Article

New Constructions of Identity-Based Dual Receiver Encryption from Lattices

Yuan Liu , Licheng Wang *, Xiaoying Shen and Lixiang Li

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China; yuanl_1011@163.com (Y.L.); shenxiaoying@bupt.edu.cn (X.S.); lixiang@bupt.edu.cn (L.L.)

* Correspondence: wanglc2012@126.com

Received: 7 April 2020; Accepted: 26 May 2020; Published: 28 May 2020

Abstract: Dual receiver encryption (DRE), being originally conceived at CCS 2004 as a proof technique, enables a ciphertext to be decrypted to the same plaintext by two different but dual receivers and becomes popular recently due to itself useful application potentials such secure outsourcing, trusted third party supervising, client puzzling, etc. Identity-based DRE (IB-DRE) further combines the bilateral advantages/facilities of DRE and identity-based encryption (IBE). Most previous constructions of IB-DRE are based on bilinear pairings, and thus suffers from known quantum algorithmic attacks. It is interesting to build IB-DRE schemes based on the well-known post quantum platforms, such as lattices. At ACISP 2018, Zhang et al. gave the first lattice-based construction of IB-DRE, and the main part of the public parameter in this scheme consists of $2n + 2$ matrices where n is the bit-length of arbitrary identity. In this paper, by introducing an injective map and a homomorphic computation technique due to Yamada at EUROCRYPT 2016, we propose another lattice-based construction of IB-DRE in an even efficient manner: The main part of the public parameters consists only of $2pn^{\frac{1}{p}} + 2$ matrices of the same dimensions, where $p (\geq 2)$ is a flexible constant. The larger the p and n , the more observable of our proposal. Typically, when $p = 2$ and $n = 284$ according to the suggestion given by Peikert et al., the size of public parameters in our proposal is reduced to merely 12% of Zhang et al.'s method. In addition, to lighten the pressure of key generation center, we extend our lattice-based IB-DRE scheme to hierarchical scenario. Finally, both the IB-DRE scheme and the HIB-DRE scheme are proved to be indistinguishable against adaptively chosen identity and plaintext attacks (IND-ID-CPA).

Keywords: lattice; dual receiver encryption; identity-based cryptography; learning with errors; adaptively secure

1. Introduction

With the rapid development of the internet of things, more and more user tend to encrypt their data and then outsource their data to the cloud server. These outsourced data may contain some sensitive information such as financial, medical data, national security-related data, etc. Therefore, a reliable third party or government department is required to supervise these data, and if it is necessary, the regulator can decrypt the ciphertext and view the plaintext information of these data. Dual receiver encryption (DRE) [1] allows that a ciphertext can be decrypted to the same plaintext by two independent receivers. For the above scenario, DRE is a good handy tool. It not only guarantees the encrypted transmission and storage of data, but also enables data to be supervised by a reliable third party. In addition, DRE also can form a joint program with other cryptographic scheme. In [1], Diamant et al. combined a DRE scheme with a signature scheme to achieve that a user can use a same public/secret key pair to complete the encryption and signature functions. In 2014, Chow et al. [2]

proposed a DRE-PKE joint scheme and appended some stable properties to the DRE and made it more practical in the construction of plaintext-awareness public key encryption. Furthermore, DRE also can be used to construct a client puzzles mechanism based on decryption. Design client puzzles mechanism between the clients and servers can prevent servers from suffering from resource-depletion attacks. Diament et al. pointed out in [1] that the client puzzles mechanism can be applied to secure transport protocol, e.g., TLS. The DRE cryptographic primitive can be easily construct a deniable authentication system [3]. As a special kind of PKE, DRE also face the general certificate management problem. To solve the problem of certificate management in the traditional PKE, Zhang et al. [4] gave an identity-based variant version of DRE, named identity-based dual receiver encryption (IB-DRE). In this scheme, they constructed two IB-DRE schemes based on the identity-based encryption (IBE) scheme in [5].

However, all the above (IB)-DRE schemes are based on bilinear pairing groups. Since Shor [6] proposed a polynomial time quantum algorithm in 1997 which can solve discrete logarithm problem (DLP) and prime factorization. This type of bilinear pairing groups based schemes are not secure and can not resist the quantum attack. Since then, scholars have begun to study post-quantum cryptography (PQC). Lattices-based cryptography is a research hotspot for PQC. It has the following properties: high efficiency, simplicity, parallelization and average case/worst case equivalence property. In 1997, Ajtai and Dwork [7] first constructed a public key encryption scheme by using the problem on lattices. This scheme relies on the worst-case hardness of uSVP [8], and the key and ciphertext size is too large. Until 2005, Regev [9] presented another public key encryption scheme which security based on the learning with errors (LWE) problem. He proved that a LWE-based public key encryption can resist quantum attack. Then the researchers begin to study LWE-based public key encryption scheme. Based on LWE, many public key encryption schemes have been proposed, such as LWE-based IBE schemes [10–14], LWE-based attribute-based encryption schemes [15–19]. To our knowledge, the first lattice-based IB-DRE scheme was proposed in 2018 [20] (Next we use how Zhang18 denotes it). The public parameters size in this scheme consists of $2n + 2$ matrices which lead a high storage cost and communication cost. Additionally, when some users apply for their privacy key to the key generation center (KGC) at the same time, KGC may face great system pressure. Therefore, in order to reduce the storage cost, it is meaningful to construct a lattice-based IB-DRE with short public parameters and then extend it a hierarchical scenario to reduce the stress of KGC.

OUR CONTRIBUTION. In this paper, we firstly propose a new lattice-based construction of IB-DRE scheme which can resist quantum attack. By using a homomorphic computation technique and an injective map function, comparing to the first lattice-based IB-DRE [20], we reduce the public parameters size from $2n + 2$ matrices to $2pn^{\frac{1}{p}} + 2$ matrices where n is the bit-length of arbitrary identity and $p(\geq 2)$ is a flexible constant. By choosing appropriate p and n , the pp size can be reduced by almost at least 88% compared to Zhang18. In addition, considering the hierarchical scenario, we extend it to a hierarchical IB-DRE (HIB-DRE), which is not considered in Zhang18. A HIB-DRE can reduce the stress of the key generation center (KGC). The public parameters size of the HIB-DRE is also reduced from $2dn + 2$ matrices to $2dpn^{\frac{1}{p}} + 2$ matrices where d is the maximum hierarchy depth. Finally, our lattice-based IB-DRE scheme and HIB-DRE scheme are proved to be indistinguishable against adaptively chosen identity and plaintext attacks (IND-ID-CPA) in the standard model. Additionally, to improve the encryption efficiency, our two schemes also can convert to a multi-bit encryption scheme by using the same method in [11].

2. Preliminaries

Notation. We use lowercase black italic alphabet for vectors, as in $\mathbf{u}$, uppercase black italic alphabet for matrices, as in $\mathbf{A}$. $[n]$ denotes a integer set $\{1, 2, \dots, n\}$. $\mathbb{Z}_q$ denotes an integer set of mod q residue class. $\mathbf{u} \in \mathbb{Z}_q^n$ is a n -dimension column vector. A $n \times m$ matrix is denoted by $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ where $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_m)$. $\|\mathbf{A}\|$ denotes the ℓ_2 -norm length of the longest column of $\mathbf{A}$. $\tilde{\mathbf{A}}$ denotes the Gram–Schmidt orthogonalization of the vectors $\mathbf{a}_1, \dots, \mathbf{a}_m$. We refer to $\|\tilde{\mathbf{A}}\|$ as the Gram–Schmidt norm of $\mathbf{A}$.

2.1. Integer Lattice

Definition 1 (Lattices). $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in \mathbb{R}^m$ are n linearly independent vectors, and the lattice Λ generated by the following formula:

$$\Lambda = L(\mathbf{B}) = \left\{ \sum_{i=1}^n x_i \mathbf{b}_i : x_i \in \mathbb{Z}, (i = 1, \dots, n) \right\}.$$

Note that $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n]$ is a basis of Λ , n is the rank and m is the dimension.

Definition 2 (Integer lattices). For prime q , $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and $\mathbf{u} \in \mathbb{Z}_q^n$, define:

$$\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m \text{ s.t. } \exists \mathbf{s} \in \mathbb{Z}_q^n, \mathbf{A}^\top \mathbf{s} = \mathbf{y} \pmod{q}\}.$$

$$\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m \text{ s.t. } \mathbf{A}\mathbf{y} = \mathbf{0} \pmod{q}\}.$$

$$\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m \text{ s.t. } \mathbf{A}\mathbf{y} = \mathbf{u} \pmod{q}\}.$$

2.2. Discrete Gaussians

Definition 3 (Discrete Gaussian). For a positive integer $s \in \mathbb{R}$ and a vector $\mathbf{c} \in \mathbb{R}^m$, we defined a Gaussian distribution with center $\mathbf{c}$ and variance s as follow:

$$\mathcal{D}_{\Lambda, \sigma, \mathbf{c}} = \frac{\rho_{\sigma, \mathbf{c}}(\mathbf{x})}{\rho_{\sigma, \mathbf{c}}(\Lambda)} = \frac{\rho_{\sigma, \mathbf{c}}(\mathbf{x})}{\sum_{\mathbf{x} \in \Lambda} \rho_{\sigma, \mathbf{c}}(\mathbf{x})}$$

where $\sigma > 0$ is a parameter, and $\rho_{\sigma, \mathbf{c}}(\mathbf{x}) = \exp(-\pi \frac{\|\mathbf{x} - \mathbf{c}\|^2}{\sigma^2})$.

