INFORMATICA, 2019, Vol. 30, No. 3, 595–612

DOI: http://dx.doi.org/10.15388/Informatica.2019.220

Efficient Certificate-Based Signature with Short Key and Signature Sizes from Lattices

Yuh-Min TSENG*, Tung-Tso TSAI, Jui-Di WU, Sen-Shan HUANG

Department of Mathematics, National Changhua University of Education, Jin-De Campus,
Chang-Hua City 500, Taiwan
e-mail: ymtseng@cc.ncue.edu.tw

Received: May 2018; accepted: March 2019

Abstract. Certificate-based cryptography (CB-PKC) is an attractive public key setting, which reduces the complexity of public key infrastructure in traditional public key settings and resolves the key escrow problem in ID-based public key settings. In the past, a large number of certificate-based signature and encryption schemes were proposed. Nevertheless, the security assumptions of these schemes are mainly relied on the difficulties of the discrete logarithm and factorization problems. Unfortunately, both problems will be resolved when quantum computers come true in the future. Public key cryptography from lattices is one of the important candidates for post-quantum cryptography. However, there is little work on certificate-based cryptography from lattices. In the paper, we propose a new and efficient certificate-based signature (CBS) scheme from lattices. Under the short integer solution (SIS) assumption from lattices, the proposed CBS scheme is shown to be existential unforgeability against adaptive chosen message attacks. Performance comparisons are made to demonstrate that the proposed CBS scheme from lattices is better than the previous lattice-based CBS scheme in terms of private key size and signature size.

Key words: lattice, certificate-based signature, post-quantum cryptography, short integer solution.

1. Introduction

In traditional public key settings (Rivest *et al.*, 1978; ElGamal, 1985), a public key infrastructure (PKI) is required to manage users' certificates, which are issued by a trusted certificate authority (CA) to offer the link relationships between users' identities and the associated public keys. When a party would like to use the other party's public key, she/he must first inquire and validate the certificate of the other party using the public key infrastructure. Typically, certificate management in such a public key infrastructure is pricey.

To simplify certificate management in traditional public key settings, Shamir (1984) presented the notion of identity (ID)-based public key settings while Boneh and Franklin (2001) realized the ID-based public key setting from the Weil pairing and presented the first ID-based encryption scheme. For the cryptographic schemes (Tseng *et al.*, 2016; Tsai *et al.*, 2017) under ID-based public key settings, a trusted private key generator (PKG) is responsible to generate private keys of all users, but such settings suffer from the

*Corresponding author.

key escrow problem. To solve the key escrow problem, Al-Riyami and Paterson (2003) proposed a new public key paradigm, namely, certificateless public key setting. Nevertheless, both ID-based and certificateless public key settings did not employ public key certificates so that both public key settings must offer extra revocation mechanisms to revoke compromised users from the public key settings. Fortunately, several studies (Tseng and Tsai, 2012; Tsai and Tseng, 2015; Hung *et al.*, 2016b; Tseng *et al.*, 2018; Wu *et al.*, 2018) have well addressed the revocation problem of ID-based and certificateless public key settings.

The other solution resolving the key escrow problem in ID-based public key settings is the notion of certificate-based public key settings, which is presented by Gentry (2003). In the meantime, it also simplifies certificate management and the complexity of public key infrastructure, in traditional public key settings. In Gentry's certificate-based public key setting, a user independently generates the associated private/public keys while sending the public key to a certificate authority (CA). By the user's public key and identity information, the CA generates a certificate and sends it to the user. For the revocation problem, the CA may update non-revoked users' certificates periodically without requiring extra revocation mechanisms. When a user would like to decrypt a ciphertext or sign a message, the user must own both private key and valid certificate. Numerous certificate-based cryptographic studies have been proposed, such as certificate-based encryption schemes (Galindo *et al.*, 2008; Lu and Li, 2014; Gao *et al.*, 2015) and certificate-based signature schemes (Li *et al.*, 2007; Wu *et al.*, 2009; Li *et al.*, 2012; Hung *et al.*, 2016a).

As we all know, the security of cryptographic mechanisms must be based on the difficulties or assumptions of some hard problem. Typically, most of the existing cryptographic schemes/protocols under aforementioned public key settings are mainly relied on the difficulties of the discrete logarithm and factorization problems with large prime numbers. Unfortunately, both problems will be resolved when quantum computers come true in the future. In such a case, those cryptographic schemes/protocols based on both hard problems would become insecure (Shor, 1997). Recently, researchers have constructed several new mathematical approaches to withstand quantum attacks. Lattice-based cryptography is one of the main candidates for post-quantum cryptography because of its efficiency and security (Bernstein, 2009).

1.1. *Related Work*

Under traditional public key settings, Goldreich *et al.* (1997) proposed the first signature and encryption schemes from lattices. Afterward, several lattice-based signature schemes (Gentry *et al.*, 2008; Lyubashevsky, 2009; 2012) were proposed to enhance security and performance. Gentry *et al.* (2008) adopted the Gaussian sampling technique to generate a user's private key while employing the hash-and-sign approach to sign a message. In such a case, the size of the resulting private key is too large while the computation cost of the signing process is inefficient. To improve the signing performance, Lyubashevsky (2009) employed the Fiat-Shamir transformation technique to generate signatures. Furthermore, Lyubashevsky (2012) proposed the other lattice-based signature scheme which uses the rejection sampling technique to sign a message while reducing the signature size.

By employing Gentry *et al.*'s private key generation method (Gentry *et al.*, 2008), Ruckert (2010) presented two ID-based signature schemes from lattices. Both schemes were, respectively, proved to be secure in the random oracle model and the standard model. However, the sizes of private key and the resulting signature are still lengthy. To improve the security and performance, lattice-based IBS schemes (Liu *et al.*, 2013; Tian and Huang, 2014) were proposed. For the revocation problem of ID-based public key settings, Xiang (2015) adopted the binary tree structure to construct a revocable ID-based signature scheme from lattices. In addition, by the revocation technique in Tseng and Tsai (2012), Tseng *et al.* (2018), Hung *et al.* (2017a) employed the NTRU lattices in Ducas *et al.* (2014) to shorten the private key and signature sizes.

Tian and Huang (2015) proposed the first lattice-based certificateless signature scheme. They also employed Gentry *et al.*'s method (Gentry *et al.*, 2008) to generate users' private keys so that the sizes of private key and the resulting signature turn out to be lengthy. Very recently, Hung *et al.* (2017b) employed the revocation technique of certificateless public key setting in Tsai and Tseng (2015), Hung *et al.* (2016b) to present the first lattice-based revocable certificateless signature scheme while improving the performance of Tain and Huang's scheme.

In the past, there is little work on the design of certificate-based signature (CBS) scheme over lattices. Indeed, Tian and Huang (2015) also presented the first CBS scheme from lattices. The proposed scheme was proved to be existential unforgeability against adaptive chosen message attacks in the random oracle model. In addition, as Tain and Huang's lattice-based certificateless signature scheme, their CBS scheme from lattices also employs the same method in Gentry *et al.* (2008) to generate private key. The form of a user's private key generated in Gentry *et al.* (2008) consists of two matrices $\mathbf{M}_1 \in Z_q^{n_1 \times k}$ and $\mathbf{M}_2 \in Z_q^{n_2 \times k}$, where $n_1, n_2 > 5k \log q$ and q is a prime number. Hence, in Tain and Huang's CBS scheme, the size of the resulting signature is also lengthy. In such a case, their scheme is inefficient.

1.2. *Contribution and Organization*

In the paper, a new and efficient certificate-based signature (CBS) scheme from lattices is proposed. In our scheme, a user's certificate and private key are generated by using Ducas *et al.*'s key extract algorithm over NTRU lattices in Ducas *et al.* (2014). Instead of Gentry *et al.*'s key extract algorithm over GPV lattices Gentry *et al.*, 2008, Ducas *et al.*'s key extract algorithm employed a particular sampling algorithm to produce short trapdoor (private key or certificate). Furthermore, we employ the rejection sampling technique to sign a message. The size of the resulting signature is also shortened. Hence, our CBS scheme from lattices has shorter private key and signature sizes than Tain and Huang's CBS scheme from lattices (Tian and Huang, 2015). Under the short integer solution (SIS) assumption from lattices (Micciancio and Regev, 2007), the proposed CBS scheme is shown to be existential unforgeability against adaptive chosen message attacks for two adversaries, namely, Type I (general attacker) and Type II (malicious CA). Performance comparisons are made to demonstrate that the proposed CBS scheme from lattices is better than the previous lattice-based CBS schemes.

