Journal of Universal Computer Science, vol. 25, no. 3 (2019), 282-293
submitted: 28/3/18, accepted: 30/12/18, appeared: 28/3/19 © J.UCS

An Identity-Based Signcryption on Lattice without Trapdoor

Xianmin Wang
(School of Computer Science, Guangzhou University
Guangzhou, China
xianmin@gzhu.edu.cn)

Yu Zhang
(School of Electrical and Information Engineering and Beijing
Key Laboratory of Intelligent Processing for Building Big Data, Beijing
University of Civil Engineering and Architecture, Beijing, China
State Key Laboratory in China for GeoMechanics and Deep Underground
Engineering, China University of Mining and Technology, Beijing, China
zhangyuscholar@bucea.edu.cn)

Brij Bhooshan Gupta
(Department of Computer Engineering, National Institute of Technology
Kurukshetra, India
gupta.brij@gmail.com)

Hongfei Zhu*
(School of Computer Science and Technology, Beijing Institute of Technology
Beijing, China
zhf0374@126.com
*Corresponding author)

Dongxi Liu
(Data61, CSIRO, Sydney, Australia
Dongxi.Liu@data61.csiro.au)

Abstract: Identity-based signcryption schemes based on large integer factorization and discrete logarithm problems were considered to be insecure for the quantum computer attack. Thus, choosing a quantum-resist platform and constructing secure schemes based on new hard assumptions are challenges. In this paper, we propose an alternative scheme — an identity-based signcryption on lattice, which does not need to rely on a trapdoor. Meanwhile, our scheme achieves IND-CCA2 and sUF-CMA security, and it is also secure against the current quantum algorithm attacks based on LWE problem for lattice. Furthermore, we demonstrate that the newly proposed scheme has much shorter secret key size, and higher speeds in signcryption and unsigncryption stages, compared with some exiting identity-based signcryption schemes.

Key Words: Identity based signcryption, Quantum attack, Lattice, Unforgeability
Category: L.4.0

1 Introduction

Signcryption as an important cryptographic primitive, which can simultaneously achieve public key encryption and signature in one logical step. In 1997, Zheng initially introduced signcryption that combined digital-signature with public-key algorithm, whose cost is greatly reduced than those sign-then-encrypt schemes [Zheng 1997]. Since signcryption provides confidentiality, integrity, authentication of information and non-repudiation. Then it can be used in many applications, such as electronic transaction protocol [Tan et al., 2018A, Zhang 2018A], mobile agent protocol [Groba et al., 2018, Zhang et al., 2018B], content protection [Yu et al., 2018A], key management [Anzani et al., 2017] and routing protocol. Due to its confidentiality and authentication, signcryption plays an important role in cloud computing [Shen 2018A, Xue et al., 2019, Yu et al., 2018B, Yang et al., 2018] and Internet of things [Stergiou et al., 2018, Guan et al., 2017, Alaba et al., 2017, Yu et al., 2019], where users can further reduce the local computational cost based on cloud computing and data sharing [Lyu et al., 2017, Mollah et al., 2017, Jindal et al., 2018, Pitchai et al., 2016] by combining with some proxy computing technologies. In addition, since there is no need to maintain users' public-key list in identity-based public key algorithms [Shamir 1984, Li et al., 2015A, Yu et al.,2017, Li et al., 2019], some identity-based signcryption schemes were proposed with lower computation and communication cost [Malone-Lee 2002, Libert and Quisquater, 2003, Chow et al., 2003, Boyen 2003, Barreto et al., 2005]. However, with rapid development of the quantum computing [Shor 1997], the cryptographic schemes based on the cryptographic intractable problems on number theory have been threatened, then the quantum attacks also bring risks to those signcryption schemes based on large integer factorization and discrete logarithm problem, etc.

To resist the current quantum algorithm attacks, lattice-based public key cryptosystems have become the most active branch of anti-quantum cryptography. Lattices provided researchers with rich cryptographic hard assumptions such as learning with errors (LWE), small integer solution (SIS), shortest vector problem (SVP) and shortest independent vector problem (SIVP), where the researchers have built a reduction between the LWE problem and hidden subgroup problem on dihedral group, and the hidden subgroup problem has been proved to be secure against quantum attacks. Based on these hard problems on lattices, lattice-based signcryptions were proposed. In 2012, Li et al [Li et al., 2013] constructed a lattice-based signcryption scheme that has the characteristics of fast computing on lattices. The scheme achieves adaptively indistinguishability against chosen ciphertext attacks (IND-CCA2) and existentially unforgeability chosen message attacks (eUF-CMA). In 2013, Yan et al [Yan et al., 2013] designed a novel lattice-based signcryption scheme, and the security can be proved in the standard model. In this scheme, Yan et al presented an efficient trapdoor generation algorithm, and used Chameleon hash function to remove the trapdoor and construct a challenge tuple in the proof. Compared with the schemes in the random oracle model at that time, Yan's signcryption algorithm is more efficient. In 2014, Lu et al [Lu et al., 2014] gave a lattice-based signcryption scheme, where the security of encryption algorithm is based on the LWE problem and the security of signature depends upon the SIS problem. However, almost all lattice-based schemes cannot show the high asymptotic computation efficiency. The main reason is that the dimension of the lattice must be very large to meet the security requirements. The rank of the lattice is generally 200, while the dimension of the lattice is over 54 thousand. Then, one-time encryption (or signature) needs about 10 million modular multiplications. In particular, the signature algorithm based on the original image sampling is the most time-consuming. In sum, to propose a more secure and efficient lattice-based scheme, on one hand, we need to construct good lattices to realize the security without large dimensions; on the other hand, we should seek new methods to design efficient signcryption schemes.

