Journal of Computers Vol. 31 No. 1, 2020, pp. 320-331
doi:10.3966/199115992020023101029

Chosen-ciphertext Secure Hierarchical Identity-based Encryption from R-LWE

Xue-Feng Jiang, Ting Wang*, Zhi-Wei Sun

School of Artificial Intelligence, Shenzhen Polytechnic, Shenzhen, 518055 China
{jiangxuefeng, wangt, sunzw}@szpt.edu.cn

Received 2 December 2019; Revised 2 January 2020; Accepted 2 February 2020

Abstract. Identity-based encryption (IBE) is a new public key encryption system, any string can be its public key, private key is generated by the private key generator that owns the main private key. Hierarchical identity-based encryption (HIBE) is an extension of IBE, which can lighten the burden of the center of private-key generation greatly. HIBE is more suitable for the protection of large organizations and distributed environments, and it can isolate damage when some a private key is disclosed. In this paper, a more secure and efficient HIBE scheme from lattice is presented. First, we propose a chosen-plaintext attacks (CPA) secure HIBE scheme from the learning with errors over rings (R-LWE), on this basis, a new HIBE scheme that is secure against adaptive chosen-ciphertext attacks (CCA) is constructed, whose security is based on the hardness of the shortest vector problem (SVP). Analyses indicate the proposed scheme is more efficient than correlative cryptosystems and CCA-secure in the random oracle model.

Keywords: chosen-ciphertext security, encryption, HIBE, R-LWE

1 Introduction

As adversaries and hackers become more active and sophisticated, the theft of users' private information often leads to a lot of losses, and many network application environments are facing increasingly severe security situation. Therefore, more and more cryptography researchers pay attention to the research of higher level provable security. It has been proved that many applications facing more attacks need stronger security level, that is, security against adaptive chosen-ciphertext attacks (CCA) [1]. CCA not only satisfies the security of ciphertext in distinguish ability in selective plaintext attack (CPA), but also provides the adversary with additional access to the decryption oracle. For this reason, CCA security has been regarded as a very important security standard of public key encryption scheme. However, there are relatively few effective methods to construct a public key cryptosystem that meets this higher security requirement.

Naor and Yung [2] first give a method to construct the non-adaptive chosen-ciphertext secure scheme. Later it was extended by Dolev et al. [1] to the case of adaptive chosen-ciphertext security, which uses CPA security encryption scheme and non-interactive zero knowledge (NIZK) proof system [3]. In 2006, Boneh et al [4] proposed a general mode of building CCA secure encryption, which is also adopted in this paper. This mode provides an effective method to construct CCA secure encryption scheme by means of any IBE algorithm and strong first signature algorithm. This method provides a new way to construct CCA secure encryption scheme and avoids the formal evidence system in the former scheme. It has important theoretical and practical significance. Inspired by the CHK transformation, [5] proposes an alternative paradigm to design CCA-secure D-PKE scheme. All of the above CCA secure public key cryptosystems are based on traditional difficulties.

Lattice cryptography has many advantages, such as high efficiency, low computational complexity, more difficult to solve than classical cryptography, and it is recognized as resistant to quantum attacks, so it has a better application prospect. In 1997, Ajtai and Dwork [6] constructed the first public-key

* Corresponding Author

cryptosystem based on the worst-case hardness of a lattice problem, which was the first cryptosystem to provide security proof based worst-case hardness assumptions on lattice problems, however, the execution efficiency of this system is quite inefficient. In 2005, Regev [7] proposed an important cryptography primitive called learning with errors (LWE), and proved the hardness of the problem under the quantum reduction, that is, if there is an effective probabilistic polynomial time algorithm to solve the LWE problem, then there is an effective quantum algorithm to solve the approximate lattice problem, at the same time, a public key encryption scheme based on LWE problem is given.

In 2009, based on previous work [8], Peikert [9] further proved the hardness of LWE problem under the traditional reduction. Furthermore, using hybrid encryption and strong one time signature, he first gave a natural CCA-secure encryption based on LWE problem, which not only provides a different choices from the traditional mode, but also has many advantages, such as simpler description, analysis and tighter underlying approximation factors. In 2013, Yang et al. [10] proposed a CCA secure public key encryption scheme based on the assumption of R-LWE. which can support the integrity verification and block encryption, but its public and private key sizes and expansion factors are still relatively large, which also leads to its encryption efficiency is not high enough.

The reason why LWE has a strong attraction is that it not only has good generality and can resist the attack of quantum algorithm, but also has high efficiency and low complexity operation. So a large number of encryption schemes from LWE have been put forward in recent years, such as identity based encryption schemes [11-13], homomorphic encryption [14-15], and other encryption schemes [16-17]. In order to further improve the efficiency of encryption scheme from lattice, Lyubashevsky et al. [18] discussed LWE problem on ideal lattice and integer polynomial ring in Eurocrypt 2010, namely, the learning with errors over rings (R-LWE) assumption, and gave an encryption scheme from R-LWE. For possessing the simpler algebraic structure, the assumption can be used to construct more efficient schemes and the efficiency of the schemes based on R-LWE have been greatly improved generally, such as encryption schemes [19-20]. In this paper, we will construct a CCA-secure hierarchical identity-based encryption (HIBE) scheme from R-LWE assumption.

HIBE is an extension of IBE, which was first given by Horwitz and Lynn [22], which can lighten the burden of the center of private-key generation greatly. HIBE scheme permits multiple levels of trusted private-key authorities to generate secret keys. This encryption is more suitable for the protection of large organizations and distributed environments, and it can isolate damage when secret-key is exposed. At present, there is almost no CCA secure HIBE schemes, all of the above correlative schemes have their corresponding advantages and application scenes, and the detailed descriptions are summarized in Table 1. However, they tend to be inefficient for practical applications.

