Journal of Network Intelligence ©2018 ISSN 2414-8105 (Online)
Taiwan Ubiquitous Information Volume **3**, Number **3**, August **2018**

An Identity-Based Ring Signcryption Scheme in Ideal Lattice

Yiru Sun[1], Weimin Zheng[2,*]

[1]Institute of Information Engineering, Chinese Academy of Sciences
Beijing 100093,China

[2]College of Computer Science and Engineering,
Shandong University of Science and Technology,Qingdao 266590,China
*Corresponding author:zhengweimin@sdust.edu.cn

Received Jan 2018; revised March 2018

Abstract. *The existing signcryption schemes based on bi-linear pairings were proved to be insecure in quantum computing environment. Lattice is simple in operation, and the difficult problems based on lattice are hard to solve. In order to resist the quantum attack, we presented an identity-based ring signcryption scheme that is provably secure under the standard model by using the Ducas' ideal lattice technology, which is based on the assumption of the hardness of lattice problem small integer solutions (SIS). This scheme mainly includes four algorithms: Keygen(), Extract(), Signcrypt(), Unsigncrypt(). To some extent, the scheme in this paper that has a high practical value in electronic cash payment system, security certification lightweight authentication and other fields shortens the bytes of private key, public key and the signcryption, improves the operation efficiency. The security of scheme also indirectly ensure the security in electronic cash payment system, security certification and so on.*

Keywords: Ideal lattice, Standard model, Identity-based, Ring signcryption, SIS

1. **Introduction.** As the combination of encryption system and digital signature system, identity-based signcryption scheme is an important technology in lightweight authentication, which plays an essential role in electronic cash payment system, security certification and other fields. The concept of signcryption was put forward by Zheng[1] for the first time in 1997, and meanwhile, he also proposed a concrete signcryption scheme that could achieve both encryption and digital signature at the same time, as well as reduce the computation complexity compared with the traditional signature-encryption schemes while still has the problems of complex certificate management and key escrow security, at the same time, it presented an open problem: using the public key cryptosystems to design the related signcryption schemes. Malone - Lee[2] showed the first identity-based signcryption scheme, and also defined the corresponding security model in 2002.

Libert[3] proved that Malone's signcryption scheme is not secure in 2003, and proposed one new signcryption scheme by using the bilinear pairings. Since then, scholars all over the world have been paying more and more attention to the identity-based signcryption scheme, and many of these schemes have been proposed gradually[4-7]. For example, to solve the recipient identity leakage and decryption unfairness problem, Pang et al.[8] proposed a fair identity-based multi-recipient anonymous signcryption scheme in 2014, and provided the corresponding proof of confidentiality and unforgeability. Deng et al.[9]

proposed a new signcryption scheme based on identity in 2014, which reduced the cost of computation to a certain extent, and they also provided a security proof in the random oracle model. The signcryption schemes above are mostly based on bilinear pairings, however, such schemes have been proved to be insecure in quantum computing environment, for instance, Shor[10] presented that the encryption schemes based on the assumption of the arithmetic problems cannot resist quantum attack efficiently in 1994. To design the identity-based signcryption schemes that can resist quantum attack, many scholars both at home and abroad have been trying to construct signcryption schemes by using the advantages and characteristics of lattice or special lattice. Reference the trapdoor generation algorithm given by Micciancio et al.[11] , Ducas and Micciancio[12] presented an short signature scheme in ideal lattice based on the difficulty assumption of Small Integer Solution(SIS) in 2014. In 2015,Yang et al.[13] constructed an identity-based signature(IBS) scheme by conferencing the ideal technology presented in reference [12] and using the special structure of ideal lattice, the scheme reduced the computation complexity and shortened the length of the signature and public key partly, and could give security proof under the standard model, however the scheme to sign only for a single ID, could not realize the anonymity.

There has no quantum computing method exist to solve the difficult problem in lattice until now, therefore, en-cryption schemes, signature schemes and signcryption schemes in lattice can resist the quantum attack. In this paper, we proposed an identity-based ring signcryption scheme provably secure under the standard model by using the ideal lattice technology presented by Ducas et al.[12], which is based on the assumption of the hardness of lattice problem SIS and could resist chosen massage and ID attack.

1.1. Background Knowledge.

Since the late 18th century, lattices were studied by several mathematicians such as Gauss. It has been showed that the security of any instances in a lattice are the same, and operations based on it are given priority to linear operation and module operation. Until now, no quantum algorithm has been found to solve difficult problems based on lattices. Ajtai[14] proposed a reduction from a worst case to a average case in 1996, which attracted many scholars' attention to lattices. More recently, lattices has become a popular research subject in computer science and information security in order to design a cryptosystem that could resist quantum attack. First of all, let's review some definitions and theorems concerning lattice.

1.2. Lattice and Ideal Lattice.

In brief, one lattice is a set of points with a periodic structure in n-dimensional space, a more formal definition of a lattice is as follows.

Definition 1. (Lattice)[13] Given linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \cdot\cdot\cdot, \mathbf{b}_n \in \mathrm{R}^m$, the lattice generated by them can be defined as:

$$L\left(\mathbf{b}_1, \cdots, \mathbf{b}_n\right) = \left\{\sum \mathbf{x_i}\mathbf{b}_i \left|\mathbf{x_i} \in \mathrm{Z}^n\right.\right\} \tag{1}$$

We refer to $\mathbf{b}_1, \mathbf{b}_2, \cdot\cdot\cdot, \mathbf{b}_n \in \mathrm{R}^m$ as one base of the lattice. Equivalently, the lattice generated by $m \times n$matrix$\mathbf{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n)$can be defined as

$$L\left(\mathbf{B}\right) = L\left(\mathbf{b}_1, \cdot\cdot\cdot, \mathbf{b}_n\right) = \left\{\mathbf{Bx}\left|\mathbf{x} \in \mathrm{Z}^n\right.\right\} \tag{2}$$

For any $\mathbf{A} \in \mathrm{Z}_q^{n\times m}$, positive integers n and q , we define the full-rank lattice model as follow:

$$\Lambda^{\perp}\left(\mathbf{A}\right) = \left\{\mathbf{z} \in \mathrm{Z}^m : \mathbf{Az} = 0 \bmod q\right\} \tag{3}$$

$$\Lambda_u^{\perp}\left(\mathbf{A}\right) = \left\{\mathbf{z} \in \mathrm{Z}^m : \mathbf{Az} = u \bmod q\right\} \tag{4}$$

Obviously,$\Lambda_u^{\perp}\left(\mathbf{A}\right) = \Lambda^{\perp}\left(\mathbf{A}\right) + x$for any$x \in \Lambda_u^{\perp}\left(\mathbf{A}\right)$.

