IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 4, 2019, accepted October 19, 2019, date of publication October 24, 2019, date of current version November 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2949429

Improved Lattice-Based Signcryption in the Standard Model

XIAOPENG YANG[1], **HAO CAO**[2,3], **WEICHUN LI**[1], **AND HEJUN XUAN**[4]

[1]Department of Electrical and Electronic Engineering, China Coast Guard Academy, Ningbo 315801, China
[2]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
[3]School of Information and Network Engineering, Anhui Science and Technology University, Chuzhou 233100, China
[4]School of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China

Corresponding author: Xiaopeng Yang (y_xp163@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61801527 and Grant 61802241, in part by the Natural Science Fund of Education Department of Anhui province under Grant KJ2017A519, and in part by the Fundamental Research Funds for the China Coast Guard Academy under Grant 2018FZJJA06.

ABSTRACT Signcryption is a basic cryptographic primitive that simultaneously captures the functions of encryption and signature. To realize comprehensive information security against quantum computing attacks, lattice-based signcryption schemes have been successively proposed. However, the performance of signcryption schemes should be improved in the lattice setting. An efficient lattice-based signcryption scheme in the standard model is proposed in this paper. Under the ring learning with errors (RLWE) assumption and the ideal short integer solution (ISIS) assumption, the proposed signcryption scheme achieves indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) and existential unforgeability under an adaptive chosen-message attack (EUF-ACMA). Our scheme not only reduces the communication and computational overhead but also realizes a new design that combines the partitioning technique with the idea of tag-based key encapsulation. The performance analysis results show that our scheme is more efficient than previous lattice-based signcryption schemes in the standard model.

INDEX TERMS Signcryption, lattice, encapsulation, ring learning with errors (RLWE) problem, ideal short integer solution (ISIS) problem.

I. INTRODUCTION

The signcryption scheme proposed by Zheng provides message authentication, confidentiality, integrity and non-repudiation of data simultaneously [1]. Hence, signcryption is more efficient than a direct combination of encryption and signature. Subsequently, some other signcryption schemes were proposed [2]–[4]. In general, there are two design ideas in signcryption: public key signcryption and hybrid signcryption. Shor pointed out that the large integer factorization problem and the discrete logarithm problem can be broken by a quantum algorithm in polynomial time [5]. Therefore, the design of quantum-resistant signcryption schemes has very important theoretical significance and realistic expectations for the future. Fortunately, as an important representative of post-quantum cryptosystems, lattice-based cryptosystems provide a rich opportunity to build post-quantum signcryption schemes. No one has yet produced such a quantum algorithm to break the worst-case problem over a lattice.

Lattice-based cryptosystems have rapidly become a research hotspot, especially in recent years. The security of lattice-based cryptographic constructions is supported by worst-case problems over a lattice. The Gaussian sampling algorithm, modular addition, and vector multiplication are used in lattice-based cryptographic algorithms that are optimized constantly. The asymptotic efficiency of a lattice-based cryptographic algorithm is higher than that for traditional number theory.

A. RELATED WORK AND DISCUSSION

Currently, lattice-based signcryption schemes are being proposed. In 2012, Li *et al.* [6] constructed a lattice-based signcryption scheme with a random oracle model (ROM) based on the preimage sampling function and hash-based signature proposed by Peikert [7]. Wang *et al.* [8] used the preimage sampling function and an indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2)

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

secure encryption algorithm [9] to construct a lattice-based hybrid encryption scheme that was proven to be secure in the ROM. In 2013, Yan *et al.* [10] constructed a lattice-based signcryption scheme that was proven to be secure in the standard model. In [10], Yan *et al.* first used the trapdoor generation technique proposed by Micciancio and Peikert [11] to build a chameleon hash function, then promoted a signature scheme from existential unforgeability under static chosen-message attack (EUF-SCMA) security to existential unforgeability under adaptive chosen-message attack (EUF-ACMA) security, and finally improved an encryption scheme from IND-CCA1 security to IND-CCA2 security by utilizing a CCA secure symmetric encryption algorithm and a collision-resistant hash function. In 2019, Yan *et al.* [12] constructed an attribute-based signcryption scheme from a lattice in the standard model. Lu *et al.* [13] in 2014 constructed a lattice-based signcryption scheme in the standard model. In [13], Lu *et al.* used Boyen's SUF-ACMA secure signature [14] and broke the malleability of ciphertext by adopting the bimode encryption method. Xiang *et al.* [15] designed an attribute-based signcryption scheme from a lattice in the ROM. Lu *et al.* [16] constructed an IND-CPA secure signcryption scheme based on a signature without a trapdoor [17] and strengthened the scheme to IND-CCA2 secure signcryption in the ROM by employing Fujisaki-Okamoto's transformation technique [18]. Although the ROM simplifies the security proof, Leuren and Nguyen [19] showed that the ROM exists as a theoretical fault. Therefore, the design of lattice-based signcryption schemes in the standard model is an important target. Sato and Shikata [20] presented a lattice-based signcryption scheme without a random oracle. G*é*rard and Merckx [21] proposed a lattice-based signcryption scheme in the ROM. Liu *et al.* [22] constructed a new lattice-based signcryption scheme in the ROM by combining an RLWE-based signature scheme and an RLWE-based key exchange scheme. Zhang *et al.* [23] presented a multi-receiver identity-based signcryption scheme from a lattice in the ROM. Meanwhile, some fine-grained signcryption schemes have been constructed, such as [24]–[27]. However, the schemes in [24]–[27] are not anti-quantum schemes.

B. OUR CONTRIBUTION

In this paper, we propose an improved lattice-based signcryption scheme. Our contributions are summarized as follows:

- There are two ways to realize adaptive security in the standard model: dual-system encryption and the partitioning technique. Katsumata and Yamada [28] constructed a homomorphic computation function in 2016 and designed an adaptively secure identity-based encryption scheme from an ideal lattice. Inspired by [28], we use the partitioning technique to ensure the CCA2 security of the proposed signcryption scheme.
- Boyen [14] in 2010 constructed an EUF-CMA secure signature from a lattice. In 2015, B*ö*hl *et al.* [29] improved and supplemented Boyen's signature scheme [14]. Based on [29], in 2016, Libert *et al.* [30] constructed a signature scheme. Compared with the use of an independent tag for each signature in [29], Libert used a random bit string tag, which was equivalent to the prime exponent in Camenisch-Lysyanskaya's signature scheme [31]. There are two methods that are used to translate a non-adaptive secure signature into a fully secure signature: the one-time signature technique and the chameleon hash technique. Inspired by [29], [30], we construct a chameleon hash from an ideal lattice to ensure the EUF-CMA security of the proposed signcryption. To achieve EUF-ACMA security, we use the confined guessing technique and the tag-based lattice trapdoor to design the signature section.
- In this paper, we introduce the encapsulation idea into the proposed signcryption scheme. The partitioning technique, the bonsai tree technique and the reconciliation technique are closely combined to strengthen the security, which provides a trade-off between efficiency and computation. The proposed signcryption scheme also utilizes ideas to optimize the sizes of the public parameters, private keys and ciphertexts, such as the $\mathbf{G}$-trapdoor technique.
- One of the crucial properties is ciphertext anonymity. In the signcryption setting, ciphertext anonymity means that ciphertexts contain no information about who created them or to whom they are intended, namely sender privacy and receiver privacy. Libert and Quisquator [3] presented the definition of ciphertext anonymity in the non-identity-based setting. To the best of our knowledge, few lattice-based signcryption schemes exist that consider ciphertext anonymity. In this paper, we discuss the ciphertext anonymity of the proposed signcryption scheme.

C. PAPER OUTLINE

This paper is organized as follows. The necessary preliminaries are introduced in Section 2. In Section 3, the proposed scheme is presented in detail, followed by a correctness and security analysis. Finally, the conclusion is drawn in Section 4.

II. PRELIMINARIES

A. NOTATION

$\mathbb{Z}$ denotes the set of integers. $\mathbb{R}$ denotes the set of real numbers. Random variables are denoted by uppercase italic letters (e.g., X). Vectors are column vectors and denoted by bold lower-case letters (e.g., $\mathbf{v}$), and $\mathbf{v}^T$ denotes the transpose of $\mathbf{v}$. Matrices are sets of column vectors and denoted by bold capital letters (e.g., $\mathbf{X}$). For a vector $\mathbf{v} \in \mathbb{R}^n$, $\|\mathbf{v}\|_p$ denotes the L_p-norm. $\mathbf{I}_m$ denotes an m-order identity matrix. For a matrix $\mathbf{A} \in \mathbb{R}^{n\times n}$, $s_1(\mathbf{A})$ denotes its spectral norm, and $\|\mathbf{A}\|_{GS}$ denotes the longest column vector of its Gram-Schmidt orthogonalization. Define a polynomial ring

$R = \mathbb{Z}[x]/\langle\Phi_m(x)\rangle$, where $\Phi_m(x) = x^{m/2} + 1$ is an m-degree cyclotomic polynomial. For $\mathbf{a}(x) = \sum_{i=1}^{n-1} a_i x^i \in R$, $\|\phi(\mathbf{a})\|_2$ denotes its norm. For a matrix $\mathbf{M} \in R^{s\times t}$, $s_1(\mathbf{M}) = \max_{\|z\|_2=1} \|z \cdot \mathbf{rot}(\mathbf{M})\|_2$ denotes its maximum singular value. We use $[\mathbf{v}_1|\mathbf{v}_2]$ (or $[\mathbf{V}_1|\mathbf{V}_2]$) and $[\mathbf{v}_1; \mathbf{v}_2]$ (or $[\mathbf{V}_1; \mathbf{V}_2]$) to denote the horizontal connection and vertical connection of two vectors (or matrices). For a polynomial ring R over $\mathbb{Z}$, we use $[-b, b]_R \subseteq R$ to denote certain elements in R in which coefficients are chosen from $[-b, b]$. If for all c there exists n_0 such that $f(n) < \frac{1}{n_0^c}$ holds for $n > n_0$, we say that the function $f : \mathbb{N} \rightarrow \mathbb{R}^+$ is negligible, denoted by $negl(n)$. For a vector $\mathbf{v} \in \mathbb{Z}_q^n$, $\mathbf{bin}(\mathbf{v}) \in \{0, 1\}^{n\lceil \log_2 q\rceil}$ denotes the binary expansion of each component. For $x \in \mathbb{R}$, define $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor \in \mathbb{Z}$. $x \leftarrow U(\mathcal{P})$: uniformly choose x from the distribution $\mathcal{P}$. $x \leftarrow_R \mathcal{D}$ or $x \in_R \mathcal{D}$: choose x according to the distribution $\mathcal{D}$. $Pr[E]$ is the occurrence probability of an event E. The statistical distance between two random variables X and Y is defined as

$$\triangle(X, Y) = \frac{1}{2}\sum_{s\in\Omega} |Pr[X = s] - Pr[Y = s]|.$$

B. SIGNCRYPTION: PRIMITIVE AND SECURITY MODEL

Definition 1: The signcryption scheme consists of the following four algorithms:

- **Setup**(1^n): Input the security parameter 1^n, and output the public parameter PP.
- **KeyGen**$(1^n, PP)$: Input 1^n and PP, and output the public/private key pair (pk, sk). Set (pk_s, sk_s) as the sender's public/private key pair. Set (pk_r, sk_r) as the receiver's public/private key pair.
- **Signcrypt**(msg, sk_s, pk_r): Signcrypt a message msg with (sk_s, pk_r), and output a ciphertext $\mathbf{C} =$ **Signcrypt**(msg, sk_s, pk_r).
- **Unsigncrypt**$(\mathbf{C}, sk_r, pk_s)$: Unsigncrypt $\mathbf{C}$ with (sk_r, pk_s). If unsigncrypted successfully, output $msg =$ **Unsigncrypt**$(\mathbf{C}, sk_r, pk_s)$; otherwise, output $\perp$.