The rest of the paper is organized as follows. In Section 2, we present several preliminaries. The framework and security notions for CBS schemes are given in Section 3. A new and efficient CBS scheme from lattices is presented in Section 4. In Section 5, the security of the proposed CBS scheme is demonstrated. In Section 6, we present performance comparisons. In Section 7, conclusions are given.

2. Preliminaries

Here, we present several preliminaries that include notations, concepts of lattices, Gaussion distribution, Gaussion sampling algorithm, rejection sampling algorithm, and security assumptions over lattices.

2.1. *Notations*

Several parameters throughout this article are defined as follows:

- N: a specific power-of-two integer.
- Z: the set of integers.
- R: the set of real values.
- Z_q: the set of integers in the interval $[-q/2, q/2)$, where q is a positive integer.
- R_q: $R_q = Z_q[X]/(X^N + 1)$, which is a ring of polynomials with coefficients in Z_q modulo $X^N + 1$.
- R^N, Z^N, Z_q^N, R_q^N: a N-vector (or N elements) of R, Z, Z_q and R_q, respectively.
- $\mathbf{x}$: a vector.
- $\mathbf{X}$: a matrix.
- $\|\mathbf{x}\|$: $\|\mathbf{x}\| = \sqrt{\sum \mathbf{x}_i^2}$ denotes the Euclidean norm of a vector $\mathbf{x}$.
- $\|\mathbf{X}\|_\infty$: $\|\mathbf{X}\|_\infty = \max[\|\mathbf{X}_i\|]$ denotes the maximum norm of all columns of a matrix $\mathbf{X}$.

2.2. *Anticirculant Matrices*

Here, we introduce the definition (Definition 1) of an anticirculant matrix and its properties (Lemma 1) as follows.

Definition 1. An $N \times N$ anticirculant matrix of $f \in R_q$ is a Toeplitz matrix represented by

$$\mathbf{C}_N(f) = \begin{bmatrix} (f) \\ (x \cdot f) \\ \vdots \\ (x^{N-1} \cdot f) \end{bmatrix} = \begin{bmatrix} f_0 & f_1 & f_2 & \cdots & f_{N-1} \\ -f_{N-1} & f_0 & f_1 & \cdots & f_{N-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -f_1 & -f_2 & \cdots & \cdots & f_0 \end{bmatrix},$$

where $f = \sum_{i=0}^{N-1} f_i x_i \in R_q$. In the sequel, $\mathbf{C}_N(f)$ is abbreviated as $\mathbf{C}(f)$.

Lemma 1. (*See* Ducas *et al.*, 2014.) *Let* $\mathbf{C}_N(f)$ *and* $\mathbf{C}_N(g)$ *be anticirculant matrices, we have* $\mathbf{C}_N(f)+\mathbf{C}_N(g)=\mathbf{C}_N(f+g)$ *and* $\mathbf{C}_N(f)\cdot\mathbf{C}_N(g)=\mathbf{C}_N(f\cdot g)$*, where* $f,g\in R_q$*.*

2.3. *Lattice and NTRU Lattice*

A lattice is a full-rank subgroup of R^n and an NTRU lattice is convolution modular lattices with a particularly efficient class, which are defined as follows.

Definition 2. Let $\mathbf{B}=\{\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_n\}$ be the basis of the n-dimensional lattice Λ, where $\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_n\in R^n$ and n are linearly independent vectors. The lattice Λ generated by the basis $\mathbf{B}$ is defined as below:

$$\Lambda=\mathcal{L}(\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_n)=\left\{\sum_{i=1}^{n}x_i\mathbf{v}_i : x_i\in R^n\right\}.$$

Definition 3. Let f, g $\in R_q$, $h=g*f^{-1}$ and q is a positive integer. The NTRU lattice $\Lambda_{h,q}=\{(u,v)\in R_q^2|u+v*h=0\}$ is a full-rank lattice of Z_q^{2N}. Indeed, the lattice $\Lambda_{h,q}$ may be generated by these rows (vectors) of

$$\mathbf{A}_{h,q}=\begin{bmatrix}-\mathbf{C}_N(h) & \mathbf{I}_N\\ q\mathbf{I}_N & \mathbf{O}_N\end{bmatrix},$$

where $\mathbf{O}_N$ is the $N\times N$ null matrix and $\mathbf{I}_N$ is the $N\times N$ unit matrix.

Indeed, the basis $\mathbf{A}_{h,q}$ is not well suitable to solve the general lattice problem when h is a uniform distribution in R_q. Thus, Hoffstein *et al.* (2003) constructed the other appropriate basis of $\Lambda_{h,q}$ as

$$\mathbf{B}_{f,g}=\begin{bmatrix}\mathbf{C}(g) & -\mathbf{C}(f)\\ \mathbf{C}(G) & -\mathbf{C}(F)\end{bmatrix},$$

where $F,G\in R_q$ such that $f*G-g*F=q$. Indeed, $\mathbf{B}_{f,g}$ is a short basis for $\Lambda_{h,q}$ and has the following properties.

Lemma 2. (*See* Ducas *et al.*, 2014.) *If* $f,g,F,G\in R_q$ *such that* $f*G-g*F=q$ *and* $h=g*f^{-1}$*, the short basis,* $\mathbf{B}_{f,g}$ *may generate the same NTRU lattice* $\Lambda_{h,q}$ *generated by the basis ,* $\mathbf{A}_{h,q}$ *while satisfying* $\|\mathbf{B}_{f,g}\|\leqslant\|\mathbf{A}_{h,q}\|$.

Lemma 3. (*See* Ducas *et al.*, 2014.) *Let* N *and* q *be a power-of-two integer and a prime, respectively. There exists a probabilistic polynomial-time* (*PPT*) *algorithm* **TrapGen**(q,N) *that may generate two polynomials* f *and* g *while computing* $h=g*f^{-1}$*, and output a short trapdoor basis* $\mathbf{B}_{f,g}$ *of* $\Lambda_{h,q}$*. It is worth mentioning that* h *is statistically close to be uniform in* R_q *and publicly published.*

2.4. *Gaussian Distribution and Sampling Technique*

In this section, we define the Gaussian distributions and sampling technique, which are useful tools for lattice-based cryptography.

Definition 4. The continuous Gaussian distribution over R^N with the centre $\mathbf{c} \in R^N$ and the standard deviation $s > 0$, is defined as

$$\rho^N_{\mathbf{c},s}(\mathbf{x}) = \left(\frac{1}{s\sqrt{2\pi}}\right)^{N e^{\frac{-\|\mathbf{x}-\mathbf{c}\|_2^2}{2s^2}}}, \quad \text{where } \mathbf{x} \in R^N.$$

Definition 5. For any lattice $\Lambda \in Z^N$, the discrete Gaussian distribution over Z^N with the standard deviation $s > 0$ and the centre $\mathbf{c} \in Z^N$, is defined as $D^N_{\mathbf{c},s}(\mathbf{x}) = \rho^N_{\mathbf{c},s}(\mathbf{x})/\rho^N_{\mathbf{c},s}(\Lambda)$, where $\mathbf{x} \in Z^N$ and $\rho^N_{\mathbf{c},s}(\Lambda) = \sum_{\mathbf{x}\in\Lambda} \rho^N_{\mathbf{c},s}(\mathbf{x})$. In the sequel, $\rho^N_{0,s}$ and $D^N_{0,s}$ are abbreviated as ρ^N_s and D^N_s respectively.

For the discrete Gaussian distribution $D^N_{\mathbf{c},\sigma}(\mathbf{x})$, Lyubashevsky (2012) gave two properties as follows.

Lemma 4. (*See* Lyubashevsky, 2012.) *Let* $\mathbf{c} \in Z^N$.

(1) *If* $\sigma = \omega(\|\mathbf{c}\|\sqrt{\log N})$, *we have* $Pr[\mathbf{x} \in D^N_\sigma; D^N_\sigma(\mathbf{x})/D^N_{\mathbf{c},\sigma}(\mathbf{x}) = O(1)] = 1 - 2^{-\omega(\log N)}$.