Lemma 1 ([10]). Let $q \geq 2$, $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ with $m > n$, $\mathbf{T}_\mathbf{A} \in \mathbb{Z}_q^{m \times m}$ be a basis for $\Lambda_q^\perp(\mathbf{A})$ and $\sigma \geq \|\tilde{\mathbf{T}}_\mathbf{A}\| \omega(\sqrt{\log m})$. Then for $\mathbf{c} \in \mathbb{R}^m$ and $\mathbf{u} \in \mathbb{Z}_q^n$, we have:

- (1). $\Pr[\mathbf{e} \sim \mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}), \sigma} : \|\mathbf{e}\| > \sigma\sqrt{m}] \leq \text{negl}(n)$.
- (2). There is a probabilistic polynomial-time (PPT) algorithm $\text{SampleGaussian}(\mathbf{A}, \mathbf{T}_\mathbf{A}, \sigma, \mathbf{c})$ that outputs a vector $\mathbf{e} \in \Lambda_q^\perp(\mathbf{A})$ drawn from a distribution statistically close to $\mathcal{D}_{\Lambda, \sigma, \mathbf{c}}$.
- (3). There is a PPT algorithm $\text{SamplePre}(\mathbf{A}, \mathbf{T}_\mathbf{A}, \mathbf{u}, \mathbf{c})$ that outputs a vector $\mathbf{e} \in \Lambda_q^{\mathbf{u}}(\mathbf{A})$ sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}), \sigma}$.

2.3. Related Algorithms

For any integer q, n, m and q is a prime, there are PPT algorithms such that:

- (1). $\text{TrapGen}(q, n)$ ([21]): outputs a pair matrices $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{T}_\mathbf{A} \in \mathbb{Z}_q^{m \times m}$ where $\mathbf{T}_\mathbf{A}$ is a basis for $\Lambda_q^\perp(\mathbf{A})$ and $m \geq 3(1 + \delta)n \log q$ for some $\delta > 0$.
- (2). $\text{SampleLeft}(\mathbf{A}, \mathbf{M}_1, \mathbf{T}_\mathbf{A}, \mathbf{u}, \sigma)$ ([11]): given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{M}_1 \in \mathbb{Z}_q^{n \times m_1}$, a basis $\mathbf{T}_\mathbf{A} \in \mathbb{Z}_q^{m \times m}$ for $\Lambda_q^\perp(\mathbf{A})$, $\mathbf{u} \in \mathbb{Z}_q^n$ and a Gaussian parameter $\sigma > \|\tilde{\mathbf{T}}_\mathbf{A}\| \omega(\sqrt{\log(m + m_1)})$, outputs a vector $\mathbf{e} \in \mathbb{Z}^{m+m_1}$ and the vector $\mathbf{e}$ is not statistically distinguishable from $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{F}_1), \sigma}$ where $\mathbf{F}_1 = [\mathbf{A} | \mathbf{M}_1]$ and $\mathbf{F}_1 \cdot \mathbf{e} = \mathbf{u} \pmod{q}$.

- (3). $\text{SampleRight}(A, B, R, T_B, u, \sigma)$ ([11]): given $A \in \mathbb{Z}_q^{n \times k}$, $B \in \mathbb{Z}_q^{n \times m}$, $R \in \mathbb{Z}_q^{k \times m}$, a basis T_B for $\Lambda_q^\perp(B)$, $u \in \mathbb{Z}_q^n$ and a Gaussian parameter $\sigma > \|\widetilde{T}_B\| s_R \omega(\sqrt{\log m})$ where $s_R = \|\widetilde{R}\| < O(\sqrt{m})$, outputs a vector $e \in \mathbb{Z}^{m+k}$ and the vector e is not statistically distinguishable from $\mathcal{D}_{\Lambda_q^u(F_2), \sigma}$ where $F_1 = [A|AR+B]$ and $F_2 \cdot e = u \pmod{q}$.

Note that in our scheme, we let $B = yG$ where $y \in \mathbb{Z}_q$ and $y \neq 0$. Then taking T_G as the input basis for the lattices $\Lambda_q^\perp(G)$.

Lemma 2 ([22]). For any integer $q \geq 2, n \geq 1, w = nt, t = \lceil \log_2 q \rceil$, there is a gadget matrix $G \in \mathbb{Z}_q^{n \times w}$ such that:

1. The lattice $\Lambda_q^\perp(G)$ has a known basis T_G where $\|\widetilde{T}_G\| \leq \sqrt{5}$.
2. There is a PPT algorithm G^{-1} that takes input a vector $u \in \mathbb{Z}_q^n$ and output a vector $x = G^{-1}(u)$ where $x \in \{0, 1\}^w$ and $Gx = u$. Note that G^{-1} is a function, not a matrix.

2.4. Homomorphic Computation

The ideal of homomorphic trapdoor computation is introduced in [14].

Let p be a positive integer, it has a function $\text{Eval}: (\mathbb{Z}_q^{n \times m})^p \rightarrow \mathbb{Z}_q^{n \times m}$ which inputs p matrices $A_1, A_2, \dots, A_p$ and outputs a matrix.

$$\text{Eval}_p(A_1, A_2, \dots, A_p) = \begin{cases} A_1 & p = 1 \\ A_1 \cdot G^{-1}(\text{Eval}_{p-1}(A_2, \dots, A_p)) & p \geq 2 \end{cases}$$

Here G^{-1} is a deterministic function that has the following feature:

$$\begin{aligned} G^{-1}: \mathbb{Z}_q^{n \times m} &\rightarrow (0, 1)^{m \times m} \\ U &\rightarrow X, \text{ s.t. } GX = U \end{aligned}$$

Lemma 3 ([14]). Let $A, A_1, \dots, A_p \in \mathbb{Z}_q^{n \times m}$ and $R_1, \dots, R_p \in \mathbb{Z}^{m \times m}$, for $i \in [p]$, it has $A_i = AR_i + y_i G$. In addition, assume that $\|R_i\| \leq m$, $|y_i| \leq \delta$ and $\delta > m$, there exists TrapEval algorithm that taking $R_1, \dots, R_p, y_1, \dots, y_p$ as input and outputs a matrix R' such that $\text{Eval}_p(A_1, A_2, \dots, A_p) = AR' + y_1 \dots y_p \cdot G$ and $\|R'\| \leq mp\delta^{p-1}$.

2.5. LWE Hardness Assumption

Definition 4. Give a prime q , a positive integer n and a distribution $\bar{\Psi}_\alpha$ over $\mathbb{Z}_q$. A $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE problem instance consists of access to an unspecified challenge oracle $\mathcal{O}$, being either a truly random sampler $\mathcal{O}'_s$ or a noisy pseudo-random sampler $\mathcal{O}_s$ carrying some constant random secret key $s \in \mathbb{Z}_q^n$, whose behaviors are as follows, respectively:

$\mathcal{O}_s$: Outputs samples of the form $(w_i, v_i) = (w_i, w_i^T s + \chi_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $s \in \mathbb{Z}_q^n$ is a uniformly distributed secret key, χ_i is a noise component from $\bar{\Psi}_{\alpha_i}$, and w_i is uniform in $\mathbb{Z}_q^n$.

$\mathcal{O}'_s$: Outputs truly uniform random samples (w_i, v_i) from $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

The $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE problem allows a number of queries to the challenge oracle $\mathcal{O}$. We say an algorithm $\mathcal{A}$ decides a $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE problem if $\text{LWEAdv}[\mathcal{A}] = |\Pr[\mathcal{A}^{\mathcal{O}_s} = 1] - \Pr[\mathcal{A}^{\mathcal{O}'_s} = 1]|$ is non-negligible for a random $s \in \mathbb{Z}_q^n$.

Theorem 1 ([9]). If there exists an efficient, possibly quantum, algorithm for deciding the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE problem for $q > 2\sqrt{n}/\alpha$ then there is an efficient quantum algorithm for approximating the SIVP and GapSVP problems to within $\tilde{O}(n/\alpha)$ factors in the ℓ_2 norm, in the worst case.

Lemma 4 ([10]). Let $\mathbf{e}$ be some vector in $\mathbb{Z}^m$ and let $\mathbf{y} \xleftarrow{R} \bar{\Psi}_\alpha^m$. Then the quantity $|\mathbf{e}^\top \mathbf{y}|$ treated as an integer in $[0, q-1]$ satisfies:

$$|\mathbf{e}^\top \mathbf{y}| \leq \|\mathbf{e}\| q \alpha \omega(\sqrt{\log m}) + \|\mathbf{e}\| \sqrt{m}/2 \quad (1)$$

with all but negligible probability in m .

As a special case, Lemma 4 shows that if $x \xleftarrow{R} \bar{\Psi}_\alpha$ is treated as an integer in $[0, q-1]$ satisfies

$$|x| \leq q \alpha \omega(\sqrt{\log m}) + 1/2 \quad (2)$$

with all but negligible probability in m .

2.6. Three Basic Lemmas

Lemma 5 ([11]). For a random matrix $\mathbf{R} \in \{-1, 1\}^{k \times m}$, there is a universal constant C such that:

$$\Pr[\|\mathbf{R}\| > C\sqrt{k+m}] < e^{-(k+m)}. \quad (3)$$

Lemma 6 (Leftover Hash Lemma [11]). For $m > (n+1)\log q + \omega(\log n)$ and a prime $q > 2$. Let $\mathbf{R} \in \{-1, 1\}^{m \times k}$, $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{B} \in \mathbb{Z}_q^{n \times k}$ be uniformly random matrices. Then the distribution $(\mathbf{A}, \mathbf{AR}, \mathbf{R}^\top \mathbf{w})$ is $\text{negl}(n)$ -close to the distribution $(\mathbf{A}, \mathbf{B}, \mathbf{R}^\top \mathbf{w})$.

Lemma 7 (Smudging out Lemma [14]). Let $\mathbf{x}_0 \in \mathbb{Z}^m$ be a fixed vector and $\|\mathbf{x}_0\|_\infty \leq \delta$. $\mathbf{x} \leftarrow \{-B, B\}^m$ is a uniformly random vector. Then the two distributions $\mathbf{x}_0$ and $\mathbf{x}_0 + \mathbf{x}$ are within statistical distance $m\delta/B$.