Definition 2: If the following event occurs with an overwhelming advantage, we say that the signcryption scheme is consistent.

$$\left[\begin{array}{c} PP \leftarrow \mathbf{Setup}(1^n) \\ (pk_s, sk_s) \leftarrow \mathbf{KeyGen}(1^n, PP) \\ (pk_r, sk_r) \leftarrow \mathbf{KeyGen}(1^n, PP) \\ \mathbf{C} = \mathbf{Signcrypt}(msg, sk_s, pk_r) \\ msg' = \mathbf{Unsigncrypt}(\mathbf{C}, sk_r, pk_s) : msg' = msg \end{array}\right].$$

A signcryption scheme realizes IND-CCA2 security and EUF-CMA security simultaneously. IND-CCA2 security is defined by a game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as follows:

- **Initiation**. $\mathcal{C}$ executes **KeyGen**$(1^n, PP)$ to generate (pk_r^*, sk_r^*) and sends (pk_r^*, PP) to $\mathcal{A}$.
- **Stage 1**. $\mathcal{A}$ executes a signcryption oracle query and an unsigncryption oracle query adaptively. $\mathcal{A}$ provides $\mathbf{C}$ with pk_s to $\mathcal{C}$. If $\mathbf{C}$ is valid, $\mathcal{C}$ returns the corresponding plaintext; otherwise, $\mathcal{C}$ outputs $\perp$.
- **Challenge**. $\mathcal{A}$ selects msg_0 and msg_1 with the same length and sends $(msg_0, msg_1, pk_s^*, sk_s^*)$ to $\mathcal{C}$. $\mathcal{C}$ chooses $b \in_R \{0, 1\}$ at random, executes $\mathbf{C}^* =$ **Signcrypt**(msg_b, pk_r^*, pk_s^*), and sends $\mathbf{C}^*$ to $\mathcal{A}$.
- **Stage 2**. $\mathcal{A}$ repeats the operations in stage 1 but cannot query the unsigncryption oracles with $(\mathbf{C}^*, pk_s^*, sk_s^*)$ directly.
- **Guess**. $\mathcal{A}$ outputs b'. $\mathcal{A}$ wins this game if $b' = b$.

The advantage of $\mathcal{A}$ in winning the IND-CCA2 game is defined as follows:

$$Adv(\mathcal{A}) = \left|Pr[b' = b] - \frac{1}{2}\right|.$$

If the above-mentioned advantage is negligible for each polynomial bounded adversary, we say that the signcryption has IND-CCA2 security.

EUF-CMA security is defined by a game between a challenger $\mathcal{C}$ and a forger $\mathcal{F}$ as follows:

- **Initiation**. $\mathcal{C}$ executes **KeyGen**$(1^n, PP)$ to generate (pk_s^*, sk_s^*) and sends (pk_s^*, PP) to $\mathcal{F}$.
- **Signcryption query**. $\mathcal{F}$ provides msg and (pk_r, sk_r) to $\mathcal{C}$. $\mathcal{C}$ executes **Signcrypt**(msg, sk_s, pk_r) and returns $\mathbf{C}$ to $\mathcal{F}$.

The advantage of $\mathcal{F}$ in winning the EUF-CMA game is defined as follows:

$$Adv(\mathcal{F}) = Pr[msg^* = \mathbf{Unsigncrypt}(\mathbf{C}^*, sk_r^*, pk_s^*)].$$

msg^* is the corresponding plaintext of $\mathbf{C}^*$ for the sender's public key pk_s^* with the limitation that $\mathbf{C}^*$ has not been previously created by the signcryption oracle. If the above-mentioned advantage is negligible for each polynomial bounded adversary, we say that the signcryption has EUF-CMA security.

Definition 3: We say that a signcryption scheme has ciphertext anonymity (i.e., key privacy, denoted by INDK-CCA security) if no PPT distinguisher has a non-negligible advantage in the following game:

- The challenger generates two private/public key pairs $(sk_{r,0}, pk_{r,0})$ and $(sk_{r,1}, pk_{r,1})$. $pk_{r,0}$ and $pk_{r,1}$ are given to the distinguisher $\mathcal{D}$.
- For $c = 0$ or $c = 1$, $\mathcal{D}$ adaptively performs the queries **Signcrypt**$(msg, sk_{r,c}, pk_r)$, for any receiver's keys pk_r, and **Unsigncrypt**$(\mathbf{C}, sk_{r,c}, pk_s)$.
- Once stage 2 is complete, $\mathcal{D}$ outputs two private keys $sk_{s,0}$ and $sk_{s,1}$ and a plaintext msg. The challenger then flips two coins $b, b' \leftarrow \{0, 1\}$ and computes a challenge ciphertext **Signcrypt**$(msg, sk_{s,b}, pk_{r,b'})$.
- $\mathcal{D}$ adaptively performs new queries as in stage 2 with the restriction that, this time, it is not allowed to query the unsigncryption of the challenge σ with the private keys $sk_{s,0}$ and $sk_{s,1}$.
- At the end of the game, $\mathcal{D}$ outputs the bits f and f' and wins if $(f, f') = (b, b')$.

The advantage of $\mathcal{D}$ in winning the INDK-CCA game is defined as follows

$$Adv_{\mathcal{D}}^{INDK} = \left|Pr[(f, f') = (b, b')] - \frac{1}{4}\right|.$$

C. LATTICE AND GAUSSIAN DISTRIBUTION

Definition 4: For a prime q, $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{u} \in \mathbb{Z}_q^n$, define the following two q-ary lattices:

$$\wedge_q^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m | \ \mathbf{Ae} = 0(\mathbf{mod}\ q)\};$$
$$\wedge_{\mathbf{u}}^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m | \ \mathbf{Ae} = \mathbf{u}(\mathbf{mod}\ q)\}.$$

Definition 5: $\rho_s(\mathbf{x}) = \exp\left\{\frac{-\pi\|\mathbf{x}\|^2}{s^2}\right\}$ denotes a standard m-dimensional Gaussian distribution centred at 0 with variance s. For a lattice $\mathcal{L}$, $s > 0$, the discrete Gaussian distribution is defined as $\mathcal{D}_{\mathcal{L},s} = \frac{\rho_s(\mathbf{x})}{\sum_{\mathbf{x}\in\mathcal{L}} \rho_s(\mathbf{x})}$. For a polynomial ring R that depends on the variable $\mathbf{x}$ over $\mathbb{R}$, $\mathcal{D}_{\mathcal{L},s}^{coeff}$ denotes the distribution of $\mathbf{a}(x) = \sum_{i=1}^{n} a_i x^i \in R$, in which the coefficient vector $(a_0, \ldots, a_{n-1}) \in \mathbb{R}^n$ follows the discrete distribution $\mathcal{D}_{\mathcal{L},s}$.

D. RING AND IDEAL LATTICE

This section systemically introduces the concepts of the ring and ideal lattice. A detailed introduction is described in [32]. Let n be a power of 2, with $m = 2n$, and define a polynomial ring $R = \mathbb{Z}[x]/\langle\Phi_m(x)\rangle$, where $\Phi_m(x) = x^{m/2} + 1$ is an m-degree cyclotomic polynomial. Let $R_q = R/qR = \mathbb{Z}[x]/\langle q, \Phi_m(x)\rangle$. Define the coefficient embedding as follows:

$$\phi : \begin{cases} R & \rightarrow \mathbb{Z}^n \\ \mathbf{a}(x) = \sum\limits_{i=1}^{n} a_i x^i & \mapsto (a_0, \ldots, a_{n-1}) \end{cases}$$

Define the ring homomorphism $\mathbf{rot}_{\Phi_m,n} : R \rightarrow \mathbb{Z}^{n\times n}$ that maps $\mathbf{a}(x) \in R$ to a matrix over $\mathbb{Z}^{n\times n}$, in which the i-th row vector is $\phi(x^i \cdot \mathbf{a}(x)\mathbf{mod}\Phi_m(x)) \in \mathbb{Z}^n$. An element of the R-model R^m is denoted as $\bar{\mathbf{x}} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)^T \in R^m$. Define two multiplication operations as follows:

$$\bar{\mathbf{x}} * \bar{\mathbf{y}} = \sum_{i=1}^{n} \mathbf{x}_i\mathbf{y}_i, \forall\ \bar{\mathbf{x}}, \bar{\mathbf{y}} \in R^m;$$
$$\bar{\mathbf{x}}\mathbf{y} = (\mathbf{x}_1\mathbf{y}, \mathbf{x}_2\mathbf{y}, \ldots, \mathbf{x}_n\mathbf{y}), \forall\ \bar{\mathbf{x}} \in R^m, \mathbf{y} \in R.$$

The following lemma shows that $R_q = R/\langle q, \Phi_m(x)\rangle$ can be regarded as a field.

Lemma 1 ([28]): Let q be a prime such that $q \equiv 3\mathbf{mod}\ 8$ and let n be a power of 2. We have the following two conclusions:

1) *$\Phi_{2n}(x) = x^n + 1$ splits as $x^n + 1 \equiv t_1t_2\mathbf{mod}\ q$ for two irreducible polynomials $t_1 = x^{n/2} + ux^{n/4} - 1 \in \mathbb{Z}_q[x]$ and $t_2 = x^{n/2} - ux^{n/4} - 1 \in \mathbb{Z}_q[x]$, where $u^2 \equiv -2\mathbf{mod}\ q$. For each $\mathbf{a} \in R_q$ satisfying $\mathbf{a} \in R_q^{\times}$, are invertible and $\|\phi(\mathbf{a})\|_2 < \sqrt{q}$.*
2) *Let n be a power of 2, q be a prime larger than $4n$ such that $q \equiv 3\mathbf{mod}\ 8$, and $k, k', \ell, \rho \in \mathbb{Z}_+$ be positive integers satisfying $k', \ell \geq 1$, $k \geq 2$, and $\rho < \frac{1}{2}\sqrt{q/n}$. Define the family of hash functions $H = \{h_{\mathbf{A}}(\mathbf{x}) | [-\rho, \rho]_R^k \rightarrow R_q^{k'}\}$, where $h_{\mathbf{A}}(\mathbf{x}) = \mathbf{Ax}$ for $\mathbf{A} \in R_q^{k'\times k}$, $\mathbf{x} \in R_q^{k\times 1}$. Then, H is a universal hash function family. For $\mathbf{A} \in_R R_q^{k'\times k}$, $\mathbf{X} \in_R R_q^{k\times\ell}$, we have*

$$\triangle\Big((\mathbf{A}, \mathbf{AX}), (\mathbf{A}, U(R_q^{k'} \times \ell))\Big) \leq \frac{\ell}{2}\sqrt{\Big(\frac{q^{k'}}{(1+2\rho)^k}\Big)^n}.$$

E. HARD PROBLEMS AND TRAPDOORS

This section introduces two hard problems: ring learning with errors (RLWE) and the ideal short integer solution (ISIS). Lyubashevsky *et al.* [32], [33] presented the reduction from the RLWE problem to worst-case SIVP (or SVP) problem. Stehlé *et al.* [34] defined the ISIS problem and presented the reduction between the ISIS and SIVP.

Definition 6: For $n \in \mathbb{Z}_+$, $k = k(n)$, and $q = q(n) \geq 2$, let $\chi = \chi(n)$ denote the noise distribution over R_q. For a probability polynomial time (PPT) adversary $\mathcal{A}$, its advantage in solving $RLWE_{q,n,m,\chi}$ is defined as follows: $Adv_{\mathcal{A}}^{RLWE_{q,n,m,\chi}} = \Big|Pr[\mathcal{A}(\{(\mathbf{a}_i, \mathbf{b}_i)\}_{i=1}^k) \rightarrow 1] - Pr[\mathcal{A}(\{(\mathbf{a}_i, \mathbf{a}_i\mathbf{s} + \mathbf{e}_i)\}_{i=1}^k) \rightarrow 1]\Big|$ with $\{\boldsymbol{a}_i\}_{i=1}^k$, $\{\mathbf{b}_i\}_{i=1}^k$, $\mathbf{s} \leftarrow_R R_q$, $\{\mathbf{e}_i\}_{i=1}^k \leftarrow \chi$. If the following advantage is negligible, we say that $RLWE_{q,n,m,\chi}$ holds.

Theorem 1 ([32]): Let $\alpha \in \mathbb{R}_+$. Let m be a power of 2. Let $\ell \in \mathbb{Z}$. $\Phi_m(x) = x^{m/2} + 1$ is an m-degree cyclotomic polynomial. Let $R = \mathbb{Z}[x]/\langle\Phi_m(x)\rangle$. Assume that the prime q satisfies $q \equiv 3\mathbf{mod}\ 8$ such that there exists another prime $p \equiv 1\mathbf{mod}\ m$ satisfying $p \leq q \leq 2p$. Let $\alpha q \geq n^{3/2}k^{1/4}\omega(\log^{9/4} n)$. There exists a PPT reduction algorithm from the SIVP (or SVP) with an $\widetilde{O}(\sqrt{n}/\alpha)$-approximating factor to $RLWE_{q,n,m,\chi}$.

Definition 7: Let $\Phi_m(x) = x^{m/2} + 1$ be an m-degree cyclotomic polynomial. Given a random polynomial set $\{\mathbf{p}_i\}_{i=1}^k$ independently chosen from $R_q = \mathbb{Z}[x]/\langle q, \Phi_m(x)\rangle$, define a vector $\bar{\mathbf{p}}(x) \in R_q$ and find a nonzero vector $\bar{z}(x) \in R^k$ such that $\sum_{i=1}^k p_iz_i = 0$ satisfies $\|\bar{z}\|_2 \leq \beta$.