Theorem 1.[12] Given a lattice Λ, which is of dimension , suppose that one of its bases is $\mathbf{B}$, then for any real number$\varepsilon > 0$, the smoothing parameter$\eta_\varepsilon(\Lambda)$ satisfied

$$\eta_\varepsilon(\Lambda) \le \left\| \tilde{\mathbf{B}} \right\| \cdot \sqrt{{}^{\log(2n(1+{}^1/_\varepsilon))}/_\pi} \tag{5}$$

Micciancio D[15] presented the first definition of the cyclic lattice in 2002, which effectively solved the problems of long keys and low operation efficiency in general lattices; Lyubashevsky V, Micciancio D[16] putted forward the concept of the ideal lattice for the first time in 2006. In simple terms, the ideal lattice is one generalization of cyclic lattices, the ideal of one ring and has some special algebraic structures. Cryptosystems proposed in ideal lattices could also shorten the length of keys, and improve the operation efficiency.

Definition 2. (Ideal lattice)[14] We refer to the ideal of polynomial ring ${}^{\mathrm{Z}[x]}/_{f(x)}asf(x)-$ ideal lattice if the following properties are satisfied:
1) The leading coefficient of$f(x)$is 1;
2) $f(x)$is irreducible inZ;
3) $\|g(x)\,h(x) \bmod f(x)\| < \mathit{poly}(n) \cdot \|g(x)\| \cdot \|h(x)\|$ is satisfied for any polynomial $g(x)$and$h(x)$in ring $\mathrm{Z}[x]$ with the Euclidean norm $\|\cdot\|$.

Let $\mathrm{R}_q = {}^{\mathrm{Z}[x]}/_{((x^n+1),q)}$ for cyclotomic polynomial $x^n + 1$ in this paper.

Using the trapdoor of a lattice, we can design some signature schemes and sign schemes that have higher security and computing efficiency. Now, we present the definition of a trapdoor, and some positive properties that were used in the scheme of this paper.

Using the trapdoor of a lattice, we can design some signature schemes and sign schemes that have higher security and computing efficiency. Now, we present the definition of a trapdoor, and some positive properties that were used in the scheme of this paper.

Definition 3.[12] For any matrix $\mathbf{A} \in \mathrm{R}_q^{n\times(w+k)}$,$\mathbf{G} \in \mathrm{R}_q^{n\times k}$, we refer to$\mathbf{R}$ as a $\mathbf{G}-$ trapdoor of$A$if there is $\mathbf{R} \in \mathrm{R}_q^{w\times k}$ satisfying.

$$\mathbf{A}\begin{pmatrix}\mathbf{R}\\ \mathbf{I}\end{pmatrix} = \mathbf{HG} \tag{6}$$

for invertible tag matrix $\mathbf{H} \in \mathrm{R}_q^{n\times n}$. Obviously, for any $0 < m' \le m$,$\mathbf{R}$ has a prolongation $[\mathbf{R}, 0] \in \mathrm{R}_q^{m\times k}$ in the definition above.

Theorem 2.[12] Let$n \ge 4$be a power of 2,$q \ge 3$be a power of 3, set$\mathrm{R}_q = {}^{\mathrm{Z}[x]}/_{((x^n+1),q)}$, then any nonzero polynomial$f \in \mathrm{R}_q$with the highest power $d < {}^n/_2$ is invertible inR_q, and the coefficients of$f$are taken from$\{0, \pm 1\}$.

Theorem 3.[12] $s_1(\mathbf{r}) \le \|\mathbf{r}\|_1 = \sum\limits_i r_i$for any$\mathbf{r} \in \mathrm{R}_q$.

1.3. Gaussian Distribution and Difficult Problems in Lattice.

Gaussian distribution in lattice is an indispensable part of some signature schemes and signcryption schemes, so we present the following formal definition of discrete Gaussian distribution and some important properties.

Definition 4. (Discrete Gaussian distribution)[15] Let Λ be a lattice, then the discrete Gaussian distribution in Λ with midpoint $\mathbf{c} \in \mathrm{R}^m$ and parameter $\sigma > 0$ can be defined as follows:

$$D_{\Lambda,\sigma,\mathbf{c}} = {}^{\rho_{\sigma,\mathbf{c}}(\mathbf{x})}/_{\rho_{\sigma,\mathbf{c}}(\Lambda)} \tag{7}$$

(7) for $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp\left({}^{-\pi\|\mathbf{x}-\mathbf{c}\|^2}/_{\sigma^2}\right)$ and $\rho_{\sigma,\mathbf{c}}(\Lambda) = \sum\limits_{\mathbf{x}\in\Lambda} \rho_{\sigma,\mathbf{c}}(\mathbf{x})$.

Theorem 4.[12] $s_1(\mathbf{R}) \le s\sqrt{n}\cdot O\left(\sqrt{w}+\sqrt{k}+\omega\left(\sqrt{\log n}\right)\right)$ can be set up with greatly probability if $\mathbf{R}$ obeys the $w \times k$ Gaussian distribution $D_{\mathrm{R}_s,s}^{w\times k}$ with midpoint $\mathbf{c}=0$ and parameter $s>0$ in R_s.

Theorem 5.[12] (Smoothing lemma) Let $n \ge 4$ be a power of 2, $q \ge 3$ be a power of 3, $w \ge 2\lceil\log q\rceil + 2$, $s \ge \omega\left(\sqrt{\ln nq}\right)$, set $\mathrm{R}_q = {}^{\mathrm{Z[x]}}/_{((\mathbf{x}^n+1),q)}$, then the statistical distance between $\sum\limits_i x_i a_i$ and R_q is negligible if we independently and randomly select $x_i\,(i=1,\cdots,w)$ from the Gaussian distribution $D_{\mathrm{R}_q,s}$ with midpoint $\mathbf{c}=0$ and parameter $s>0$ in R_q , select $\mathbf{A}=[a_1,\cdots,a_m]\in\mathrm{R}_q^{1\times m}$ with greatly probability.

Theorem 6.[12] The in-equation $s_1\left((t-t')_{[i]}\right) \le \left\|(t-t')_{[i]}\right\|_1 \le c_i - c_{i-1}$ was established for any $i<d$ and tag $t,t'\in\mathrm{T}$.