2.7. Definitions of (H)IB-DRE and Adaptive-ID Security Model

Identity-based dual receiver encryption (IB-DRE) enables a ciphertext to be decrypted to the same plaintext by two different receivers since it embeds two independent user's identity in the encrypt phase. Considering the definition of IB-DRE in [20]. We give the following definition of IB-DRE. An IB-DRE scheme consists the following four algorithms.

- (1). $\text{Setup}(1^n) \rightarrow (pp, msk)$: on input the security parameter 1^n . This algorithm outputs the public parameters pp and master secret key msk .
- (2). $\text{KeyGen}(pp, id, msk) \rightarrow sk_{id}$: On input the public parameter pp , a user's identity id and the master secret key msk . This algorithm KeyGen outputs the secret key sk_{id} . In the scheme, we let id_1, id_2 denote the first receiver and the second receiver respectively.
- (3). $\text{Encrypt}(pp, id_1, id_2, \mu) \rightarrow c$: on input the public parameter pp , the user's identities id_1, id_2 and the message bit $\mu \in \{0, 1\}$. This algorithm outputs the ciphertext c .
- (4). $\text{Decrypt}(pp, sk_{id_i}, c) \rightarrow \mu$: on input the public parameter pp , a user's secret key $(sk_{id_i})_{i' \in \{1, 2\}}$, and the ciphertext c . This algorithm outputs a message μ .

The definition of IB-DRE can be easily extended to a hierarchical IB-DRE by following the method in [11].

Correctness. For all identities $id_{i'}$, all message μ and the ciphertext $c \leftarrow \text{Encrypt}(pp, id_1, id_2, \mu)$, we have $\Pr[\text{Decrypt}(pp, sk_{id_1}, c) = \text{Decrypt}(pp, sk_{id_2}, c) = \mu] = 1 - \text{negl}(n)$.

The definition of adaptive-ID security model is adapted from [11]. It can be described by a IND-ID-CPA game between a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$ as follows:

Setup. The challenger $\mathcal{B}$ runs the $\text{Setup}(1^n)$ algorithm to generate the public parameters pp and the master key msk , and send pp to $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ makes secret key queries for different identities adaptively.

Challenge. The adversary $\mathcal{A}$ sends a message bit $\mu^* \in \{0, 1\}$ and the target identities (id_1^*, id_2^*) to $\mathcal{B}$, and the target identities (id_1^*, id_2^*) should not be asked in **Phase 1**. The challenger $\mathcal{B}$ randomly chooses $r \in \{0, 1\}$ and a randomly ciphertext space $\mathcal{C}$. If $r = 0$, it send the challenge ciphertext $c^* = \text{Encrypt}(pp, id_1^*, id_2^*, \mu^*)$ to $\mathcal{A}$. If $r = 1$, it send a randomly challenge ciphertext $c^* \in \mathcal{C}$ to $\mathcal{A}$.

Phase 2. The adversary $\mathcal{A}$ also makes secret key queries for different identities adaptively as **Phase 1**. It can not ask for (id_1^*, id_2^*) .

Guess. The adversary $\mathcal{A}$ outputs its guess $r' \in \{0, 1\}$ and wins if $r' = r$. We define the advantage of the adversary $\mathcal{A}$ in attacking IB-DRE scheme as $\varepsilon = |\Pr[r' = r] - \frac{1}{2}|$.

3. Adaptively Secure IB-DRE Scheme with Short Public Parameters

As we all know, in the adaptively secure IBE scheme in [11], for an identity $id = (b_1, b_2, \dots, b_n) \in \{0, 1\}^n$, the key generation matrix/encryption matrix is $F_{id} = [A_0 | B_0 + \sum_{i=1}^n b_i A_i]$ where $(A_i)_{i \in [n]}$ is the matrices in the public parameters. Thus, if we want to construct an adaptively secure identity based dual receiver encryption (IB-DRE) scheme, the public parameters will be $2n + 2$ matrices which lead to high storage cost.

In this section, we propose an adaptively secure IB-DRE scheme with short public parameters. There are four algorithms in this scheme: Setup, KeyGen, Encrypt and Decrypt. The main method to reduce the public parameters is that in the Setup phase we introduce an injective map function which can map a n -bits identity to a subset of $[1, l]^p$, and here we let $l = \lceil n^{\frac{1}{p}} \rceil$. Additionally, we also introduce a homomorphic computation technique to ensure that our scheme achieves a strong secure notion, i.e., indistinguishability of ciphertext under the adaptive chosen-identity chosen-plaintext attack (IND-ID-CPA). For the key generation matrix/encryption matrix, let $\mathcal{H}(id) = B_0 + \sum_{i=1}^n b_i A_i$, then $F_{id} = [A_0 | \mathcal{H}(id)]$. In the KeyGen phase, we use the same SampleLeft algorithm in [11] to generated the two independent users' secret keys but change the way $\mathcal{H}(id)$ is generated. $\mathcal{H}(id)$ is computed by a function Eval: $(\mathbb{Z}_q^{n \times m})^p \rightarrow \mathbb{Z}_q^{n \times m}$ of the public parameters where function Eval is a part of homomorphic computation technique. When encrypting a message bit, it should use two independent receivers' public keys to encrypt the message. Then the ciphertext can be decrypted to the same message by the two independent receivers.

By doing this, we reduce the size of public parameters from $2n + 2$ (i.e., $O(n)$) matrices to $2pn^{\frac{1}{p}} + 2$ (i.e., $O(n^{\frac{1}{p}})$) matrices where p is a flexible constant and can affect the reduction cost. Next we will describe our scheme step by step.

3.1. Our Construction

The adaptively secure IB-DRE scheme with short public parameters consists the following four algorithms.

- (1). $\text{Setup}(1^n) \rightarrow (pp, msk)$: on input the security parameter 1^n . This algorithm outputs the public parameters pp and master secret key msk , do:
 - Perform algorithm TrapGen to generate a uniformly matrix $A_0 \in \mathbb{Z}_q^{n \times m}$ and a trapdoor $T_{A_0} \in \mathbb{Z}^{m \times m}$.
 - For an identity $id = (b_1, b_2, \dots, b_n) \in \{0, 1\}^n$, select an injective map $\mathcal{F}$ that maps an identity to a subset $\mathcal{F}(id)$ of $[1, l]^p$ where $l = \lceil n^{\frac{1}{p}} \rceil$.
 - For $(i, j) \in [p, l]$, select $2pl$ matrices $A_{i,j}, A'_{i,j}$.
 - Select a uniformly random matrices B_0 and a uniformly random vector $u \in \mathbb{Z}_q^n$.

The public parameter $pp = \{A_0, (A_{i,j}, A'_{i,j})_{(i,j) \in [p,l]}, B_0, u\}$, the master secret key $msk = \{T_{A_0}\}$.

Recall that by the function $\text{Eval}_p: (\mathbb{Z}_q^{n \times m})^p \rightarrow \mathbb{Z}_q^{n \times m}$, for the two identities $\mathcal{F}(\text{id}_1), \mathcal{F}(\text{id}_2)$, we have a deterministic function $\mathcal{H}$ such that

$$\mathcal{H}(\text{id}_1) = B_0 + \sum_{(j_1, j_2, \dots, j_p) \in \mathcal{F}(\text{id}_1)} \text{Eval}_p(A_{1,j_1}, A_{2,j_2}, \dots, A_{p,j_p}).$$

$$\mathcal{H}(\text{id}_2) = B_0 + \sum_{(j_1, j_2, \dots, j_p) \in \mathcal{F}(\text{id}_2)} \text{Eval}_p(A'_{1,j_1}, A'_{2,j_2}, \dots, A'_{p,j_p}).$$

- (2). $\text{KeyGen}(pp, \text{id}, msk) \rightarrow sk_{\text{id}}$: On input the public parameter pp , the user's identity id and the master secret key msk . This algorithm KeyGen outputs the secret key sk_{id} , it works as follows:

- It runs algorithm $\text{SampleLeft}(A_0, \mathcal{H}(\text{id}), u, T_{A_0})$ to generate e such that $F_{\text{id}} \cdot e = u$ where $F_{\text{id}} = [A_0 | \mathcal{H}(\text{id})]$. Then it set $sk_{\text{id}} = e \in \mathbb{Z}_q^{2m}$.
- For two independent receivers, we let e_1 and e_2 denote the first and second receiver's secret key.

The two independent receivers' secret keys are $sk_{\text{id}_1} = e_1 \in \mathbb{Z}_q^{2m}$, $sk_{\text{id}_2} = e_2 \in \mathbb{Z}_q^{2m}$.

- (3). $\text{Encrypt}(pp, \text{id}_1, \text{id}_2, \mu) \rightarrow c$: On input the public parameter pp , the user's identities id_1, id_2 and the message bit $\mu \in \{0, 1\}$. This algorithm outputs the ciphertext c . it works as follows:

- It firstly gets $\mathcal{H}(\text{id}_1)$ and $\mathcal{H}(\text{id}_2)$ as above.
- Choose a randomly uniform vector $s \in \mathbb{Z}_q^n$, and error terms $x \xleftarrow{\Psi_\alpha} \mathbb{Z}_q$, $x_{1,1}, x_{1,2}, \xleftarrow{\Psi_\alpha^m} \mathbb{Z}_q^m$, and $x_{2,1}, x_{2,2} \leftarrow \{-B, B\}^m$, compute

$$c_0 = u^\top s + x + \mu \lfloor q/2 \rfloor \in \mathbb{Z}_q.$$

$$c_1 = F_{\text{id}_1}^\top s + \begin{bmatrix} x_{1,1} \\ x_{2,1} \end{bmatrix} \in \mathbb{Z}_q^{2m}.$$

$$c_2 = F_{\text{id}_2}^\top s + \begin{bmatrix} x_{1,2} \\ x_{2,2} \end{bmatrix} \in \mathbb{Z}_q^{2m}.$$

The ciphertext is $c = \{c_0, c_1, c_2\}$.

