} \bmod q$. Since $\|\mathbf{v}^*\|, \|\mathbf{v}\| \leq O(\sqrt{l+d}(nk)^{3/2}) \cdot \omega(\sqrt{\log n})^3$, $\|z\| \leq (s_1(\mathbf{R}_{id^*}) + s_1(\mathbf{T}_{\mu^*})) \cdot \|\mathbf{v}^* - \mathbf{v}\| \leq O((l+d)(nk)^2) \cdot \omega(\sqrt{\log n})^4$, then $z' = \begin{bmatrix} z \\ 0 \end{bmatrix}$ is a solution to the given SIS example.

5.3. Efficient

The IBS scheme presented in this paper only needs a small quantity of SampleD sampling computations in both user private key extraction stage and signature stage, however, other lattice-based IBD schemes [10, 11] proposed recently need SampleD sampling computations, ToBasis computations[8] and other time-consuming computations such as determination of vector linear independence, so the IBS scheme presented in this paper enjoys a much higher computing speed compared with other similar IBS schemes. As the identity-based public key cryptography is mainly used in a variety of resource-limited situations, this scheme as presented in this paper is more suitable for actual uses.

6. Conclusion

This paper presents an efficient lattice-based IBS scheme and proves that it satisfies strong unforgeability against selective ID and static chosen message attack. Compared with other exiting similar schemes, the one presented in this paper enjoys greater operational efficiency. In addition, it is easy to see that the proposed scheme is easy to be scaled into the hierarchical identity-based signature (HIBS) scheme [15]. Our next step will be to explore the application of the lattice-based IBS scheme in e-commerce, cloud computing and other fields, in order to effectively tackle security concerns put forward in these fields.

References

- [1] X. Zhang, Y. Han, D. Hao and Z. Lv, "ARPPS: Augmented Reality Pipeline Prospect System", 22th International Conference on Neural Information Processing (ICONIP **2015**), Istanbul, Turkey. In press.
- [2] W. Gu, Z. Lv and M. Hao, "Change detection method for remote sensing images based on an improved Markov random field", Multimedia Tools and Applications, (**2016**).
- [3] Z. Lu, C. Esteve, J. Chirivella and P. Gagliardo, "A Game Based Assistive Tool for Rehabilitation of Dysphonic Patients", 3rd International Workshop on Virtual and Augmented Assistive Technology (VAAT) at IEEE Virtual Reality 2015 (VR2015), Arles, France, IEEE, (**2016**).
- [4] Z. Lv, A. Halawani, S. Feng, H. Li and S. Ur Rehman, "Multimodal Hand and Foot Gesture Interaction for Handheld Devices", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 11, no. 1s, Article 10, (**2014**) October, 19 pages.
- [5] Y. Lin, J. Yang, Z. Lv, W. Wei and H. Song, "A Self-Assessment Stereo Capture Model Applicable to the Internet of Things", Sensors, (**2015**).
- [6] W. Ou, Z. Lv and Z. Xie, "Spatially Regularized Latent topic Model for Simultaneous object discovery and segmentation", The 2015 IEEE International Conference on Systems, Man, and Cybernetics (SMC **2015**).
- [7] Y. Wang, Y. Su and G. Agrawal, "A Novel Approach for Approximate Aggregations Over Arrays", In Proceedings of the 27th international conference on scientific and statistical database management, ACM, (**2015**).
- [8] Z. Lv, A. Halawani, S. Feng, S. ur Rehman and H. Li, "Touch-less Interactive Augmented Reality Game on Vision Based Wearable Device", Personal and Ubiquitous Computing, (**2015**).
- [9] J. Yang, S. He, Y. Lin and Z. Lv, "Multimedia cloud transmission and storage system based on internet of things", Multimedia Tools and Applications. (**2016**).
- [10] D. Jiang, X. Ying, Y. Han and Z. Lv, "Collaborative Multi-hop Routing in Cognitive Wireless Networks", Wireless Personal Communications. (**2015**).
- [11] W. Wang, Z. Lu, X. Li, W. Xu, B. Zhang and X. Zhang, "Virtual Reality Based GIS Analysis Platform", 22th International Conference on Neural Information Processing (ICONIP **2015**), Istanbul, Turkey.
- [12] Z. Lv, C. Esteve, J. Chirivella and P. Gagliardo, "Clinical Feedback and Technology Selection of Game Based Dysphonic Rehabilitation Tool", 2015 9th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth2015), IEEE, (**2015**).

Authors

Wang Jin-feng, she received her M.S. degree in software engineering from Chongqing university in Chongqing, China. She is currently a lecturer in Chongqing College of Electronic Engineering. Her research interest is mainly in the area of Computer Software, Mechanical and Electrical Integration. She has published several research papers in scholarly journals in the above research areas and has participated in several books.