In this paper, we provide an alternative method for constructing an identity-based signcryption (IBSC) scheme on lattice. Inspired by [Lyubashevsky 2012, Tian and Huang 2016], we remove the use of trapdoor in our scheme and prove that the scheme achieves IND-CCA2 and sUF-CMA security. Meanwhile, it is also secure against the current quantum algorithm attacks based on LWE problem for given lattices. Furthermore, we analyze its efficiency by comparing with some exiting identity-based signcryption schemes. Our scheme has the following merits:

- (a) The newly proposed scheme has much shorter secret key size than those of the schemes in [Li et al., 2013, Yan et al., 2013];
- (b) It has higher speeds in signcryption and unsigncryption stages than that of scheme in [Yan et al., 2013].

Organization. In Section 2, we introduce the definitions of lattice and IBSC. Section 3 shows how to construct IBSC schemes. In Section 4, we present the security of proposed scheme, and then compare our scheme with other IBSC schemes. Finally, we draw conclusions in Section 5.

2 Preliminaries

2.1 Definitions of Lattice and Important Tools

In this section, we will present the knowledge of lattice and some important tools, which can be seen from [Lyubashevsky 2012, Zhu et al., 2017].

Definition 2.1 (Lattice). linearly independent vectors $d_1, d_2, ..., d_n$ are denoted as the a basis of lattice, which can also be denoted as a Matrix $\boldsymbol{D}$. The generated lattice can be written as $\Lambda(\mathrm{D}) = \Lambda(d_1, d_2, ..., d_n) = \{\boldsymbol{D}x | x \in \mathbb{Z}_n\}$.

Definition 2.2 (q-ary lattice). q is a prime, $\boldsymbol{D} \in \mathbb{Z}_q^{n\times m}$. $\mathcal{L}^{\perp}(\boldsymbol{D}) = \{e \in \mathbb{Z}^n : \boldsymbol{De} = 0(mod\ q)\}$ is q-ary lattice.

Definition 2.3 ($SIS_{q,n,m,\beta}$ [Lyubashevsky 2012]). For a matrix $D \leftarrow \mathbb{Z}_q^{n\times m}$, SIS is to find a $\boldsymbol{v} \in \mathbb{Z}^m$ satisfying $\boldsymbol{Dv} = 0, \boldsymbol{v} \leq \beta, \beta \in \mathbb{R}, q \in \mathbb{Z}^+$.

Let $q \geq 2$ be an integer and let χ on $\mathbb{Z}_q$, the LWE's decision version $LWE_{q,\chi}$ is to differentiate between the distribution $A_{s,\chi}$ and the distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ of the variable $(\alpha, \alpha^T s + x)$, here $\alpha \leftarrow \mathbb{Z}_q^n$ is uniform and $x \leftarrow \chi$ obeys gaussian distribution. The LWE problem's standard version is finding $s \in \mathbb{Z}_q^n$ given access to any desired $poly(n)$ number of samples from $A_{s,\chi}$ for some arbitrary s.

Definition 2.4 (Discrete Gaussian Distribution) Define $\forall s > 0$, $y \in \mathbb{R}^N$, c as Gaussian distribution's center. The Gaussian function is denoted as $\rho_{s,c}(x) = exp(\frac{-\pi||y-c||^2}{s^2})$. Then the discrete Gaussian distribution on Λ is $D_{\mathcal{L},s,c}(y) = \frac{\rho_{s,c}(y)}{\rho_{s,c}(\mathcal{L})}$.