- (4). $\text{Decrypt}(pp, sk_{\text{id}_1}/sk_{\text{id}_2}, c) \rightarrow \mu$: On input the public parameter pp , a secret key $(sk_{\text{id}_{i'}})_{i' \in \{1,2\}}$ and the ciphertext c , do:

- For $i' \in \{1, 2\}$, compute $\mu' = c_0 - e_{i'}^\top c_{i'}$.
- $\mu = 1$ if $|\mu' - \lfloor q/2 \rfloor| < \lfloor q/4 \rfloor$. Otherwise $\mu = 0$.
- Finally, it outputs the message μ .

3.2. Correctness

We firstly compute

$$\begin{aligned} \mu' &= c_0 - e_{i'}^\top c_{i'} \\ &= u^\top s + x + \mu \lfloor q/2 \rfloor - e_{i'}^\top (F_{\text{id}_{i'}}^\top s + \begin{bmatrix} x_{1,i'} \\ x_{2,i'} \end{bmatrix}) \\ &= \mu \lfloor q/2 \rfloor + x - e_{i'}^\top \begin{bmatrix} x_{1,i'} \\ x_{2,i'} \end{bmatrix} \end{aligned} \quad (4)$$

Let $\mathbf{e}_{i'} = \begin{bmatrix} (e_{i'})_1 \\ (e_{i'})_2 \end{bmatrix}$ where $(e_{i'})_1, (e_{i'})_2 \in \mathbb{Z}^m$. Based on Lemma 1 and the formulas in Equations (1) and (2), the error term

$$\begin{aligned} & \left| x - \mathbf{e}_{i'}^\top \begin{bmatrix} \mathbf{x}_{1,i'} \\ \mathbf{x}_{2,i'} \end{bmatrix} \right| \\ & \leq |x| + \left| \mathbf{e}_{i'}^\top \begin{bmatrix} \mathbf{x}_{1,i'} \\ \mathbf{x}_{2,i'} \end{bmatrix} \right| \\ & = |x| + |(\mathbf{e}_{i'})_1^\top \mathbf{x}_{1,i'}| + |(\mathbf{e}_{i'})_2^\top \mathbf{x}_{2,i'}| \\ & \leq q\alpha\omega(\sqrt{\log m}) + \frac{1}{2} + \sigma\sqrt{m}q\alpha\omega(\sqrt{\log m}) + \frac{\sigma m}{2} \\ & \quad + \sigma\sqrt{m} \cdot O(B\sqrt{m}) \\ & \leq q\alpha\sigma m\omega(\sqrt{\log m}) + O(B\sigma m) \end{aligned} \quad (5)$$

To ensure the correctness of decryption and preform the security proof, we need that:

- the error term is less than $q/5$ with overwhelming probability(w.h.p)(i.e., $\alpha < [\sigma m\omega(\sqrt{\log m})]^{-1}$, and $q = \Omega(B\sigma m)$),
- the TrapGen algorithm can operate (i.e., $m > 3(1 + \delta)n \log q$ for some $\delta > 0$),
- the Leftover Hash Lemma can be applied to security proof (i.e., $m > (n + 1) \log q + \omega(\log n)$),
- the SampleLeft and SampleRight algorithm can operate (i.e., $\sigma > \sigma_{TG} B\sqrt{m}\omega(\sqrt{\log m})$ where $\sigma_{TG} = O(\sqrt{n \log q})$),
- the Regev's LWE reduction applies (i.e., $q > 2\sqrt{n}/\alpha$) and
- the security reduction applies (i.e., $\alpha q m^{5/2}(1 + p^p n^{cp-c+1})/B \leq \frac{p}{n+1} \cdot (\frac{1}{pn^c})^{p+1}$ i.e., $B \geq \alpha q m^{5/2} p^{2p} n^{2cp+2}$).

3.3. Security

Theorem 2. If the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE assumption holds, the above IB-DRE scheme is IND-ID-CPA secure.

Proof. Let $\mathcal{A}$ be a probabilistic polynomial-time(PPT) adversary that can break our IB-DRE scheme with advantage $\varepsilon > 0$. Then there exists a reduction that solves the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE problem with an negligible advantage. Let $Q = Q(n)$ is the upper bound of the number of KeyGen queries and $I = \{(\mathbf{id}_1^*, \mathbf{id}_2^*), (\mathbf{id}_1^l, \mathbf{id}_2^l)_{j \in [Q]}\}$ where $(\mathbf{id}_1^*, \mathbf{id}_2^*)$ are the challenge IDs and $(\mathbf{id}_1^l, \mathbf{id}_2^l)_{j \in [Q]}$ are the queried IDs. Different from $Q \leq \frac{q}{2}$ in [11], here we let $Q \leq \frac{n^c}{4} - 1$ where $c = c(n)$. We show the security via the following games. In each game, we define a value $r \in \{0, 1\}$ and let W_i denote the event that the adversary correctly guesses the challenge bit, i.e., the challenger outputs $r' = r$ in **Game_i**. $|\Pr[W_i] - \frac{1}{2}|$ is the adversary's advantage.

Game₀. This is the real IND-ID-CPA game between an adversary $\mathcal{A}$ and the challenger. We have

$$|\Pr[W_0] - \frac{1}{2}| = |\Pr[r' = r] - \frac{1}{2}| = \varepsilon.$$

Game₁. This game is as same as **Game₀** except we add an abort event at the end of the game. The challenger chooses randomly $y_{i,j}, y'_{i,j} \leftarrow [1, pn^c]$ and $y_0 \leftarrow [-(n+1)(pn^c)^p, 0]$. Let $\mathbf{y} = \{y_0, (y_{i,j})_{(i,j) \in [p,l]}\}$ and $\mathbf{y}' = \{y_0, (y'_{i,j})_{(i,j) \in [p,l]}\}$. Let H and H' be two function where

$$\begin{aligned} H(\mathbf{id}_1) &= y_0 + \sum_{(j_1, j_2, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1)} y_{i,j_1} \cdots y_{i,j_p} \\ H'(\mathbf{id}_2) &= y_0 + \sum_{(j_1, j_2, \dots, j_p) \in \mathcal{F}(\mathbf{id}_2)} y'_{i,j_1} \cdots y'_{i,j_p} \end{aligned}$$

For $I = \{(\mathbf{id}_1^*, \mathbf{id}_2^*), (\mathbf{id}_1^l, \mathbf{id}_2^l)_{j \in [Q]}\}$, the challenger checks whether the following formula holds:

$$H(\mathbf{id}_1^*) = 0 \wedge H'(\mathbf{id}_2^*) = 0 \bigwedge_{j=1}^Q (H(\mathbf{id}_1^l) \neq 0 \wedge H'(\mathbf{id}_2^l) \neq 0).$$

If they do not hold, the game aborts, i.e., the challenger outputs a random $r' \in \{0, 1\}$. Otherwise, the challenger outputs $r' = r$. By Lemma 8, we have

$$|\Pr[W_1] - \frac{1}{2}| \geq \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(\varepsilon - \frac{2Q}{n^c}\right).$$

Lemma 8 ([11,14]). Let $\eta(I)$ denotes the non-abort probability, and $\eta(I) = \Pr[H(\mathbf{id}_1^*) = 0 \wedge H'(\mathbf{id}_2^*) = 0 \wedge_{j=1}^Q (H(\mathbf{id}_1^l) \neq 0 \wedge H'(\mathbf{id}_2^l) \neq 0)]$. $\eta_{\min}, \eta_{\max}$ denote the minimum and maximum probability of $\eta(I)$, respectively. Then we have $|\Pr[W_1] - \frac{1}{2}| = \eta_{\min} \cdot |\Pr[W_0] - \frac{1}{2}| - (\eta_{\max} - \eta_{\min})/2 \geq \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(\varepsilon - \frac{2Q}{n^c}\right)$.

Proof of Lemma 8. For $(Q+1)$ -tuple identities, the non-abort probability $\eta(I) = \Pr[H(\mathbf{id}_1^*) = 0 \wedge H'(\mathbf{id}_2^*) = 0 \wedge_{j=1}^Q (H(\mathbf{id}_1^l) \neq 0 \wedge H'(\mathbf{id}_2^l) \neq 0)]$. As we know, the non-abort probability is taken over $\mathbf{y} = \{y_0, (y_{i,j})_{(i,j) \in [p,l]}\}$ and $\mathbf{y}' = \{y_0, (y'_{i,j})_{(i,j) \in [p,l]}\}$ which are chose in **Game**₁. For any $y_{i,j}$ and $y'_{i,j}$, we can find a $y_0 \leftarrow [-(n+1)(pn^c)^p, 0]$ such that $\Pr[H(\mathbf{id}_1^*) = 0]$ and $\Pr[H'(\mathbf{id}_2^*) = 0]$ are

$$0 \leq \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^*)} y_{1,j_1}, \dots, y_{p,j_p} \leq \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^*)} (pn^c)^p < (n+1)(pn^c)^p, \quad (6)$$

$$0 \leq \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_2^*)} y'_{1,j_1}, \dots, y'_{p,j_p} \leq \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_2^*)} (pn^c)^p < (n+1)(pn^c)^p. \quad (7)$$

We have $\Pr[H(\mathbf{id}_1^*) = 0] = \Pr[H'(\mathbf{id}_2^*) = 0] = \frac{1}{n+1} \cdot \left(\frac{1}{pn^c}\right)^p$. Therefore, the upper bound of non-abort probability $\eta(I)$ is

$$\eta(I) \leq \Pr[H(\mathbf{id}_1^*) = 0 \wedge H'(\mathbf{id}_2^*) = 0] = \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p}. \quad (8)$$