Theorem 7.[12] Input the matrix $\mathbf{A}'\in\mathrm{R}_q^{1\times w}$,tag $\mathbf{H}\in\mathrm{R}_q$ and parameter $\sigma > \omega\left(\sqrt{\ln(nw)}\right)$, there has a polynomial time algorithm *Gentrap* $(\mathbf{A}',\mathbf{H},\sigma)$ that outputs the matrix $\mathbf{A}''\in\mathrm{R}_q^{1\times k}$ and a G-trapdoor $\mathbf{R}\in\mathrm{R}_q^{w\times k}$, wherein the tag $\mathbf{H}$ of matrix $\mathbf{A}=[\mathbf{A}',\mathbf{A}'']$ satisfied $s_1(\mathbf{R}) = s\cdot O\left(\sqrt{k}+\sqrt{w}+\omega\left(\sqrt{\log_2 n}\right)\right)$. The matrix $\mathbf{A}'$ obeys uniform distribution with great probability and matrix $\mathbf{A}''$ statistical close to uniform distribution if $w \ge 2(\lceil\log_2 q\rceil)+1$. The algorithm *Gentrap* $(\mathbf{A}',\mathbf{H},\sigma)$ could be abbreviated to algorithm *Gentrap* $(w,\mathbf{H},\sigma)$ if $\mathbf{A}''$ is evenly choose at random. Usually, a scheme in the field of cryptography is based on some difficult mathematical problems. The security of signcryption scheme in this paper is based on SIS assumption.

Definition 5.[10] ($RingSIS_{q,n,m,\beta}$) Given vector $\mathbf{A}\in\mathrm{R}_q^{1\times m}$, let q be an integer, and β be a polynomial, then the problem $RingSIS_{q,n,m,\beta}$ with parameters (q,n,m,β) is: To find a nonzero vector $\mathbf{y}\in\{\mathbf{v}\in\mathrm{Z}^m : \|\mathbf{v}\|\le\beta\}$, which satisfied $\mathbf{Ay}=0 \bmod q$. SIS assumption: The probability of that the enemy could solve the problem SIS successfully is negligible if he doesn't know the trapdoor.

2. **Definitions and Models.**

The formal definition of a ring signature scheme was proposed by Bender, Katz, Morselli et al.[16] in 2009, and the definition of anonymity and unforgeable were also proposed respectively according to different security strength. The anonymity of the scheme in this paper is its strongest definition from the reference [16], and we added the unforgeable requirements to the select-ring security as a related definition of unforgeability that is stronger than the fixed-ring attack model in reference [20]. Therefore, we give the following definition of a identity-based ring signcryption scheme, and one can refer to the model proposed by Bender et al [16] for its security definition.

2.1. **The Formal Definition of An Identity-based Ring Signcryption Scheme.** .

Definition 6. One identity-based ring signcryption scheme should meet the consistency constraint.

$\mathbf{M} = Unsigncrypt\left(\mathbf{P},h',\mathbf{T}_{\mathbf{ID}_r},\mathbf{P}_{\mathbf{ID}_s}\right)ifh' = Signcrypt\left(\mathbf{P},\mathbf{M},\mathbf{T}_{\mathbf{ID}_s},\mathbf{P}_{\mathbf{ID}_r}\right)$, it includes the follows four probability polynomial time (PPT) algorithms:

1) *KeyGen* (n): Input the security parameter n, then one master key$\mathbf{R}$and public parameter *pp* would be outputted;

2) *Extract* $(\mathbf{R},\mathbf{ID})$: Input the public parameter*pp*, the master key$\mathbf{R}$and one user's identity$\mathbf{ID}$, then the corresponding public key and private key $(\mathbf{P}_{\mathbf{ID}},\mathbf{T}_{\mathbf{ID}})$ would be outputted;

3) *Signcrypt* $(\mathbf{P},\mathbf{M},\mathbf{T}_{\mathbf{ID}_s},\mathbf{P}_{\mathbf{ID}_r})$: Input the public parameter*pp*, a senders' ring $\mathbf{P} = (\mathbf{ID}_1,\cdots,\mathbf{ID}_l)$, the private key of $\mathbf{ID}_s\in\mathbf{P}$ is $\mathbf{T}_{\mathbf{ID}_{ss}}$, the public key $\mathbf{P}_{\mathbf{ID}_r}$of the receiver and message $\mathbf{M}$, the ring signcryption h' of $\mathbf{M}$ signed by sender $\mathbf{ID}_s$ would be outputted;

4) *Unsigncrypt* $\left(\mathbf{P}, h^{'}, \mathbf{T}_{\mathbf{ID}_r}, \mathbf{P}_{\mathbf{ID}_s}\right)$: Input the public parameter*pp*, one senders' ring $\mathbf{P} = (\mathbf{ID}_1, \cdot\cdot\cdot, \mathbf{ID}_l)$ and its signcryption $h^{'}$. We would accept the signcryption $h^{'}$ and output one message $\mathbf{M}$ if $h^{'}$ is valid; otherwise output 'Invalid'.

2.2. **The Security Definition of An Identity-based Ring Signcryption Scheme.** Suppose that an identity-based ring signcryption scheme meets 3 conditions: confidentiality, anonymity and unforgeability, then it is considered a secure scheme. We put forward the following formal definitions according to the model that is constructed by Bender et al.

Definition 7. (Anonymity) Suppose that the enemy A could wins the following game in polynomial time, and the preponderance is $P_{adv} = P_{suc} - {}^{1}/_{2}$ with probability P_{suc}. One signcryption scheme is considered to be anonymous if $P_{adv}$is negligible. 1) Input the security parameter n, the mimic B runs algorithm $KeyGen\,(n)$, then sends the results: one master key $\mathbf{R}$ and public parameter *pp* to A;

2) The enemy A submits a senders' ring $\mathbf{P}$, two identities $\mathbf{ID}_0, \mathbf{ID}_1 \in \mathbf{P}$and message $\mathbf{M} \in (0,1)^*$ for signcryption inquiry, B selects $i \in \{0,1\}$ randomly, and computes the private key $\mathbf{T}_{\mathbf{ID}_{si}}$ of $\mathbf{ID}_i$ to runs $Signcrypt\,(\mathbf{P}, \mathbf{M}, \mathbf{T}_{\mathbf{ID}_{si}}, \mathbf{P}_{\mathbf{ID}_r})$, then sends the signcryption $h^{'}$ to A;

3) The enemy A conjectures the signcryption $\mathbf{ID}$ as $i^{'}$, then A wins out if $\mathbf{ID}_{i'} = \mathbf{ID}_i$.

Definition 8. (Unforgeability) Suppose that the probability P_{suc} that A could wins the following game in polynomial time is negligible, then the scheme is considered to be unforgeable and could resist chosen massage and ID attack.