Lemma 2 ([34]): Let $R_q = \mathbb{Z}[x]/\langle q, \Phi_m(x)\rangle$. Let q be a power of 3. Let $m \geq 2\lceil\log_2 q\rceil$, $\sigma \geq \omega(\sqrt{\ln nm})$, $n \geq 4$. If we choose $\mathbf{A} \leftarrow U(R_q^m)$ uniformly, sample a random vector $\mathbf{x}_i \leftarrow \mathcal{D}_{R,s}(i = 1, \ldots, m)$ independently; then, the distribution of $\sum_i \mathbf{a}_i\mathbf{x}_i$ is statistically close to the uniform distribution over R.

Lemma 3 (Trapdoor Generation Algorithm [34]): The randomized algorithm TrapGen outputs a vector $\mathbf{a} \in R_q^k$ and a matrix $\mathbf{T_a} \in R^{k\times k}$, where $\mathbf{rot}(\mathbf{a}^T)^T \in \mathbb{Z}_q^{n\times nk}$ is a full-rank matrix and $\mathbf{rot}(\mathbf{T_a}) \in \mathbb{Z}^{nk\times nk}$ is a basis for $\Lambda_q^{\perp}(\mathbf{rot}(\mathbf{a}^T)^T)$ such that $\mathbf{a}$ is $negl(n)$-close to uniform.

Lemma 4 (Preimage Sampling Algorithm [7]): The preimage sampling algorithm PreSample involves the input of a vector $\mathbf{a} \in R_q^k$, a short basis $\mathbf{T_a} \in R^{k\times k}$ as a trapdoor, where $\mathbf{rot}(\mathbf{a}^T)^T \in \mathbb{Z}_q^{n\times nk}$ is a full-rank matrix and $\mathbf{rot}(\mathbf{T_a}) \in \mathbb{Z}^{nk\times nk}$ is a basis for $\Lambda_q^{\perp}(\mathbf{rot}(\mathbf{a}^T)^T)$, a Gaussian parameter

$\sigma \geq \|\mathbf{rot}(\mathbf{T_a})\|_{GS} \cdot \omega(\sqrt{\log nk})$, and a vector $\mathbf{u} \in R_q$. This algorithm works as follows: First, it chooses an arbitrary $\mathbf{t} \in R_q^k$ via the linear algebra equation $\mathbf{a} \ast \mathbf{t} = \mathbf{u}(\mathbf{mod}\ q)$ (except for a negligible fraction of $\mathbf{rot}(\mathbf{a}^T)^T$ such that $\mathbf{t}$ always exists). Then, the algorithm outputs $\mathbf{e} \leftarrow (\mathcal{D}^{coeff}_{\Lambda^{\perp}_{\phi(\mathbf{t})}(\mathbf{rot}(\mathbf{a}^T)^T),\sigma})^k$.

F. BONSAI TREE TECHNIQUE AND SAMPLING ALGORITHM

Lemma 5 (Left Sampling Algorithm [33]): Let n be a power of 2 and q be a prime such that $q \equiv 3\mathbf{mod}\ 8$. The randomized algorithm $\mathbf{e} \leftarrow SampleLeft(\mathbf{a}, \mathbf{b}, \mathbf{u}, \mathbf{T_a}, \sigma)$ is defined such that, given vectors $\mathbf{a}, \mathbf{b} \in R_q^k$, where $\mathbf{rot}(\mathbf{a}^T)^T$ and $\mathbf{rot}(\mathbf{b}^T)^T \in \mathbb{Z}_q^{n\times nk}$ are full-rank, an element $\mathbf{u} \in R_q$, a matrix $\mathbf{T_a} \in R^{k\times k}$ such that $\mathbf{rot}(\mathbf{T_a}) \in \mathbb{Z}^{nk\times nk}$ is the trapdoor basis of the lattice $\Lambda^{\perp}(\mathbf{rot}(\mathbf{a}^T)^T)$, and a Gaussian parameter $\sigma \geq \|\mathbf{rot}(\mathbf{T_a})\|_{GS} \cdot \omega(\sqrt{\log nk})$, the algorithm outputs a vector $\mathbf{e} \in R^{2k}$ sampled from a distribution that is negl(n)-close to $\mathcal{D}^{coeff}_{\Lambda^{\perp}_{\phi(\mathbf{u})}([\mathbf{rot}(\mathbf{a}^T)^T|\mathbf{rot}(\mathbf{b}^T)^T]),\sigma}$, i.e., $[\mathbf{a}|\mathbf{b}]\mathbf{e}^T = \mathbf{u}$, $\phi(\mathbf{e}) \in \mathbb{Z}^{2nk}$ is distributed according to $\mathcal{D}_{\Lambda^{\perp}_{\phi(\mathbf{u})}([\mathbf{rot}(\mathbf{a}^T)^T|\mathbf{rot}(\mathbf{b}^T)^T]),\sigma}$.

Lemma 6 (Right Sampling Algorithm [28]): The randomized algorithm $\mathbf{e} \leftarrow Sampleright(\mathbf{a}, \mathbf{g_b}, \mathbf{R}, \mathbf{y}, \mathbf{u}, \mathbf{T_{g_b}}, s)$ is defined such that, given vectors $\mathbf{a}, \mathbf{g_b} \in R_q^m$, where $\mathbf{b} = \mathbf{aR} + \mathbf{y}\mathbf{g_b}$, such that $\mathbf{rot}(\mathbf{a}^T)^T$ and $\mathbf{rot}(\mathbf{g_b}) \in \mathbb{Z}_q^{n\times nm}$ are full-rank matrices, elements $\mathbf{y} \in R_q^*$ and $\mathbf{u} \in R_q$, a matrix $\mathbf{R} \in R^{m\times m}$, a matrix $\mathbf{T_{G_b}} \in R^{m\times m}$ such that $\mathbf{rot}(\mathbf{T_{g_b}}) \in \mathbb{Z}^{nm\times nm}$ is the basis of $\Lambda^{\perp}(\mathbf{rot}(\mathbf{g_b}))$, and a Gaussian parameter $s > s_1(\mathbf{R}) \cdot \|\mathbf{rot}(\mathbf{T_{g_b}})\|_{GS} \cdot \omega(\sqrt{\log nm})$, the algorithm outputs a vector $\mathbf{e} \in R^{2m}$ sampled from a distribution that is negl(n)-close to $\mathcal{D}^{coeff}_{\Lambda^{\perp}_{\phi(\mathbf{u})}([\mathbf{rot}(\mathbf{a}^T)^T|\mathbf{rot}(\mathbf{b}^T)^T]),s}$, i.e., $[\mathbf{a}|\mathbf{b}]\mathbf{e}^T = \mathbf{u}$, $\phi(\mathbf{e}) \in \mathbb{Z}^{2nm}$ is distributed according to $\mathcal{D}_{\Lambda^{\perp}_{\phi(\mathbf{u})}([\mathbf{rot}(\mathbf{a}^T)^T|\mathbf{rot}(\mathbf{b}^T)^T]),s}$.

Lemma 7 (Bonsai Tree Technique [33]): Let n be a power of 2 and q be a prime such that $q \equiv 3\mathbf{mod}\ 8$. The deterministic PPT algorithm ExtBasis$(\mathbf{T_a}, \mathbf{c} = [\mathbf{a}|\mathbf{b}])$ is defined such that, given vectors $\overline{\mathbf{a}} \in R_q^m$ and $\overline{\mathbf{b}} \in R_q^{\overline{m}}$, where $\mathbf{rot}(\mathbf{a}^T)^T \in \mathbb{Z}_q^{n\times nm}$ and $\mathbf{rot}(\mathbf{b}^T)^T \in \mathbb{Z}_q^{n\times n\overline{m}}$ are full-rank matrices, and a matrix $\mathbf{T_a} \in R^{m\times m}$ such that $\mathbf{rot}(\mathbf{T_a}) \in \mathbb{Z}^{nm\times nm}$ is the trapdoor basis of $\Lambda^{\perp}(\mathbf{rot}(\mathbf{a}^T)^T)$, the algorithm outputs $\mathbf{T_c} \in \mathbb{Z}_q^{(m+\overline{m})\times(m+\overline{m})}$ such that $\mathbf{rot}(\mathbf{T_c}) \in \mathbb{Z}_q^{n(m+\overline{m})\times n(m+\overline{m})}$ is the trapdoor basis of $\Lambda^{\perp}([\mathbf{rot}(\mathbf{a}^T)^T, \mathbf{rot}(\mathbf{b}^T)^T])$.

G. RECONCILIATION TECHNIQUES

Here, we present a brief description of the reconciliation techniques, as the detailed explanation is elaborated in [35]. Let $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor \in \mathbb{Z}$. Let $I_0 = \{0, 1, \ldots, \lfloor \frac{q}{4} \rceil - 1\}$ and $I_1 = \{-\lfloor \frac{q}{4} \rceil, \ldots, -1\}$.

Definition 8: A modular 2 rounding function is defined as

$$\lfloor \cdot \rceil_2 : \begin{cases} \mathbb{Z}_q & \rightarrow \mathbb{Z}_2 \\ x & \mapsto \lfloor \frac{2}{q} \cdot x \rceil \end{cases}$$

Definition 9: The cross-rounding function is defined as follows:

$$\langle \cdot \rangle_2 : \begin{cases} \mathbb{Z}_q & \rightarrow \mathbb{Z}_2 \\ x & \mapsto \lfloor \frac{4}{q} \cdot x \rfloor \end{cases}$$

Lemma 8 ([35]): For an even module q, if $x \in \mathbb{Z}_q$ is uniformly random, the distribution of $\lfloor x \rceil_2$ is the randomly uniform distribution over $\mathbb{Z}_q$ given $\langle x \rangle_2$.

Definition 10: For an even module q, for $e \in E \doteq [-\frac{q}{8}, \frac{q}{8}) \bigcap \mathbb{Z}$, $y \in \mathbb{Z}_q$ and $b \in \mathbb{Z}_2$, define the reconciliation function $\mathbf{rec} : \mathbb{Z}_q \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ as follows:

$$\mathbf{rec}(y, b) = \begin{cases} 0, & \textit{if } y \in I_b + E(\mathbf{mod}\ q); \\ 1, & \textit{otherwise}. \end{cases}$$

Definition 11: ([35]) For an even module q, for $e \in E = \big[-\frac{q}{8}, \frac{q}{8}\big) \bigcap \mathbb{Z}$ and $x \in \mathbb{Z}$, if $y = x + e(\mathbf{mod}\ q)$, then $\mathbf{rec}(y, \langle x \rangle_2) = \lfloor x \rceil_2 = \mathbf{rec}(x, \langle x \rangle_2)$ holds, given $\langle x \rangle_2$.

Definition 12: The randomization function is defined as follows:

$$\mathbf{dbl} : \begin{cases} \mathbb{Z}_q & \rightarrow \mathbb{Z}_{2q} \\ x & \mapsto \overline{x} = 2x - \overline{e}(\mathbf{mod}\ 2q) \end{cases}$$

The random noise $\overline{e} \in \mathbb{Z}_2$ can be 0, 1 or -1 with a probability of $\frac{1}{2}$, $\frac{1}{4}$ or $\frac{1}{4}$, respectively.

Lemma 9 ([35]): For an odd module q, if $x \in \mathbb{Z}_q$ is uniformly random and $\overline{x} \leftarrow \mathbf{dbl}(x) \in \mathbb{Z}_{2q}$, then the distribution of $\lfloor \overline{x} \rceil_2$ is uniformly random given $\langle x \rangle_2$.

H. HOMOMORPHIC COMPUTATION

We introduce the homomorphic computation and lemma in [28]. Let $d \in \mathbb{N}$. $\mathbf{g}_b^{-1}$ is a deterministic polynomial time (PT) algorithm that inputs $\mathbf{u} \in R_q$ and outputs $\mathbf{P} = \mathbf{g}_b^{-1}(\mathbf{u})$ such that $\mathbf{g}_b\mathbf{P} = \mathbf{u}$. A hash function $PubEval_d : (R_q^k)^d \rightarrow R_q^k$, which inputs $\mathbf{b}_1, \ldots, \mathbf{b}_d \in R_q^k$, outputs a vector in R_q^k. If $d = 1$, we have $PubEval_d(\mathbf{b}_1, \ldots, \mathbf{b}_d) = \mathbf{b}_1$. If $d \geq 2$, we have $PubEval_d(\mathbf{b}_1, \ldots, \mathbf{b}_d) = \mathbf{b}_1\mathbf{g}_b^{-1}(PubEval_{d-1}(\mathbf{b}_2, \ldots, \mathbf{b}_d))$.