Next we give the lower bound of non-abort probability $\eta(I)$.

$$\begin{aligned} \eta(I) &= \Pr[H(\mathbf{id}_1^*) = 0 \wedge H'(\mathbf{id}_2^*) = 0 \bigwedge_{j=1}^Q (H(\mathbf{id}_1^l) \neq 0 \wedge H'(\mathbf{id}_2^l) \neq 0)] \\ &= \Pr[H(\mathbf{id}_1^*) = 0 \bigwedge_{j=1}^Q H(\mathbf{id}_1^l) \neq 0] \cdot \Pr[H'(\mathbf{id}_2^*) = 0 \bigwedge_{j=1}^Q H'(\mathbf{id}_2^l) \neq 0]. \end{aligned} \quad (9)$$

Then we calculate the lower bound of $\Pr[H(\mathbf{id}_1^*) = 0 \wedge_{j=1}^Q H(\mathbf{id}_1^l) \neq 0]$ and $\Pr[H'(\mathbf{id}_2^*) = 0 \wedge_{j=1}^Q H'(\mathbf{id}_2^l) \neq 0]$, respectively.

$$\begin{aligned}
& \Pr[H(\mathbf{id}_1^*) = 0 \bigwedge_{j=1}^Q H(\mathbf{id}_1^j) \neq 0] \\
&= \Pr[\bigwedge_{j=1}^Q H(\mathbf{id}_1^j) \neq 0 | H(\mathbf{id}_1^*) = 0] \cdot \Pr[H(\mathbf{id}_1^*) = 0] \\
&= \left(1 - \Pr[\bigvee_{j=1}^Q H(\mathbf{id}_1^j) = 0 | H(\mathbf{id}_1^*) = 0]\right) \cdot \Pr[H(\mathbf{id}_1^*) = 0] \\
&\geq \left(1 - \sum_{j \in Q} \Pr[H(\mathbf{id}_1^j) = 0 | H(\mathbf{id}_1^*) = 0]\right) \cdot \Pr[H(\mathbf{id}_1^*) = 0] \\
&= \frac{1}{n+1} \cdot \left(\frac{1}{pn^c}\right)^p \cdot \left(1 - \sum_{j \in Q} \Pr[H(\mathbf{id}_1^j) = 0 | H(\mathbf{id}_1^*) = 0]\right) \\
&\geq \frac{1}{n+1} \cdot \left(\frac{1}{pn^c}\right)^p \cdot \left(1 - \frac{Q}{n^c}\right).
\end{aligned} \tag{10}$$

The last equation follows the fact that since $H(\mathbf{id}_1^*) = 0$, so we have $y_0 = -\sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^*)} y_{1,j_1}, \dots, y_{p,j_p}$. Then the probability of

$$\begin{aligned}
& \Pr[H(\mathbf{id}_1^j) = 0 | H(\mathbf{id}_1^*) = 0] = \Pr\left[y_0 + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^j)} y_{1,j_1}, \dots, y_{p,j_p} = 0\right] \\
&= \Pr\left[-\sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^*)} y_{1,j_1}, \dots, y_{p,j_p} + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^j)} y_{1,j_1}, \dots, y_{p,j_p} = 0\right].
\end{aligned} \tag{11}$$

Since $\mathbf{id}_1^* \neq \mathbf{id}_1^j$ and $\mathcal{F}$ is an injective function, then $\mathcal{F}(\mathbf{id}_1^j) \neq \mathcal{F}(\mathbf{id}_1^*)$, the equation $\sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^j)} y_{1,j_1}, \dots, y_{p,j_p} - \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^*)} y_{1,j_1}, \dots, y_{p,j_p}$ can be seen as a polynomial with degree p . Since $y_{i,j} \leftarrow [1, pn^c]$, the probability of

$$\Pr\left[-\sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^*)} y_{1,j_1}, \dots, y_{p,j_p} + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathbf{id}_1^j)} y_{1,j_1}, \dots, y_{p,j_p} = 0\right] \leq \frac{p}{pn^c} = \frac{1}{n^c}. \tag{12}$$

By the same method, we can get $\Pr[H'(\mathbf{id}_2^*) = 0 \bigwedge_{j=1}^Q H'(\mathbf{id}_2^j) \neq 0] = \frac{1}{n+1} \cdot \left(\frac{1}{pn^c}\right)^p \cdot \left(1 - \frac{Q}{n^c}\right)$. Finally, the non-abort probability

$$\eta(I) = \Pr[H(\mathbf{id}_1^*) = 0 \bigwedge_{j=1}^Q H(\mathbf{id}_1^j) \neq 0] \cdot \Pr[H'(\mathbf{id}_2^*) = 0 \bigwedge_{j=1}^Q H'(\mathbf{id}_2^j) \neq 0] \geq \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(1 - \frac{Q}{n^c}\right)^2. \tag{13}$$

Then we have $\eta_{\min} = \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(1 - \frac{Q}{n^c}\right)^2$, $\eta_{\max} = \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p}$. Finally,

$$\begin{aligned}
& \left|\Pr[W_1] - \frac{1}{2}\right| \geq \eta_{\min} \cdot \varepsilon - (\eta_{\max} - \eta_{\min})/2 \\
&= \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(1 - \frac{Q}{n^c}\right)^2 \cdot \varepsilon - \frac{\frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} - \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(1 - \frac{Q}{n^c}\right)^2}{2} \\
&= \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(1 - \frac{Q}{n^c}\right)^2 \cdot \varepsilon - \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \left(\frac{1}{2} - \frac{1}{2}\left(1 - \frac{Q}{n^c}\right)^2\right) \\
&\geq \frac{1}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(\varepsilon - \frac{2Q}{n^c}\right)
\end{aligned} \tag{14}$$

The last inequality due to that $\varepsilon \leq \frac{1}{2}$. $\square$

Game₂. In this game, we change the way $A_{i,j}, A'_{i,j}$ and B_0 are generated. The challenger firstly chooses $\mathbf{y} = \{y_0, (y_{i,j})_{(i,j) \in [p,l]}\}$, $\mathbf{y}' = \{y_0, (y'_{i,j})_{(i,j) \in [p,l]}\}$ as **Game₁** and then chooses three matrices $R_0, R_{i,j}, R'_{i,j} \in \{-1, 1\}^{m \times m}$. Compute

$$B_0 = A_0 R_0 + y_0 G \quad (15)$$

$$A_{i,j} = A_0 R_{i,j} + y_{i,j} G \quad (16)$$

$$A'_{i,j} = A_0 R'_{i,j} + y'_{i,j} G \quad (17)$$

Based on Lemma 6, the distribution $(A, A_0 R_0 + y_0 G, A_0 R_{i,j} + y_{i,j} G, A_0 R'_{i,j} + y'_{i,j} G)$ is $\text{negl}(n)$ -close to the distribution $(A, B_0, A_{i,j}, A'_{i,j})$. Therefore, we have

$$|\Pr[W_1] - \Pr[W_2]| = \text{negl}(n).$$

Before the next game, for any $id \in \mathcal{ID}$, we make a definition as follow. Let

$$R_{id_1} = R_0 + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(id_1)} \text{TrapEval}_p(R_{1,j_1}, \dots, R_{p,j_p}),$$

$$R_{id_2} = R_0 + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(id_2)} \text{TrapEval}_p(R'_{1,j_1}, \dots, R'_{p,j_p}).$$

Based on Lemma 3, we have

$$\begin{aligned} \|R_{id_1}\| &\leq \|R_0\| + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(id_1)} \|\text{TrapEval}_p(R_{1,j_1}, \dots, R_{p,j_p})\| \\ &\leq m + nmp(pn^c)^{p-1} = m(1 + p^p n^{cp-c+1}). \end{aligned} \quad (18)$$

$\|R_{id_2}\|$ is the same as $\|R_{id_1}\|$.

Game₃. In this game, we show that when we change the ciphertext is generated, the distributions $x_{2,i'}$ and $R_{id_{i'}}^\top x_{1,i'} + x_{2,i'}$ are within statistical distance $\alpha q m^{5/2} (1 + p^p n^{cp-c+1}) / B$ where $i' \in \{1, 2\}$.

The challenge ciphertext is generated as follows: the challenger firstly chooses $s \in \mathbb{Z}_q^n$, $x \xleftarrow{\Psi_\alpha} \mathbb{Z}_q^n$, $x_{1,1}, x_{1,2} \xleftarrow{\Psi_\alpha^m} \mathbb{Z}_q^m$, $x_{2,1}, x_{2,2} \leftarrow \{-B, B\}^m$ and computes $R_{id_1}^*, R_{id_2}^*$. The challenge ciphertext

$$c_0^* = u^\top s + x + \mu^* \lfloor q/2 \rfloor,$$

$$c_1^* = (A_0 | \mathcal{H}(id_1^*))^\top s + \begin{bmatrix} x_{1,1} \\ R_{id_1^*}^\top x_{1,1} + x_{2,1} \end{bmatrix},$$

$$c_2^* = (A_0 | \mathcal{H}(id_2^*))^\top s + \begin{bmatrix} x_{1,2} \\ R_{id_2^*}^\top x_{1,2} + x_{2,2} \end{bmatrix}.$$

$\mu^* \in \{0, 1\}$ is the message chosen by $\mathcal{A}$.