1) Input the security parameter n, the mimic B runs algorithm $KeyGen\,(n)$, then reserves the master key $\mathbf{R}$ and sends public parameter *pp* to A; 2) The enemy A randomly selects one sender $\mathbf{ID} \in \mathbf{P}$ for the private key extraction in polynomial time, the mimic B runs algorithm $Extract\,(\mathbf{R}, \mathbf{ID})$, then sends the result to A;

3) The enemy A selects one senders' ring $\mathbf{P}$and message $\mathbf{M} \in (0,1)^*$for signcryption inquiry in polynomial time, the mimic B runs algorithm $Signcrypt\,(\mathbf{P}, \mathbf{M}, \mathbf{T}_{\mathbf{ID}_s}, \mathbf{P}_{\mathbf{ID}_r})$, then sends the signcryption to A;

4) Output one bogus ring signcryption $h^{''} = \left(\mathbf{t}^{'}, \mathbf{c}^{'}, \mathbf{g}^{'}\right)$ of message$\mathbf{M}^{'}$that is forged by A, we consider that A wins the game if the verification result of $\left(\mathbf{t}^{'}, \mathbf{c}^{'}, \mathbf{g}^{'}\right)$ is message $\mathbf{M}^{'}$ be outputted while none element of $\mathbf{P}^{'}$has been operated the private key extraction inquiry, and $\left(\mathbf{P}^{'}, \mathbf{M}^{'}\right)$ hasn't been operated signcryption inquiry

3. **Our Proposed Signcryption Scheme.** For $i \in \{1, 2, \cdot\cdot\cdot, d\}$, any real constant $c > 1$, $\alpha > {}^{1}/_{(c-1)}$, $d = \lfloor \log_c ({}^{n}/_{2\alpha}) \rfloor = O\,(\log_c n)$, length $c_0 = 0$, $c_i = \lfloor \alpha c^i \rfloor$ is strictly increasing, define the set of tag prefix $\mathrm{T}_i = \{0,1\}^{c_i}$. To ensure every tag prefix $\mathbf{t} = (t_0, t_1, \cdot\cdot\cdot, t_{c_i-1}) \in \mathrm{T}_i$ using related ring element $t\,(x) = \sum_{j<c_i} t_j x^j \in \mathrm{R}_q$, wherein $t_j \in \{0,1\}$, $c_i \le c_d \le {}^{n}/_{2}$, then $t\,(x) - t'\,(x)$ is reversible in R_q for any two different tag prefixes $t, t' \in \mathrm{R}_i$. For any arbitrary full tag $\mathbf{t} \in \mathrm{T} = \mathrm{T}_d$, $i \le d$, note $\mathbf{t}_{\le \mathbf{i}} \in \mathrm{T}_i$ is the prefix of length c_i, $\mathbf{t}_{[\mathbf{i}]} = \mathbf{t}_{\le \mathbf{i}}\,(x) - \mathbf{t}_{\le \mathbf{i-1}}\,(x) \in \mathrm{R}_q$.

This method constructed the tag prefix that is different from the tag in references [11] and [19] is dependent on the reversibility of tags and the property of set descripted in theorem 6, the detailed steps are as follows.

1 $KeyGen\,(n)$: Run algorithm $GenTrap\,(w, \mathbf{I}, \sigma) \to (\mathbf{A}, \mathbf{R})$, setup parameters $\sigma = \omega\left(\sqrt{\log n}\right)$, $\mathbf{A} \in \mathrm{R}_q^{1\times m}$, $\mathbf{R} \in \mathrm{R}_q^{w\times k}$, n is power of 2, $q = 3^k$, $k$is an integer, $m = w + k$, $d + 3$

independent-random vectors $\mathbf{A}_0, \mathbf{B}_0, \cdots, \mathbf{B}_d, \mathbf{U} \in \mathrm{R}_q^{1\times k}$, $v \in \mathrm{R}_q$, and random matrix $\mathbf{L} \in \mathrm{R}_q^{(m+k)\times(m+2k)}$, the system select two collision-resistant hash functions: $H : (0,1)^* \to (0,1)^{m+k}$ and $h : (0,1)^* \to (0,1)^k$, $T_i = 0, 1^{ci}$

The system output master key $\mathbf{R}$, and disclose public parameter $pp = \{\mathbf{A}, \mathbf{A}_0, \mathbf{B}_0, \cdots, \mathbf{B}_d, \mathbf{U}, v, \mathbf{L}\}$.

2 *Extract* $(\mathbf{R}, \mathbf{ID})$: Input the public parameter *pp*, master key $\mathbf{R}$, and compute the public key of the identity $\mathbf{ID}$

$$\mathbf{P_{ID}} = [\mathbf{A}\,|\mathbf{A}_0 + H\,(\mathbf{ID})] \in \mathrm{R}_q^{1\times(m+k)} \tag{8}$$

We could gain $\mathbf{P_{ID}}$' trapdoor $\mathbf{T} \in \mathrm{R}_q^{m\times k}$via algorithm DelTrap by making use of the trapdoor $\mathbf{R}$of $\mathbf{A}$with parameter $\sigma' = \sqrt{n}\cdot\omega(\log n)^{3/2}$, and the senders'(the receivers') public key and private key $(\mathbf{P}_{\mathbf{ID}_s}, \mathbf{T}_{\mathbf{ID}_s})$ ($(\mathbf{P}_{\mathbf{ID}_r}, \mathbf{T}_{\mathbf{ID}_r})$) would be outputted finally.

3 *Signcrypt* $(\mathbf{P}, \mathbf{M}, \mathbf{T}_{\mathbf{ID}_{ss}}, \mathbf{P}_{\mathbf{ID}_r})$:

Input public parameter *pp*, one senders' ring $\mathbf{P} = (\mathbf{ID}_1, \cdots, \mathbf{ID}_l)$, the private key of $\mathbf{ID}_s$is $\mathbf{T}_{\mathbf{ID}_{ss}}$, message $\mathbf{M} \in (0,1)^{nk} \subset \mathrm{R}_q^k$, and randomly select a tag $t \in T = T_d$. Let

$$\mu = h\,(\mathbf{P}\,\|\mathbf{M}) \in \mathrm{R}_q^k \tag{9}$$

$$\mathbf{P}_t = \left[\mathbf{P_{ID}}\,|\mathbf{B}_0 + \sum_{i=1}^{d} t_i\mathbf{B}_i\right] \in \mathrm{R}_q^{1\times(m+2k)} \tag{10}$$

$$u = \mathbf{U}\cdot\mu + v \in \mathrm{R}_q \tag{11}$$

(11) For the trapdoor of $\mathbf{P_{ID}}$could be derived from $\mathbf{P}_t$' trapdoor by extending zero, then according to $\mathbf{P_{ID}}$' trapdoor $\mathbf{T} \in \mathrm{R}_q^{m\times k}$, we could get one random sampling $\mathbf{e} \in \mathrm{R}_q^{m+2k}$in $D_{\Lambda_u^\perp(\mathbf{P}_t),s'}$by running algorithm SampleD with parameter $\mathrm{s}' = \sqrt{d}\cdot n\cdot\omega(\log n)^{5/2}$, let

$$\mathbf{c} = \mathbf{M} \oplus h\,(\mathbf{L}, \mathbf{e}) \in \mathrm{R}_q^k \tag{12}$$

$$\mathbf{g} = \mathbf{P}_{\mathbf{ID}_r}\cdot\mathbf{L} + \mathbf{e} \in \mathrm{R}_q^{m+2k} \tag{13}$$

then the signcryption $h' = (\mathbf{t}, \mathbf{c}, \mathbf{g})$of message $\mathbf{M}$signed by $\mathbf{ID}_s$would be outputted. 4 *Unsigncrypt* $\left(\mathbf{P}, h', \mathbf{T}_{\mathbf{ID}_r}, \mathbf{P}_{\mathbf{ID}_{ss}}\right)$: Input public parameter *pp*, one senders' ring $\mathbf{P} = (\mathbf{ID}_1, \cdots, \mathbf{ID}_l)$ and its signcryption h'. First of all, we should decrypt the ciphertext $h'$by making use of receiver' private key $\mathbf{T}_{\mathbf{ID}_r}$to solve for $\mathbf{L}, \mathbf{e}$. Compute

$$\mathbf{M} = \mathbf{c} \oplus h\,(\mathbf{L}, \mathbf{e}) \in \mathrm{R}_q^k \tag{14}$$

to recover message $\mathbf{M}$, then let

$$\mathbf{P_{ID}} = [\mathbf{A}\,|\mathbf{A}_0 + H\,(\mathbf{ID})] \in \mathrm{R}_q^{1\times(m+k)} \tag{15}$$

$$\mathbf{P}_t = \left[\mathbf{P_{ID}}\,|\mathbf{B}_0 + \sum_{i=1}^{d} t_i\mathbf{B}_i\right] \in \mathrm{R}_q^{1\times(m+2k)} \tag{16}$$

$$\mu = h\,(\mathbf{P}\,\|\mathbf{M}) \in \mathrm{R}_q^k \tag{17}$$

$$u = \mathbf{U}\cdot\mu + v \in \mathrm{R}_q \tag{18}$$

(18) Verify that $\mathbf{P}_t\cdot\mathbf{e} = u\,(\mathrm{mod}q)$and $\|\mathbf{e}\| \le s'\cdot\sqrt{m+2k}$. The receiver would accept signcryption $h'$and message $\mathbf{M}$would also be outputted if equations $\mathbf{P}_t\cdot\mathbf{e} = u\,(\mathrm{mod}q)$and $\|\mathbf{e}\| \le s'\cdot\sqrt{m+2k}$above were valid, otherwise, 'Invalid' would be outputted.

4. **Analyses of Signcryption Scheme.** We present the analysis of the effectiveness, confidentiality, anonymity and unforgeability of the scheme in this paper according to the way that we use to prove a mathematical theorem, and the specific process is as follows.

4.1. Validity Analysis. .

Theorem 6. The identity-based ring signcryption scheme in ideal lattice proposed in this paper is valid. Proof. During the process of algorithm *Signcrypt* $(\mathbf{P}, \mathbf{M}, \mathbf{T}_{\mathbf{ID}_{ss}}, \mathbf{P}_{\mathbf{ID}_r})$, the sender **ID** encrypted message **M** by using the public key $\mathbf{P}_{\mathbf{ID}_r}$ of the receiver, so the latter must makes use of his own private key $\mathbf{T}_{\mathbf{ID}_r}$ to firstly compute the random matrix **L** and signature e during the process of algorithm $Unsigncrypt\left(\mathbf{P}, h^{'}, \mathbf{T}_{\mathbf{ID}_r}, \mathbf{P}_{\mathbf{ID}_{ss}}\right)$, then recovers the message **M**, and verify the signcryption finally. So the signcryption scheme in this paper meets the confidentiality. Since $\sigma = \omega\left(\sqrt{\log n}\right)$, so $\mathbf{A} \in \mathrm{R}_q^{1\times m}$ is close to the uniform distribution in statistics. For **R** is **G**- trapdoor of **A** and $s_1(\mathbf{R}) \leq \sqrt{n} \cdot \omega(\log n)$, so $\left\|\tilde{\mathbf{S}_{\mathbf{A}}}\right\| \leq \sqrt{n} \cdot \omega(\log n)$ and $\eta_\varepsilon\left(\Lambda^\perp(\mathbf{A})\right) \leq \sqrt{n} \cdot \omega(\log n)^{3/2}$. Because $\sigma^{'} = \sqrt{n} \cdot \omega(\log n)^{3/2}$, so

$$\sigma^{'} \geq \eta_\varepsilon\left(\Lambda^\perp(\mathbf{A})\right) \tag{19}$$

Then algorithm Extract could be implemented effectively. For the trapdoor of$\mathbf{P}_{\mathbf{ID}}$could be derived from$\mathbf{P}_t$' trapdoor by extending zero,and $s_1(\mathbf{T}) \leq n \cdot \omega(\log n)^2$, so

$$s^{'} = \sqrt{d} \cdot n \cdot \omega(\log n)^{5/2} > \omega(\log n) \cdot s_1(\mathbf{T}) \tag{20}$$

then algorithm Signcrypt could be implemented effectively, and $\mathbf{P}_t \cdot \mathbf{e} = u\,(\mathrm{mod} q)$, $\|\mathbf{e}\| \leq s^{'} \cdot \sqrt{m + 2k}$. In conclusion, the signcryption scheme in this paper is correct.

4.2. Security analysis.

4.2.1. *Anonymity.* .