Table 1. The properties of the correlative schemes

Scheme	Techniques	Assumption	Limitations
[4]	based on any IBE scheme	BDH	inefficient for basing on BDH, unsecure in quantum environment
[9]	witness-recovering decryption approach, trapdoor functions	LWE	private and public key size is large, the efficiency is low
[10]	ID-Trap, stronger regularity bound theorem	R-LWE	private and public key size is large, expansion is bad
[12]	bonsai trees	LWE	the efficiency of encryption and decryption is low, not CCA-secure
[22]	binary tree encryption, random oracle	LWR	the HIBE scheme is not CCA-secure

In order to construct an efficient CCA-secure HIBE scheme, we propose a CPA-secure HIBE scheme from R-LWE, which is more efficient than the scheme in [12, 22]. Then, based on Guneysu's signature scheme [21] and the proposed HIBE scheme, we give a CCA-secure HIBE encryption scheme from R-LWE for the first time, which can realize batch encryption over rings, having a low encryption expansion factor and a higher encryption and decryption efficiency, and the encryption expansion factor is invariable with the increase of the level, message and security parameter.

The rest of the paper is arranged as follows. In the second section, the basic knowledge is introduced. In the third section, firstly, the definition of HIBE is introduced, then a HIBE scheme is proposed along with its efficiency and security analysis. In Section 4, based on the scheme in Section 3 and the signature scheme in [23], a CCA secure HIBE scheme is constructed. Finally, the fifth section summarizes the paper.

2 Preparation

2.1 Learning with Errors over Rings (R-LWE)

Suppose $f(x)=x^n+1\in Z[x]$, where n is security parameter, which is a power of 2 making $f(x)$ irreducible, $R=Z[x]/<f(x)>$ is an integer polynomial ring modulo $f(x)$, $q=1 \bmod 2n$ is a large common prime modulus, $R_q=R/<q>=Z_q[x]/<f(x)>$ is the ring of integer polynomials. Elements of R_q can be represented by the polynomials, coefficients come from $\{(-q+1)/2,\cdots,-1,0,1,\cdots,(q-1)/2\}$.

The R-LWE assumption can be described as follows [18]. Suppose $s\in R_q$ is a uniformly random, which is secret, define two distributions over $R_q\times R_q$: (1) $(a,b=a\times s+e)\in R_q\times R_q$, where a is chosen from R_q randomly and e is a "small" error term selected from a distribution χ over R_q. (2) $(a,\ c)$, where a, c are chosen from R_q randomly. The purpose of the R-LWE assumption is to distinguish the above two distributions. That is to say, if R-LWE assumption is hard, then the set $(a,a\times s+e)$ is pseudo-random, where all operations are implemented in R_q.

Lyubashevsky et al. [18] proved that the R-LWE assumption on ideal lattice is difficult to any polynomial time (even quantum) attacker.

2.2 Sampling from Discrete Gaussians

The discrete Gaussians distribution is defined as follows [11].

Denition 1. The n dimensional Gaussian function $\rho_{\sigma,c}:R^n\to(0,1]$ is given by $\rho_{\sigma,c}(x)=\exp(-\frac{\|x-c\|^2}{2\sigma^2})$. For any $c\in R^n$, real $s>0$, and n dimensional lattice Λ, define the Discrete Gaussians distribution as: $\rho_{\Lambda,\sigma,c}(x)=\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\Lambda)}$, $x\in\Lambda$, where $\rho_{\sigma,c}(\Lambda)=\sum_{x\in\Lambda}\rho_{\sigma,c}(x)$.

Now let's introduce some of the conclusions that will be used in this paper.

Theorem 1 (short basis [24]). Suppose $C>1$ is a constant, $TrapGen(q,n)$ is a probabilistic polynomial time algorithm. For $m\geq Cn\lg q$, outputs $(A\in Z_q^{n\times m},T\in Z^{m\times m})$ such that:

- A is close to a uniform matrix in $Z_q^{n\times m}$.
- T is a basis of $\wedge_q^{\perp}(A)$.
- The norm of all the rows in T ($\|T\|$) is bounded by $O(n\log n)$.

Theorem 2 (Randomizing a basis [12]). For a rank n matrix $A\in Z_q^{n\times m}$. Suppose $T\in Z^{m\times m}$ be an arbitrary basis of $\Lambda^{\perp}(A)\subseteq Z^m$. For a parameter $\sigma\geq\|\tilde{T}\|\cdot\omega(\sqrt{\log n})$, there is a PPT algorithm $RandBasis(T,s)$ that outputs another basis T' of $\Lambda^{\perp}(A)$ such that $\|T'\|\leq\sigma\sqrt{m}$.

Theorem 3 (Extending a basis [12]). For a rank n matrix $A\in Z_q^{n\times m}$. Suppose $T\in Z^{m\times m}$ be an arbitrary basis of $\Lambda^{\perp}(A)\subseteq Z^m$ and $\overline{A}\subseteq Z_q^{n\times\overline{m}}$ be an arbitrary matrix. There is a deterministic polynomial-time algorithm $ExtBasis(T,A'=A\|\overline{A})$ that outputs a basis T' of $\Lambda^{\perp}(A')\subseteq Z^{m+\overline{m}}$ such that $\|\tilde{T}'\|=\|\tilde{T}\|$.

Theorem 4 (Delegating a basis [11]). Given a PPT algorithm $SampleISIS(A,T,\sigma,u)$, a matrix $A\in Z_q^{n\times m}$, a basis T of $\wedge^{\perp}(A)$, a parameter $\sigma\geq\|T\|\cdot\omega(\sqrt{\log n})$, and a vector $u\in Z^n$, outputs an

element x such that $Ax = u$.

Theorem 5 ([11]). The algorithm *Sample*ISIS(A, T, σ, u) gives a collection of trapdoor one-way functions with preimage sampling, if inhomogeneous smallest integer solution ($ISIS_{q,m,\sigma\sqrt{m}}$) problem is hard on the average.

2.3 Signature Scheme from R-LWE

In this part, we introduce a briefly signature scheme in [23], which will be used in in Section 4.