Lemma 10 ([28]): Let $\mathbf{y}_1, \ldots, \mathbf{y}_d \in R$, $\mathbf{a}, \mathbf{b}_1, \ldots, \mathbf{b}_d \in R_q^k$, $\mathbf{R}_1, \ldots, \mathbf{R}_d \in R^{k\times k}$ such that $\mathbf{b}_i = \mathbf{aR}_i + \mathbf{y}_i\mathbf{g_b}$, $\forall i \in [d]$. Assume $s_1(\mathbf{R}_i) \leq B$, $\|\phi(\mathbf{y}_i)\|_1 \leq \delta$, $\forall i \in [d]$. Given $\mathbf{y}_1, \ldots, \mathbf{y}_d$ and $\mathbf{R}_1, \ldots, \mathbf{R}_d$, the algorithm $PubEval_d$ outputs $\mathbf{R}' \in R^{k\times k}$ such that $PubEval_d(\mathbf{b}_1, \ldots, \mathbf{b}_d) = \mathbf{aR}' + \mathbf{y}_1 \cdot \cdots \cdot \mathbf{y}_d\mathbf{g_b} \in R_q^k$.

III. THE PROPOSED SIGNCRYPTION SCHEME

A. CONSTRUCTION

- **Setup**(1^n)
  Let 1^n be the security parameter. Generate the system parameters and components as follows:
  1) Let an odd prime q be a prime such that $q \equiv 3(\mathbf{mod}\ 8)$. Let $m = 2^{\kappa}$ with $\kappa \geq 2$. Let $\Phi_m(x) = x^{m/2} + 1$ be the m-degree cyclotomic polynomial. Let $R = \mathbb{Z}[x]/(\Phi_m(x))$ and $R_q = \mathbb{Z}[x]/(q, \Phi_m(x))$.

2) Choose $\overline{\mathbf{a}}, \overline{\mathbf{b}_0}, \overline{\mathbf{c}_0} \in R_q^m$ with $\ell = O(n)$, and select $\mathbf{u} \in R_q$ and $\mathbf{d} \in R_q^{n\lceil \log q \rceil}$ randomly. Let $\mathbf{g}_b = [1|2|\cdots|2^{m-1}]$, and define $\mathbf{G} \triangleq \mathbf{I}_n \otimes \mathbf{g}_b$ as follows:

$$\mathbf{G} = \begin{pmatrix} \mathbf{g}_b & & & \\ & \mathbf{g}_b & & \\ & & \ddots & \\ & & & \mathbf{g}_b \end{pmatrix} \in \mathbb{Z}_q^{n \times nm}$$

Note that all of the elements of $\mathbf{G}$ on the primary diagonal are $\mathbf{g}_b$, while the other elements are 0.

3) Choose the hash functions:
   - Let the *bits* $\in \{0,1\}^{k'}$. Choose $\mathbf{b}_0, \mathbf{b}_{i,j} \in_R R_q^m$ randomly for $(i,j) \in [2] \times [(k')^{1/2}]$. The deterministic function $H_1 : \{0,1\}^{k'} \to R_q^m$ is defined as $H_1(bits) = \mathbf{b}_0 + \sum_{(i,j)\in[1,k']^2} PubEval_d(\mathbf{b}_{1,j_1}, \ldots, \mathbf{b}_{2,j_2})$.
   - $H_2 : \{0,1\}^* \to \{0,1\}^{128}$ is a pairwise independent hash function.
   - $H_3 : \{0,1\}^* \to R_q$ is a universal one-way hash function.

4) The chameleon hash function is $CM_{\left[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}\right]} : R_q^m \times R_q^m \to R_q$. Output the public key $HK_R = \left[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}\right]$, and keep the private key $CK_R = \mathbf{T}_{\overline{\mathbf{c}_0}}$ as a secret, where $\mathbf{rot}(\mathbf{T}_{\overline{\mathbf{c}_0}}) \in \mathbb{Z}_q^{nm \times nm}$ is the trapdoor basis of the lattice $\Lambda^{\perp}(\mathbf{rot}(\overline{\mathbf{c}_0}^T)^T)$. This chameleon hash function inputs $\left[\mathbf{h} \in \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m | \mathbf{s}_1 \in \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m\right]$ and outputs

$$\mathbf{c}_M \triangleq CM_{\left[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}\right]}(\mathbf{h}, \mathbf{s}_1) = \overline{\mathbf{b}_0} * \mathbf{h} + \overline{\mathbf{c}_0} * \mathbf{s}_1.$$

   Verify the properties of chameleon hash function as follows:
   - Collision-resistant property: Suppose there exists a collision $[\mathbf{h}|\mathbf{s}_1] \neq [\mathbf{h}'|\mathbf{s}_1'] \in \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m \times \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m$; then, $\mathbf{t} = [\mathbf{h} - \mathbf{h}'|\mathbf{s}_1 - \mathbf{s}_1'] \neq 0$ is a solution of $[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}] * \mathbf{t} = 0$, which satisfies

$$\|\mathbf{t}\|^2 \leq \|\mathbf{h} - \mathbf{h}'\|^2 + \|\mathbf{s}_1 - \mathbf{s}_1'\|^2 \leq 8\sigma_1^2 mn.$$

     That is, $ISIS_{q,n,m,2\sqrt{2mn},\sigma_1}$ is solvable. Thus, $CM_{\left[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}\right]}$ is collision-resistant.
   - Trapdoor collision: Input $\mathbf{h}, \mathbf{h}' \in R_q^m$, $\mathbf{s}_1 \leftarrow \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m$, and find $\mathbf{s}_1' \in \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m$ such that $CM_{\left[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}\right]}(\mathbf{h}, \mathbf{s}_1) = CM_{\left[\overline{\mathbf{b}_0}|\overline{\mathbf{b}_0}\right]}(\mathbf{h}, \mathbf{s}_1')$; i.e., solve a short vector that satisfies the following equation:

$$\overline{\mathbf{c}_0} * \mathbf{s}_1' = \overline{\mathbf{b}_0} * (\mathbf{h} - \mathbf{h}') + \overline{\mathbf{c}_0} * \mathbf{s}_1 \triangleq \mathbf{X}(\mathbf{mod}\ q).$$

     According to **Lemma II.4**, there exists a PPT algorithm that outputs a trapdoor basis $\mathbf{T}_{\overline{\mathbf{c}}_0} \in R^{m \times m}$. Solve the short vector $\mathbf{s}_1'$ that is $negl(n)$-close to $\left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m$ by using $PreSample(\mathbf{T}_{\overline{\mathbf{c}}_0}, \mathbf{X})(\mathbf{mod}\ q)$. In fact, in the preimage sampling algorithm, the solution vector $\mathbf{s}_1'' \in \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m$ is computed by solving the equation $\overline{\mathbf{c}_0} * \mathbf{s}_1'' = \mathbf{X}(\mathbf{mod}\ q)$. Next, a vector $\mathbf{z}$ is chosen randomly under the condition that $\mathbf{z}$ belongs to $\wedge_q^{\perp}(\mathbf{rot}(\overline{\mathbf{c}_0}^T)^T)$ and $\mathbf{z}$ is close to $-\mathbf{s}_1''$. Then, the vector $\mathbf{s}_1' = \mathbf{z} - (-\mathbf{s}_1'')$ is output. $\overline{\mathbf{c}_0} * \mathbf{s}_1' = \overline{\mathbf{c}_0} * [\mathbf{z} - (-\mathbf{s}_1'')] = \overline{\mathbf{c}_0} * \mathbf{z} + \overline{\mathbf{c}_0} * \mathbf{s}_1'' = \mathbf{X}(\mathbf{mod}\ q)$.
   - Uniformity: Because $\overline{\mathbf{c}_0} \leftarrow U(R_q^m)$, $\mathbf{s}_1' \sim \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m$, by part 2 of **Lemma II.1**, we have that the distribution of $\overline{\mathbf{c}_0} * \mathbf{s}_1$ is statistically close to the uniform distribution over R. On the other hand, due to $\overline{\mathbf{b}_0} \leftarrow U(R_q^m)$, $\mathbf{h} \sim \left(\mathcal{D}_{\mathbb{Z}^n,\sigma_1}^{coeff}\right)^m$, and part 2 of **Lemma II.1**, we have a distribution of $\overline{\mathbf{b}_0} * \mathbf{h}$ that is statistically close to the uniform distribution over R. By **Lemma II.3**, we have that the output distribution of $CM_{\left[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}\right]}$ is statistically close to the uniform distribution over R.

5) AES-128-bit algorithm $\sum = (EK, DK)$.

The public parameter PP contains $(q, m, R, \overline{\mathbf{a}}, \overline{\mathbf{b}_0}, \overline{\mathbf{c}_0}, \mathbf{G}, H_1, H_2, H_3, CM_{\left[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}\right]}, \Sigma)$.

- **KeyGen**$(1^n, PP)$

  Execute *TrapGen* to generate $(pk_s = \overline{\mathbf{a}_s} \in R_q^m, sk_s = \mathbf{T}_{\overline{\mathbf{a}_s}} \in R^{m\times m})$ and generate $(pk_r = \overline{\mathbf{a}_r} \in R_q^m, sk_r = \mathbf{T}_{\overline{\mathbf{a}_r}} \in R^{m\times m})$. $\mathbf{rot}(\mathbf{T}_{\overline{\mathbf{a}_s}}) \in \mathbb{Z}^{nm\times nm}$ is the trapdoor basis of $\Lambda_q^{\perp}(\mathbf{rot}(\overline{\mathbf{a}_s}^T)^T)$, while $\mathbf{rot}(\mathbf{T}_{\overline{\mathbf{a}_r}}) \in \mathbb{Z}^{nm\times nm}$ is the trapdoor basis of $\Lambda^{\perp}(\mathbf{rot}(\overline{\mathbf{a}_r}^T)^T)$. We explain the algorithm *TrapGen* in detail below. Generate the random polynomials $\overline{\mathbf{a}_1} = (\mathbf{a}_1, \ldots, \mathbf{a}_{m_1})^T \in R_q^{m_1\times 1}$. Construct a random matrix $\overline{\mathbf{a}_2}$ with a structured matrix $\mathbf{T}_{\overline{\mathbf{a}_s}} \in R^{m\times m}$ such that $\mathbf{T}_{\overline{\mathbf{a}_s}} * \overline{\mathbf{a}_s} = 0$ and $\mathbf{T}_{\overline{\mathbf{a}_s}}$ is a basis of the module $\Lambda^{\perp}(\mathbf{rot}(\overline{\mathbf{a}_s}^T)^T)$, where $\overline{\mathbf{a}_s} = [\overline{\mathbf{a}_1}|\overline{\mathbf{a}_2}]$. First construct an HNF-like basis $\mathbf{F}$ of the module $\Lambda^{\perp}(\mathbf{rot}(\overline{\mathbf{a}_s}^T)^T)$ with $\overline{\mathbf{a}_s}$. Next, construct a unimodular matrix $\mathbf{Q}$ such that $\mathbf{T}_{\overline{\mathbf{a}_s}} = \mathbf{QF}$ is a short basis of the module. More precisely, $\mathbf{T}_{\overline{\mathbf{a}_s}}$ has the following form:

$$\begin{pmatrix} \mathbf{V} & \mathbf{P} \\ \mathbf{D} & \mathbf{B} \end{pmatrix} = \underbrace{\begin{pmatrix} -\mathbf{I}_{m_1} & \mathbf{P} \\ 0 & \mathbf{B} \end{pmatrix}}_{\mathbf{Q}} \cdot \underbrace{\begin{pmatrix} \mathbf{H} & 0 \\ \mathbf{U} & \mathbf{I}_{m_2} \end{pmatrix}}_{\mathbf{F}}$$

  By setting $\mathbf{B}$, the lower triangular matrix with diagonal coefficients, equal to 1, the matrix $\mathbf{Q}$ is unimodular. In this design principle, we hope that $\mathbf{F} * \overline{\mathbf{a}_s} = 0$. Hence, we should set $\mathbf{H} * \overline{\mathbf{a}_1} = 0$ and $\overline{\mathbf{a}_2} = -\mathbf{U} * \overline{\mathbf{a}_1}$. By setting $\mathbf{H}$ to be an HNF-like matrix, we can guarantee that $\mathbf{H}$ is a basis of $\Lambda_q^{\perp}(\mathbf{rot}(\overline{\mathbf{a}_1}^T)^T)$ and that $\mathbf{F}$ is a basis of $\Lambda_q^{\perp}(\mathbf{rot}(\overline{\mathbf{a}_s}^T)^T)$. By setting $\mathbf{U} = \mathbf{W} + \mathbf{R}$, with $\mathbf{W}$ and $\mathbf{R}$ being a random matrix, we have that $\overline{\mathbf{a}_2}$ is almost uniformly random in R. The i-th row of $\mathbf{R}$ is chosen from $(\{-1,0,1\}^n)^r \times (\{0\}^n)^{m_1-r}$. The specific construction methods of $\mathbf{H}$ and $\mathbf{W}$ are described in [34], so we omit them here. In a similar way, we can generate $\mathbf{T}_{\overline{\mathbf{a}_r}}$.