Theorem 7. The identity-based ring signcryption scheme in ideal lattice proposed in this paper is unconditionally anonymous. Proof. Input the security parameter , the system randomly selects two collision-resistant hash functions, $d + 3$ Proof. Input the security parameter , the system randomly selects two collision-resistant hash functions, independent-random vectors$\mathbf{A}_0, \mathbf{B}_0, \cdots, \mathbf{B}_d, \mathbf{U} \in \mathrm{R}_q^{1\times k}$,$v \in \mathrm{R}_q$, and one random matrix $\mathbf{L} \in \mathrm{R}_q^{(m+k)\times(m+2k)}$. The mimic B operates algorithm$KeyGen\,(n)$, then the master key **R** and public parameter $pp = \{\mathbf{A}, \mathbf{A}_0, \mathbf{B}_0, \cdots, \mathbf{B}_d, \mathbf{U}, v, \mathbf{L}\}$ would be outputted and sends to A. The enemy A submits one senders' ring **P**, two identities$\mathbf{ID}_0, \mathbf{ID}_1 \in \mathbf{P}$and message$\mathbf{M} \in (0,1)^*$ for signcryption inquiry. The mimic B randomly selects $i \in \{0, 1\}$, operates algorithm *Extract* $(\mathbf{R}, \mathbf{ID})$firstly, then he could gets the public key and private key$(\mathbf{P}_{\mathbf{ID}_{si}}, \mathbf{T}_{\mathbf{ID}_{si}})$ of$\mathbf{ID}_i$ and the receiver's public key and private key$(\mathbf{P}_{\mathbf{ID}_r}, \mathbf{T}_{\mathbf{ID}_r})$. Secondly, B operates algorithm*Signcrypt* $(\mathbf{P}, \mathbf{M}, \mathbf{T}_{\mathbf{ID}_{si}}, \mathbf{P}_{\mathbf{ID}_r})$, and sends the signature of message that is signed by$\mathbf{ID}_i$to A. Suppose that B has made use of the private key $\mathbf{T}_{\mathbf{ID}_{1-i}}$ of $\mathbf{ID}_{1\text{-}i}$for signcryption to get one signature $\mathbf{e}^{'}$, for all valid signatures that are outputted by the sigcryption scheme in this paper are random vectors in a given set for one fixed senders' ring **P**and message **M**, and the verification vector of **e** and $\mathbf{e}^{'}$ is $\mathbf{P}_t$, namely $\mathbf{P}_t \cdot \mathbf{e} = \mathbf{P}_t \cdot \mathbf{e}^{'} = u\,(\mathrm{mod} q)$, therefore the signature e and $e^{'}$have the same discrete Gaussian distribution. That is to say that the advantage P_{adv} of A is negligible, thus the identity-based ring signcryption scheme is anonymous.

4.2.2. *Unforgeability.* .

Theorem 8. Suppose that the enemy A could forges one ring signcryption responding to the scheme in this paper in non-negligible probability and time , then there has one mimic B who could solves problem $RingSIS_{q,n,m,\beta}$with parameter$\beta = dn^3 \cdot \omega(\log n)^{9/2}$ in time $\tau^{'} = \tau + poly\,(n)$ and probability $\varepsilon^{'} = {}^{\varepsilon}/_{|\mathrm{T}_{i^*}|}$ by invoking the algorithm of A, which needs at most polynomial sender's private key inquiry and signcryption inquiry. Proof. We could provide one concrete analysis according to references[11]and[12]as follows:

Setup:n is power of 2,$q = 3^k$,k is a integer,$m = w + k$,$d + 3$ independent-random vectors $\mathbf{A}_0, \mathbf{B}_0, \cdots, \mathbf{B}_d, \mathbf{U} \in \mathrm{R}_q^{1\times k}$,$v \in \mathrm{R}_q$, and random matrix $\mathbf{L} \in \mathrm{R}_q^{(m+k)\times(m+2k)}$, the system randomly selects two collision-resist hash functions:

$H : (0,1)^* \to (0,1)^{m+k}$ and $h : (0,1)^* \to (0,1)^k$, and one tag prefix set $T_i = 0, 1^{ci}$ [10], $\mathbf{P}$ is the largest senders' ring,$H(\mathbf{P}^*) = H(\mathbf{ID}_1) \| \cdots \| H(\mathbf{ID}_{i^*})$
for any ring $\mathbf{P}^* = \{\mathbf{ID}_1, \cdots, \mathbf{ID}_{i^*}\} \in \mathbf{P}$.

For a identity$\mathbf{ID}$, the mimic B operates $(\mathbf{A}_0, \mathbf{R}_0) \leftarrow \mathit{TrapGen}(\mathbf{A}, \mathbf{H}_0, \sigma)$ with parameters $\sigma = \omega\left(\sqrt{\log n}\right)$,$\mathbf{H}_0 = 1 \in \mathrm{R}_q$, then$\mathbf{R}_0$ is one trapdoor of $[\mathbf{A}, \mathbf{A}_0]$, that's $\mathbf{A}_0 = \mathbf{H}_0\mathbf{G} - \mathbf{A}\mathbf{R}_0$. B operates$(H(\mathbf{ID}), \mathbf{R}_{\mathbf{ID}}) \leftarrow \mathit{TrapGen}(\mathbf{A}, \mathbf{H}_{\mathbf{ID}}, \sigma)$ with parameters$\sigma = \omega\left(\sqrt{\log n}\right)$,$\mathbf{H}_0 = \mathbf{ID}$, then$\mathbf{R}_{\mathbf{ID}}$ is one trapdoor of $[\mathbf{A}, H(\mathbf{ID})]$, that's $H(\mathbf{ID}) = \mathbf{H}_{\mathbf{ID}}\mathbf{G} - \mathbf{A}\mathbf{R}_{\mathbf{ID}}$. So we could know by the definition of trapdoor that$\mathbf{R}_0 + \mathbf{R}_{\mathbf{ID}}$ is one trapdoor of $[\mathbf{A}, \mathbf{A}_0 + H(\mathbf{ID})]$, and $\mathbf{H}_0 + \mathbf{H}_{\mathbf{ID}} = \mathbf{ID} - \mathbf{ID}^*$ is invertible when $\mathbf{ID} \neq \mathbf{ID}^*$. B operates$\left(\mathbf{B}_i, \mathbf{R}_i^{'}\right) \leftarrow \mathit{TrapGen}\left(\mathbf{A}, \mathbf{H}_i^{'}, \sigma\right)$ with parameters$i = 0, 1, \cdots, d$,$\sigma = \omega\left(\sqrt{\log n}\right)$. Let

$$\mathbf{H}_i^{'} = \begin{cases} 0 \in \mathrm{R}_q, i > i^* \\ 0 \in \mathrm{R}_q, 1 \le i \le i^* \\ -\mathbf{t}^*_{\le \mathbf{i}^*}, i = 0 \end{cases} \tag{21}$$