- KeyGen(1^n) : Signing Key $s_1, s_2 \leftarrow R_1$, verification Key $a \leftarrow R_q, b \leftarrow as_1 + s_2$, and note $\{sk = (s_1, s_2), vk = (a, b)\} \leftarrow$ keyGen .
- Sign$(sk = (s_1, s_2), m)$: (1) $y_1, y_2 \leftarrow R_k\ (k < q)$. (2) $c = \mathrm{H}(ay_1 + y_2, m)$, where H is a hash function that maps arbitrary bit strings into a small polynomial. (3) $\sigma_1 \leftarrow s_1 c + y_1, \sigma_2 \leftarrow s_2 c + y_2$. (4) if $\| \sigma_1 \|$ or $\| \sigma_2 \| > \beta$, go to step1, where β is a fixed bound. (5) output $\sigma = (\sigma_1, \sigma_2, c)$.
- Verify$\{vk = (a, b), m, \sigma = (\sigma_1, \sigma_2, c)\}$: Accept iff $\| \sigma_1 \|, \| \sigma_2 \| \leq \beta$ and $c = H(a\sigma_1 + \sigma_2 - bc, m)$.

3 Hierarchical Identity-based Encryption

3.1 Definition

Definition 2 ([4]). A l level hierarchical identity-based encryption (HIBE) scheme can be described by a tuple of PPT algorithms (HIBE*Setup*, HIBE*Der*, HIBE*Enc*, HIBE*Dec*) :

- HIBE*Setup*$(1^n, 1^l)$: Given a security parameter 1^n. Output a master public key mpk and a master secret key sk_ε (assume that $n, l = l(n)$ and ID-vector v are implicit in public key pk_v and secret key sk_v), note $(mpk, sk_\varepsilon) \leftarrow$ HIBE*Setup*$(1^n, 1^l)$.
- HIBE*Der*$(v, sk_v, v.r)$: Given an ID-vector $v \in (\mathcal{ID})^{<l}$, the associated secret key sk_v and $r \in \mathcal{ID}$. Output the secret key $sk_{v.r}$ associated with the ID-vector $v.r$, note $sk_{v.r} \leftarrow$ HIBE*Der*$_{sk_v}(v, v.r)$.
- HIBE*Enc*(v, pk_v, M) : Given an ID-vector $v \in (\mathcal{ID})^{<l}$, the public key pk_v and a message. Output a ciphertext C, note $C \leftarrow$ HIBE*Enc*$_{pk_v}(v, M)$.
- HIBE*Dec*(v, sk_v, C) : Given an ID-vector $v \in (\mathcal{ID})^{<l}$, the secret key sk_v associated with the ID-vector v and a ciphertext C. Output a message M or $\perp$, note $M \leftarrow$ HIBE*Dec*$_{sk_v}(v, C)$.

For all (mpk, sk_ε) output by HIBE*Setup*, $v \in (\mathcal{ID})^{<l}$, sk_v correctly generated for the ID-vector v (in fact, the initial sk_v is the master secret key sk_ε), and the M in message space, there is always HIBE*Dec*$_{sk_v}(v,$ HIBE*Enc*$_{pk_v}(v, M)) = M$.

In Definition 2, if user A has a secret key sk_v (the length of v as $|v| = t (t < l)$ and $|\varepsilon| = 0$), any other user B can make secret key query to A using its identity $r \in \mathcal{ID}$ and A returns the next level secret key $sk_{v.r}\ (|v.r| = t + 1)$ to B.

3.2 Encryption Scheme

- $H : \mathcal{ID} \to Z_q^{n \times m}, h : (\mathcal{ID})^{\leq l} \to Z_q^n$ are random oracles that map identities to the elements of $Z_q^{n \times m}$ and Z_q^n respectively;
- $\tilde{L}_i$ is an upper bound on the Gram-Schmidt lengths of its secret short basis;
- $\sigma_i\ (1 \leq i \leq l)$ is the Gaussian parameter used to generate that secret basis, where $\sigma_i \geq \tilde{L}_j \cdot \omega(\sqrt{\log n})\ (\forall j < i)$.

Based on R-LWE problem, an efficient l level HIBE scheme $\mathcal{HIBE}$ can be constructed as follows.

- HIBE*Setup*(1^n): Given security parameter n, integer $m \geq Cn \lg q$ ($m = 2^d, d \in Z$), a sufficiently large

prime modulus $q = 1 \bmod (2m)$ and the maximal length l of ID-vectors. Run $TrapGen(q, n, m)$ to get a matrix $A_0 \in Z_q^{n \times m}$ and a trapdoor $T_0 \subset \Lambda_q^{\perp}(A)$ ($\| T_0 \| \leq \tilde{L}_0$), where $mpk = (A_0, l)$ is the master public key and $sk_{\varepsilon} = T_0$ is master secret key.

- HIBE$Der(v, sk_v = (T_v, s_v), v' = v.r)$: Given an ID-vector $v = (v_1, \cdots, v_t) \in (\mathcal{ID})^{t<l}$, the corresponding secret key sk_v (including secret short basis and decryption secret key) and $r \in \mathcal{ID} (r \notin \{v_1, \cdots, v_t\})$. To obtain the new secret key $sk_{v.r}$ associated with the ID-vector $v.r$, the following operations are performed:

(1) If the pair $(v.r, sk_{v.r})$ is in local storage, return $sk_{v.r}$. Otherwise, compute

$$u_{v.r} = h(v, r) \in Z_q^n,\ A_{v.r} = A_v \| A_v^r \in Z_q^{n \times 2^{t+1} m}$$

where A_v^r can be obtained by replacing the part A_0 of A_v using A_r, and the detailed computation can be described as follows:

a) If $|v| = 1$ (namely $v = v_1 \in \mathcal{ID}$), then

$$A_v = A_0 \| A_{v_1} \in Z_q^{n \times 2m},\ A_{v.r} = (A_0 \| A_{v_1}) \| (A_v \| A_v^r) \in Z_q^{n \times 2^2 m}$$

b) If $|v| = 2$ (namely $v = (v_1, v_2) \in (\mathcal{ID})^2$), then

$$A_v = (A_0 \| A_{v_1}) \| (A_{v_2} \| A_{v_1}) \in Z_q^{n \times 2^2 m}$$

$$A_{v.r} = A_v \| A_v^r = [(A_0 \| A_{v_1}) \| (A_{v_2} \| A_{v_1})] \| [(A_r \| A_{v_1}) \| (A_{v_2} \| A_{v_1})] \in Z_q^{n \times 2^3 m}$$

c) If $|v| = t$ (namely $v = (v_1, \cdots, v_t) \in (\mathcal{ID})^{t<l}$), it is easy to know that

$$A_{v.r} = A_v \| A_v^r \in Z_q^{n \times 2^{t+1} m}$$

where $A_r = H(r),\ A_{v_i} = H(v_i) \in Z_q^{n \times m} (i \leq t)$.