- **Signcrypt**$(msg \in \{0,1\}^{\ell}, sk_s, pk_r)$
  1) Compute $\mathbf{h} = H_1(msg, \overline{\mathbf{a}_r}) \in \left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m$.
  2) Choose $\tau \leftarrow U(\{0,1\}^{\ell})$ randomly, and compute $\overline{\mathbf{a}_\tau} = \left[\overline{\mathbf{a}_s} | \overline{\mathbf{a}} + \Sigma_{i=1}^{\ell} \tau[i] \cdot \overline{\mathbf{a}_i}\right] \in R_q^{2m}$. Compute the trapdoor basis $\mathbf{rot}(\mathbf{T}_\tau) \in \mathbb{Z}^{2nm \times 2nm}$ of $\Lambda_q^{\perp}(\overline{\mathbf{a}_\tau})$ by invoking $ExtBasis\left(\mathbf{T}_{\bar{\mathbf{a}}_\tau}, \bar{\mathbf{a}}_\tau\right)$.
  3) Sample $\mathbf{s}_1 \leftarrow \left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m$, and compute the chameleon hash function as follows
  $$\mathbf{c}_M \triangleq CM_{\left[\overline{\mathbf{b}_0}|\overline{\mathbf{c}_0}\right]}(\mathbf{h}, \mathbf{s}_1) = \overline{\mathbf{b}_0} * \mathbf{h} + \overline{\mathbf{c}_0} * \mathbf{s}_1.$$
  $\mathbf{c}_M$ is used to define $\mathbf{u}_M = \mathbf{u} + \mathbf{d} \cdot \mathbf{bin}(\mathbf{c}_M) \in R_q$, where $\mathbf{c}_M = \mathbf{G} \cdot \mathbf{bin}(\mathbf{c}_M)$. By utilizing the trapdoor basis $\mathbf{T}_{\overline{\mathbf{a}_\tau}}$, solve a short vector solution $\mathbf{v} \leftarrow \mathcal{D}_{\Lambda^{\mathbf{u}_M}(\overline{\mathbf{a}_\tau}),\sigma_2}$ of the following equation: $\overline{\mathbf{a}_\tau} * \mathbf{v} = \mathbf{u}_M (\mathbf{mod}\ q)$. In fact, this step invokes $\mathbf{v} \leftarrow SampleLeft(\overline{\mathbf{a}_\tau}, \mathbf{u}_M, \mathbf{T}_{\overline{\mathbf{a}_\tau}}, \sigma_2)$ to output the vector $\mathbf{v}$ that is $negl(n)$-close to $\mathcal{D}^{coeff}_{\Lambda^{\perp}_{\phi(\overline{\mathbf{u}_M})}\left(\mathbf{rot}\left(\overline{\mathbf{a}_\tau}^T\right)^T\right),\sigma_2}$. Output $(\tau, \mathbf{v}, \mathbf{s}_1)$.
  4) Parse $\mathbf{v}$ as $\mathbf{v} = \left[\mathbf{v}_1 \in R_q^m | \mathbf{v}_2 \in R_q^m\right]$. Select $\mathbf{s}_2 \in R_q$ randomly, sample $\mathbf{e}_2 \leftarrow \chi_{\sigma_2}$, and choose $\mathbf{r}_2 \in \{0,1\}^{\ell}$ randomly. Let $\mathbf{c}_0 = H_3(\mathbf{r}_2, \mathbf{v}_1)$, and compute $\mathbf{w} = \mathbf{s}_2\mathbf{c}_0 + \mathbf{e}_2$, $\overline{\mathbf{w}} \leftarrow \mathbf{dbl}(\mathbf{w})$, $\mathbf{c}_1 = \langle \overline{\mathbf{w}} \rangle_2$, and $\mathbf{c}_2 = \lfloor \overline{\mathbf{w}} \rceil_2$.
  5) Let $\mathbf{c}_3 = H_1(\mathbf{c}_1, \mathbf{v}_2) \in R_q^m$, and compute $\mathbf{E} = \left[\overline{\mathbf{a}_r} | \mathbf{c}_3\right] \in R_q^{2m}$.
  6) Sample $\mathbf{e}_3 = [\mathbf{e}_{3,1} | \mathbf{e}_{3,2}] \leftarrow \left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^{2m}$, and compute $\mathbf{c}_4 = \mathbf{s}_2\mathbf{E} + \mathbf{e}_3 \in R_q^{2m}$.
  7) Compute
  $$\mathbf{c}_5 = EK_{H_2(\mathbf{c}_2)}\left(msg \| \phi(\mathbf{v}_2) \| \phi(\mathbf{s}_1) \| \mathbf{r}_2\right).$$
  Finally, output the ciphertext
  $$\mathbf{C} = (\tau, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5).$$
- **Unsigncrypt**$(\mathbf{C}, sk_r, pk_s)$
  1) Compute $\mathbf{E} = \left[\overline{\mathbf{a}_r} | \mathbf{c}_3\right]$.
  2) Sample $\overline{\mathbf{e}_3} \in R_q^m$, where each column vector of the matrix $\mathbf{rot}(\overline{\mathbf{e}_3}^T)^T \in \mathbb{Z}_q^{n \times nm}$ follows $\mathcal{D}_{\mathbb{Z}^{nm},2}$.
  3) By using $sk_r = \mathbf{T}_{\overline{\mathbf{a}_r}}$, find the short solution $\mathbf{z} = \overline{\mathbf{e}_2} \in R_q^m$ of the equation
  $$\overline{\mathbf{a}_r} * \mathbf{z} = \mathbf{c}_0 - \mathbf{c}_3 * \overline{\mathbf{e}_3}.$$
  4) Compute $\mathbf{w}_1 = \mathbf{c}_4 * \left[\overline{\mathbf{e}_2} | \overline{\mathbf{e}_3}\right]$, $\mathbf{rec}(\mathbf{w}_1, \mathbf{c}_1) = \lfloor \overline{\mathbf{w}_1} \rceil_2$.
  5) Compute $DK_{H_2\left(\lfloor \overline{\mathbf{w}_1} \rceil_2\right)}(\mathbf{c}_5)$, and parse the result as $\left(\widetilde{msg} \| \widetilde{\phi(\mathbf{v})} \| \widetilde{\phi(\mathbf{s}_1)} \| \widetilde{\mathbf{r}_2}\right)$.
  6) Recover $\phi^{-1}\left(\widetilde{\phi(\mathbf{v})}\right) = \widetilde{\mathbf{v}}$, and parse $\widetilde{\mathbf{v}} = \left(\widetilde{\mathbf{v}_1} \in R_q^m, \widetilde{\mathbf{v}_2} \in R_q^m\right)$.
  7) Compute $\widetilde{\mathbf{h}} = H_1(\widetilde{msg}, \overline{\mathbf{a}_r}) \in R_q^m$, and build $\widetilde{\mathbf{c}_M} = \overline{\mathbf{b}_0} * \widetilde{\mathbf{h}} + \overline{\mathbf{c}_0} * \phi^{-1}\left(\widetilde{\phi(\mathbf{s}_1)}\right)$. Next, verify whether the following two conditions hold
  $$\begin{cases} \overline{\mathbf{a}_\tau} * \widetilde{\mathbf{v}} = \mathbf{u} + \mathbf{d} \cdot \mathbf{bin}\left(\widetilde{\mathbf{c}_M}\right) \\ \|\phi(\widetilde{\mathbf{v}})\|_2 \le \sigma_2\sqrt{2mn} \end{cases}$$
  If the conditions hold, output $\widetilde{msg}$; otherwise, output $\perp$.

B. CORRECTNESS

Lemma 11: If $4\sigma_1 mn + \sqrt{n} \cdot (1 + 2\sigma_1) \le \frac{q}{4}$, the receiver can correctly unsigncrypt with an overwhelming advantage.

Proof: Compute

$$\begin{aligned} \mathbf{w}_1 &= \mathbf{c}_4 * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} = (\mathbf{s}_2\mathbf{E} + \mathbf{e}_3) * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} \\ &= \mathbf{s}_2\mathbf{E} * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} + \mathbf{e}_3 * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} \\ &= \mathbf{s}_2\left[\overline{\mathbf{a}_r} | \mathbf{c}_3\right] * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} + \mathbf{e}_3 * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} \\ &= \mathbf{s}_2\left(\overline{\mathbf{a}_r} * \overline{\mathbf{e}_2} + \mathbf{c}_3 * \overline{\mathbf{e}_3}\right) + \mathbf{e}_3 * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} \\ &= \mathbf{s}_2\left(\mathbf{c}_0 - \mathbf{c}_3 * \overline{\mathbf{e}_3}\right) + \mathbf{s}_2\mathbf{c}_3 * \overline{\mathbf{e}_3} + \mathbf{e}_3 * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} \\ &= \mathbf{s}_2\mathbf{c}_0 + \mathbf{e}_3 * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix}. \\ \mathbf{w}_1 - \mathbf{w} &= \mathbf{s}_2\mathbf{c}_0 + \mathbf{e}_3 * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} - (\mathbf{s}_2\mathbf{c}_0 + \mathbf{e}_2) \\ &= \mathbf{e}_3 * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix} - \mathbf{e}_2. \end{aligned}$$

Let $\bar{\mathbf{e}}$ be the random noise of $\bar{\mathbf{e}} \leftarrow \mathbf{dbl}(\mathbf{w})$; then, we have $\overline{\mathbf{w}} = 2\mathbf{w} - \bar{\mathbf{e}}$. The receiver can unsigncrypt correctly with an overwhelming advantage if $\|2\mathbf{e} + \bar{\mathbf{e}}\| \le \frac{q}{4}$ holds, i.e., if the following condition holds:

$$\begin{aligned} \|2\mathbf{e} + \bar{\mathbf{e}}\|_2 &\le 2\left\|[\mathbf{e}_{3,1} | \mathbf{e}_{3,2}] * \begin{pmatrix} \overline{\mathbf{e}_2} \\ \overline{\mathbf{e}_3} \end{pmatrix}\right\|_2 + 2\|\mathbf{e}_2\|_2 + \|\bar{\mathbf{e}}\|_2 \\ &\le 2\sqrt{2}\sigma_1\sqrt{mn} \cdot (\sqrt{2}\sigma_1\sqrt{mn}) + 2\sigma_1\sqrt{n} + \sqrt{n} \\ &= 4\sigma_1 mn + \sqrt{n} \cdot (1 + 2\sigma_1) \\ &\le \frac{q}{4}. \end{aligned}$$

C. SECURITY

Theorem 2: The proposed signcryption scheme has EUF-CMA security under the $ISIS_{q,n,m}$ hard problem.

Proof: Suppose there exists a forger F that can forge the signcryption and that there exists a simulator that can forge the signature of the SUF-CMA signature scheme.

Initiation. $\mathcal{F}$ executes **KeyGen** and **Signcrypt** to obtain PP and $(\mathbf{A}_s^*, T_s^*)$ and sends PP and $\mathbf{A}_s^*$ to $\mathcal{F}$.

Signcryption. $\mathcal{F}$ executes the signcryption oracle as follows: $\mathcal{F}$ submits msg and $\mathbf{A}_r$. $\mathcal{C}$ executes $\mathbf{C}' \leftarrow$ **Signcrypt**$(msg, \mathbf{A}_r, \mathbf{T}_s^*)$ and sends $\mathbf{C}'$ to $\mathcal{F}$.

Forgery. $\mathcal{F}$ outputs $(\mathbf{A}_r^*, \mathbf{T}_r^*)$ and fresh ciphertext $\mathbf{C}^*$. $\mathcal{C}$ executes the following steps:

1) Use sk_r^* to decrypt $\mathbf{c}_2$.
2) Use $H_2\left(\lfloor \overline{\mathbf{w}_2} \rceil_2\right)$ to decrypt $\mathbf{c}_5$ such that $\mathcal{F}$ obtains $msg \| \phi(\mathbf{v}_2) \| \phi(\mathbf{s}_1) \| \mathbf{r}_2$.
3) Parse $\phi(\mathbf{v}) = [\phi(\mathbf{v}_1) | \phi(\mathbf{v}_2)]$.