Theorem 2.5 (Rejection Sampling Theorem). Define V as one of $\mathbb{Z}^m$'s subset, the elements' norm of V are not greater than T, $\sigma = \omega(T\sqrt{logm})$ is the element in $\mathbb{R}$, M is a constant, $h : V \rightarrow \mathbb{R}$ is a probability distribution. There are two algorithms. The first algorithm is described as $v \leftarrow h, z \leftarrow D_{v,\sigma}^m, generate(z, v)$ with probability $min(\frac{D_\sigma^m(z)}{MD_{v,\sigma}^m(z)}, 1)$. The other algorithm is such that $v \leftarrow h, z \leftarrow D_\sigma^m, output(z, v)$ with probability $\frac{1}{M}$. Then the first algorithm' distribution does not exceed the second algorithm's statistical distance $\frac{2^{-\omega(logm)}}{M}$. Meanwhile, The first one can output something with probability greater than $\frac{1-2^{-\omega(logm)}}{M}$.

2.2 Identity-based Signcryption Scheme

An IBSC scheme is constitute of four algorithms($ST_\varepsilon, EX_\varepsilon, SC_\varepsilon$, US_ε), we denotes $\mathcal{S}$ and $\mathcal{R}$ respectively as sender and receiver, $params$ and mk as system parameters and master key respectively, and sk_{id_i} as private key. The definition is described as follows.

- $ST_\varepsilon(1^n)$ generates $params$ and mk.
- $EX_\varepsilon(params, mk, id)$ produces sk_{id_i} according to one's identity id_i, $i = \mathcal{R}$ or $\mathcal{S}$.
- $SC_\varepsilon(id_\mathcal{R}, m, sk_\mathcal{S})$ outputs a ciphertext σ.
- $US_\varepsilon(params, id_\mathcal{S}, sk_\mathcal{R}, \sigma)$ recovers the initial message m if σ passes the verification, otherwise reject it.

IBSC must meet the conditions of confidentiality and authenticity, i.e., confidentiality means the IBSC scheme can be indistinguishable to defeat adaptive chosen ciphertext attacks (IND-CCA2) [Malone-Lee 2002]. Meanwhile, the authenticity means IBSC scheme can be strong unforgeable against adaptive chosen message attacks (sUF-CMA).

Definition 2.4 (IND-CCA2). Define C as challenger, an IBSC scheme is IND-CCA2 secure if no PPT adversary $\mathcal{A}$ can win the IND-CCA2 game with negligible probability.

- Setup: C executes $ST(1^k)$ to produce (mpk, msk) and run $\mathcal{A}$ as its subprogram.

- Phase 1: The adversary $\mathcal{A}$ can perform any number queries of polynomial bound in an adaptive method.

- ET queries: $\mathcal{A}$ selects one id. C runs algorithm $ET(id)$ to produce S_{id} and send it to $\mathcal{A}$.

- SC queries: $\mathcal{A}$ chooses one id_s, one id_r and a message m. C runs $ET(id_s)$ to generate S_{id_r}, runs $SC(m, S_{id_s}, id_r)$ to generate encrypted message ψ, and then delivers ψ to $\mathcal{A}$.

- US queries: $\mathcal{A}$ chooses id_s, id_r, and a encrypted message ψ. C runs $ET(id_r)$ to generate S_{id_r}, runs $US(\psi, S_{id_r}, id_s)$ to recover the original message, and delivers it to $\mathcal{A}$.

- Challenge: $\mathcal{A}$ can decide when to end Phase1. $\mathcal{A}$ will choose m_0 and m_1, id_s^*, and id_r^*. id_r^* could not be queried in ET in Phase 1. C can randomly chooses a bit p from $\{0, 1\}$, runs $SC(m_\delta, s_{id_s^*}, id_r^*)$ to output ψ^*, and then deliver ψ^* to $\mathcal{A}$.

- Phase 2 : $\mathcal{A}$ can execute any times of queries of a polynomial bound adaptively again as in Phase1, we assume that id_r^* will not be queried in EX query and ψ^* will not be queried by US queries.

- Guess: $\mathcal{A}$ will output a bit $p^{'}$. If $p^{'}$ equals to p, then $\mathcal{A}$ wins.

  $\mathcal{A}$'s advantage is denoted as $Adv(\mathcal{A}) = [Pr[p^{'} = p] - 1/2]$, here $Pr[p^{'} = p]$ is the probability of $p^{'} = p$.

Definition 2.5 (sUF-CMA). An IBSC is sUF-CMA secure, if no PPT adversaries $\mathcal{A}$ can win sUF-CMA game with a negligible probability.

- Setup: C execute runs $ST(1_k)$ to produce (mpk, msk) and runs $\mathcal{A}$ as its subroutine.

- Attack: $\mathcal{A}$ executes a number queries of a polynomial bound like in IND-CCA2 game.
- Forgery: $\mathcal{A}$ produces a tuple $(m^*, \psi^*, id_s^*, id_r^*)$. Here, we assume id_s^*'s private key will not be queried, also ψ^* will not be returned by SC oracle when querying $m^*, S_{id_r^*}, id_s^*$ in attack phase. if $US(\psi^*, S_{id_r^*}, id_s^*)$ does not output $\perp$, then $\boldsymbol{A}$ wins.