(2) Run algorithms *ExtBasis* and *RandBasis* simultaneity to get lattice $\Lambda^{\perp}(A_{v.r})$ and new short basis $T_{v.r} = Z_q^{2^{t+1} m \times 2^{t+1} m}$ associated with the ID-vector $v.r$

$$T_{v.r} \leftarrow RandBasis(ExtBasis(T_v, A_{v.r}), \sigma_{t+1})$$

(3) Run algorithm *Sample*ISIS$(A_{v.r}, T_{v.r}, \sigma_{t+1}, u_{v.r})$ to get a decryption secret key $s_{v.r} \in \Lambda_{u_{v.r}}^{\perp}(A_{v.r})$. Let $sk_{v.r} = (T_{v.r}, s_{v.r})$, saving $(v.r, sk_{v.r})$, and return $sk_{v.r}$ to user;

(4) Compute public key $pk_{v.r} = (a, b = a \times s_{v.r} + e)$, where $a \leftarrow R_q^{t+1} \overset{\Delta}{=} Z_q[x] / < x^{2^{t+1} m} + 1 >$ is uniformly random and e is some "small" random error term chosen from error distribution $\gamma_{t+1} \subset R_q^{t+1}$;

- HIBE$Enc(v, pk_v = (a, b = a \times s_v + e), M)$: Choose a "small" $t \in R_q^v$ randomly. Output the ciphertext

$$(c_1, c_2) = (a \cdot t + e_1, b \cdot t + e_2 + [q/2] \cdot M) \in R_q^t \times R_q^t$$

Where e_1, e_2 are "small" errors chosen from distribution $\gamma_t \subset R_q^v$, $M \in \{0,1\}^{2^t m}$ is the message requiring encryption, which can be regarded as the element of $R_q^t = Z_q[x] / < x^{2^t m} + 1 >$.

- HIBE$Dec(v, sk_v, (c_1, c_2))$: Compute $M' = c_2 - c_1 \cdot s_v$. Output 0 if the coefficient $m'_i (i = 0, 1, \cdots, 2^t m - 1)$ of M' is closer to 0 than to $[q/2]$ modulo q, otherwise output 1.

Claim 1. The l level HIBE scheme $\mathcal{HIBE}$ is correct.

Proof. Consider a ciphertext $(c_1, c_2) = (a \cdot t + e_1, b \cdot t + e_2 + [q/2] \cdot M) \in R_q^t \times R_q^t$ of a $2^t m$ bit message $M \in \{0,1\}^{2^t m}$ under the ID-vector $v(|v| = t)$ and public key $(a, b = a \cdot s_v + e)$, where $t \leftarrow R_q^t, e_i \leftarrow \gamma_t \subset R_q^t (i = 1, 2)$, the decryption can be computed as

$$\begin{aligned} M' &= c_2 - c_1 \cdot s_v \\ &= b \cdot t + e_2 + [q/2] \cdot M - (a \cdot t + e_1) \cdot s_v \\ &= (a \cdot s_v + e) \cdot t + e_2 + M \cdot [q/2] - (a \cdot t + e_1) \cdot s_v \\ &= M \cdot [q/2] + (e \cdot t + e_2 - e_1 \cdot s_v) \end{aligned}$$

Because the private key s_v is obtained from the algorithm $Sample\text{ISIS}(A_v, T_v, \sigma_t, u_v)$, s_v satisfies the condition of the $ISIS_{q,m,\beta}$ problem, so the coefficient of s_v is small. On the other hand, algorithms HIBE*Der* and HIBE*Enc* show that $e, e_1, e_2, t \in R_q^t$ are "small" polynomials. Hence the algorithm HIBE*Dec* can output the coefficient $m_i (i = 0,1,\cdots,m-1)$ of M correctly if the coefficients of $(e \cdot t + e_2 - e_1 \cdot s_v)$ are at distance at most $q/5$ from 0 (modulo q) via choosing a sufficiently large prime modulus q.

3.3 Security Analysis

Claim 2. For any parameters n、m、l、q、d、C and $f(x)$ satisfying the conditions of the proposed scheme, the l level HIBE scheme $\mathcal{HIBE}$ is selective-ID secure against chosen-plaintext attacks (IND-sID-CPA) in the random oracle model, assuming that the R-LWE is hard.

Proof. Suppose $\mathcal{A}$ is a PPT adversary that can distinguish between the encryptions of messages of its choice with the advantage ϵ in a chosen-plaintext attack. The adversary $\mathcal{A}$ works as follows:

- $\mathcal{A}$ outkputs a "target" ID-vector v^* ($|v^*| = t$).
- *Setup*: Takes a security parameter 1^n, runs HIBE*Setup*(1^n) to obtain ($mpk = (A_0, l), sk = T_0$), and give mpk to $\mathcal{A}$.
- *Queries*1: Suppose challenger has secret key sk_v, $\mathcal{A}$ may adaptively issues private key extraction queries to challenger corresponding to identities $r \in \mathcal{ID}$, as long as $v.r$ is not a prefix of the "target" ID-vector v^*. Challenger runs HIBE*Der*$(v, sk_v, v.r)$ to get the pair $(sk_{v.r}, pk_{v.r})$ and return them to $\mathcal{A}$.
- *Challenge*: After queries, $\mathcal{A}$ outputs two plaintexts $M_0, M_1 \in \{0,1\}^{2^l m}$. Challenger runs HIBE*Der*$(\varepsilon, sk_\varepsilon, v^*)$ to get s_{v^*}, a bit $b \in \{0,1\}$ is chosen at random, and $\mathcal{A}$ is given the public key $pk^* = (a, b = a \times s_{v^*} + e)$ and the "challenge ciphertext"

$$(a \cdot t + e_1, b \cdot t + e_2 + [q/2] \cdot M_b) \leftarrow \text{HIBE}Enc(v^*, pk^*, M_b).$$

- *Queries*2: $\mathcal{A}$ can go on to issue private key extraction queries as above.
- *Output*: $\mathcal{A}$ outputs a guess b'.