Since the signature scheme has SUF-CMA security, the proposed signcryption scheme has SUF-CMA security.

Theorem 3: The proposed signcryption scheme has IND-CCA2 security under the $RLWE_{q,n,m,\left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m}$ hard problem.

Proof: Define the following games between the challenger and the adversary. E_i denotes the event $b' = b$.

Game$_0$ This game is similar to the game defined for IND-CCA2 security. The ciphertext space is $\{0,1\}^l \times R_q \times \{0,1\}^{mn} \times R_q^m \times R_q^{2m} \times \Omega$. In the challenge stage, the adversary $\mathcal{A}$ sets $\mathbf{C}^* \leftarrow_R \{0,1\}^l \times R_q \times \{0,1\}^{mn} \times R_q^m \times R_q^{2m} \times \Omega$ and outputs a guess $\widehat{b}$. Finally, the challenger $\mathcal{C}$ sets $b' = \widehat{b}$. By definition, we have $\left|Pr\left[E_0\right] - \frac{1}{2}\right| = \varepsilon$.

Game$_1$ This game changes the key generation algorithm. Let pk_r be a random matrix, and execute *TrapGen* to generate pk_s, sk_s. The other steps are identical to the corresponding steps in **Game**$_0$. For $m_0, m_1 \in \mathbb{Z}$, $m_0 \leq m_1$, $c \in \mathbb{Z}^+$. Let $[m_0, m_1]_{R,c} = \left\{\Sigma_{i=0}^{c-1} b_i x^i | b_i \in [m_0, m_1], \forall i \in [0, i-1]\right\} \subseteq R$. This notation denotes a set that consists of all polynomials whose degrees are below $d-1$, and the coefficients are chosen form $[m_0, m_1]$. The challenger chooses $y_0 \leftarrow_R \left[-\kappa(cn)^d, -1\right]_{R,(c-1)d+1}, y_{i,j} \leftarrow_R [1,n]_{R,c}, (i,j) \in [d] \times [\ell], y = (y_0, \{y_{i,j}\}_{(i,j)\in[d,\ell]})$. Define $F_y(bits) = y_0 + \Sigma_{(j_1,\ldots,j_d)\in S(bits)} y_{1,j_1} \cdots y_{d,j_d}$. The challenger checks whether the following condition holds $F_y(bit^*) = 0 \wedge F_y(bits_1) \in R_q^* \wedge \cdots \wedge F_y(bits_q) \in R_q^*$. $bits^*$ is the challenge bit, while $bits_1, \cdots, bits_q$ are the bit strings that the adversary queries to H_3. If the above-mentioned condition does not hold, the challenger omits the output of the adversary, sets $b' \leftarrow_R \{0,1\}$, and terminates the challenge. If it holds, the challenger sets $b' = \widehat{b}$. In this case, we have $\left|Pr\left[E_1 - \frac{1}{2}\right]\right| \leq negl(n)$.

Game$_2$ Change the game such that when $F_y(bit^*)$ does not hold, the challenger terminates at the end of the game. The challenger $\mathcal{C}$ chooses $R_0, R_{i,j} \leftarrow_R [-\lambda, \lambda]^{k\times k}, \forall (i,j) \in [d] \times [\ell]$ and computes $\mathbf{b}_0 = \overline{\mathbf{a}_\tau} R_0 + y_0 \mathbf{g}_b$ and $\mathbf{b}_{i,j} = \overline{\mathbf{a}_\tau} R_{i,j} + y_{i,j}\mathbf{g}_b$. The other steps are identical to those of **Game**$_1$. By part 2 of **Lemma II**.**1**., we obtain that the following distributions are statistically indistinguishable:

$$\left(\overline{\mathbf{a}_\tau}, \overline{\mathbf{a}_\tau} R_0 + y_0 \mathbf{g}_b, \left\{\overline{\mathbf{a}_\tau} R_{i,j} + y_{i,j}\mathbf{g}_b\right\}\right) \approx_S \left(\overline{\mathbf{a}_\tau}, \mathbf{b}_0, \{\mathbf{b}_{i,j}\}\right)$$

Then, we have $\left|Pr[E_2] - Pr[E_1]\right| \leq negl(n)$.

Game$_3$ For $bits^* \in \{0,1\}^*$, define $R_{bits} = R_0 + \Sigma TrapEval_d(R_{1,j_1}, \ldots, R_{d,j_d}, y_{1,j_1}, \ldots, y_{d,j_d})$ Furthermore, we have $H_3(bits) = \overline{\mathbf{a}_\tau} R_{bits} + F_y(bits)\mathbf{g}_b$, $Pr[E_3] = Pr[E_2]$.

Game$_4$ In this game, the challenger randomly chooses $\overline{\mathbf{a}_\tau} \leftarrow_R R_q^{2m}$. When the adversary queries the bit string to H_3, the challenger first computes R_{bits}. If $F_y(bits) \notin R_q^*$, the challenger terminates the challenge and computes $\mathbf{v} \leftarrow SampleRight\left(\overline{\mathbf{a}_\tau}, \mathbf{g}_b, R_{bits}, F_y(bits), \mathbf{u}_M, \mathbf{T}_{\mathbf{g}_b}, \sigma_2\right)$. When we choose the parameter σ_2 properly, the above distribution is statistically close to the following distribution: $\mathbf{v} \leftarrow SampleLeft\left(\overline{\mathbf{a}_\tau}, \mathbf{u}_M, \mathbf{T}_{\overline{\mathbf{a}_\tau}}, \sigma_2\right)$ Thus, we have $|Pr[E_4] - Pr[E_3]| \leq negl(n)$.

Game$_5$ Randomly choose $\mathbf{v} \leftarrow_R R_q^{2m}$, and label $\mathbf{v} = \left[\mathbf{v}_1 \in R_q^m | \mathbf{v}_2 \in R_q^m\right]$. Randomly choose $\mathbf{s}_2 \leftarrow_R R_q$, sample $\mathbf{e}_2 \leftarrow \chi_{\sigma_1}$, randomly choose $\mathbf{r}_2 \in \{0,1\}^l$, let $\mathbf{c}_0 = H_3(\mathbf{r}_2, \mathbf{v}_1)$, and compute $\mathbf{w} = \mathbf{s}_2\mathbf{c}_0 + \mathbf{e}_2$, $\overline{\mathbf{w}} \leftarrow \mathbf{dbl}(\mathbf{w})$, $\mathbf{c}_1 = \langle\overline{\mathbf{w}}\rangle_2$, $\mathbf{c}_2 = \lfloor\overline{\mathbf{w}}\rceil_2$, and $\mathbf{c}_3^* = H_1(\mathbf{c}_1, \mathbf{v}_2)$. If $b = 0$, the challenger produces the valid ciphertext. If $b = 1$ and $F_y(bits^*) = 0$ hold, the challenger selects $\mathbf{s} \leftarrow_R R_q$, samples $\mathbf{e} \leftarrow \left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m$, computes $\mathbf{v} = \mathbf{s}\overline{\mathbf{a}_\tau} + \mathbf{e} \in R^{2m}$, and then computes $\mathbf{c} \in \mathbb{Z}_q^{2nm} \leftarrow ReRand\left(\mathbf{rot}\left(\left[\mathbf{I}_k | R_{bits^*}\right]\right), \phi(\mathbf{v}), \sigma_1, \frac{\sigma'}{2\sigma_1 q}\right)$. Note that $\mathbf{c} = \left(\phi(\mathbf{s})\mathbf{rot}\left(\overline{\mathbf{a}_\tau}\right)\right) \cdot \mathbf{rot}\left(\left[\mathbf{I}_k | R_{bits^*}\right]\right) = \phi(\mathbf{s}) \cdot \mathbf{rot}\left(\left[\overline{\mathbf{a}_\tau} | H(bits^*)\right]\right) + \mathbf{e}' = \phi\left(\mathbf{s}\left[\overline{\mathbf{a}_\tau} | H(bits^*)\right]\right) + \mathbf{e}'$ with $\mathbf{e}' \leftarrow_R \left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma'}\right)^m$. Let $T = \left\{\Sigma_{i=0}^n a_i x^i | a_i \in \{-1,1\}\right\}$, and randomly choose $\mathbf{T}^* \in T^{m\times m}$ (all else being equal). Compute $\overline{\mathbf{e}_3}$ that satisfies $\mathbf{e} = (\mathbf{c}_3 - \mathbf{c}_3^*)^{-1}\mathbf{c}_0$. Let $\overline{\mathbf{e}_2} = -\mathbf{T}^*\overline{\mathbf{e}_3}$ such that the following equation holds: $\overline{\mathbf{a}_\tau} * \overline{\mathbf{e}_2} + (\mathbf{c}_3 - \mathbf{c}_3^*) * \overline{\mathbf{e}_3} = \mathbf{c}_0$. Because $\mathbf{c}_4 = \phi^{-1}(\mathbf{c})$ of **Game**$_5$ is statistically close to that of **Game**$_4$, we have $\left|Pr[E_5] - Pr[E_4]\right| \leq negl(n)$.

Game$_6$ If $b = 0$, the challenger chooses $\mathbf{v}_0 \leftarrow_R R_q$, $\mathbf{v}' \leftarrow_R R_q^m$, and $\mathbf{e}' \leftarrow \left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma}\right)^m$ and executes $\mathbf{c} \leftarrow ReRand\left(\mathbf{rot}\left(\left[\mathbf{I}_k | R_{bits^*}\right]\right), \phi(\mathbf{v}), \sigma_1, \frac{\sigma'}{2q\sigma_1}\right)$ with $\mathbf{v} = \mathbf{v}' + \mathbf{e}'$. Compute and output the challenge ciphertext. As demonstrated below, **Game**$_5$ and **Game**$_6$ are statistically indistinguishable. Assume that there exists an adversary $\mathcal{A}$ that can differentiate **Game**$_5$ and **Game**$_6$ with an overwhelming advantage. Then, we can construct a distinguisher $\mathcal{D}$ that breaks the RLWE problem as follows:

- **Initiation**. $\mathcal{D}$ inputs the RLWE instances $\left\{\mathbf{a}_i, \mathbf{v}_i\right\}_{i=0}^m \in \left(R_q \times R_q\right)^{m+1}$. Without loss of generality, suppose that $\mathbf{v}_i = \mathbf{v}_i' + \mathbf{e}_i'$ with $\mathbf{e}_i' \leftarrow_R \mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma}$. $\mathcal{F}$ differentiates between $\mathbf{v}_i' = \mathbf{a}_i\mathbf{s}_2$ and $\mathbf{v}_i' \leftarrow_R R_q$.
- **Setup**. $\mathcal{D}$ sets $\mathbf{u} \triangleq \mathbf{a}_0$, $\mathbf{a} = (\mathbf{a}_1 \ldots, \mathbf{a}_m)$, and $\mathbf{v} = (\mathbf{v}_1 \ldots, \mathbf{v}_m)$, chooses $\mathbf{y}$ according to **Game**$_1$, chooses $R_0, R_{i,j}, \mathbf{b}_0$ and $\mathbf{b}_{i,j}$ according to **Game**$_2$, and returns $\mathbf{b}_0, \mathbf{u}, \mathbf{d}, \overline{\mathbf{a}}, \overline{\mathbf{b}_0}, \overline{\mathbf{c}_0}, \mathbf{b}_{i,j}$ and $\overline{\mathbf{a}_i}$ to $\mathcal{A}$. $\mathcal{D}$ randomly selects $b \leftarrow_R \{0,1\}$ and keeps it secretly. Stage 1 and stage 2 respond to the queries from $\mathcal{A}$ using $R_0, R_{i,j}$.
- **Challenge**. When $\mathcal{A}$ queries for the challenge bit $bits^*$, $\mathcal{D}$ computes $F_y(bits^*)$. If $F_y(bits^*) \neq 0$, $\mathcal{D}$ sets $b' \leftarrow_R \{0,1\}$. If $F_y(bits^*) = 0$, $\mathcal{D}$ computes R_{bits^*} and $\mathbf{c}$ and outputs $\mathbf{c}$, when $b = 0$. $\mathcal{D}$ randomly chooses $\overline{\mathbf{w}}$, $\mathbf{c}_2 \in R_q$, $\mathbf{c}_4 \in R_q^{2m}$ and outputs the ciphertext, when $b = 1$.
- **Guess**. $\mathcal{A}$ outputs the guess $\widehat{b}$. $\mathcal{D}$ sets $b' = \widehat{b}$. If $b' = b$, $\mathcal{D}$ outputs 1; otherwise, it outputs 0.
- **Analysis**. When $\overline{\mathbf{w}}$ is randomly chosen, $\lfloor\overline{\mathbf{w}}\rceil_2$ is a uniform distribution given $\langle\overline{\mathbf{w}}\rangle_2$. $\mathcal{D}$ simulates the view $\{\mathbf{a}_i, \mathbf{v}_i' + \mathbf{e}_i = \mathbf{a}_i\mathbf{s}_2 + \mathbf{e}_i\}_{i=0}^m$ in **Game**$_6$ and the view $\mathbf{v}_i' \leftarrow_R R_q$ in **Game**$_5$. Therefore, we have $\left|Pr[E_6] - Pr[E_5]\right| \leq Adv_{\mathcal{D}}^{RLWE_{n,m+1,q,\left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m}}$.