(2) *If* $\alpha > 0$ *and* $\sigma = \alpha\|\mathbf{c}\|$, *we have* $Pr[\mathbf{x} \in D^N_\sigma; D^N_\sigma(\mathbf{x})/D^N_{\mathbf{c},\sigma}(\mathbf{x}) < e^{12/\alpha+1/(2\sigma^2)}] = 1 - 2^{-100}$.

In the following, let us introduce the Gaussian sampling technique over general lattices. Indeed, one takes a noise vector from a Gaussian distribution and adds this noise vector to a lattice, she/he may obtain a distribution which is very close to uniform distribution (Micciancio and Regev, 2007). Based on this fact, Gentry *et al.* (2008) proposed a trapdoor (private key) generation algorithm by using the Gaussian sampling technique from lattices. Furthermore, Ducas *et al.* (2014) improved Gentry *et al.*'s trapdoor generation algorithm to propose a specific sampling algorithm over NTRU lattices to reduce the private key size by using a short basis $\mathbf{B}_{f,g}$ generated in Lemma 2. Ducas *et al.*'s trapdoor generation algorithm has the following property.

Lemma 5. (*See* Ducas *et al.*, 2014.) *Let* $\mathbf{B}_{f,g}$ *be a short basis of an N-dimensional lattice* Λ. *Let* $\tilde{\mathbf{B}}_{f,g}$ *be the Gram–Schmidt orthogonalization of* $\mathbf{B}_{f,g}$. *If* $s \geqslant \|\tilde{\mathbf{B}}_{f,g}\|\omega(\sqrt{\log N})$ *and* $0 < \varepsilon < 1$, *we have*

$$Pr\big[\|\mathbf{x} - \mathbf{c}\| > s\sqrt{N}\big] \leqslant \frac{1+\varepsilon}{1-\varepsilon}2^{-N} \quad \textit{for any } \mathbf{c} \in Z^N \textit{ and } \mathbf{x} \in D^N_{\mathbf{c},s}.$$

And there exists an PPT algorithm $\mathbf{GauSample}(\mathbf{B}_{f,g}, s, \mathbf{c})$ *that produces a distribution statistically close to* $D^N_{\mathbf{c},s}$.

2.5. *Rejection Sampling Technique*

In our CBS scheme from lattices, we employ the rejection sampling technique to sign a message. The rejection sampling technique was proposed by Lyubashevsky (2012). Its idea is to make the distribution of a resulting signature be independent of the signing key. In addition, the rejection sampling technique requires just a few matrix-vector multiplications and rejection samplings so that it is simple and efficient. The idea of the rejection sampling technique works as follows. If a signer with the signing key $\mathbf{S}$ would like to generate a signature σ on a message m, the signer first chooses a random vector $\mathbf{y}$ from some distribution (i.e. Gaussian distribution) and computes the candidate signature $\mathbf{z}$. Namely, the signer first uses the signing key $\mathbf{S}$ to multiply the resulting vector $\mathbf{c}$ of some function with inputting message m and then adds the random vector $\mathbf{y}$, denoted as $\mathbf{z} = \mathbf{Sc} + \mathbf{y}$. Without loss of generality, let the distribution $D_\sigma^N(\mathbf{x})$ be the target distribution and the signature is the distribution vector $D_{\mathbf{Sc},\sigma}^N(\mathbf{x})$. If $D_\sigma^N(\mathbf{x}) \leqslant M \cdot D_{\mathbf{Sc},\sigma}^N(\mathbf{x})$ for all $\mathbf{x}$, then the candidate signature $\mathbf{z}$ may be generated with probability $D_\sigma^N(\mathbf{z})/M \cdot D_{\mathbf{Sc},\sigma}^N(\mathbf{z})$. If the resulting signature does not satisfy the above condition, then the signature $\mathbf{z}$ will be rejected. The expected number of times that the process generates a valid signature is M.

2.6. *SIS Assumption from Lattices*

Here, we present a mathematical assumption, called the short integer solution (SIS) assumption from lattices. The difficulty of the SIS problem is equal to that of the worst-case of short independent vector problem (SIVP) up to a polynomial approximation factor (Ajtai, 1996). The SIS problem and assumption are defined as follows.

Definition 6. $\mathrm{SIS}_{q,N,\beta}$ problem: let q be a positive integer, β be a real number, and $f_1, f_2, \dots, f_N$ be polynomials chosen uniformly and independently from R_q. The $\mathrm{SIS}_{q,N,\beta}$ problem is to find non-zero integers $r_1, r_2, \dots, r_N$ such that $\sum_{i=1}^N r_i f_i = 0$ mod q and $\|(r_1, r_2, \dots, r_N)\| \leqslant \beta$.

Definition 7. $\mathrm{SIS}_{q,N,\beta}$ assumption: for the $\mathrm{SIS}_{q,N,\beta}$ problem defined above, there exists no probabilistic polynomial-time adversary A with non-negligible probability who can find such non-zero integers $r_1, r_2, \dots, r_N$.

By Ducas *et al.* (2014), the SIS problem on NTRU lattices is to find a pair $(\mathbf{z}_1, \mathbf{z}_2)$ such that $\mathbf{z}_1 + h * \mathbf{z}_2 = 0$ and $\|(\mathbf{z}_1, \mathbf{z}_2)\| \leqslant \beta$. The statistical distance between the distribution of $h = g/f$ and the uniform distribution of R_q is negligible (Stehle and Steinfeld, 2013).

3. Framework and Adversary Model of CBS

In this section, the framework and adversary model of certificate-based signature (CBS) schemes are defined here. They are identical to the framework and adversary model in Li *et al.* (2007), Wu *et al.* (2009), Li *et al.* (2012), Hung *et al.* (2016a).

In a CBS scheme, there are two kinds of roles, namely, users (signers/verifiers) and a trusted certificate authority (CA). A user independently generates her/his private/public key pair and sends the public key to the CA. And, the CA uses a system private key to generate and send the associated certificate to the user. An CBS scheme consists of five algorithms, namely, *Setup*, *User key generation*, *Certificate extract*, *Sign* and *Verify* algorithms defined as follows.

Definition 8. A certificate-based signature (CBS) scheme consists of five algorithms:

- Setup algorithm is probabilistic, which is performed by the CA. It takes as input a security parameter and returns the system private key S_{CA} and public parameters PP. The system private key S_{CA} is kept secret by the CA itself.
- User key generation algorithm is probabilistic, which is performed by users. It takes as input the identity *ID* of a user and returns the associated private key S_{ID} and public key P_{ID}. In addition, it also publishes the public key P_{ID} in a public directory.
- Certificate extract algorithm is deterministic, which is performed by the CA. It takes as input the system private key S_{CA}, the public parameters PP and a user's identity *ID* with public key P_{ID}, and returns the associated certificate C_{ID} to the user.
- Sign algorithm is probabilistic, which is performed by users. It takes as input a message m, her/his private key S_{ID} and certificate C_{ID}, and returns a signature ρ.
- Verify algorithm is deterministic, which is performed by users. It takes as input a signature ρ, a message m and a user's identity *ID* with the public key P_{ID}, and outputs either "accept" or "reject".

In the following, we define the existential unforgeability of CBS schemes against adaptive chosen-message attacks (EUF-CBS-ACMA). The EUF-CBS-ACMA attacks consist of two types of adversaries, namely, Type I and Type II adversaries.

- Type I adversary (uncertified entity): This adversary is a general attacker (uncertified entity) who can obtain secret key of any entity. Meanwhile, it is allowed to acquire certificate of any entity, except the certificate of an attacking target entity.
- Type II adversary (honest-but-curious CA): This adversary acts as the honest-but-curious CA so that it holds the system private key S_{CA} and can generate certificate of any entity. Meanwhile, it is allowed to acquire secret key of any entity, except the secret key of an attacking target entity.

In the following, an adversary model of CBS schemes against the EUF-CBS-ACMA attacks is presented.

Definition 9. An CBS scheme provides existential unforgeability against adaptive chosen-messageattacks (EUF-CBS-ACMA) if no probabilistic polynomial-time (PPT) adversary A has a non-negligible advantage in the following game played between a challenger C and the adversary A.

- Setup. The challenger C runs the Setup algorithm to generate the system private key S_{CA} and public parameters PP. In addition, PP is sent to A. If A is of Type I adversary,

S_{CA} is kept secret by C. If A is of Type II adversary, C sends the system private key S_{CA} to A.