In order to prove the security of the above scheme, a distinguisher D between the following two distributions is constructed

$$\{(a, a \cdot s_{v^*} + e) : a \leftarrow R_q^t, s_{v^*} \in R_q^t, e \leftarrow \gamma_t \subset R_q^t\} \text{ and } \{\text{Unif}(R_q^t \times R_q^t)\}$$

D takes as input $(a \in R_q^t, c \in R_q^t)$ and runs the adversary $\mathcal{A}$ with (a, b) ($b = a \cdot s_{v^*} + e$) as the public key. When receiving messages $M_0, M_1 \in \{0,1\}^{2^l m}$ from $\mathcal{A}$, D chooses $b \in \{0,1\}$, $t \in R_q^t$ randomly, and returns the challenge ciphertext $(a \cdot t + e_1, c \cdot t + e_2 + [q/2] \cdot M_b)$. Outputs 1 if $\mathcal{A}$ guesses the right b and 0 otherwise.

If c is uniformly random, then the challenge ciphertext is also random, regardless of the multiplication and addition. Hence in this case D outputs 1 with probability at most 1/2. On the other hand, if $c = a \cdot s_{v^*} + e$, then ciphertext is $(a \cdot t + e_1, (a \cdot s_{v^*} + e) \cdot t + e_2 + [q/2] \cdot M_b)$, which is subject to the output distribution of HIBE*Enc*(v^*, pk^*, M_b). Based on the known assumption $\mathcal{A}$ can guess the right b with probability (1+ϵ)/2, that is to say, D outputs 1 with the same probability, so D has advantage at

least $\epsilon/2$. Therefore if $\mathcal{A}$ can distinguish the encryptions of the messages he chooses, then D can distinguish the two distributions $(a, a \cdot s_{v^*} + e)$ and $\{\mathrm{Unif}(R_q^t \times R_q^t)\}$, in other words, D can successfully solve R-LWE assumption.

3.4 Efficiency Analysis

We compare our proposed scheme with the HIBE scheme in [12]. The comparisons are summarized in Table 2. Let ID-vector is $v(|v|=t, 0 \le t \le l)$, as secret key $s_v \in \Lambda_{u_v}^{\perp}(A_v) \subset R_q^t$ is chosen from R_q^t at random, its size is $2^t m \log q$, and the size of public key is two times of the private key, namely $2^{t+1} m \log q$. Compared to the scheme in [12], although the size of the public key and private key size in our scheme is long, the scheme can encrypt $2^t m$ bit messages simultaneity, while the scheme in [12] can encrypt one bit message each time.

Table 2. Efficiency comparison between our scheme and the scheme in [12, 21]

Cryptosystem	Cash et al.'s scheme [12]	Scheme in [21]	Our scheme
Private key size	$tm \log q$	$\tilde{O}(n^2 d^2 l)$	$2^t m \log q$
Public key size	$n(tm+1)\log q$	$\tilde{O}(n^2 d^2 l)$	$2^{t+1} m \log q$
Message size	1	1	$2^t m$
Expansion	$(tm+1)\log q$	$2\log q$	$2\log q$
Worst-case problem	GapSVP/SIVP	LWR	ideal-SVP
Operations for encryption per bit	$(2tnm - tm + 2n)\log q$	$\tilde{O}(m)$	$\tilde{O}(m)$
Operations for decryption per bit	$2tm\log q$	$\tilde{O}(m)$	$\tilde{O}(m)$

Table 2 describes the efficiency measures and underlying problems for lattice-based cryptosystems with worst-case connections. "Expansion" is the amortized ratio of ciphertext length to plaintext length. The datum in Table 2 shows that our scheme is more efficient than the cryptosystem in [12, 21] as a whole. Especially the message size, expansion, operation for encryption per bit are incomparable to the Cash scheme. With the increase of the level t, the size of the public key and private key size will become bigger, but the message size that proposed scheme can encrypt is also becoming bigger, and the expansion is always invariable. On the other hand, with the increase of t, the message size that Cash scheme can encrypt isn't becoming bigger, though the size of the public key and private key size is also increasing. Hence the computation cost of the Cash scheme will increase with the increase of t, and the efficiency of encryption and decryption will decline. While the efficiency of our scheme is invariable in this process, just the message bits required to be computed will become large.

4 CCA-secure HIBE Encryption from R-LWE

4.1 Definition

Definition 3 ([26]). An encryption scheme is CCA-secure if the advantages of any PPT adversary $\mathcal{A}$ in the following game are negligible:

Setup : Challenger runs the algorithm $Setup(1^n)$, outputs (PK, SK), and give 1^n and PK to $\mathcal{A}$.

*Queries*1 : $\mathcal{A}$ can make some queries to the $Decry_{SK}(\cdot)$.

Challenge : After queries, $\mathcal{A}$ gives two messages M_0, M_1. A bit b is chosen from {0,1} randomly, and $\mathcal{A}$ is given the "challenge ciphertext C^*" of the message M_b.

*Queries*2 : $\mathcal{A}$ can proceed to make queries to the $Decry_{SK}(\cdot)$ except that he can't ask about the

decryption of C^*.

Output: $\mathcal{A}$ outputs a guess b'.

It is said that $\mathcal{A}$ succeeds if $b' = b$, and note the probability of success by $\Pr[Succ]$. The advantage of $\mathcal{A}$ can be defined as $Adv = |\Pr[Succ] - 1/2|$.