Game$_7$ Randomly choose $\mathbf{v} \leftarrow_R R^{2m}$, $\mathbf{c}_3 \leftarrow_R R_q^m$, and $\mathbf{e}_{3,1}, \mathbf{e}_{3,2} \leftarrow \left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m$, compute $\mathbf{E} = \left[\overline{\mathbf{a}_r} | \mathbf{c}_3\right]$, $\mathbf{c}_4 = \mathbf{s}_2\mathbf{E} + [\mathbf{e}_{3,1} | \mathbf{e}_{3,2}]$, and output the ciphertext. Observe $\phi(\mathbf{v}) = \phi(\mathbf{v}' + \mathbf{e}) = \phi(\mathbf{e}') + \phi(\mathbf{e}) \in \mathbb{Z}_q^{nm}$ with $\phi(\mathbf{e}) \leftarrow \mathcal{D}_{\mathbb{Z}^{nm},\sigma}$. In addition, note that $\mathbf{c} = \phi(\mathbf{v}') \cdot \mathbf{rot}\left(\left[\mathbf{I}_m | R_{bits^*}\right]\right) + \mathbf{e}' = \phi\left(\left[\mathbf{v}' | \mathbf{v}' R_{bits^*}\right]\right)$. The distribution of $\mathbf{e}'$ is statistically close to the distribution of $\mathbf{e}' \leftarrow_R \mathcal{D}_{\mathbb{Z}^{2nm},\sigma'}$. The distribution of $\mathbf{c}_1 = \phi^{-1}(\mathbf{c})$ in **Game**$_7$ and the distribution of that in **Game**$_6$ are statistically indistinguishable. Thus, we have $\left|Pr[E_7] - Pr[E_6]\right| \leq negl(n)$.

Game$_8$ The challenge generates the challenge ciphertext $\mathbf{C} = (\tau, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5)$. $\mathbf{c}_4$ in **Game**$_7$ and the uniform distribution over R_q^{2m} are statistically indistinguishable under the $RLWE_{q,n,m,\left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m}$ assumption. Choose $\mathbf{v}', \mathbf{v}'' \in_R R_q^m$, and compute $\mathbf{v}'R_{bits^*}$. The distribution of $\left[\mathbf{v}'|\mathbf{v}'R_{bits^*}\right]$ is statistically close to the uniform distribution over R_q^{2m}. Thus, we have $\left|Pr[E_8] - Pr[E_7]\right| \leq negl(n)$.

Theorem 4: The proposed signcryption scheme has ciphertext anonymity (INDK-CCA security) under the $RLWE_{q,n,m,\left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m}$ *hard problem.*

Proof: Assume that there exists a PPT distinguisher $\mathcal{D}$ that has a non-negligible advantage over the INDK-CCA security of the proposed scheme; then, there exists an algorithm $\mathcal{B}$ that solves the $RLWE_{q,n,m,\left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m}$ problem. $\mathcal{B}$ uses $\mathcal{A}$ to solve this instance and plays the role of $\mathcal{D}$'s challenger. $\mathcal{B}$ executes *TrapGen* to generate $(pk_{r,0} = \overline{\mathbf{a}_{r,0}} \in R_q^m, sk_{r,0} = \mathbf{T}_{\overline{\mathbf{a}_{r,0}}} \in R^{m\times m})$ and generate $(pk_{r,1} = \overline{\mathbf{a}_{r,1}} \in R_q^m, sk_{r,1} = \mathbf{T}_{\overline{\mathbf{a}_{r,1}}} \in R^{m\times m})$. $pk_{r,0}$ and $pk_{r,1}$ are given to $\mathcal{D}$. $\mathcal{D}$ performs queries. The signcryption queries and unsigncryption queries are treated as in the proof of **Theorem III.3**.

Once stage 1 ends, $\mathcal{D}$ outputs two private keys $sk_{s,0} = \mathbf{T}_{\overline{\mathbf{a}_{s,0}}}$, $sk_{s,1} = \mathbf{T}_{\overline{\mathbf{a}_{r,1}}}$ and a plaintext *msg*. $\mathcal{B}$ sends the fake ciphertext $\mathbf{C} = (\tau, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5)$, where $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5$ are chosen randomly. $\mathcal{D}$ cannot distinguish $\mathbf{c}_4 \in R_q^{2m}$ and $\mathbf{c}_4 = \mathbf{s}_2\mathbf{E} + \mathbf{e}_3$, where $\mathbf{e}_3 = [\mathbf{e}_{3,1}|\mathbf{e}_{3,2}] \leftarrow \left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^{2m}$, because of the $RLWE_{q,n,m,\left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m}$ hard problem. Therefore, $\mathcal{D}$ cannot realize that this ciphertext is fake, and the simulation remains.

In stage 2, $\mathcal{D}$ performs the queries that are executed in stage 1. Finally, $\mathcal{D}$ outputs a guess (f, f'), which is ignored by $\mathcal{B}$. $\mathcal{B}$ cannot obtain $(msg, \overline{\mathbf{a}_{r,0}})$ or $(msg, \overline{\mathbf{a}_{r,1}})$ from H_1. If $\mathcal{D}$ can output f and f' such that $(f, f') = (b, b')$, then it can find a collision $H_1(msg, \overline{\mathbf{a}_{r,f'}}) = H_1(msg, \overline{\mathbf{a}_{r,b'}})$. We use $Adv_{\mathcal{D}}^{\mathbf{collision}}$ to denote that $\mathcal{D}$ finds a collision. In short, we have the following conclusion:

$$\begin{aligned} Adv_{\mathcal{D}}^{INDK} &\leq Adv_{\mathcal{D}}^{RLWE_{n,m+1,q,\left(\mathcal{D}^{coeff}_{\mathbb{Z}^n,\sigma_1}\right)^m}} + Adv_{\mathcal{D}}^{\mathbf{collision}} \\ &\leq negl(n). \end{aligned}$$

D. PERFORMANCE ANALYSIS AND COMPARISON

In this section, the performance of our scheme is analyzed from four aspects: the PK size, SK size, ciphertext overhead and concrete execution time. Meanwhile, we compare our scheme with other lattice-based schemes in [12], [20]–[23] to demonstrate that our scheme achieves better performance. The schemes in [26] and [27] are not anti-quantum signcryption schemes. It is assumed that the output of the hash algorithm is 128 bits and that the random number is 128 bits to achieve AES-128 security.

1) COMPUTATIONAL OVERHEAD

Here, we mainly consider the operation time of the hash function t_h, the dot multiplication t_d, the polynomial multiplication t_p, the Gaussian sampling algorithm t_g and the pairing operation time t_{pair}. We have implemented these cryptography operations using the C/C++ PBC library on a 64-bit Windows 10 Thinkpad X1 notebook and a 64-bit Ubuntu 14.4 LTS Think Center desktop as shown in **Table 1**. In addition, **Table 2** shows the implementation time of the related schemes when $n = 256$, $m = 512$, and $q = 4093$.

TABLE 1. Time for the cryptography operation.

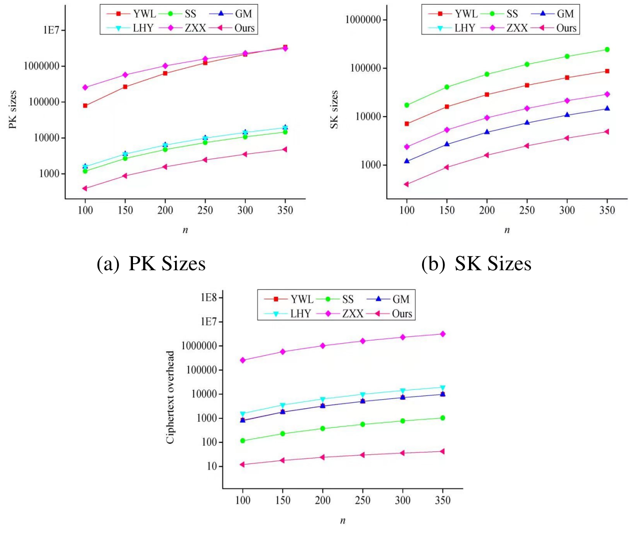
Cryptography Operation	Time
t_h	0.3 ms
t_d	0.27 ms
t_p	0.44 ms
t_g	0.52 ms
t_{pair}	9.35 ms

TABLE 2. Comparison of the execution times.

	KeyGen	Signcryption	Unsigncryption
[10]	670 ms	2212 ms	2228 ms
[12]	115343 ms	69369 ms	356515 ms
[13]	533 ms	912 ms	988 ms
[20]	808 ms	2153 ms	1570 ms
[21]	624 ms	1842 ms	622 ms
[22]	399 ms	757 ms	450 ms
[23]	604 ms	677 ms	677 ms
[26]	324 ms	756 ms	747 ms
[27]	1500 ms	2000 ms	1000 ms
Ours	266 ms	644 ms	716 ms

2) COMMUNICATION OVERHEAD

In Fig. 1, to simplify the analysis, we set $q = 277063$. We compare our scheme with YWL [12], SS [20], GM [21], LHY [22] and ZXX [23] in terms of the communication



(a) PK Sizes

(b) SK Sizes

(c) Ciphertext Sizes

FIGURE 1. Comparison of the communication overheads of the existing signcryption schemes based on lattices.

overhead when choosing different dimensions n. According to Fig. 1, the communication costs of our signcryption schemes are lower than those of other lattice-based signcryption schemes. The measurement units of the vertical coordinate are kilobytes (KB).

TABLE 3. Comparison of the PK/SK sizes.

	PK	SK
[6]	$6n^2 \log^2 q$	$36n^2 \log^2 q \log(n \log q)$
[8]	$12n^3 \log^3 q$	$72n^2 \log^2 q \log(n \log q)$
[10]	$2n^2 \log^2 q$	$\frac{1}{2} n^2 \log^2 q \log(\log n)$
[12]	$2n^3 \log^2 q$	$16n^2 \log^3 q + 2n^2 \log^2 q$
[13]	$12n^2 \log^2 q$	$36n^2 \log^2 q \log(n \log q)$
[20]	$3n^2 \log^2 q$	$3n^2 \log^2 q \log(2n \log q \log n)$
[21]	$4n^2 \log^2 q$	$3n^2 \log^2 q$
[22]	$4n^2 \log^2 q$	$6n^2 \log^2 q$
[23]	$36n^2 \log^3 q$	$6n^2 \log^2 q$
[26]	$(\lvert A_s \rvert + 2) B_G$	$(\lvert A_d \rvert + 2) B_G$
[27]	$(\lvert A_s \rvert + 2) B_G$	$(\lvert A_d \rvert + 2) B_G$
Ours	$n^2 \log^2 q$	$n^2 \log^2 q$

TABLE 4. Comparison of the ciphertext overheads.

	Ciphertext Overhead
[6]	$n + 6n \log^2 q$
[8]	$n(6n \log^2 q + 1) \log q$
[10]	$n(3 \log q + 2 \log 2q + 3) \log q$
[12]	$2n(n+5) \log^2 q$
[13]	$24n \log^2 q$
[20]	$n + (128 + 3n + 6 \log(2n \log q \log n)) n \log q$
[21]	$256 + 2n^2 (1 + \log q) \log q$
[22]	$128 + 2n^2 + 4n^2 \log^2 q$
[23]	$796 + 36n^2 \log^3 q$
[26]	$(\ell_s + \ell_e + 4) B_G + B_{tt} + \lvert msg \rvert$
[27]	$2(\ell_e + \ell_s + 2) B_G$
Ours	$2n + n(1 + 3 \log q) \log q$

Let q be the modulus. Let n be the lattice dimension. $\ell_s(\ell_e)$ denotes the number of attributes in a signing (encryption) predicate. $|A_s|(|A_d|)$ denotes the number of signing (decryption) key attributes. $\varphi(e)$ denotes the number of encryption attributes required in the designcryption process. B_G denotes the bit length of an element of the group G. B_{tt} denotes the bit length of the time stamp. $|msg|$ denotes the bit length of a message or plaintext. **Table 3** shows a comparison of the PK/SK sizes. A comparison of the ciphertext overhead is listed in **Table 4**. **Table 5** shows a concrete comparison for realizing 128-bit security when $q = 277063$, $\sigma = 3.4$, and $n = 540$. In **Table 6**, we use M_V, S_D and S_P to denote the vector multiplication, discrete sample, and preimage sample, respectively. E_x denotes the exponential operation in G. P_a denotes the pairing operation.