- Queries. The adversary A may adaptively issue the following queries to the challenger C. It is worth mentioning that if A is of Type II adversary, it does not need to issue the certificate extract query since Type II adversary knows the system private key S_{CA} and may compute the certificates of all the users.
  - User key generation query(ID). C performs the User key generation algorithm to return the associated private key S_{ID} and public key P_{ID} of the user with identity ID to A.
  - Certificate extract query(ID, P_{ID}). C performs the Certificate extract algorithm to return the associated certificate C_{ID} of the user with identity ID to A.
  - Corruption query(ID). C returns the associated private key S_{ID} of the user with identity ID to A.
  - Public key replacement query(ID, P'_{ID}). The adversary A chooses a new public key P'_{ID} for the user with identity ID. C records this public key replacement in a public directory. Meanwhile, it denotes that A knows the associated private key S_{ID} of the user with identity ID.
  - Sign query(m, ID). Given a message m and identity ID with the public key P_{ID}, C generates a valid signature ρ and returns it to A.
- Forgery. Finally, the adversary A produces a signature tuple $(\rho^*, m^*, ID^*, P_{ID^*})$. The advantage of A is defined as the probability that A wins the game. We say that A wins the game if the following conditions hold.
  1. The response of the Verify algorithm on $(\rho^*, m^*, ID^*, P_{ID^*})$ is "accept".
  2. (m^*, ID^*) has never been issued in the sign query.
  3. If A is of Type I adversary, ID^* has never been issued in the Certificate extract query.
  4. If A is of Type II adversary, it does not know the private key of the attacking target entity ID^*, namely, ID^* has never been issued in the User key generation, Public key replacement and Corruption queries.

4. An Efficient CBS Scheme from Lattices

Here, we propose a new and efficient CBS scheme from lattices. By the framework defined in Section 3, the proposed CBS scheme consists of five algorithms as below.

- *Setup* algorithm: Assume that N, q and λ are, respectively, a security parameter, a large prime and a positive integer while setting two standard deviations $s > 0$ and $\sigma > 0$. The CA runs $\mathbf{TrapGen}(q, N)$ in Lemma 3 to produce two polynomials f and g and compute $h = g * f^1$, where $f, g \in R_q$ and $\|f\|, \|g\| < s\sqrt{N}$ while h is statistically close to be uniform in R_q. In the meantime, the CA also produces is a short trapdoor basis $\mathbf{B}_{f,g}$ of the lattice $\Lambda_{h,q}$, which is viewed as the system private key S_{CA}. The CA chooses two values $p_1, p_2 \in Z_q^N$ and sets the system public key as (h, p_1, p_2). In addition, the CA selects two hash functions H_1:$\{0, 1\}^* \times Z_q^N \to Z_q^N$

and H_2:$\{0,1\}^* \times Z_q^N \times Z_q^N \to \{\mathbf{v} : \mathbf{v} \in \{-1,0,1\}^N, \|\mathbf{v}\|_1 \leqslant \lambda\}$, where $\|\mathbf{v}\|_1$ denotes the amount of non-zero elements of $\mathbf{v}$. Finally, the CA sets the public parameters PP=$\langle N, \lambda, s, \sigma, q, h, p_1, p_2, H_1, H_2\rangle$.

- *User key generation* algorithm: The user with identity ID sets her/his private key $S_{ID} = (\mathbf{s}_1, \mathbf{s}_2)$, which is randomly and uniformly chosen from $\{-d, \dots, 0, \dots, d\}^N$, where $1 \leqslant d \leqslant 31$. Meanwhile, the user computes the associated public key $P_{ID} = p_1 * \mathbf{s}_1 + p_2 * \mathbf{s}_2$.
- *Certificate extract* algorithm: Upon receiving the identity ID and public key P_{ID} of a user, the CA computes $T_{ID} = H_1(ID, P_{ID}) \in z_q^N$ and generates the user's certificate $C_{ID} = (\mathbf{s}_3, \mathbf{s}_4)$ such that $\mathbf{s}_3 + h * \mathbf{s}_4 = T_{ID}$ and $\|(\mathbf{s}_3, \mathbf{s}_4)\| < s\sqrt{2N}$ by running **GauSample**($\mathbf{B}$, s, $(T_{ID}, 0)$) in Lemma 5. The CA returns the certificate $C_{ID} = (\mathbf{s}_3, \mathbf{s}_4)$ to the user via a secure channel.
- *Sign* algorithm: Given a message $m \in \{0,1\}^*$, the user with the private key $S_{ID} = (\mathbf{s}_1, \mathbf{s}_2)$ and certificate $C_{ID} = (\mathbf{s}_3, \mathbf{s}_4)$ randomly selects $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3$ and $\mathbf{y}_4$ from the distribution D_σ^N, and computes the following values:

$$\begin{aligned}
\mathbf{c} &= H_2(m, p_1 * \mathbf{y}_1, p_2 * \mathbf{y}_2, \mathbf{y}_3 + h * \mathbf{y}_4);\\
\mathbf{z}_1 &= \mathbf{y}_1 + \mathbf{s}_1 * \mathbf{c};\\
\mathbf{z}_2 &= \mathbf{y}_2 + \mathbf{s}_2 * \mathbf{c};\\
\mathbf{z}_3 &= \mathbf{y}_3 + \mathbf{s}_3 * \mathbf{c};\\
\mathbf{z}_4 &= \mathbf{y}_4 + \mathbf{s}_4 * \mathbf{c},
\end{aligned}$$

where $\|(\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4)\| \leqslant 2\sigma\sqrt{4N}$. If $\|(\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4)\| \leqslant 2\sigma\sqrt{4N}$ does not hold, the user reruns this algorithm. By (Lyubashevsky, 2012), there exists a constant $M = O(1)$ such that the user can produce such a signature $\rho = (\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4, \mathbf{c})$ with probability $\min(D_\sigma^{4N}(\mathbf{z})/M D_{v,\sigma}^{4N}(\mathbf{z}), 1)$, where

$$\mathbf{z} = \left[\mathbf{z}_1^T \| \mathbf{z}_2^T \| \mathbf{z}_3^T \| \mathbf{z}_4^T\right]^T$$

and

$$\mathbf{v} = \left[(\mathbf{s}_1 * \mathbf{c})^T \,\|\, (\mathbf{s}_2 * \mathbf{c})^T \,\|\, (\mathbf{s}_3 * \mathbf{c})^T \,\|\, (\mathbf{s}_4 * \mathbf{c})^T\right]^T.$$

- *Verify* algorithm: Given a signature $\rho = (\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4, \mathbf{c})$, a message m and a user's identity ID with public key P_{ID}, a verifier validates the signature by the equality

$$\mathbf{c} = H_2(m, p_1 * \mathbf{z}_1 + p_2 * \mathbf{z}_2 - P_{ID} * \mathbf{c}, \mathbf{z}_3 + h * \mathbf{z}_4 - T_{ID} * \mathbf{c}).$$

If the equality holds, the algorithm returns "accept". Otherwise, the algorithm returns "reject". The correctness of the equality follows by

$$\begin{aligned}
&H_2(m, p_1 * \mathbf{z}_1 + p_2 * \mathbf{z}_2 - P_{ID} * \mathbf{c}, \mathbf{z}_3 + h * \mathbf{z}_4 - T_{ID} * \mathbf{c})\\
&\quad = H_2(m, p_1 * (\mathbf{y}_1 + \mathbf{s}_1 * \mathbf{c}) + p_2 * (\mathbf{y}_2 + \mathbf{s}_2 * \mathbf{c}) - (p_1 * \mathbf{s}_1 + p_2 * \mathbf{s}_2) * \mathbf{c},
\end{aligned}$$

$$\begin{aligned}&\mathbf{y}_3 + \mathbf{s}_3 * \mathbf{c} + h * (\mathbf{y}_4 + \mathbf{s}_4 * \mathbf{c}) - (\mathbf{s}_3 + h * \mathbf{s}_4) * \mathbf{c})\\ &= H_2(m, p_1 * \mathbf{y}_1 + p_2 * \mathbf{y}_2, \mathbf{y}_3 + h * \mathbf{y}_4).\end{aligned}$$

5. Security Analysis

According to the framework and adversary model of CBS schemes, the signing key of a user with identity *ID* include two components, namely, the private key S_{ID} and the associated certificate C_{ID}. By the EUF-CBS-ACMA game aforementioned in Definition 9, there are two kinds of adversaries, namely, Type I adversary (uncertified entity) and Type II adversary (honest-but-curious CA). Type I adversary is a general attacker without knowing the system private key S_{CA} so that it did not compute the certificate of an attacking target entity. Type II adversary acts as the honest-but-curious CA so that it holds the system private key S_{CA}, but does not know the private key of the attacking target entity.