4.2 Encryption Scheme

Suppose $H' : \{(-q+1)/2, \cdots, -1, 0, 1, \cdots, (q-1)/2\}^* \to \{0,1\}^D$ be a random oracle that maps identities to the elements of $\{0,1\}^D$. Based on the HIBE schemes in Section 3 and the signature scheme in 2.3, a CCA-secure l level HIBE encryption scheme $\mathcal{E} = (Setup, Der, Enc, Dec)$ can be constructed as follows.

- *Setup*: Run algorithm HIBE*Setup*(1^n) to get master public key $mpk' = (A_0, l)$ and master secret key $sk'_\varepsilon = T_0$, and let (mpk', sk'_ε) be the master public key and master secret key of the scheme $\mathcal{E}$ respectively, namely $mpk = mpk', sk_\varepsilon = sk'_\varepsilon$.
- $Der(v = (v_1, \cdots, v_t) \in (\{0,1\}^D)^{t<l}, sk_v, r \in \{0,1\}^D)$: Compute $\overline{r} = 0.r = (0.r_1, \cdots, r_D)$, $\overline{v} = 0.v = (0.v_1, \cdots, 0.v_t)$, where $0.v_i = (0, v_{i_1}, \cdots, v_{i_D})$, $v_i = (v_{i_1}, \cdots, v_{i_D})$ $(1 \le i \le t)$, $r = (r_1, \cdots, r_D)$. Run algorithm HIBE*Der*$(\overline{v}, sk'_{\overline{v}} = sk_v, \overline{v}.\overline{r})$ to obtain $sk'_{\overline{v}.\overline{r}} = sk'_{\overline{v.r}} = (T'_{\overline{v.r}}, s'_{\overline{v.r}})$ associated with the ID-vector $\overline{v}.\overline{r}$, and let $sk'_{\overline{v}.\overline{r}}$ be the secret key of the present scheme $\mathcal{E}$ associated with the ID-vector $v.r$, namely $sk_{v.r} = sk'_{\overline{v}.\overline{r}}$, and the public key is $pk_{v.r} = (a, b = a \times s_{v.r} + e)$.
- $Enc(v, M)$: To encrypt a message $M \in \{0,1\}^{2^{t+1}m}$, the sender performs the following operations:

  1) Run $KeyGen(1^n)$ to obtain verification key vk and signing key sk;

  2) Let $\tilde{v} = \overline{v}.(1.H'(vk)) = (0.v_1, \cdots, 0.v_t, 1.H'(vk))$ and run HIBE*Der*$(\overline{v}, sk_v, \tilde{v})$ to obtain $s'_{\tilde{v}} = s'_{\overline{v}.(1.H'(vk))}$ and $pk_{\tilde{v}}$, then run algorithm HIBE*Enc*$(\tilde{v}, pk_{\tilde{v}}, M)$ and output the ciphertext with respect to the ID-vector $\tilde{v}$: $(c_1, c_2) = (a \cdot t + e_1, b \cdot t + e_2 + [q/2] \cdot M) \in R_q^{t+1} \times R_q^{t+1}$, where $pk_{\tilde{v}} = (a, b = a \times s'_{\tilde{v}} + e)$;

  3) Compute $(\sigma_1, \sigma_2) \leftarrow Sign(sk, (c_1, c_2)) = (Sign(sk, c_1), Sign(sk, c_2))$ and output the ciphertext $(vk, (c_1, c_2), (\sigma_1, \sigma_2))$ of the message M.
- $Dec(v, sk_v, C = (vk, (c_1, c_2), (\sigma_1, \sigma_2)))$: After receiving ciphertext $(vk, (c_1, c_2), (\sigma_1, \sigma_2))$, the receiver first checks whether $Verify(vk, (c_1, c_2), (\sigma_1, \sigma_2)) \stackrel{?}{=} 1$, if not, output $\perp$. Otherwise, runs HIBE*Der*$(\overline{v}, sk_v, \tilde{v})$ to obtain $sk'_{\tilde{v}} = sk'_{\overline{v}.(1.H'(vk))}$, then run HIBE*Dec*$(\overline{v}, sk'_{\tilde{v}}, (c_1, c_2))$ and output the message M.

Claim 3. The above HIBE scehme ε is correct.

Proof. Given public key $pk_v = (a, b = a \times s_v + e)$, signing key sk and the valid ciphertext $(vk, (c_1, c_2), (\sigma_1, \sigma_2))$ of message $M \in \{0,1\}^{2^t m}$, namely

$$Verify(vk, (c_1, c_2), (\sigma_1, \sigma_2)) = 1$$

As (c_1, c_2) is obtained by algorithm HIBE*Enc* and the scheme $\mathcal{HIBE}$ is correct, the decryption algorithm *Dec* in scheme $\mathcal{E}$ can decrypt correctly by running algorithm HIBE*Dec*. Hence the HIBE scehme $\mathcal{E}$ is correct.

4.3 Security Analysis

Claim 4. The HIBE scehme $\mathcal{E}$ is selective-ID secure against chosen-ciphertext attacks in the random oracle model, assuming that the R-LWE is hard.

Proof. Let $\mathcal{A}$ be a PPT adversary attacking $\mathcal{E}$ in a chosen-ciphertext attack, v^* be a "target" ID-vector initially output by $\mathcal{A}$, and (vk^*, C^*, σ^*) denote the challenge ciphertext received by $\mathcal{A}$ during the

experiment. Let Φ denote the event that "$\mathcal{A}$ make decryption query to $Dec_{sk_{v^*}}(\cdot)$ associated with (vk^*, C, σ), where $Verify_{vk^*}(C,\sigma)=1$", assuming vk^* is chosen at the outset of the experiment. Then the following propositions are correct.

Proposition 1. $\Pr_{\mathcal{A}}[\Phi]$ is negligible.

Proposition 2. $|\Pr_{\mathcal{A}}[Succ \wedge \bar{\Phi}] + \frac{1}{2}\Pr_{\mathcal{A}}[\Phi] - \frac{1}{2}|$ is negligible.