Since $x_{1,i'} \xleftarrow{\Psi_\alpha^m}$, by the formula in Equation (18) we have

$$\begin{aligned} \|R_{id_{i'}}^\top x_{1,i'}\|_\infty &\leq \|R_{id_{i'}}^\top x_{1,i'}\| \leq \|R_{id_{i'}}^\top\| \cdot \|x_{1,i'}\| \\ &\leq m(1 + p^p n^{cp-c+1}) \cdot \alpha q \sqrt{m} \\ &= \alpha q m^{3/2} (1 + p^p n^{cp-c+1}) \end{aligned} \quad (19)$$

By Lemma 7, let $x_{2,i'}$ be a fixed vector, the distributions $x_{2,i'}$ and $R_{id_{i'}}^\top x_{1,i'} + x_{2,i'}$ are within statistical distance $\alpha q m^{5/2} (1 + p^p n^{cp-c+1}) / B \leq \frac{p}{n+1} \cdot (\frac{1}{pn^c})^{p+1}$.

Game₄. In this game, we change the way A_0 is generated. The challenger chooses a random matrix $A_0 \in \mathbb{Z}_q^{n \times m}$ instead of using the TrapGen algorithm. For the secret key queries, the challenger respond by the SampleRight instead of SampleLeft. By the definition of R_{id} , we have $\mathcal{H}(id_1) = A_0 \cdot (R_{id_1} + H(id_1)G)$, $\mathcal{H}'(id_2) = A_0 \cdot (R_{id_2} + H'(id_2)G)$. If $H(id_1) = 0$ or $H'(id_2) = 0$, the challenger aborts and returns a random bit. Otherwise, it returns e_1 and e_2 to $\mathcal{A}$ where

$$e_1 \leftarrow \text{SampleRight}(A_0, G, R_{id_1}, H(id_1), u, T_G)$$

$$e_2 \leftarrow \text{SampleRight}(A_0, G, R_{id_2}, H'(id_2), u, T_G).$$

In particular, the challenger checks if the challenge identity (id_1^*, id_2^*) satisfies $H(id_1^*) = 0$ and $H'(id_2^*) = 0$. If not, the game aborts as in **Game₁**.

Since in the adversary's view, **Game₂** and **Game₄** are identical (the public parameters, abort conditions, responses to private key queries and the challenge ciphertext). The advantage of the adversary $\mathcal{A}$ is identical to **Game₂**, i.e.,

$$|\Pr[W_2] - \Pr[W_4]| = \text{negl}(n).$$

Game₅. As we know, the ciphertext space is $\mathcal{C} \in \mathbb{Z}_q \times \mathbb{Z}_q^{2m} \times \mathbb{Z}_q^{2m}$. In this game, the challenger set the ciphertext as $c^* = \{c_0, c_1^*, c_2^*\}$ which is uniformly random in $\mathbb{Z}_q \times \mathbb{Z}_q^{2m} \times \mathbb{Z}_q^{2m}$ in the challenge phase. The advantage of the adversary $\mathcal{A}$ is 0. As shown in Lemma 9, assuming $(\mathbb{Z}_q, n, \Psi_\alpha)$ -LWE holds, **Game₄** and **Game₅** are computationally indistinguishable, i.e., $|\Pr[W_4] - \Pr[W_5]| = \text{negl}(n)$. $\square$

Lemma 9. For any PPT adversary $\mathcal{A}$, there exists a challenger $\mathcal{B}$ such that

$$|\Pr[W_4] - \Pr[W_5]| \leq \text{LWE} - \text{Adv}(\mathcal{B}).$$

Proof of Lemma 9. Suppose $\mathcal{A}$ has a non-negligible advantage in distinguishing **Game₄** and **Game₅**. We use $\mathcal{A}$ to construct an LWE algorithm denoted $\mathcal{B}$.

Recall from Definition 4 that an LWE problem instance is provided as a sampling oracle $\mathcal{O}$ which is either a truly random sampler $\mathcal{O}'_s$ or a noisy pseudo-random sampler $\mathcal{O}_s$ for a secret $s \in \mathbb{Z}_q^n$. The challenger $\mathcal{B}$ uses the adversary $\mathcal{A}$ to distinguish which the sampler it is given, and proceeds as follows:

Instance. The challenger $\mathcal{B}$ requests from $\mathcal{O}$ to obtains $(m + 1)$ LWE samples that we denote as:

$$\{(w_0, v_0), (w_1, v_1), (w_2, v_2), \dots, (w_m, v_m)\} \in (\mathbb{Z}_q^n \times \mathbb{Z}_q)$$

Setup. The challenger $\mathcal{B}$ constructs the public parameters pp as follows:

- (1) Construct a matrix $A_0 \in \mathbb{Z}_q^{n \times m}$ by assembling m LWE samples such that $A_0 = (w_1, w_2, \dots, w_m)$, and let $u = w_0$.
- (2) Choose y as in **Game₁** and constructs the remainder of the public parameters as in **Game₂**.
- (3) Send the $pp = \{A_0, (A_{i,j})_{(i,j) \in [p,l]}, (A'_{i,j})_{(i,j) \in [p,l]}, B_0, u\}$ to $\mathcal{A}$.

Queries. $\mathcal{A}$ makes secret key query. The challenger $\mathcal{B}$ computes and checks if $H(id) = 0$. If it holds, it aborts. Otherwise it generate the secret key for $\mathcal{A}$ as in **Game₄**.

Challenge. $\mathcal{A}$ sends a message bit $\mu^* \in \{0, 1\}$ and the target identities (id_1^*, id_2^*) to $\mathcal{B}$. The challenger $\mathcal{B}$ constructs $v^* = (v_1, v_2, \dots, v_m)^\top$ where $v_0, v_1, \dots, v_m \in \mathbb{Z}_q$ is the LWE samples. $\mathcal{B}$ chooses $x_{2,1}, x_{2,2} \leftarrow \{-B, B\}^m$. The challenge ciphertext

$$c_0^* = v_0 + \mu^* \lfloor q/2 \rfloor$$

$$\begin{aligned} c_1^* &= \begin{bmatrix} v^* + \mathbf{0}_m \\ R_{id_1^*}^\top v^* + x_{2,1} \end{bmatrix} \\ c_2^* &= \begin{bmatrix} v^* + \mathbf{0}_m \\ R_{id_2^*}^\top v^* + x_{2,2} \end{bmatrix}. \end{aligned}$$

$\mathcal{B}$ sends the challenge ciphertext $c^* = \{c_0^*, c_1^*, c_2^*\}$ to $\mathcal{A}$.

Note that when $\mathcal{O} = \mathcal{O}_s$, the ciphertext is valid. (We just argue only when no abort happens). Since $H(id_1^*) = 0$ and $H'(id_2^*) = 0$, we have $F_{id_1^*} = [A_0 | \mathcal{H}(id_1^*)] = [A_0 | A_0 R_{id_1^*}]$ where $\mathcal{H}(id_1^*) = A_0 \cdot (R_{id_1^*} + H(id_1^*)G) = A_0 \cdot R_{id_1^*}$. The same as $F_{id_1^*}$, we have $F_{id_2^*} = [A_0 | A_0 R_{id_2^*}]$. By definition of $\mathcal{O}_s$, we know $v^* = A_0^\top s + x$. Then we have

$$c_0^* = v_0 + \mu^* \lfloor q/2 \rfloor = (u^\top s + x_0) + \mu^* \lfloor q/2 \rfloor \quad (20)$$

$$c_1^* = \begin{bmatrix} v^* + \mathbf{0}_m \\ R_{id_1^*}^\top v^* + x_{2,1} \end{bmatrix} = \begin{bmatrix} A_0^\top s + x + \mathbf{0}_m \\ R_{id_1^*}^\top (A_0^\top s + x) + x_{2,1} \end{bmatrix} = \begin{bmatrix} A_0^\top s + x + \mathbf{0}_m \\ (A_0 R_{id_1^*})^\top s + R_{id_1^*}^\top x + x_{2,1} \end{bmatrix} = F_{id_1^*}^\top s + \begin{bmatrix} x \\ R_{id_1^*}^\top x + x_{2,1} \end{bmatrix} \quad (21)$$

The same as c_1^*, c_2^* is also valid. It is also similar to the **Game**₃.

When $\mathcal{O} = \mathcal{O}'_s$, $v_0 \in \mathbb{Z}_q$ and $v^* \in \mathbb{Z}_q^m$ are all uniform. Therefore c_0^*, c_1^*, c_2^* are uniform in $\mathbb{Z}_q \times \mathbb{Z}_q^{2m} \times \mathbb{Z}_q^{2m}$ by the Lemma 6.

Guess. After being allowed to make additional secret key queries, $\mathcal{A}$ guesses if it is interacting with a **Game**₄ or **Game**₅ challenger. $\mathcal{B}$ output $\mathcal{A}$'s guess as the answer to the LWE challenge it is trying to solve. Therefore we have $\text{LWE} - \text{Adv}(\mathcal{B}) = |\Pr[W_4] - \Pr[W_5]|$. $\square$

4. Adaptively Secure Hierarchical IB-DRE Scheme with Short Public Parameter

To lighten the pressure of the KGC, hierarchical IBE (HIBE) scheme was proposed. In HIBE, the user's identity can be described by an identity tuple, and we let $\mathcal{ID}_k = (id_1, id_2, \dots, id_k)$ denote an identity at the depth k . There are many users at each depth. In this section, we use $\mathcal{ID}_{k,1}$ and $\mathcal{ID}_{k,2}$ to denote the two arbitrary receivers at the depth k in our HIB-DRE scheme.

As we all know, when convert an selectively secure HIBE scheme in [11] to an adaptively secure HIBE, for an identity $\mathcal{ID}_k = (id_1, id_2, \dots, id_k)$ at the depth k , the key generation matrix/encryption matrix would be

$$F_{\mathcal{ID}_k} = [A_0 | B_0 + \sum_{j=1}^n b_{1,j} A_{1,j} | \dots | B_0 + \sum_{j=1}^n b_{k,j} A_{k,j}] \in \mathbb{Z}_q^{n \times (k+1)m}.$$

where $(A_{i,j})_{i \in [k], j \in [n]}$ is the matrices in the public parameters.

Therefore the public parameters would be $2dn + 2$ matrices which lead to a high storage cost. d is the maximum hierarchy depth.