The security analysis of the proposed CBS scheme is formally proved as follows. In Theorem 1, we prove that our CBS scheme from lattices is secure against Type I adversary (uncertified entity). Theorem 2 shows that the proposed CBS scheme is secure against Type II adversary (honest-but-curious CA).

Theorem 1. *Let two hash functions H_1 and H_2 be random oracles controlled by a challenger in the EUF-CBS-ACMA game. If there exists a probabilistic polynomial-time (PPT) adversary A (Type I adversary, general attacker) with non-negligible probability who can break our CBS scheme over lattices, an algorithm C can be constructed to solve the SIS problem from lattices with non-negligible probability $(1 - 2^{-\omega(\log N)})\varepsilon$, where N is the security parameter.*

Proof. Assume that N, q and λ are, respectively, a security parameter, a large prime and a positive integer while setting two standard deviations $s > 0$ and $\sigma > 0$. Assume that the algorithm C be a challenger in the EUF-CBS-ACMA game while receiving a random instance $(q, 2N, 2\lambda s\sqrt{2N} + 4\sigma\sqrt{2N})$ of the SIS problem. In the following, we demonstrate that the challenger C may obtain a non-zero vector solution $(\mathbf{u}_1, \mathbf{u}_2) \in R_q^2$ of the SIS problem if the adversary A with non-negligible probability ε who can break our CBS scheme.

- *Setup*. As the Setup algorithm in the proposed CBS scheme, C randomly chooses $p_1, p_2 \in Z_q^N$ and $h \in R_q$ while controlling the random oracles H_1 and H_2. C sets the public parameters PP=$\langle N, \lambda, s, \sigma, q, h, p_1, p_2, H_1, H_2\rangle$ and sends them to A. Initially, C constructs three empty lists L_1, L_2 and L_S.
- *Queries*. A may issue several queries to C adaptively as below:
  - H_1 *query*: Let L_1 consist of tuples of the form $\langle ID_i, P_{ID_i}, C_{ID_i}, T_{ID_i}\rangle$. For the query along with (ID_i, P_{ID_i}), C returns a response to this query by the following procedures.
    1. Search (ID_i, P_{ID_i}) in L_1. If the tuple is found, it means that this query has been already issued and the same answer T_{ID_i} is sent to A.

2. Otherwise, randomly select $\mathbf{s}_{i3}, \mathbf{s}_{i4} \in D_s^N$ such that $\|(\mathbf{s}_{i3}, \mathbf{s}_{i4})\| < s\sqrt{2N}$, and compute $T_{ID_i} = \mathbf{s}_{i3} + h * \mathbf{s}_{i4}$. Finally, C adds $\langle ID_i, P_{ID_i}, C_{ID_i} = (\mathbf{s}_{i3}, \mathbf{s}_{i4}), T_{ID_i} \rangle$ in L_1 and sends T_{ID_i} to A.

- H_2 *query*: Let L_2 consist of tuples of the form $\langle m_j, v_j, w_j, \mathbf{c}_j \rangle$. For the query along with (m_j, v_j, w_j), C returns a response to this query by the following procedures.
  1. Search (m_j, v_j, w_j) in L_2. If the tuple is found, it means that this query has been already issued and the same answer $\mathbf{c}_j$ is sent to A.
  2. Otherwise, randomly select $\mathbf{c}_j \in Z_q^N$. Finally, C adds $\langle m_j, v_j, w_j, \mathbf{c}_j \rangle$ in L_2 and sends $\mathbf{c}_j$ to A.
- *User key generation query*: Let L_S consist of tuples of the form $\langle ID_i, S_{ID_i}, P_{ID_i} \rangle$. For the query along with ID_i, C returns a response to this query by the following procedures.
  1. Search ID_i in L_S. If the tuple is found, it means that this query has been already issued and the same answer $S_{ID_i} = (\mathbf{s}_{i1}, \mathbf{s}_{i2})$ is sent to A.
  2. Otherwise, randomly select $\mathbf{s}_{i1}, \mathbf{s}_{i2} \in \{-d, \dots, 0, \dots, d\}^N$, where $1 \leqslant d \leqslant 31$, and compute the public key $P_{ID_i} = (p_1 * \mathbf{s}_{i1} + p_2 * \mathbf{s}_{i2})$ Finally, C adds $\langle ID_i, S_{ID_i}, P_{ID_i} \rangle$ in L_S and sends $S_{ID_i} = (\mathbf{s}_{i1}, \mathbf{s}_{i2})$ to A.
- *Certificate extract query*: For the query along with (ID_i, P_{ID_i}), C returns a response to this query by the following procedures.
  1. Search (ID_i, P_{ID_i}) in L_1. If the tuple is found, it means that this query has been already issued and the same answer C_{ID_i} is sent to A.
  2. Otherwise, issue the H_1 query to obtain the tuple $\langle ID_i, P_{ID_i}, C_{ID_i}, T_{ID_i} \rangle$ and return C_{ID_i} to A.
- *Corruption query*: For the query along with ID_i, C returns a response to this query by the following procedures.
  1. Search ID_i in L_S. If the tuple is found, it means that this query has been already issued and the same answer S_{ID_i} is sent to A.
  2. Otherwise, issue the *User key generation query* to obtain the tuple $\langle ID_i, S_{ID_i}, P_{ID_i} \rangle$ and return S_{ID_i} to A.
- *Public key replacement query*: A issues this query along with a new public key P'_{ID_i} of ID_i to replace the old public key P_{ID_i}, C replaces the P_{ID_i} of $\langle ID_i, S_{ID_i}, P_{ID_i} \rangle$ in L_S with P'_{ID_i}.
- *Sign query*: For the query along with a message m_j and (ID_i, P_{ID_i}), the challenger C performs the following procedures to generate a valid signature.
  1. Respectively search ID_i in L_1 and L_S to get the tuples $\langle ID_i, P_{ID_i}, C_{ID_i}, T_{ID_i} \rangle$ and $\langle ID_i, S_{ID_i}, P_{ID_i} \rangle$
  2. Randomly choose $\mathbf{c}_j \in \{\mathbf{v} : \mathbf{v} \in \{-1, 0, 1\}^N, \|\mathbf{v}\|_1 \leqslant \lambda\}$ and $\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4 \in D_\sigma^N$ such that $\|(\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4)\| \leqslant 2\sigma\sqrt{4N}$, and compute $v_j = p_1 * \mathbf{z}_1 + p_2 * \mathbf{z}_2$ - $P_{ID_i} * \mathbf{c}_j$ and $w_j = \mathbf{z}_3 + h * \mathbf{z}_4$ - $T_{ID_i} * \mathbf{c}_j$.
  3. Send the signature $\rho = (\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4, \mathbf{c}_j)$ to A while adding $\langle m_j, v_j, w_j, \mathbf{c}_j \rangle$ in L_2. Note that the signature ρ is valid because the following equality holds:

$$\begin{aligned}\mathbf{c}_j &= H_2(m_j, p_1 * \mathbf{z}_1 + p_2 * \mathbf{z}_2 - P_{ID_i} * \mathbf{c}_j, \mathbf{z}_3 + h * \mathbf{z}_4 - T_{ID_i} * \mathbf{c}_j) \\ &= H_2(m_j, v_j, w_j)\end{aligned}$$

- *Forgery*. Finally, the adversary A generates a signature tuple $(\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{z}_3^*, \mathbf{z}_4^*, \mathbf{c}^*)$ on some message m^* for some ID^*.