As

$$
\begin{aligned}
&|\Pr_{\mathcal{A}}[Succ] - 1/2| \\
=&|\Pr_{\mathcal{A}}[Succ \wedge \Phi] + \Pr_{\mathcal{A}}[Succ \wedge \bar{\Phi}] - \frac{1}{2}\Pr_{\mathcal{A}}[\Phi] + \frac{1}{2}\Pr_{\mathcal{A}}[\Phi] - \frac{1}{2}| \\
\le&|\Pr_{\mathcal{A}}[Succ \wedge \Phi] - \frac{1}{2}\Pr_{\mathcal{A}}[\Phi]| + |\Pr_{\mathcal{A}}[Succ \wedge \bar{\Phi}] + \frac{1}{2}\Pr_{\mathcal{A}}[\Phi] - \frac{1}{2}| \\
\le&\frac{1}{2}\Pr_{\mathcal{A}}[\Phi] + |\Pr_{\mathcal{A}}[Succ \wedge \bar{\Phi}] + \frac{1}{2}\Pr_{\mathcal{A}}[\Phi] - \frac{1}{2}| \quad (0 \le \Pr_{\mathcal{A}}[Succ \wedge \Phi] \le \Pr_{\mathcal{A}}[\Phi])
\end{aligned}
$$

Hence the adversary's advantage is negligible if the propositions described above are correct.

The correctness of Proposition 1 is straightforward. If $\Pr_{\mathcal{A}}[\Phi]$ is not negligible, $\mathcal{A}$ can output a valid ciphertext (vk^*, C, σ) with $Verify(C,\sigma)=1$, then the signature scheme $\mathcal{S}$ in Section 3 will be not secure. So the Proposition 1 is correct from Claim 2.

To proof the correctness of the Proposition 2, a PPT adversary $\mathcal{A}'$ attacking the scheme $\mathcal{HIBE}$ can be constructed as follows:

1. *Setup* : $\mathcal{A}'$ runs $\mathcal{A}$ and outputs a "target" ID-vector v^* ($|v^*|=t$) of $\mathcal{A}$, runs *KeyGen* to get $(vk^* \in R_q \times R_q, sk^* \in R_q)$ and output a "target" ID-vector $V^* = \overline{v}^*.(1.H'(vk^*))$ of $\mathcal{A}'$, then $\mathcal{A}'$ is given the public key PK_{vk^*}, and $\mathcal{A}'$ gives it to $\mathcal{A}$.

2. *Queries*1: When $\mathcal{A}$ issues private key extraction query for identity $r \in \mathcal{ID}$, $\mathcal{A}'$ requests the private key $sk'_{\overline{v}.\overline{r}}$ for ID-vector $\overline{v}.\overline{r}$ and return it to $\mathcal{A}$. Where $v.r$ is not a prefix of the "target" ID-vector v^*, and $\overline{v}.\overline{r}$ is not the prefix of the "target" ID-vector V^*.

3. *Queries*2: When $\mathcal{A}$ makes a decryption query $Dec(v,(vk,(c_1,c_2),(\sigma_1,\sigma_2)))$, $\mathcal{A}'$ proceeds as follows:

1) If $v = v^*$ and $vk = vk^*$, $\mathcal{A}'$ outputs $\perp$.

2) If $v \neq v^*$, or if $v = v^*$ and $vk \neq vk^*$, $\mathcal{A}'$ requests the private key $sk'_{\overline{v}.(1.H'(vk))}$, then decrypts the ciphertext $(vk,(c_1,c_2),(\sigma_1,\sigma_2))$ and returns the result to $\mathcal{A}$. Where $\overline{v}.(1.H'(vk))$ is not a prefix of V^*.

4. *Challenge* : After the queries, $\mathcal{A}$ outputs two messages M_0, M_1, and $\mathcal{A}'$ sends M_0, M_1 to challenger, A bit $b \in \{0,1\}$ is randomly chosen and $\mathcal{A}'$ is given a "challenge ciphertext" $(c_1^*, c_2^*) \leftarrow \text{HIBE}Enc(vk^*, PK_{vk^*}, M_b)$, $\mathcal{A}'$ then computes $(\sigma_1^*, \sigma_2^*) \leftarrow Sign(sk^*, (c_1^*, c_2^*))$ and returns $(vk^*, (c_1^*, c_2^*), (\sigma_1^*, \sigma_2^*))$ to $\mathcal{A}$.

5. *Queries*3: $\mathcal{A}$ may continue to make private key extraction and decryption queries, and $\mathcal{A}'$ answers them as before.

6. *Output* : $\mathcal{A}$ outputs a guess b, and $\mathcal{A}'$ outputs the same guess.

As $\mathcal{A}'$ never requests the secret key for the "target" ID-vector V^* or its prefix, $\mathcal{A}'$ is a legal PPT adversary. So $\mathcal{A}'$ provides a perfect simulation for $\mathcal{A}$. It is easy to see that:

$$|\Pr_{\mathcal{A}'}[Succ]-\frac{1}{2}| = |\Pr_{\mathcal{A}'}[\bar{\Phi}\wedge Succ]+\Pr_{\mathcal{A}'}[\Phi\wedge Succ]-\frac{1}{2}|$$

$$= |\Pr_{\mathcal{A}}[Succ\wedge\bar{\Phi}]+\Pr_{\mathcal{A}'}[Succ]\cdot\Pr_{\mathcal{A}}[\Phi]-\frac{1}{2}|$$

$$= |\Pr_{\mathcal{A}}[Succ\wedge\bar{\Phi}]+\frac{1}{2}\Pr_{\mathcal{A}}[\Phi]-\frac{1}{2}|$$

Obviously $|\Pr_{\mathcal{A}'}[Succ]-\frac{1}{2}|$ is negligible from Claim 2 in Section 3, hence Proposition 2 is correct.

4.4 Efficiency Analysis

It is easy to see that the efficiency of the scheme $\mathcal{E}$ is decided by the efficiency of the encryption scheme $\mathcal{HIBE}$ and the signature scheme. The efficiency analysis of $\mathcal{E}$ is shown in Table 3, where t is the level of the hierarchical identity-based encryption scheme $\mathcal{E}$.