In this section, we construct an adaptively secure HIB-DRE scheme with short public parameters. There are also four algorithms in this scheme: Setup, KeyGen, Encrypt and Decrypt. In this scheme, we use the same injective map function and homomorphic computation technique to reduce the size of public parameters from $2dn + 2$ matrices to $2dpn^{\frac{1}{p}} + 2$ matrices. Different to the adaptively secure IB-DRE scheme in Section 3, we use the SampleBasisLeft [11] algorithm to generate the user's secret key, and SampleBasisRight algorithm for the security proof. In the KeyGen phase, it needs to input a secret key for the identity at depth $l - 1$, and then outputs a secret key for the identity at depth l .

SampleBasisLeft(M_1, M, T_{M_1}, σ): On input two matrices $M_1 \in \mathbb{Z}_q^{n \times m_1}$, $M \in \mathbb{Z}_q^{n \times m}$, a "short" basis T_{M_1} of $\Lambda_q^\perp(M_1)$ and a Gaussian parameter $\sigma \geq \|\widetilde{T_{M_1}}\| \omega(\sqrt{\log m + m_1})$. This algorithm outputs a short basis E of $\Lambda_q^\perp(F_1)$ where $F_1 = [M_1 | M]$.

SampleBasisRight($A_0, G_{id}, R, T_G, \sigma_k$): On input three matrices $A_0 \in \mathbb{Z}_q^{n \times m}$, $G_{id} \in \mathbb{Z}_q^{n \times m_1}$, $R \in \mathbb{Z}_q^{m \times m_1}$, a basis T_G of $\Lambda_q^\perp(G)$ and a Gaussian parameter $\sigma_k > \|\widetilde{T}_G\| \cdot s_R \omega(\sqrt{\log m})$ where $G_{id} = H(id)G$ and $s_R = \|\widetilde{R}\|$. This algorithm outputs a short basis E of $\Lambda_q^\perp(F_2)$ where $F_2 = [A_0 | A_0 R + G_{id}]$.

4.1. Our Construction

The adaptively secure HIB-DRE scheme with short public parameters consists the following four algorithms.

- (1). Setup($d, 1^n$) $\rightarrow$ (pp, msk): on input the maximum hierarchy depth d and the security parameter 1^n . This algorithm outputs the public parameters pp and master secret key msk , do:
 - Perform algorithm TrapGen to generate a uniformly matrix $A_0 \in \mathbb{Z}_q^{n \times m}$ and a trapdoor $T_{A_0} \in \mathbb{Z}^{m \times m}$.
 - For all identities $(\mathcal{ID}_k)_{k \in [d]} = (id_1, id_2, \dots, id_k)_{k \in [d]}$ where $id_k \in \{0, 1\}^n$, select an injective map $\mathcal{F}$ that maps an identity to a subset $\mathcal{F}(\mathcal{ID}_k)$ of $[1, l]^p$ where $l = \lceil n^{\frac{1}{p}} \rceil$.
 - For $(i, j) \in [p, l]$ and $k \in [d]$, select $2dpl$ matrices $A_{i,j}^k, \bar{A}_{i,j}^k$.
 - Select a uniformly random vector $u = (u_1, u_2, \dots, u_n)^\top \in \mathbb{Z}_q^n$ and a uniformly random matrix $B_0 \in \mathbb{Z}_q^{n \times m}$.

The public parameter $pp = \{A_0, (A_{i,j}^k, \bar{A}_{i,j}^k)_{(i,j) \in [p,l], k \in [d]}, B_0, u\}$, the master secret key $msk = \{T_{A_0}\}$.

For two arbitrary receivers $\mathcal{ID}_{k,1}, \mathcal{ID}_{k,2}$ at the depth k . Recall that by the function $\text{Eval}_p: (\mathbb{Z}_q^{n \times m})^p \rightarrow \mathbb{Z}_q^{n \times m}$, for the two identities $\mathcal{F}(\mathcal{ID}_{k,1}), \mathcal{F}(\mathcal{ID}_{k,2})$, let

$$B_{i,j}^k = \sum_{(j_1, j_2, \dots, j_p) \in \mathcal{F}(\mathcal{ID}_{k,1})} \text{Eval}_p(A_{1,j_1}^k, A_{2,j_2}^k, \dots, A_{p,j_p}^k),$$

$$\bar{B}_{i,j}^k = \sum_{(j_1, j_2, \dots, j_p) \in \mathcal{F}(\mathcal{ID}_{k,2})} \text{Eval}_p(\bar{A}_{1,j_1}^k, \bar{A}_{2,j_2}^k, \dots, \bar{A}_{p,j_p}^k).$$

Then construct

$$\mathcal{H}(\mathcal{ID}_{k,1}) = B_0 + B_{i,j}^1 | B_0 + B_{i,j}^2 | \dots | B_0 + B_{i,j}^k,$$

$$\mathcal{H}(\mathcal{ID}_{k,2}) = B_0 + \bar{B}_{i,j}^1 | B_0 + \bar{B}_{i,j}^2 | \dots | B_0 + \bar{B}_{i,j}^k.$$

Note that for $i' \in \{1, 2\}$, $F_{\mathcal{ID}_{k,i'}} = [A_0 | \mathcal{H}(\mathcal{ID}_{k,i'})] \in \mathbb{Z}_q^{n \times (k+1)m}$.

- (2). KeyGen($pp, \mathcal{ID}_{k,i'}, sk_{\mathcal{ID}_{k-1,i'}}, msk$) $\rightarrow sk_{\mathcal{ID}_{k,i'}}$: On input the public parameter pp , the user's identity $\mathcal{ID}_{k,i'}$ at depth k where $i' \in \{1, 2\}$, the secret key $sk_{\mathcal{ID}_{k-1,i'}}$ corresponding to an identity $\mathcal{ID}_{k-1,i'}$ at depth $k-1$ and the master secret key msk . This algorithm KeyGen outputs a secret key $sk_{\mathcal{ID}_{k,i'}}$ as follow:

$$E_1 \leftarrow \text{SampleBasisLeft}(F_{\mathcal{ID}_{k-1,1}}, B_0 + B_{i,j}^k, sk_{\mathcal{ID}_{k-1,1}}, \sigma_k).$$

$$E_2 \leftarrow \text{SampleBasisLeft}(F_{\mathcal{ID}_{k-1,2}}, B_0 + \bar{B}_{i,j}^k, sk_{\mathcal{ID}_{k-1,2}}, \sigma_k).$$

The secret key is $sk_{\mathcal{ID}_{k,i'}} = E_{i'}$.

- (3). Encrypt($pp, \mathcal{ID}_{k,1}, \mathcal{ID}_{k,2}, \mu$) $\rightarrow c$: On input the public parameter pp , the user's identities $\mathcal{ID}_{k,1}, \mathcal{ID}_{k,2}$ and the message bit $\mu \in \{0, 1\}$. This algorithm outputs the ciphertext c . It works as follows:

- It firstly gets $F_{\mathcal{ID}_{k,1}} = [A_0 | \mathcal{H}(\mathcal{ID}_{k,1})]$ and $F_{\mathcal{ID}_{k,2}} = [A_0 | \mathcal{H}(\mathcal{ID}_{k,2})]$ as above.

- Choose a randomly uniform vector $\mathbf{s} \in \mathbb{Z}_q^n$, and a uniformly random matrix $\mathbf{R} \leftarrow \{-1, 1\}^{m \times km}$.
- Choose error terms $x \xleftarrow{\Psi_{\alpha_k}} \mathbb{Z}_q, \mathbf{x}_{1,1}, \mathbf{x}_{1,2}, \xleftarrow{\Psi_{\alpha_k}^m} \mathbb{Z}_q^m$. Let $\mathbf{x}_{2,1} = \mathbf{R}^\top \mathbf{x}_{1,1}, \mathbf{x}_{2,2} = \mathbf{R}^\top \mathbf{x}_{1,2}$, compute

$$c_0 = \mathbf{u}^\top \mathbf{s} + x + \mu \lfloor q/2 \rfloor \in \mathbb{Z}_q.$$

$$\mathbf{c}_1 = \mathbf{F}_{\mathcal{ID}_{k,1}}^\top \mathbf{s} + \begin{bmatrix} \mathbf{x}_{1,1} \\ \mathbf{x}_{2,1} \end{bmatrix} \in \mathbb{Z}_q^{(k+1)m}.$$

$$\mathbf{c}_2 = \mathbf{F}_{\mathcal{ID}_{k,2}}^\top \mathbf{s} + \begin{bmatrix} \mathbf{x}_{1,2} \\ \mathbf{x}_{2,2} \end{bmatrix} \in \mathbb{Z}_q^{(k+1)m}.$$

The ciphertext is $\mathbf{c} = \{c_0, \mathbf{c}_1, \mathbf{c}_2\}$.

- (4). Decrypt($pp, sk_{\mathcal{ID}_{k,i'}}, \mathbf{c}$) $\rightarrow \mu$: On input the public parameter pp , a secret key $(sk_{\mathcal{ID}_{k,i'}})_{i' \in \{1,2\}}$ where $\mathcal{ID}_{k,i'}$ at depth k and the ciphertext $\mathbf{c}$, do:

- Set $\bar{\sigma}_k = \sigma_k \sqrt{(k+1)m\omega(\sqrt{\log km})}$.
- For $i' \in \{1,2\}$, set $\mathbf{e}_{\mathcal{ID}_{k,i'}} \leftarrow \text{SamplePre}(\mathbf{F}_{\mathcal{ID}_{k,i'}}, sk_{\mathcal{ID}_{k,i'}}, \mathbf{u}, \bar{\sigma}_k)$. Then $\mathbf{F}_{\mathcal{ID}_{k,i'}} \mathbf{e}_{\mathcal{ID}_{k,i'}} = \mathbf{u}$ and $\|\mathbf{e}_{\mathcal{ID}_{k,i'}}\| \leq \bar{\sigma}_k \sqrt{(k+1)m}$.
- Compute $\mu' = c_0 - \mathbf{e}_{\mathcal{ID}_{k,i'}}^\top \mathbf{c}_{i'} \in \mathbb{Z}_q$.
- $\mu = 1$ if $|\mu' - \lfloor q/2 \rfloor| < \lfloor q/4 \rfloor$. Otherwise $\mu = 0$.
- Finally, it outputs the message μ .