The advantage of $\mathcal{A}$ is defined as the probability that it wins.

3 Our IBSC scheme

Now we will introduce a new IBSC $\varepsilon = (ST_\varepsilon, EX_\varepsilon, SC_\varepsilon, US_\varepsilon)$. In the beginning, we will define some denotations as follows: $\mathcal{S}$, $\mathcal{R}$ are respectively the sender and the receiver. Private Key generator is short for PKG, $q \geq 3$ is a prime, M is a real. $m > 5nlogq$, k, and λ are positive integers. $\tilde{L} = O(\sqrt{nlogq})$ is the bound, $s = \tilde{L}\omega(\sqrt{logn})$ is gaussian parameter, $\sigma = 12s\lambda m$ is standard deviation.

Then the detailed scheme is described as follows:

(1) $ST_\varepsilon(1^n)$

- The algorithm runs $TrapGen(q, n)$ [Tian and Huang 2016] to obtain $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ with lattice $\Lambda^\perp(\boldsymbol{A})$'s one basis $\boldsymbol{D} \in \mathbb{Z}_q^{n\times m}$ satisfying $\tilde{L} \geq ||\tilde{\boldsymbol{D}}||$.
- The algorithm Chooses hash: $H : \{0,1\}^* \rightarrow \{v : v \in \{-1,0,1\}^k, ||v||_1 \leq \lambda\}$, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^{n\times k}$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^{n\times k}$.
- The algorithm will generate $paras = (\boldsymbol{A}, H, H_1, H_2)$ and master private key $msk = \boldsymbol{D}$.

(2) $ET_\varepsilon(paras, msk, id_i)$

PKG run algorithm $SampleMat(A, D, s, H_1(id_i))$ [Tian and Huang 2016] to obtain a signing key $sk_{id_i} = S_{id_i} \in \mathbb{Z}^{m\times k}$, here $i = \mathcal{S}$ or $\mathcal{R}$. S_{id_i} should satisfy

$$\begin{cases} AS_{id_i} = H_1(id_i) \\ ||S_{id_i}|| \leq s\sqrt{m} \end{cases} \tag{1}$$

(3) $SC_\varepsilon(m, S_{id_\mathcal{S}}, id_\mathcal{R})$

Given $paras$, $m \in \{0,1\}^*$, $\mathcal{S}$'s secret key $S_{id_\mathcal{S}}$, and receiver's identity $id_\mathcal{R}$.

- $\mathcal{S}$ selects a random $y \leftarrow D_\sigma^m$ and computes

$$r = H_2(Ay, H_1(id_\mathcal{R})) \tag{2}$$

- $\mathcal{S}$ computes

$$c = H(r, AS_{id_{\mathcal{S}}}) \bigoplus m \tag{3}$$

- $\mathcal{S}$ computes

$$z = S_{id_{\mathcal{S}}} r + y \tag{4}$$

- Then $\mathcal{S}$ outputs (c,z) with probability $min(\frac{D_{\sigma}^{m}(z)}{MD_{\sigma,S_{id_{\mathcal{S}}}h}(z)}, 1)$. The signature tuple is (r,c,z).

(4) $US_{\varepsilon}((r,c,z), id_{\mathcal{S}}, S_{id_{\mathcal{R}}})$
$\mathcal{R}$ will compute

$$h = H_2(Az - H_1(id_{\mathcal{S}})r, AS_{id_{\mathcal{R}}}) \tag{5}$$

and then $\mathcal{R}$ can get the original message

$$m = H(h, H_1(id_{\mathcal{S}})) \bigoplus c \tag{6}$$

If equation 7 are true, we accept the original message. Otherwise, we reject it.

$$\begin{cases} ||z|| \leq 2\sigma\sqrt{m} \\ h = r \end{cases} \tag{7}$$

4 Security and Performances

In this section, we will analyze the security of our IBSC scheme, then we compare our scheme with other IBSC schemes in terms of performances.

4.1 Correctness and Security

Theorem 1 (Correctness) our IBSC scheme satisfies correctness.

Proof. According to our IBSC scheme's construction process, we can obtain $Az - H_1(id_s)r = A(S_{id_s}r + y) - H_1(id_s)r = AS_{id_s}r + Ay - H_1(id_s)r = Ay$. Also we can get $AS_{id_r} = H_1(id_r)$.

Therefore, $H_2(Az - H_1(id_s)r, AS_{id_r}) = H_2(Ay, H_1(id_r))$. We can get the original message by computing $H(h, H_1(id_s)) \bigoplus c$. If $h = r$, we output the message m, otherwise we reject it.