Table 3. Efficiency analysis of the scheme $\mathcal{E}$

Private key size	Public key size	Message length	Expansion	Operation
$2^t m\log q$	$2^{t+1} m\log q$	$2^t m$	$2\log q$	Vector operation

5 Conclusion

Due to the flexible structure and simple implementation of lattice cryptography, based on R-LWE assumption, a CPA-secure HIBE scheme is proposed in this paper firstly, then adopting the construction paradigm of Boneh et al., we construct a HIBE scheme that is secure against adaptive chosen-ciphertext attacks based on the scheme proposed above. As the proposed schemes mainly use modular addition and modular multiplication operations in the ring of integer polynomials, especially based on the special algebraic structure of R-LWE, hence they are more efficient. Analysis also indicates the efficiency of the proposed HIBE schemes is incomparable to the HIBE schemes from LWE.

According the theoretical analysis, the proposed HIBE scheme is CCA secure even under the quantum attack environment, suiting for distributed environment with large amount of data. However, as applying the preimage sampling function, it still tends not to be efficient enough for practical applications. In future, we will focus on the optimization of the construction of the HIBE cryptosystem, the feasibility test and further simulation of the presented system in practical application, we also plan to study the more efficient other encryption systems from lattice in the standard model.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61602316) and the Science & Technology Innovation Projects of Shenzhen (ZDSYS20140430164957660).

References

[1] D. Dolev, C. Dwork, M. Naor, Non-Malleable Cryptography, SIAM J. on Computing 30(2)(2000) 391-437.

[2] M. Naor, M. Yung, Public-key cryptosystems provably-secure against chosen-ciphertext attacks, in: Proc. 22nd ACM Symp. on Theory of Computing (STOC), 1990.

[3] U. Feige, D. Lapidot, A. Shamir, Multiple non-interactive zero-knowledge proofs under general assumptions, SIAM J. on Computing 29(1)(1999) 1-28.

[4] D. Boneh, R. Canetti, S. Halevi, J. Katz, Chosen-ciphertext security from identity-based encryption, SIAM J. on Computing 36(5)(2006) 915-942.

[5] H. Meijuan, Y. Bo, Z. Yi, W. Xin, Z. Yanwei, X. Zhe, A generic construction of CCA-secure deterministic encryption, Information Processing Letters 154(2020) 105865. https://doi.org/10.1016/j.ipl.2019.105865.

[6] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, in: Proc. 29th ACM Symp. on Theory of Computing (STOC), 1997.

[7] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in: Proc. 37th ACM Symp. on Theory of Computing (STOC), 2005.

[8] C. Peikert, B. Waters, Lossy trapdoor functions and their applications, in: Proc. the 40th Annual ACM Symposium on Theory of Computing, 2008.

[9] C. Peikert, Public-key cryptosystems from the worst-case shortest vector problem, in: Proc. 41th ACM Symp. on Theory of Computing (STOC), 2009.

[10] X. Yang, L. Wu, M. Zhang, W. Zhang, Public-key encryption scheme based on R-LWE, Journal on Communications 34(2)(2013)23-30.

[11] C. Gentry, C. Peikert, V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in: Proc. 40th ACM Symp. on Theory of Computing (STOC), 2008.

[12] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert, Bonsai trees, or how to delegate a lattice basis, in: Proc. 29th Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2010.

[13] H. Jinqiu, J. Mingming, G. Yuyan, S. Wangan, Efficient identity-based multi-bit proxy re-encryption over lattice in the standard model, Journal of Information Security and Applications 47(2019) 329-334.

[14] Z. Brakerski, V. Vaikuntanathan, Efficient fully homomorphic encryption from (standard) LWE, in: Proc. the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011.

[15] K.S. Tushar, R. Mayank, K. Takeshi, Efficient private database queries using ring-LWE somewhat homomorphic encryption, Journal of Information Security and Applications 49(2019) 102406, https://doi.org/10.1016/j.jisa.2019.102406.

[16] A. Akavia, S. Goldwasser, V. Vaikuntanathan, Simultaneous hardcore bits and cryptography against memory attacks, in: Proc. 6th Theory of Cryptography Conf. (TCC), 2009.

[17] S. Agrawal, D. Boneh, X. Boyen, Efficient lattice (H) IBE in the standard model, in: Proc. 29th Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2010.

[18] V. Lyubashevsky, C. Peikert, O. Regev, On ideal lattices and learning with errors over rings, in: Proc. 29th Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2010.

[19] Z. Brakerski, V. Vaikuntanathan, Fully homomorphic encryption from ring-LWE and security for key dependent messages, Advances in Cryptology-CRYPTO'11 6841(2011) 505-524.

[20] X. Zhang, C. Xu, C. Jin, R. Xie, J. Zhao, Efficient fully homomorphic encryption from RLWE with an extension to a threshold encryption scheme, Future Generation Computer Systems 36(2014) 180-186

[21] F. Fuyang, L. Bao, L. Xianhui, L. Yamin, J. Dingding, X. Haiyang, (Deterministic) Hierarchical Identity-based Encryption from Learning with Rounding over Small Modulus, in: Proc. the 11th ACM on Asia Conference on Computer and Communications, 2016.

[22] J. Horwitz, B. Lynn, Toward hierarchical identity-based encryption, in: Proc. the Advances in Cryptology-Eurocrypt'02, 2002.

[23] T. Guneysu, V. Lyubashevsky, T. Poppelmann, Practical lattice-based cryptography: A signature scheme for embedded systems, in: E. Prouff, P. Schaumont (Eds.), Cryptographic Hardware and Embedded Systems C CHES 2012, Springer, Switzerland, 2012, pp. 530-547.

[24] J. Alwen, C. Peikert, Generating shorter bases for hard random lattices, in: Proc. 26th Int. Symp. on Theoretical Aspects of Computer Science (STACS), 2009.

[25] V. Lyubashevsky, Lattice signatures without trapdoors, in: Proc. of 31th Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2012.

[26] M. Bellare, A. Desai, D. Pointcheval, P. Rogaway, Relations among notions of security for public-key encryption schemes, in: Proc. 18th Int. Cryptology Conf. (CRYPTO), 1998.