Assume that A may generate a valid signature $\rho^* = (\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{z}_3^*, \mathbf{z}_4^*, \mathbf{c}^*)$. By the Forking lemma (Pointcheval and Stern, 2000), the challenger C can generate the other valid signature $(\mathbf{z}_1', \mathbf{z}_2', \mathbf{z}_3', \mathbf{z}_4', \mathbf{c}')$ such that $\mathbf{c}^* \neq \mathbf{c}'$ by the same random tape with different hash value of H_2 *query*. Because $(\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{z}_3^*, \mathbf{z}_4^*, \mathbf{c}^*)$ and $(\mathbf{z}_1', \mathbf{z}_2', \mathbf{z}_3', \mathbf{z}_4', \mathbf{c}')$ are two valid signatures on the message m^* for (ID^*, P_{ID^*}), we can obtain the equality

$$\begin{aligned}&H_2\big(m^*, p_1 * \mathbf{z}_1^* + p_2 * \mathbf{z}_2^* - P_{ID^*} * \mathbf{c}^*, \mathbf{z}_3^* + h * \mathbf{z}_4^* - T_{ID^*} * \mathbf{c}^*\big) \\ &\quad = H_2\big(m^*, p_1 * \mathbf{z}_1' + p_2 * \mathbf{z}_2' - P_{ID^*} * \mathbf{c}', \mathbf{z}_3' + h * \mathbf{z}_4' - T_{ID^*} * \mathbf{c}'\big),\end{aligned}$$

which reduces to

$$\mathbf{z}_3^* + h * \mathbf{z}_4^* - T_{ID^*} * \mathbf{c}^* = \mathbf{z}_3' + h * \mathbf{z}_4' - T_{ID^*} * \mathbf{c}'.$$

Since $T_{ID^*} = \mathbf{s}_3 + h * \mathbf{s}_4$, we have

$$\begin{aligned}&\mathbf{z}_3^* + h * \mathbf{z}_4^* - (\mathbf{s}_3 + h * \mathbf{s}_4) * \mathbf{c}^* = \mathbf{z}_3' + h * \mathbf{z}_4' - (\mathbf{s}_3 + h * \mathbf{s}_4) * \mathbf{c}'; \\ &\mathbf{z}_3^* - \mathbf{z}_3' - \mathbf{s}_3\big(\mathbf{c}^* - \mathbf{c}'\big) + h * \big(\mathbf{z}_4^* - \mathbf{z}_4' - \mathbf{s}_4\big(\mathbf{c}^* - \mathbf{c}'\big)\big) = 0; \\ &(1, h) * \big(\mathbf{z}_3^* - \mathbf{z}_3' - \mathbf{s}_3\big(\mathbf{c}^* - \mathbf{c}'\big), \mathbf{z}_4^* - \mathbf{z}_4' - \mathbf{s}_4\big(\mathbf{c}^* - \mathbf{c}'\big)\big) = 0.\end{aligned}$$

Afterward, C sets $(\mathbf{u}_1, \mathbf{u}_2) = (\mathbf{z}_3^* - \mathbf{z}_3' - \mathbf{s}_3(\mathbf{c}^* - \mathbf{c}'), \mathbf{z}_4^* - \mathbf{z}_4' - \mathbf{s}_4(\mathbf{c}^* - \mathbf{c}'))$.

If we have $\|(\mathbf{z}_3^* - \mathbf{z}_3', \mathbf{z}_4^* - \mathbf{z}_4')\| \leqslant 4\sigma\sqrt{2N}$ and $\|(\mathbf{s}_3, \mathbf{s}_4)\| \leqslant s\sqrt{2N}$ with overwhelming probability, we can obtain $\|(\mathbf{u}_1, \mathbf{u}_2)\| \leqslant 2\lambda s\sqrt{2N} + 4\sigma\sqrt{2N}$. As stated in Lemma 3, the distribution of $h = g/f$ is statistically close to the uniform distribution of R_q (Stehle and Steinfeld, 2013). The SIS problem on NTRU lattice is to find a pair $(\mathbf{u}_1, \mathbf{u}_2) \in R_q^2$ such that $\mathbf{u}_1 + h * \mathbf{u}_2 = 0$ and $\|(\mathbf{u}_1, \mathbf{u}_2)\| \leqslant \beta$, where β is $2\lambda s\sqrt{2N} + 4\sigma\sqrt{2N}$. According to the same probability analysis in Lyubashevsky (2012), since A can break our CBS scheme with non-negligible probability ε, we may construct the challenger C to solve the SIS problem with non-negligible probability$(1 - 2^{-\omega(\log N)})\varepsilon$. □

Theorem 2. *Let two hash functions H_1 and H_2 are random oracles controlled by a challenger in the EUF-CBS-ACMA game. If there exists an PPT adversary A (Type II adversary, honest-but-curious CA) with non-negligible probability ε who can break our CBS scheme from lattices, an algorithm C can be constructed to resolve the SIS problem from lattices with non-negligible probability $(1 - 2^{-\omega(\log N)})\varepsilon$, where N is the security parameter.*

Proof. Assume that N, q and λ are, respectively, a security parameter, a large prime and a positive integer while setting $1 \leqslant d \leqslant 31$ and two standard deviations $s > 0$ and $\sigma > 0$. Assume that the algorithm C be a challenger in the EUF-CBS-ACMA game while receiving a random instance $(q, 2N, 2\lambda d\sqrt{2N} + 4\sigma\sqrt{2N})$ of the SIS problem. In the following, we demonstrate that the challenger C may obtain a non-zero vector solution $(\mathbf{u}_1, \mathbf{u}_2) \in R_q^2$ of the SIS problem if the adversary A with non-negligible probability ε who can break our CBS scheme.

- *Setup*. As the Setup algorithm in the proposed CBS scheme, C sets the public parameters $PP = \langle N, \lambda, s, \sigma, q, h, p_1, p_2, H_1, H_2\rangle$, where H_1 and H_2 are random oracles. C also produces a short trapdoor basis $\mathbf{B}$ of the lattice $\Lambda_{h,q}$, which is viewed as the system private key S_{CA}. In the meantime, the system private key S_{CA} and the public parameters $PP = \langle N, \lambda, s, \sigma, q, h, p_1, p_2, H_1, H_2\rangle$ are sent to A. Initially, C constructs three empty lists L_1, L_2 and L_S.
- *Queries*. A may issue several queries to C adaptively as below:
  - H_1 *query*: Let L_1 consist of tuples of the form $\langle ID_i, P_{ID_i}, C_{ID_i}, T_{ID_i}\rangle$. For the query along with (ID_i, P_{ID_i}), C returns a response to this query by the following procedures.
    1. Search (ID_i, P_{ID_i}) in L_1. If the tuple is found, it means that this query has been already issued and the same answer T_{ID_i} is sent to A.
    2. Otherwise, randomly select $T_{ID_i} \in Z_q^N$ and perform **GauSample**($\mathbf{B}$, $\mathbf{s}$, $(T_{ID}, 0)$) to get $\mathbf{s}_{i3}, \mathbf{s}_{i4} \in D_s^N$ such that $\|(\mathbf{s}_{i3}, \mathbf{s}_{i4})\| < s\sqrt{2N}$. Finally, the challenger C adds $\langle ID_i, P_{ID_i}, C_{ID_i} = (\mathbf{s}_{i3}, \mathbf{s}_{i4}), T_{ID_i}\rangle$ in L_1 and sends T_{ID_i} to A.
  - H_2 *query*: As the response of H_2 query in Theorem 1.
  - *User key generation query*: Let L_S consist of tuples of the form $\langle ID_i, S_{ID_i}, P_{ID_i}\rangle$. For the query along with ID_i, C returns a response to this query by the following procedures.
    1. Search ID_i in L_S. If the tuple is found, it means that this query has been already issued and the same answer $S_{ID_i} = (\mathbf{s}_{i1}, \mathbf{s}_{i2})$ is sent to A.
    2. Otherwise, randomly select $\mathbf{s}_{i1}, \mathbf{s}_{i2} \in \{-d, \dots, 0, \dots, d\}^N$, where $1 \leqslant d \leqslant 31$, and compute the public key $P_{ID_i} = (p_1 * \mathbf{s}_{i1} + p_2 * \mathbf{s}_{i2})$ Finally, C adds $\langle ID_i, S_{ID_i}, P_{ID_i}\rangle$ in L_S and sends $S_{ID_i} = (\mathbf{s}_{i1}, \mathbf{s}_{i2})$ to A.
  - *Certificate extract query*: As the response of *User key generation query* in Theorem 1.
  - *Corruption query*: As the response of *User key generation query* in Theorem 1.
  - *Public key replacement query*: A issues this query along with a new public key P'_{ID_i} of ID_i to replace the old public key P_{ID_i}, C replaces the P_{ID_i} of $\langle ID_i, S_{ID_i}, P_{ID_i}\rangle$ in L_S with P'_{ID_i}.
  - *Sign query*: As the response of *User key generation query* in Theorem 1.
- *Forgery*. Finally, the adversary A generates a signature tuple $(\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{z}_3^*, \mathbf{z}_4^*, \mathbf{c}^*)$ on some message m^* for some ID^*.