TABLE 5. Concrete comparison.

	PK	SK	Ciphertext size	Standard Model
[6]	6,320 KB	131,591 KB	12 KB	No
[8]	37,133,790 KB	263,183 KB	6,321 KB	No
[10]	2,107 KB	5,731 KB	11 KB	Yes
[12]	12×10^6 KB	26,388 KB	23,280 KB	Yes
[13]	12,641 KB	131,591 KB	25,28 2KB	Yes
[20]	34,599 KB	588,183 KB	1,097 KB	Yes
[21]	46,132 KB	34,599 KB	24,347 KB	No
[22]	46,132 KB	69,198 KB	46,203 KB	No
[23]	7,473,389 KB	69,198 KB	7,473,389 KB	No
[26]	2340 KB	2340 KB	4826 KB	No
[27]	2340 KB	2340 KB	9288 KB	No
Ours	1,053 KB	1,053 KB	6.34 KB	Yes

TABLE 6. Comparison of the computational efficiencies.

	Signcryption cost	Unsigncryption cost
[6]	$S_P + M_V$	$2M_V$
[8]	$S_P + n \log q(S_D + M_V)$	$(n \log q + 2) M_V$
[10]	$S_P + 5S_D + 5M_V$	$S_P + 9M_V$
[12]	$S_P + 3S_D + 8M_V$	$S_P + 9M_V$
[13]	$S_P + 2S_D + 4M_V$	$6M_V$
[20]	$8M_v + 5S_D + S_P$	$8M_V + 2S_P$
[21]	$2S_D + 8M_V$	$5M_V$
[22]	$4S_D + 10M_V$	$5M_V$
[23]	$S_P + 2M_V$	$2M_V$
[26]	$(4\ell_s + 2\ell_e + 7) E_x$	$(\ell_s + 2\varphi(e) + 2) E_x + (\ell_s + 5) P_a$
[27]	$(2\ell_s + \ell_e + 4) E_x$	$(\ell_s + 2) E_x + P_a$
Ours	$S_P + 4M_V$	$S_P + 3M_V$

IV. CONCLUSION

In this paper, we have proposed a more efficient standard model signcryption scheme based on lattices by carefully combining the partitioning technique with several favourable algebraic properties of the tag-based lattice trapdoor, the RLWE problem and the ISIS problem. Compared to current lattice-based signcryption schemes, the proposed scheme not only provides a novel construction idea but also reduces the sizes of the public keys, private keys and ciphertexts. With the rapid development of cloud services, key exposure has been highlighted as a serious security issue. Inspired by [36], it will be interesting to construct an efficient lattice-based key-exposure resilient aggregate signcryption scheme for secure cloud storage, which we leave for future work.

REFERENCES

[1] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption)," in *Advances in Cryptology*, vol. 1294. Santa Barbara, CA, USA: Springer, 1997, pp. 165–179.

[2] X. Boyen, "Multipurpose identity-based signcryption," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 2729. Santa Barbara, CA, USA: Springer, 2003, pp. 383–399. doi: 10.1007/978-3-540-45146-4_23.

[3] B. Libert and J.-J. Quisquater, "Efficient signcryption with key privacy from gap Diffie-Hellman groups," in *Public Key Cryptography—PKC*, vol. 2947. Singapore: Springer, 2004, pp. 187–200. doi: 10.1007/978-3-540-24632-9_14.

[4] F. Li, M. Shirase, and T. Takagi, "Certificateless hybrid signcryption," in *Proc. ISPEC*, vol. 5451. Xi'an, China: Springer, 2009, pp. 112–123. doi: 10.1007/978-3-642-00843-6_11.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1999. doi: 10.1137/S0097539795293172.

[6] F. Li, F. T. B. Muhaya, M. K. Khan, and T. Takagi, "Lattice-based signcryption," *Concurrency Comput., Pract. Exper.*, vol. 25, no. 4, pp. 2112–2122, 2012. doi: 10.1002/cpe.2826.

[7] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 40th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, May 2008, pp. 197–206. doi: 10.1145/1374376.1374407.

[8] F. Wang, C. Wang, and Y. Hu, "Post-quantum secure hybrid signcryption from lattice assumption," *Appl. Math. Inf. Sci.*, vol. 6, no. 1, pp. 23–28, 2012. doi: 10.18576/amis.

[9] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," in *Proc. STOC*. Bethesda, MD, USA: Springer, 2009, pp. 333–342. doi: 10.1145/1536414.1536461.

[10] J. Yan, L. Wang, L. Wang, Y. Yang, and W. Yao, "Efficient lattice-based signcryption in standard model," *Math. Problems Eng.*, vol. 2013, Aug. 2013, Art. no. 702539. doi: 10.1155/2013/702539.

[11] D. Micciancio and C. Peikert, "Trapdoors for lattices: Simpler, tighter, faster, smaller," in *Proc. EUROCRYPT*. Cambridge, UK: Springer, 2012, pp. 700–718. doi: 10.1007/978-3-642-29011-4_41.

[12] J. Yan, L. Wang, H. Ahmad, J. Yue, W. Yao, and M. Li, "Attribute-based signcryption from lattices in the standard model," *IEEE Access*, vol. 7, pp. 56039–56050, 2019. doi: 10.1109/ACCESS.2019.2900003.

[13] X. Lu, Q. Wen, L. Wang, C. Yang, and Z. Jin, "A lattice-based signcryption scheme without random oracles," *Frontiers Comput. Sci.*, vol. 8, no. 4, pp. 667–675, 2014. doi: 10.1007/s11704-014-3163-1.

[14] X. Boyen, "Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more," in *Public Key Cryptography*. Paris, France: Springer, 2010, pp. 499–517. doi: 10.1007/978-3-642-13013-7_29.

[15] X. Xiang, H. Li, Z. Liu, and M. Wang, "Hidden attribute-based signcryption scheme for lattice," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 1780–1787, 2014. doi: 10.1002/sec.875.

[16] X. Lu, Q. Wen, J. Du, and L. Wang, "A Lattice-based signcryption scheme without trapdoors," *J. Electron. Inf. Technol.*, vol. 38, no. 9, pp. 2287–2293, 2016.

[17] S. Bai and S. D. Galbraith, "An improved compression technique for signatures based on learning with errors," in *Proc. Cryptographer's Track RSA Conf.* San Francisco, CA, USA: Springer, 2014, pp. 28–47. doi: 10.1007/978-3-319-04852-9_2.

[18] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," *J. Cryptol.*, vol. 26, no. 1, pp. 80–101, 2013. doi: 10.1007/3-540-48405-1_34.

[19] G. Leurent and P. Q. Nguyen, "How risky is the random-oracle model?" in *Proc. CRYPTO*. Santa Barbara, CA, USA: Springer, 2009, pp. 445–464. doi: 10.1007/978-3-642-03356-8_26.

[20] S. Sato and J. Shikata, "Lattice-based signcryption without random oracles," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 10786. Cham, Switzerland: Springer, 2018, pp. 331–351. doi: 10.1007/978-3-319-79063-3_16.

[21] F. Gérard and K. Merckx, "SETLA: Signature and encryption from lattices," in *Cryptology and Network Security* (Lecture Notes in Computer Science), vol. 11124. Cham, Switzerland: Springer, 2018, pp. 299–320. doi: 10.1007/978-3-030-00434-7_15.

[22] Z. Liu, Y.-L. Han, and X.-Y. Yang, "A signcryption scheme based learning with errors over rings without trapdoor," in *Proc. NCTCS*, vol. 1069. Singapore: Springer, 2019, pp. 168–180. doi: 10.1007/978-981-15-0105-0_11.

[23] X. Zhang, C. Xu, and J. Xue, "Efficient multi-receiver identity-based signcryption from lattice assumption," *Int. J. Electron. Secur. Digit. Forensics*, vol. 10, no. 1, pp. 20–38, 2018. doi: 10.1504/ijesdf.2018.089202.

[24] C. Chen, J. Chen, H. W. Lim, Z. Zhang, and D. Feng, "Combined public-key schemes: The case of ABE and ABS," in *Provable Security*, vol. 7496. Berlin, Germany: Springer, 2012, pp. 53–69. doi: 10.1007/978-3-642-33272-2_5.

[25] K. Emura, A. Miyaji, and M. S. Rahman, "Dynamic attribute-based signcryption without random oracles," *Int. J. Adv. Comput. Technol.*, vol. 2, no. 3, pp. 199–211, 2012. doi: 10.1504/IJACT.2012.045589.

[26] Y. Rao, "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing," *Future Gener. Comput. Syst.*, vol. 67, pp. 133–151, Feb. 2017. doi: 10.1016/j.future.2016.07.019.

[27] F. Deng, H. Xiong, Y. Wang, L. Peng, J. Geng, and Z. Qin, "Ciphertext-policy attribute-based signcryption with verifiable outsourced designcryption for sharing personal health records," *IEEE Access*, vol. 6, pp. 39473–39486, 2018. doi: 10.1109/ACCESS.2018.2843778.

[28] S. Katsumata and S. Yamada, "Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps," in *Advances in Cryptology—ASIACRYPT*. Hanoi, Vietnam: Springer, 2016, pp. 682–712. doi: 10.1007/978-3-662-53890-6_23.

[29] F. Böhl, D. Hofheinz, J. Koch, C. Striecks, and T. Jager, "Confined guessing: New signatures from standard assumptions," *J. Cryptol.*, vol. 28, no. 1, pp. 176–208, 2015. doi: 10.1007/s00145-014-9183-z.

[30] B. Libert, S. Ling, K. Nguyen, H. Wang, and F. Mouhartem, "Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions," in *Advances in Cryptology—ASIACRYPT*. Hanoi, Vietnam: Springer, 2016, pp. 373–403. doi: 10.1007/978-3-662-53890-6_13.

[31] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *Security in Communication Networks*. Amalfi, Italy: Springer, 2002, pp. 268–289. doi: 10.1007/3-540-36413-7_20.

[32] V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for ring-LWE cryptography," in *Advances in Cryptology—EUROCRYPT*. Athens, Greece: Springer, 2013, pp. 35–54. doi: 10.1007/978-3-642-38348-9_3.

[33] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *J. Cryptol.*, vol. 25, no. 4, pp. 601–639, 2012. doi: 10.1007/s00145-011-9105-2.

[34] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa, "Efficient public key encryption based on ideal lattices," in *Advances in Cryptology—ASIACRYPT*. Tokyo, Japan: Springer, 2009, pp. 617–635. doi: 10.1007/978-3-642-10366-7_36.

[35] C. Peikert, "Lattice cryptography for the Internet," in *Post-Quantum Cryptography*. Waterloo, ON, Canada: Springer, 2014, pp. 197–219. doi: 10.1007/978-3-319-11659-4_12.

[36] X. Zhang, H. Wang, and C. Xu, "Identity-based key-exposure resilient cloud storage public auditing scheme from lattices," *Inf. Sci.*, vol. 472, pp. 223–234, Jan. 2019. doi: 10.1016/j.ins.2018.09.013.

XIAOPENG YANG received the B.S. degree in applied mathematics and the M.S. degree in algebra and codings from the Anqing Normal University of China, Anhui, China, in 2009 and 2012, respectively, and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2017. He is currently with the China Coast Guard Academy. His research interests include cryptography and information security.

HAO CAO received the B.S. degree in applied mathematics, and the M.S. degree in applied mathematics from the Huaibei Normal University of China, Anhui, China, in 2000 and 2007, respectively, and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2019. He is currently with the Huaibei Normal University of China. His research interests include cryptography and quantum teleportation.

WEICHUN LI received the B.E. degree in forest engineering from the Inner Mongolia Forestry College of China, Inner Mongolia, China, in 1990, and the M.S. degree in forest engineering from the Nanjing Forestry University of China, Jiangsu, China, in 1993. He is currently with the China Coast Guard Academy. His research interests include cryptography and quantum teleportation.

HEJUN XUAN received the B.S. degree in computer science and technology from Xinyang Normal University, China, in 2012, and the Ph.D. degree in computer software and theory from Xidian University, China, in 2018. He is currently with the School of Computer and Information Technology, Xinyang Normal University. His research interests include cloud/grid/cluster computing and scheduling in parallel and distributed systems.