By using lemma 2 and Lemma 3 described in [Xie et al., 2016], z is close to a vector from D_{σ}^{m}. Thus, we can get $||z|| \leq 2\sigma\sqrt{m}$ with probability at least $1 - 2^{-m}$.

Theorem 2 (IND-CCA2) if an adversary $\mathit{\Gamma}$ can win IND-CCA2 games in a time t with non-negligible advantage ε after q_e times ET queries, q_s times SC queries, q_u times US queries, and q_{H_1}, q_{H_2}, q_H queries respectively to oracles H_1, H_2, H, there has a polynomial algorithm C who can solve LWE problem with advantage $\epsilon^{'} \geq \epsilon - q_H q_u / 2^n$ in time $t^{'} < t + (q_u + q_H)t_H + q_u t_{H_2}$.

Proof. in the beginning, we assume adversary $\mathit{\Gamma}$ can win IND-CCA2 game with non-negligible probability ε, then we can construct an algorithm C who can run $\mathit{\Gamma}$ as its subprogram.

Suppose the challenger C receives a random LWE instance $(\tilde{S}, \tilde{z} = \tilde{S}\tilde{r} + \tilde{y})$, his goal is to compute $\tilde{S}$. C can run $\mathit{\Gamma}$ as its subprogram to get $\tilde{S}$ and be a challenger in the game.

Setup: Suppose C runs algorithm ST_ϵ to generate $params = A, H, H_1, H_2, H$ and master secret key $msk = B$. Then C delivers $paras$ to $\mathit{\Gamma}$.

Phase 1: C holds lists L_1, L_2, L to simulate H_1, H_2, H oracles respectively, and replies for the queries as belows:

H_1 oracle: once receiving id_i query $(1 \leq i \leq q_{h_1})$, C will initially check whether there exists a corresponding value $H_1(id_i)$ in L_1. If there exists, $H_1(id_i)$ will be returned. Otherwise, C will select a random $h_{1_i} \in \mathbb{Z}_q^{n \times k}$, stores (id_i, h_{1_i}) into L_1, then C will return h_{1_i} to $\mathit{\Gamma}$.

H_2 oracle: once receiving Ay_i, h_{2_i} query $(1 \leq i \leq q_{h_2})$, C will initially check whether there exists a corresponding value h_{2_i} in L_2. If there exists, h_{2_i} will be returned. Otherwise, C will select a random $h_{2_i} \in \mathbb{Z}_q^{n \times k}$, stores $(Ay_i, id_i, h_{1i}, h_{2i})$ into L_2, and returns h_{2i} to $\mathit{\Gamma}$.

H oracle: once receiving $r_i, AS_i)$ query $(1 \leq i \leq q_H)$, C will initially check whether there exists a corresponding H_i in L. If there exists, H_i will be returned. Otherwise, C will select a random $h_i \in \mathbb{Z}_q^{n \times k}$, inserts (r_i, AS_i, h_i) into L, and returns h_i to $\mathit{\Gamma}$.

EX_ϵ query: When $\mathit{\Gamma}$ queries $id_i (1 \leq i \leq q_e)$ to get a secret key, C will initially search in L_1, if there exists a corresponding value for id_i, C will return h_{id_i}. Otherwise, C will select a random h_{id_i}, stores $(id_i, h_{id_i}, S_{id_i})$ to L_1 and returns h_{1i} to $\mathit{\Gamma}$.

SC_ϵ query: $\mathit{\Gamma}$ will execute a SC_ϵ query for m_i with id_A and id_B. If $id_A \neq id_j$, C will first get a secret key for id_A by querying ET_ϵ oracle, then C will run $SC(id_A, S_{id_B}, sig)$ to answer C 's query.

US_ϵ query: if $\mathit{\Gamma}$ queries a (c, r, z) for US_ϵ query with id_A and id_B. If $id_B \neq id_j$, C will first obtain a secret key for id_B by querying EX_ϵ oracle. After that, C will return $US(c, r, z, id_A, S_{id_B})$ to answer $\mathit{\Gamma}$.

Challenge: After $\mathit{\Gamma}$ finishes a larger number of queries, $\mathit{\Gamma}$ will select id_A^* and id_B^*, that he wants to be challenged. Then $\mathit{\Gamma}$ submits m_0, m_1 to $\mathit{\Gamma}$. C will randomly choose $r^* \leftarrow \{0,1\}^*, z^* \leftarrow \{0,1\}^*$, and set $z^* = \tilde{z}$. At last, C will return $\sigma^* = (c^*, r^*, z^*)$ to $\mathit{\Gamma}$.