Assume that A may generate a valid signature $\rho^* = (\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{z}_3^*, \mathbf{z}_4^*, \mathbf{c}^*)$. By the Forking lemma (Pointcheval and Stern, 2000), the challenger C can generate the other valid signature $(\mathbf{z}'_1, \mathbf{z}'_2, \mathbf{z}'_3, \mathbf{z}'_4, \mathbf{c}')$ such that $\mathbf{c}^* \neq \mathbf{c}'$ by the same random tape with different hash value of H_2 *query*. Because $(\mathbf{z}_1^*, \mathbf{z}_2^*, \mathbf{z}_3^*, \mathbf{z}_4^*, \mathbf{c}^*)$ and $(\mathbf{z}_1', \mathbf{z}_2', \mathbf{z}_3', \mathbf{z}_4', \mathbf{c}')$ are two valid signatures on the message m^* for (ID^*, P_{ID^*}), we can obtain the equality

$$\begin{aligned} & H_2\big(m^*, p_1 * \mathbf{z}_1^* + p_2 * \mathbf{z}_2^* - P_{ID^*} * \mathbf{c}^*, \mathbf{z}_3^* + h * \mathbf{z}_4^* - T_{ID^*} * \mathbf{c}^*\big) \\ & \quad = H_2\big(m^*, p_1 * \mathbf{z}_1' + p_2 * \mathbf{z}_2' - P_{ID^*} * \mathbf{c}', \mathbf{z}_3' + h * \mathbf{z}_4' - T_{ID^*} * \mathbf{c}'\big), \end{aligned}$$

which reduces to

$$p_1 * \mathbf{z}_1^* + p_2 * \mathbf{z}_2^* - P_{ID^*} * \mathbf{c}^* = p_1 * \mathbf{z}_1' + p_2 * \mathbf{z}_2' - P_{ID^*} * \mathbf{c}'.$$

Since $P_{ID_i} = p_1 * \mathbf{s}_{i1} + p_2 * \mathbf{s}_{i2}$, we have

$$\begin{aligned} & p_1 * \mathbf{z}_1^* + p_2 * \mathbf{z}_2^* - (p_1 * \mathbf{s}_{i1} + p_2 * \mathbf{s}_{i2}) * \mathbf{c}^* \\ & \quad = p_1 * \mathbf{z}_1' + p_2 * \mathbf{z}_2' - (p_1 * \mathbf{s}_{i1} + p_2 * \mathbf{s}_{i2}) * \mathbf{c}'; \\ & p_1 * \big(\mathbf{z}_1^* - \mathbf{z}_1'\big) + p_2 * \big(\mathbf{z}_2^* - \mathbf{z}_2'\big) - p_1 * \mathbf{s}_{i1}\big(\mathbf{c}^* - \mathbf{c}'\big) - p_2 * \mathbf{s}_{i2}\big(\mathbf{c}^* - \mathbf{c}'\big) = 0; \\ & p_1 * \big(\mathbf{z}_1^* - \mathbf{z}_1' - \mathbf{s}_{i1}\big(\mathbf{c}^* - \mathbf{c}'\big)\big) + p_2 * \big(\mathbf{z}_2^* - \mathbf{z}_2' - \mathbf{s}_{i2}\big(\mathbf{c}^* - \mathbf{c}'\big)\big) = 0; \\ & (p_1, p_2) * \big(\mathbf{z}_1^* - \mathbf{z}_1' - \mathbf{s}_{i1}\big(\mathbf{c}^* - \mathbf{c}'\big), \mathbf{z}_2^* - \mathbf{z}_2' - \mathbf{s}_{i2}\big(\mathbf{c}^* - \mathbf{c}'\big)\big) = 0. \end{aligned}$$

Afterward, C sets $(\mathbf{u}_1, \mathbf{u}_2) = (\mathbf{z}_1^* - \mathbf{z}_1' - \mathbf{s}_{i1}(\mathbf{c}^* - \mathbf{c}'), \mathbf{z}_2^* - \mathbf{z}_2' - \mathbf{s}_{i2}(\mathbf{c}^* - \mathbf{c}'))$.

If we have $\|(\mathbf{z}_1^* - \mathbf{z}_1', \mathbf{z}_2^* - \mathbf{z}_2')\| \leqslant 4\sigma\sqrt{2N}$ and $\|(\mathbf{s}_1, \mathbf{s}_2)\| \leqslant 2d\lambda\sqrt{2N}$ with overwhelming probability, we can obtain $\|(\mathbf{u}_1, \mathbf{u}_2)\| \leqslant 2d\lambda\sqrt{2N} + 4\sigma\sqrt{2N}$. As stated in Lemma 3, the distribution of $h = g/f$ is statistically close to the uniform distribution of R_q (Stehle and Steinfeld, 2013). The SIS problem on NTRU lattice is to find a pair $(\mathbf{u}_1, \mathbf{u}_2) \in R_q^2$ such that $\mathbf{u}_1 + h * \mathbf{u}_2 = 0$ and $\|(\mathbf{u}_1, \mathbf{u}_2)\| \leqslant beta$, where β is $2d\lambda\sqrt{2N} + 4\sigma\sqrt{2N}$. According to the same probability analysis in Lyubashevsky (2012), since A can break our CBS scheme with non-negligible probability ε, we may construct the challenger C to solve the SIS problem with non-negligible probability $(1 - 2^{-\omega(\log N)})\varepsilon$. □

6. Comparisons

Table 1 lists the comparisons between Tian and Huang's CBS scheme (Tian and Huang, 2015) and our CBS scheme in terms of lattice type, private key size/bit-length and signature size/bit- length. For the generation of a user's private key, Tian and Huang's CBS scheme adopted the GPV lattice in Gentry *et al.* (2008), instead, our proposed CBS scheme employed Ducas *et al.*'s sampling algorithm over NTRU lattices (Ducas *et al.*, 2014). For both the private key size and signature size under the same security parameters N=512, $q \approx 2^{26}$, $k = 512$, $\lambda = 14$ and $d = 31$, our scheme is better than those of Tian and Huang's CBS scheme. By Lyubashevsky (2012), we have $n_1 > 2N \log q$, $n_2 > 64 + N \log q$, $s_1 = \sqrt{n_1}\omega(\sqrt{\log N})$, $s_2 = \sqrt{n_2}\omega(\sqrt{\log N})$, $\sigma_1 = 12 s_1 \lambda n_1$, $\sigma_2 = 12 s_2 \lambda n_2$, $s = N^{5/2}\sqrt{2q}\omega(\sqrt{\log N})$, $\sigma = 12 s \lambda N$ while choosing $n_1 = 38400$ and $n_2 = 25600$. According to Table 1, our scheme is much better than Tian and Huang's CBS scheme in terms of private key and signature sizes.

Table 1
Comparisons between Tian and Huang's CBS scheme and ours.

	Tian and Huang's CBS scheme (Tian and Huang, 2015)	Our CBS scheme
Lattice type	GPV lattice	NTRU lattice
Private key size	$2n_1k\log(s_1\sqrt{n_1}) + 2n_2k\log(s_2\sqrt{n_2})$	$4N\log(s\sqrt{N})$
Private key bit-length	595222811	85166
Signature size	$n_1\log(12\sigma_1) + n_2\log(12\sigma_2) + \lambda(\log k + 1)$	$4N\log(12\sigma) + \lambda(\log N + 1)$
Signature bit-length	675496	87161

7. Conclusions

Lattice-based cryptography is an important candidate for post-quantum cryptography. In the paper, a new and efficient CBS scheme from lattices was proposed, which possesses the merits of both CBS scheme and lattice-based cryptography. Based on the SIS assumption from lattices and in the random oracle model, we formally demonstrated the security of our lattice-based CBS scheme against Type I adversary (general attackers) and Type II adversary (the honest-but-curious CA), namely, achieving existential unforgeability against adaptive chosen message attacks for both adversaries. Comparisons with the previous CBS schemes from lattices were given to demonstrate the merits of our proposed CBS scheme in terms of private key size and signature size.