then $\mathbf{R}_i^{'}$ is one trapdoor of $[\mathbf{A}, \mathbf{B}_i]$, that's $\mathbf{B}_i = \mathbf{H}_i\mathbf{G} - \mathbf{A}\mathbf{R}_i$.$\mathbf{B}_i$is statically close to the uniform distribution by reasoning from theorem 7. For $\sigma \ge \omega\left(\sqrt{\log n}\right)$, and$s_1\left(\mathbf{R}_i^{'}\right) \le \sqrt{n} \cdot \omega\left(\sqrt{\log n}\right)$, so$\mathbf{R}_t^{'} = \mathbf{R}_0 + \sum\limits_{i=1}^{d} t_i\mathbf{B}_i^{'}$is one trapdoor of $\left[\mathbf{A}, \mathbf{B}_0 + \sum\limits_{i=1}^{d} t_i\mathbf{B}_i\right]$ with tag $\mathbf{H}_t^{'} = \mathbf{t}_{\le \mathbf{i}^*} - \mathbf{t}^*_{\le \mathbf{i}^*}$. Evidently though,$\mathbf{H}_t^{'} = 0$ if$\mathbf{t}^*_{\le \mathbf{i}^*}$ is the prefix of $\mathbf{t}$, that's $\mathbf{t}^*_{\le \mathbf{i}^*} = \mathbf{t}_{\le \mathbf{i}^*}$, otherwise $\mathbf{H}_t^{'}$ is intervible. The mimic B randomly selects $\mathbf{P}^*$,$\mathbf{M}^*$ and $\mathbf{t}^*$ (the extension of $\mathbf{t}^*_{\le \mathbf{i}^*}$) to operated algorithm *Signcrypt* for one signature $\mathbf{e}^* \leftarrow D^m_{\mathrm{R},s}$ of message $\mathbf{M}^*$ signed by $\mathbf{P}^*$. Compute

$$\begin{aligned} \mathbf{P}_{\mathbf{t}*} = \left[\mathbf{P}_{\mathbf{ID}^*} \middle| \mathbf{B}_0 + \sum_{i=1}^{d} t_i\mathbf{B}_i\right] = \\ \left[\mathbf{A} \middle| \mathbf{A}_0 + H(\mathbf{ID}^*) \middle| \mathbf{B}_0 + \sum_{i=1}^{d} t_i\mathbf{B}_i\right] = \\ \left[\mathbf{A} \left| -\mathbf{A}\mathbf{R}_{\mathbf{ID}^*} \right| \mathbf{H}_t^*\mathbf{G} - \mathbf{A}\mathbf{R}_t^*\right] \end{aligned} \tag{22}$$

$$v\,(\mathrm{mod} q) = \mathbf{P}_{t^*} \cdot \mathbf{e}^* - \mathbf{U} \cdot \mu^* \tag{23}$$

Where $\mathbf{R}_{\mathbf{ID}^*}$ is one trapdoor of $\mathbf{P}_{\mathbf{ID}^*}$, and $\mathbf{R}_t^*$is one trapdoor of $\mathbf{P}_{t^*}$. Private key extraction inquiry: The enemy A randomly selects one identity $\mathbf{ID} \in \mathbf{P}$ for private key extraction inquiry in polynomial time, B operates algorithm $\mathit{Extract}(\mathbf{R}, \mathbf{ID})$, and sends the result to A. Signcryption inquiry: The enemy A selects one senders' ring $\mathbf{P}$and message $\mathbf{M} \in (0,1)^*$ for signcryption inquiry in polynomial time, B operates algorithm $\mathit{Signcrypt}(\mathbf{P}, \mathbf{M}, \mathbf{T}_{\mathbf{ID}_s}, \mathbf{P}_{\mathbf{ID}_r})$, and sends the signcryption$h^{'}$ to A. Finally, the enemy A outputs one forged ring signcryption $h^{''} = \left(\mathbf{t}^{'}, \mathbf{c}^{'}, \mathbf{g}^{'}\right)$ of $\mathbf{M}^{'}$, the mimic B hopes that $\mathbf{t}^{'}_{\le \mathbf{i}^*} = \mathbf{t}^*_{\le \mathbf{i}^*}$, and its probability is${}^1/_{|\mathrm{T}_{i^*}|}$. Then B uses the private key $\mathbf{T}_{\mathbf{ID}_r}$ of the receiver to solve for $\mathbf{L}^*$,$\mathbf{e}^*$,$\mathbf{L}^{'}, \mathbf{e}^{'}$, and recover messages$\mathbf{M}^*$ and $\mathbf{M}^{'}$, so

$$\mathbf{P}_{t^*} \cdot \mathbf{e}^* = \mathbf{U} \cdot \mu^* + v\,(\mathrm{mod} q) \tag{24}$$

$$\mathbf{P}_{t^{'}} \cdot \mathbf{e}^{'} = \mathbf{U} \cdot \mu^{'} + v\,(\mathrm{mod} q) \tag{25}$$

For $\mathbf{t}^{'}_{\le \mathbf{i}^*} = \mathbf{t}^*_{\le \mathbf{i}^*}$,$\mathbf{H}^{'}_{t^*} = \mathbf{H}^{'}_{t^{'}} = 0$, on the contrary, terminate the simulation. Compute.

$$\left[\mathbf{A}\left|-\mathbf{A}\mathbf{R}_{\mathbf{ID}^*}\right.\left|-\mathbf{A}\mathbf{R}'_{t^*}\right.\left|-\mathbf{A}\mathbf{R}_{\mathbf{U}}\right.\right]\cdot\begin{bmatrix}\mathbf{e}_1^*\\ \mathbf{e}_2^*\\ \mathbf{e}_3^*\\ \mu^*\end{bmatrix}=v\,(\mathrm{mod}q)=\left[\mathbf{A}\left|-\mathbf{A}\mathbf{R}_{\mathbf{ID}'}\right.\left|-\mathbf{A}\mathbf{R}'_{t'}\right.\left|-\mathbf{A}\mathbf{R}_{\mathbf{U}}\right.\right]\cdot\begin{bmatrix}\mathbf{e}_1^{'}\\ \mathbf{e}_2^{'}\\ \mathbf{e}_3^{'}\\ \mu^{'}\end{bmatrix} \tag{26}$$