Phase 2: After $\mathit{\Gamma}$ finishes a large number of queries adaptively as in former step. id_B^* will not be queries in ET oracle, and σ^* will not be queried in US oracle.

Guess: $\mathit{\Gamma}$ will generate one $p^{'}$, which can be ignored by C. C searches in L for tuple (r_i, AS_i, H_i). For each of them, C will check whether $\tilde{z} = \tilde{A}S_i + y_i$ keeps. If it keeps , C will stop and output S_i as one solution of LWE problem. Otherwise, C stops and outputs $false$.

Now we will need to analyze the success probability of C. We denote E_H as the event that $\mathit{\Gamma}$ query the H oracle during the simulation. So we can get$Pr[p^{'} = p] = 1/2 + 1/2Pr[E_H]$, then we can get $\epsilon = |2Pr[p^{'} = p] - 1| \leq Pr[E_H]$. Following the method of [Li et al., 2013], we can get C can solve LWE problem with $\epsilon^{'} \geq \epsilon - q_H q_u/2^n$ in time $t^{'} < t + (q_u + q_H)t_H + q_u t_{H_2}$.

Theorem 2 (sUF-CMA) if one adversity $\mathit{\Gamma}$ can win sUF-CMA game with non-negligible probability ε_{sc} in a time t after q_e times ET_ϵ queries, q_s times SC_ϵ queries, q_u times US_ϵ queries, and q_{H_1}, q_{H_2}, q_H times queries respectively to oracles H_1, H_2, H, there is an algorithm C who can solve SIS problem with probability at least $1/2(1 - 2^{-\omega(logn)})$.

Proof. assume a polynomial algorithm C gets one instance of SIS $\tilde{A}x = 0$ mod q, his aim is to find a x as $||x|| \leq (4\sigma + 2s\lambda)\sqrt{m}$. C can run $\mathit{\Gamma}$ as its subprogram, and be a challenger for $\mathit{\Gamma}$.

C initially runs ST_ϵ to generate $paras$. Then $\mathit{\Gamma}$ can execute a larger number of queries for oracle, ET_ϵ queries, SC_ϵ queries, and US_ϵ queries. C will answer $\mathit{\Gamma}$'s queries. When receiving $Ay, H_1(id_R))$ query, C answers as follows:

C randomly chooses s_{id} $(||s_{id}|| \leq s\sqrt{m+w})$, sets $Az - H_1(id_s)(A||r) = Ay$, C stores (m_i, r_i, y_i, h_{2i}) to L_2, and returns h_{2i} to $\mathit{\Gamma}$.

At last, if C never aborts, $\mathit{\Gamma}$ will obtain one sig^* on m^*, where m^* has never been queried for id_A^*, id_B^*. Then C can run US_ϵ for sig^* and get r^*, m^* by running ET_ϵ to obtain id_B^*'s secret key, which meets the requirements of $s_{id}^* \leq s\sqrt{m}$ and $(Az - H_1(id_S)r = Ay$. Before forging sig^*, $\mathit{\Gamma}$ queried H_2 for m^*, r^*. Thus, C searches in L_2 for $m^*, r^*, s_{id_i}, h_{2_i}$, such that $(Az^* - H_1(id_S)r^*) = Ay$

if $id_A^* = id_j$, C can obtains the following equation $A(z - z^* - S_{id_S}r + S_{id_S}r^*) = 0$. Due to $||z^*||, ||z|| \leq 2\sigma\sqrt{m}$ and by design $||S_{ID}r^*||, ||S_{ID}r|| \leq s\lambda\sqrt{m}$, we obtain $z - z^* - S_{id_S}r + S_{id_S}r^* \leq (4\sigma + 2s\lambda)\sqrt{m}$.

So we need to present $z - z^* - S_{id_S}r + S_{id_S}r^* \neq 0$ with non-negligible probability. By the preimage min-entropy property [Li et al., 2013], with probability no less than $(1 - 2^{-\omega(logn)})$. We can obtain another signing key S_{id}, $z - z^* - S_{id_S}r + S_{id_S}r^* \neq 0$ with probability at least 1/2, so we can solve SIS problem with probability $1/2(1 - 2^{-\omega(logn)})$, we prove this theorem.

4.2 Performance

We now compare our IBSC's performance with Yan's scheme [Yan et al., 2013] and Li's scheme [Li et al., 2013]. From Table 1, we can see the SC speed of our scheme's is $O(1)$, it is the same with Li's scheme, it is faster than Yan's scheme. Our scheme's US speed is $O(1)$, it is faster than that of Yan's scheme. The user's secret key of our scheme is $mk \log q$, it is shorter than that of Yan's scheme and L's scheme. The security of Yan's scheme is proved in the standard model, our scheme and Li's scheme are secure in the random oracle (ROM). The performance comparison is given as below.