Acknowledgements. This research was partially supported by Ministry of Science and Technology, Taiwan, under contract no. MOST106-2221-E-018-007-MY2.

References

Ajtai, M. (1996). Generating hard instances of lattice problems. In: *Proceedings of STOC'96*. ACM, pp. 99–108.

Al-Riyami, S.S., Paterson, K.G. (2003). Certificateless public key cryptography. In: *Proceedings of ASIACRYPT'03*, *LNCS*, Vol. 2894, pp. 452–473.

Bernstein, D.J. (2009). Introduction to post-quantum cryptography. In: *Post-Quantum Cryptography*. Springer-Verlag, Berlin, Germany, pp. 1–14.

Boneh, D., Franklin, M. (2001). Identity-based encryption from the Weil pairing. In: *Proceedings of CRYPTO'01*, *LNCS*, Vol. 2139, pp. 213–229.

Ducas, L., Lyubashevsky, V., Prest, T. (2014). Efficient identity-based encryption over NTRU lattices. In: *Proceedings of ASIACRYPT'14*, *LNCS*, Vol. 8874, pp. 22–41.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4), 469–472.

Galindo, D., Morillo, P., Rafols, C. (2008). Improved certificate-based encryption in the standard model. *Journal of Systems and Software*, 81(7), 1218–1226.

Gao, W., Wang, G., Wang, X., Chen, K. (2015). Generic construction of certificate-based encryption from certificateless encryption revisited. *The Computer Journal*, 58(10), 2747–2757.

Gentry, C. (2003). Certificate-based encryption and the certificate revocation problem. In: *Proceedings of EURORYPT'03*, *LNCS*, Vol. 2656, pp. 272–293.

Gentry, C., Peikert, C., Vaikuntanathan, V. (2008). How to use a short basis: trapdoors for hard lattices and new cryptographic constructions. In: *Proceedings of STOC'08*. ACM, pp. 197–206.

Goldreich, O., Goldwasser, S., Halevi, S. (1997). Public-key cryptosystems from lattice reduction problems. In: *Proceedings of CRYPTO'97*, *LNCS*, Vol. 1294, pp. 112–131.

Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J., Whyte, W. (2003). Ntrusign: digital signatures using the ntru lattice. In: *Proceedings of CT-RSA'03*, *LNCS*, Vol. 2612, pp. 122–140.

Hung, Y.H., Huang, S.S., Tseng, Y.M. (2016a). A short certificate-based signature scheme with provable security. *Information Technology and Control*, 45(3), 243–253.

Hung, Y.H., Tseng, Y.M., Huang, S.S. (2016b). A revocable certificateless short signature scheme and its authentication application. *Informatica*, 27(3), 549–572.

Hung, Y.H., Tseng, Y.M., Huang, S.S. (2017a). Revocable ID-based signature with short size over lattices. *Security and Communication Networks*, 2017. Article ID-7571201.

Hung, Y.H., Tseng, Y.M., Huang, S.S. (2017b). Lattice-based revocable certificateless signature. *Symmetry*, 9. Article ID-242.

Li, J., Huang, X., Mu, Y., Susilo, W., Wu, Q. (2007). Certificate-based signature: security model and efficient construction. In: *Proceedings of EUROPKI'07*, *LNCS*, Vol. 4582. pp. 110–125.

Li, J., Huang, X., Zhang, Y., Xu, L. (2012). An efficient short certificate-based signature scheme. *Journal of Systems and Software*, 85(2), 314–322.

Liu, Z.H., Hu, Y.P., Zhang, X.S., Li, F. (2013). Efficient and strongly unforgeable identity-based signature scheme over lattices in the standard model. *Security and Communication Networks*, 6(1), 69–77.

Lu, Y., Li, J. (2014). Efficient certificate-based encryption scheme secure against key replacement attacks in the standard model. *Journal of Information Science and Engineering*, 30(5), 1553–1568.

Lyubashevsky, V. (2009). Fiat-Shamir with aborts: applications to lattice and factoring-based signatures. In: *Proceedings of ASIACRYPT'09*, *LNCS*, Vol. 5912, pp. 598–616.

Lyubashevsky, V. (2012). Lattice signatures without trapdoors. In: *Proceedings of EUROCRYPT'12*, *LNCS*, Vol. 7237, pp. 738–755.

Micciancio, D., Regev, O. (2007). Worst-case to average-case reductions based on Gaussian measure. *SIAM Journal on Computing*, 37(1), 267–302.

Pointcheval, D., Stern, J. (2000). Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13, 361–396.

Rivest, R.L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

Ruckert, M. (2010). Strongly unforgeable signatures and hierarchical identity-based signatures over lattices without random oracles. In: *Proceedings of PQC'10*, *LNCS*, Vol. 6061, pp. 182–200.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In: *Proceedings of Crypto'84*, *LNCS*, Vol. 196, pp. 47–53.

Shor, P.W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509.

Stehle, D., Steinfeld, R. (2013). *Making NTRUEnrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices*. Cryptology ePrint Archive, Report 2013/4. Available source file from http://eprint.iacr.org/2013/004.

Tian, M., Huang, L. (2014). Efficient identity-based signature over lattices. In: *Proceedings of SEC'14*, *IFIP*, Vol. 428, pp. 321–329.

Tian, M., Huang, L. (2015). Certificateless and certificate-based signatures from lattices. *Security and Communication Networks*, 8(8), 1575–1586.

Tsai, T.T., Tseng, Y.M. (2015). Revocable certificateless public key encryption. *IEEE Systems Journal*, 9(3), 824–833.

Tsai, T.T., Huang, S.S., Tseng, Y.M. (2017). SIBSC: separable identity-based signcryption for resource-constrained devices. *Informatica*, 28(1), 193–214.

Tseng, Y.M., Tsai, T.T. (2012). Efficient revocable ID-based encryption with a public channel. *The Computer Journal*, 55(4), 475–486.

Tseng, Y.M., Huang, S.S., Tsai, T.T., Ke, J.H. (2016). List-free ID-based mutual authentication and key agreement protocol for multi-server architectures. *IEEE Transactions on Emerging Topics in Computing*, 4(1), 102–122.

Tseng, Y.M., Tsai, T.T., Huang, S.S., Huang, C.P. (2018). Identity-based encryption with cloud revocation authority and its applications. *IEEE Transactions on Cloud Computing*, 6(4), 1041–1053.

Wu, W., Mu, Y., Susilo, W., Huang, X. (2009). Certificate-based signatures revisited. *Journal of Universal Computer Science*, 15(8), 1659–1684.

Wu, J.D., Tseng, Y.M., Huang, S.S., Chou, W.C. (2018). Leakage-resilient certificateless key encapsulation scheme. *Informatica*, 29(1), 125–155.

Xiang, X. (2015). Adaptive secure revocable identity-based signature scheme over lattices. *Computer Engineering*, 41(10), 126–129.

Y.-M. Tseng is currently a professor in the Department of Mathematics, National Changhua University of Education, Taiwan. He is a member of IEEE Computer Society, IEEE Communications Society and the Chinese Cryptology and Information Security Association (CCISA). He has published over one hundred scientific journal and conference papers on various research areas of cryptography, security and computer network. His research interests include cryptography, network security, computer networks and mobile communications. He serves as an editor of several international journals.

T.-T. Tsai is currently a senior engineer in HON HAI Technology Group, Taiwan. His research interests include applied cryptography and pairing-based cryptography. He received the PhD degree from the Department of Mathematics, National Changhua University of Education, Taiwan, in 2014 under the Professor Yuh-Min Tseng.

J.-D. Wu received the BS degree from the Department of Mathematics, National Changhua University of Education, Taiwan, in 2006. He received the MS degree from the Department of Mathematics, National Changhua University of Education, Taiwan, in 2008. He is currently a PhD candidate in the Department of Mathematics, National Changhua University of Education, Taiwan. His research interests include applied cryptography and pairing-based cryptography.

S.-S. Huang is currently a professor in the Department of Mathematics, National Changhua University of Education, Taiwan. His research interests include number theory, cryptography, and network security. He received his PhD from the University of Illinois at Urbana-Champaign in 1997 under the supervision of professor Bruce C. Berndt.