Let $\mathbf{y}=\left(\mathbf{e}_1^*-\mathbf{e}_1^{'}\right)+\left(\mathbf{R}_{\mathbf{ID}'}\mathbf{e}_2^{'}-\mathbf{R}_{\mathbf{ID}^*}\mathbf{e}_2^*\right)+\left(\mathbf{R}_{t'}\mathbf{e}_3^{'}-\mathbf{R}_{t^*}\mathbf{e}_3^*\right)+\mathbf{R}_{\mathbf{U}}\left(\mu^{'}-\mu^*\right)$, then $\mathbf{Ay}=0\,(\mathrm{mod}q)$. It is obvious that $\mathbf{y}$ is a small positive integer that is valid in greatly probability(specific proof could be found in reference[10]). For $\mathbf{e}^*,\mathbf{e}^{'}$ are valid signatures, $\|\mathbf{e}^*\|,\|\mathbf{e}^{'}\|\le s^{'}\cdot\sqrt{m+2k}\le\sqrt{d}\cdot n^{3/2}\cdot\omega(\log n)^{5/2}$. $s_1\left(\mathbf{R}_t^{'}\right)\le n\cdot\omega(\log n)^2$, $s_1\left(\mathbf{R}_{\mathbf{ID}}\right)\le n^{3/2}\cdot\omega\left(\log n\right)$,$\|\mu^*\|,\|\mu^{'}\|\le O\left(nk\right)$,$s_1\left(\mathbf{R}_{\mathbf{U}}\right)=\sqrt{n}\cdot\omega\left(\log n\right)$for any$\mathbf{t}\in\mathrm{T}$. Above all, $\|\mathbf{y}\|\le dn^3\cdot\omega(\log n)^{9/2}$. Because the probability of one successful simulation is according to$|\mathrm{T}_{i^*}|$, so $\varepsilon^{'}={}^{\varepsilon}/_{|\mathrm{T}_{i^*}|}$.

5. **Conclusions.** The identity-based signcryption scheme in lattice is one of important developments in digital signature that could resist quantum computation, and ensure the security of electronic cash payment system, security certification and so on. Based on the assumption of the hardness of lattice problem SIS, we proposed one identity-based ring signcryption scheme that is provably secure under the standard model by using the trapdoor generation algorithm proposed by Micciancio et al.[13] and the ideal lattice technology presented by Ducas[10]. It is confidential, anonymous, unforgeable, and fortunately, it has shorter public key, private key and higher operation efficiency compared with previous schemes. It could be extended to the identity-based proxy/blind signcryption scheme in ideal lattice, and the next direction of work is try to design new signature or signcryption schemes with shorter key and signature based on ideal lattice.

REFERENCES

[1] Y. L. Zheng. Digital signcryption or how to achieve cost(signature & encryption) cost(signature) + cost(encryption), *Proc of CRYPTO97*, 1997, pp. 165-179.

[2] J. Malone-L. Identity-based signcryption [EB/OL]. In Proceedings of Public Key Cryptography(PKC). http://eprint.lacr.Org/2002/098.

[3] B. libert, J. J. quisquater. A new identity-based signcryption scheme from pairings, *Proc of hte IEEE Information Theory Workshop*, 2003, pp. 155-168.

[4] S. M. Chow, S. yiu, L. Hui, et al. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity, *Proc of Information Security and Cryptology,* 2004, pp. 352-269.

[5] P. barreto, b libert, n mccullagh. Efficient forward and provably secure ID-based signatures and signcryption from bilinear maps, *Proc of ASIACRYPT05*, 2005, pp. 515-532.

[6] G. Yu, X. Ma, Y. Shen, et al. Provable secure identity-based generalized signcryption scheme *Journal of Theoretical Computer Science* , 2010. vol. 411, no. (40-42), pp. 3614-3624.

[7] S. Li, C. Zeng, J L. Identity-based signcryption scheme , *Journal of Computer Engineering*, 2010, vol. 36, no. 8, pp. 135-137(in Chinese).

[8] L. J. Pang, H. X. Li, J J Cui, Y. M. Wang. Design and analysis of a fair ID-based multi-receiver anonymous signcryption , *Journal of Journal of Software*, 2014, vol. 25, no. 10, pp. 2409-2420 (in Chinese).

[9] L Z Deng,X B Wang, Y Y Qu. High-efficient signcryption scheme based on identity , *Journal of Computer Engineering & Science*,2014,36(3), pp. 441-445.

[10] P W Shor. Polynomial-time algorithm for prime fac-torization and discrete logarithms on a quantum computer, Siam Review, 1997, vol. 26, no. 5, pp. 1484-1509.

[11] D Micciancio, C Peikert. Trapdoors for lattices, pp. Simpler, tighter, faster, smaller [C] In, Advances in CryptologyEUROCRYPT 2012. Berlin: Springer, 2012, pp. 700718.

[12] L. ducas, d micciancio. Improved short lattice signatures in the standard model [C] In: Advances in Cryptology-Crypto 2014. Springer Berlin Heidelberg, 2014, pp. 335-352.

[13] D. T. Yang, C. G. Xu, L. xu, X. Zhang. Identity-based signature scheme over ideal lattices , *Journal of Journal of Cryptologic Research*, 2015, vol. 2, no. 4, pp. 306316.

[14] M. Ajtai. Generating hard instances of lattice problems [C] In: Proceeding of the 28th Annual ACM Symposium on Theory of Computing. 1996, pp. 99-108.

[15] D. MIcciancio. Improved cryptographic hash functions without worst-case/average-case connection. Proceedings of the thiry-fourth annual ACM symposium on Theory of computing, 2002, pp. 609-618.

[16] V. Lyubashevsky, D Micciancio. Generalized compact knapsacks are collision resistant , *Journal of Electronic Colloquium on Computational Complexity*, 2006, no. 142, pp. 144-155.

[17] A .Bender, J. Katz, R. Morselli. Ring signature: Stronger definitions, and constructions without random oracles. *Journal of Cryptology*, 2009, vol. 22, no. 1, pp. 114-138.

[18] F H WANG, Y P HU, C X WANG. A lattice-based ring signature scheme from bonsai trees. *Journal of Electronic & Information Technology*, 2010, vol. 32, no. 10, pp. 2400-2403(in Chinese).

[19] X. BOYEN. Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more [C]// PKC 2010: Proceedings of the 2010 Public Key Cryptography. Berlin Springer, 2010, pp. 499- 517.

[20] Y. H. Li, M. M. Tian, L. S. Huang. An identity-based ring signature scheme from lattice , *Journal of Journal of Chinese Computer Systems*, 2013, vol. 34, no. 8, pp. 1768-1771.

[21] Y. R. Sun, X. Q. Liang, Y. F. Shang. An identity-based signature scheme in ideal lattice , *Journal of Journal of applications of computer*, 2016, vol. 36, no.7, pp. 1861-1865.