Table 1: Performance Comparison

IBSC Scheme	[Yan et al., 2013]	[Li et al., 2013]	Our scheme
Hard Problem	LWR/LWE	LWE/ISIS	LWE/ SIS
SC speed	$O(n)$	$O(1)$	$O(1)$
US speed	$O(n)$	$O(1)$	$O(1)$
Size of secret key	$n^2 \log^2 q \log(\log n)$	mnl_q/m^2l_q	$mk \log q$
Security model	Standard model	ROM	ROM

5 Conclusions

In this paper, we design a lattice-based IBSC scheme by using rejection sampling theorem. Then we demonstrate our IBSC scheme is secure, i.e., it satisfies IND-CCA2 and sUF-CMA. After that, we compare our scheme's performance with other existing IBSC schemes, the results show that our scheme outperforms other schemes in terms of user's secret key, our scheme's SC speed and US speed are faster than that of Yan's scheme. In addition, Yan's scheme and Li's scheme are constructed based on trapdoor, our scheme does not need to rely on a trapdoor.

Acknowledgements

This work was partly supported by Beijing Municipal Education Commission under Grant(No.KM201510016009), and Excellent Teachers Development Foundation of BUCEA(No.21082717046), and National Key R&D Program of China (No.2016YFC060090).

References

[Alaba et al., 2017] Alaba, F. A., Othman, M., Hashem, I. A. T., Alotaibi, F.: Internet of things security: A survey, Journal of Network & Computer Applications, Vol 88, (2017), pp.10-28.

[Anzani et al., 2017] Anzani, M., Javadi, H. H. S., Modirir, V.: Key-management scheme for wireless sensor networks based on merging blocks of symmetric design, Wireless Networks, Vol 1, (2017), pp. 1-13.

[Barreto et al., 2005] Barreto, P. S. Libert, B., McCullagh, N., Quisquater, J. J.: Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, International Conference on the Theory and Application of Cryptology and Information Security, Springer, (2005), pp.515-532.

[Boyen 2003] Boyen, X., Multipurpose identity-based signcryption, Annual International Cryptology Conference, Springer, (2003), pp. 383-399.

[Chow et al., 2003] Chow, S. S., Yiu, S. M., Hui, L. C., Chow, K.: Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity, International Conference on Information Security and Cryptology, Springer, (2003), pp. 352-369.

[Groba et al., 2018] Groba, A. M., Lobo, P. J., Chavarrias, M.: Slack-time closed-loop control system for multimedia mobile devices, IEEE Transactions on Consumer Electronics, Vol 64, No 2 (2018), pp. 162-170.

[Guan et al., 2017] Guan, Z., Li, J., Wu, L., et al. Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid, IEEE Internet of Things Journal, Vol 4, No 6 (2017), pp. 1934-1944.

[Jindal et al., 2018] Jindal, A., Dua, A., Kumar, N., et al. Providing Healthcare-as-a-Service Using Fuzzy Rule-Based Big Data Analytics in Cloud Computing, IEEE Journal of Biomedical & Health Informatics, (2018), pp. 1-1.

[Li et al., 2013] Li, F., Bin Muhaya, F. T., Khan, M. K., Takagi, T. Lattice-based signcryption, Concurrency and Computation: Practice and Experience, Vol 25, No 14 (2013), pp. 2112-2122.

[Li et al., 2015A] Li, J., Li, J., Chen, X., Lou W. Identity-based Encryption with Outsourced Revocation in Cloud Computing, IEEE Transactions on Computers, Vol 64, No 2 (2015), pp. 425-437.

[Li et al., 2019] Y. Li, Y. Yu, W. Susilo, G. Min, J. Ni, R. Choo,. Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems. IEEE Trans. on Dependable and Secure Computing, 16(1) (2019), 72-83.

[Libert and Quisquater, 2003] Libert, B., Quisquater, J. J.: A new identity based signcryption scheme from pairings, Proceedings of 2003 IEEE Information Theory Workshop, IEEE, (2003), pp. 155-158.

[Lu et al., 2014] Lu, X., Wen, Q., Jin, Z., et al.: A lattice-based signcryption scheme without random oracles, Frontiers of Computer Science, Vol 8, No 4 (2014), pp. 667-675.

[Lyu et al., 2017] Lyu, Y., Lee, V.C.S., Chow, C.Y., et al. R-Sharing: Rendezvous for Personalized Taxi Sharin, IEEE Access, Vol 99, (2017), pp. 1-1.

[Lyubashevsky 2012] Lyubashevsky, V. Lattice signatures without trapdoors, Advances in Cryptology–EUROCRYPT, Springer, (2012), pp. 738-755.

[Malone-Lee 2002] Malone-Lee, J. Identity-based signcryption, IACR Cryptology ePrint Archive (2002), pp. 1-8. http://eprint.iacr.org/.

[Mollah et al., 2017] Mollah. M. B., Azad, M. A. K., Vasilakos, A. Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things, IEEE Cloud Computing, Vol 4, No 1, (2017), pp. 34-42.

[Pitchai et al., 2016] Pitchai, R., Jayashri, S., Raja, J. Searchable Encrypted Data File Sharing Method Using Public Cloud Service for Secure Storage in Cloud Computing, Wireless Personal Communications, Vol 90, No 2 (2016), pp. 947-960.

[Shamir 1984] Shamir, A. Identity-based cryptosystems and signature schemes, Advances in cryptology, Springer, (1984), pp. 47-53.

[Shen 2018A] Shen, J., Gui, Z., Ji, S., et al. Cloud-aided Lightweight Certificateless Authentication Protocol with Anonymity for Wireless Body Area Networks, Journal of Network and Computer Applications, Vol 106, (2018), pp. 117-123.

[Shor 1997] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithme on a quantum computer, SIAM Journal on Computing, (1997), 1484-1509.

[Stergiou et al., 2018] Stergiou, C., Psannis, K. E., Kim, B. G., Gupta, B. Secure integration of IoT and cloud computing, Future Generation Computer Systems, Vol 78, (2018), pp. 964-975.

[Tan et al., 2018A] Tan, Y. A., Xue, Y., Liang, C., Zheng, J., et al. A root privilege management scheme with revocable authorization for android devices, Journal of Network and Computer Applications, Vol 107, No 4 (2018), pp. 69-82.

[Tian and Huang 2016] Tian M., Huang L. Identity-based signatures from lattices: Simpler, faster, shorter, Fundamenta Informaticae, Vol 145, No 2 (2016), pp. 171-187.

[Xie et al., 2016] Xie, J., Hu, Y., Gao, J., Gao, W. Efficient identity-based signature over ntru lattice, Frontiers of Information Technology and Electronic Engineering, Vol 17, (2016), pp. 135-142.

[Xue et al., 2019] L. Xue, Y. Yu, Y. Li, M. H. Au, X. Du, B. Yang, Efficient attribute-based encryption with attribute revocation for assured data deletion, Information Science, 479 (2019), 640-650.

[Yan et al., 2013] Yan, J., Wang, L., Wang, L., et al. Efficient lattice-based signcryption in standard model, Mathematical Problems in Engineering, Vol 11, (2013), pp. 1-18.

[Yang et al., 2018] Yang, L., Han, Z., Huang, Z., Ma, J. A remotely keyed file encryption scheme under mobile cloud computing, Journal of Network and Computer Applications, Vol 106, (2018), pp. 90C99.

[Yu et al.,2017] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, Min, G., Identity-Based Remote Data Integrity Checking with Perfect Data Privacy P-reserving for Cloud Storage, IEEE Trans. Information Forensics and Security, 12(4) (2017), 767-778.

[Yu et al., 2018A] Y. Yu, Y. Li, X. Du, R. Chen, G. Yang, Content Protection in Named Data Networking: Challenges and Potential Solutions, IEEE Communications Magazine 56(11) (2018), 82-87.

[Yu et al., 2018B] Y. Yu, L. Xue, Y. Li, X. Du, M. Guizani, B. Yang, Assured Data Deletion with Fine-Grained Access Control for Fog-Based Industrial Applications, IEEE Trans. on Industrial Informatics, 14(10) (2018), 4538-4547.

[Yu et al., 2019] Y. Yu, Y. Ding, Y. Zhao, Y. Li, X. Du, M. Guizani. LR-Coin: Leakage-resilient Cryptocurrency Based on Bitcoin for Data Trading in IoT, IEEE Internet of Things Journal, DOI 10.1109/JIOT.2018.2878406, https://ieeexplore.ieee.org/document/8513813.

[Zhang 2018A] Zhang, X., Tan, Y. A., Liang, C., Li, Y., Li, J. A covert channel over volte via adjusting silence periods, IEEE Access, Vol 6 (2018), pp. 9292-9302.

[Zhang et al., 2018B] Zhang, X., Liang, C., Zhang, Q., Li, Y., et al. Building covert timing channels by packet rearrangement over mobile networks, Information Sciences, Vol 445, (2018), pp. 66-78.

[Zheng 1997] Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption) ¡¡ cost (signature) + cost (encryption), Annual International Cryptology Conference, Springer, (1997), pp. 165-179.

[Zhu et al., 2017] Zhu, H., Tan, Y. A., Zhang, X., et al. A round-optimal lattice-based blind signature scheme for cloud services, Future Generation Computer Systems, Vol 73, (2017), pp.106-114.