4.2. Correctness

We firstly compute

$$\begin{aligned} \mu' &= c_0 - \mathbf{e}_{\mathcal{ID}_{k,i'}}^\top \mathbf{c}_{i'} \\ &= \mathbf{u}^\top \mathbf{s} + x + \mu \lfloor q/2 \rfloor - \mathbf{e}_{\mathcal{ID}_{k,i'}}^\top (\mathbf{F}_{\mathcal{ID}_{k,i'}}^\top \mathbf{s} + \begin{bmatrix} \mathbf{x}_{1,i'} \\ \mathbf{x}_{2,i'} \end{bmatrix}) \\ &= \mu \lfloor q/2 \rfloor + x - \mathbf{e}_{\mathcal{ID}_{k,i'}}^\top \begin{bmatrix} \mathbf{x}_{1,i'} \\ \mathbf{x}_{2,i'} \end{bmatrix} \end{aligned} \quad (22)$$

Let $\mathbf{e}_{\mathcal{ID}_{k,i'}} = \begin{bmatrix} (\mathbf{e}_{\mathcal{ID}_{k,i'}})_1 \\ (\mathbf{e}_{\mathcal{ID}_{k,i'}})_2 \end{bmatrix}$ where $(\mathbf{e}_{\mathcal{ID}_{k,i'}})_1 \in \mathbb{Z}^m, (\mathbf{e}_{\mathcal{ID}_{k,i'}})_2 \in \mathbb{Z}^{km}$. Then we have $\|(\mathbf{e}_{\mathcal{ID}_{k,i'}})_1\| \leq \bar{\sigma}_k \sqrt{m}$ and $\|(\mathbf{e}_{\mathcal{ID}_{k,i'}})_2\| \leq \bar{\sigma}_k \sqrt{km}$ where $\bar{\sigma}_k = \sigma_k \sqrt{(k+1)m\omega(\sqrt{\log km})}$. Since $\mathbf{x}_{2,i'} = \mathbf{R}^\top \mathbf{x}_{1,i'}$, by Equation (3), $\|\mathbf{x}_{2,i'}\| = \|\mathbf{R}^\top \mathbf{x}_{1,i'}\| \leq O(\sqrt{km})$

Refer to the formulas in Equations (1) and (2), the error term

$$\begin{aligned} &|x - \mathbf{e}_{\mathcal{ID}_{k,i'}}^\top \begin{bmatrix} \mathbf{x}_{1,i'} \\ \mathbf{x}_{2,i'} \end{bmatrix}| \\ &\leq |x| + |\mathbf{e}_{\mathcal{ID}_{k,i'}}^\top \begin{bmatrix} \mathbf{x}_{1,i'} \\ \mathbf{x}_{2,i'} \end{bmatrix}| \\ &= |x| + |(\mathbf{e}_{\mathcal{ID}_{k,i'}})_1^\top \mathbf{x}_{1,i'}| + |(\mathbf{e}_{\mathcal{ID}_{k,i'}})_2^\top \mathbf{x}_{2,i'}| \\ &\leq q\alpha_k\omega(\sqrt{\log m}) + \frac{1}{2} + \bar{\sigma}_k \sqrt{m} q\alpha_k\omega(\sqrt{\log m}) + \frac{\bar{\sigma}_k m}{2} + \bar{\sigma}_k \sqrt{km} \cdot O(\sqrt{km}) \\ &\leq qk^2\alpha_k\sigma_k m\omega(\sqrt{\log m}) + O(k^{3/2}\sigma_k m^2) \end{aligned} \quad (23)$$

To ensure the correctness of decryption and preform the security proof, for all $1 \leq k \leq d$, we need that:

- the error term is less than $q/5$ with overwhelming probability (w.h.p) (i.e., $\alpha_k < [\sigma_k m \omega(\sqrt{\log m})]^{-1}$, and $q = \Omega(k^{3/2} \sigma_k m^2)$),
- the TrapGen algorithm can operate (i.e., $m > 3(1 + \delta)n \log q$ for some $\delta > 0$),
- the Leftover Hash Lemma can be applied to security proof (i.e., $m > (n + 1) \log q + \omega(\log n)$),
- the SampleBasisLeft and SampleBasisRight algorithm can operate (i.e., $\sigma_k > \sigma_{TG} \sqrt{m} \omega(\sqrt{\log m})$ where $\sigma_{TG} = O(\sqrt{n \log q})$), and
- the Regev's LWE reduction applies (i.e., $q > 2\sqrt{n}/\alpha$).

4.3. Security

Theorem 3. *If the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE assumption holds, the above HIB-DRE scheme is IND-ID-CPA secure.*

Proof. Let $\mathcal{A}$ be a probabilistic polynomial-time(PPT) adversary that can break our IB-DRE scheme with advantage $\varepsilon > 0$. Then there exists a reduction that solves the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE problem with an negligible advantage. Let $Q = Q(n)$ is the upper bound of the number of KeyGen queries and $I = \{(\mathcal{ID}_{k,1}^*, \mathcal{ID}_{k,2}^*), (\mathcal{ID}_{k,1}^l, \mathcal{ID}_{k,2}^l)_{j \in [Q]}\}$ denotes the challenge IDs. Different from $Q \leq \frac{q}{2}$ in [11], here we let $Q \leq \frac{n^c}{4} - 1$ where $c = c(n)$. We show the security via the following games. In each game, we define a value $r \in \{0, 1\}$ and let W_i denote the event that the adversary correctly guessed the challenge bit, i.e., the challenger output $r' = r$ in **Game_i**. $|\Pr[W_i] - \frac{1}{2}|$ is the adversary's advantage.

Game₀. This is the real IND-ID-CPA game between an adversary $\mathcal{A}$ and the challenger. So we have

$$|\Pr[W_0] - \frac{1}{2}| = |\Pr[r' = r] - \frac{1}{2}| = \varepsilon.$$

Game₁. The same as **Game₁** in Section 3.3, in this game we also add an abort event at the end of the game. The challenger chooses $\mathbf{y} = \{y_0, (y_{i,j}^k)_{(i,j) \in [p,l], k \in [d]}\}$ where $y_0 \leftarrow [-(n+1)(pn^c)^p, 0]$ and $y_{i,j}^k \leftarrow [1, pn^c]$. Let $h_{id_k} = y_0 + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(id_k)} y_{i,j_1}^k \cdots y_{i,j_p}^k$ and H be a function such that

$$H(\mathcal{ID}_k) = h_{id_1} | h_{id_2} | \cdots | h_{id_k}.$$

For the challenge IDs, the challenger checks whether $H(\mathcal{ID}_{k,i'}^*) = 0$ and $H(\mathcal{ID}_{k,i'}^l) \neq 0$ where $i' \in \{1, 2\}$. If they do not hold, the game aborts. Otherwise, the challenger outputs $r' = r$.

Different to the Lemma 8, the probability $\eta(I)$ satisfies

$$\frac{k}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(1 - \frac{Q}{n^c}\right)^2 \leq \eta(I) \leq \frac{k}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p}.$$

Then by $|\Pr[W_1] - \frac{1}{2}| = \eta_{\min} \cdot \varepsilon - (\eta_{\max} - \eta_{\min})/2$, we have

$$|\Pr[W_1] - \frac{1}{2}| \geq \frac{k}{(n+1)^2} \cdot \left(\frac{1}{pn^c}\right)^{2p} \cdot \left(\varepsilon - \frac{2Q}{n^c}\right)$$

Game₂. In this game, we change the way $A_{i,j}^k, \bar{A}_{i,j}^k, B_0$ are generated. The challenger firstly chooses $\mathbf{y} = \{y_0, (y_{i,j}^k)_{(i,j) \in [p,l], k \in [d]}\}$, $\mathbf{y}' = \{y_0, (\bar{y}_{i,j}^k)_{(i,j) \in [p,l], k \in [d]}\}$ as **Game₁** and chooses three matrices $R_0, R_{i,j}^k, \bar{R}_{i,j}^k \in \{-1, 1\}^{m \times m}$. Compute

$$B_0 = A_0 R_0 + y_0 G \quad (24)$$

$$A_{i,j}^k = A_0 R_{i,j}^k + y_{i,j}^k G \quad (25)$$

$$\bar{A}_{i,j}^k = A_0 \bar{R}_{i,j}^k + \bar{y}_{i,j}^k G \quad (26)$$

Based on Lemma 6, the distribution $(A, A_0 R_0 + y_0 G, A_0 R_{i,j}^k + y_{i,j}^k G, A_0 \bar{R}_{i,j}^k + \bar{y}_{i,j}^k G)$ is $\text{negl}(n)$ -close to the distribution $(A, B_0, A_{i,j}^k, \bar{A}_{i,j}^k)$. Therefore, we have

$$|\Pr[W_1] - \Pr[W_2]| = \text{negl}(n).$$

Before the next game, let

$$\begin{aligned}\hat{R}_{\mathcal{ID}_{k,1}} &= R_0 + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathcal{ID}_{k,1})} \text{TrapEval}_p(R_{1,j_1}^k, \dots, R_{p,j_p}^k), \\ \hat{R}_{\mathcal{ID}_{k,2}} &= R_0 + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathcal{ID}_{k,2})} \text{TrapEval}_p(\bar{R}_{1,j_1}^k, \dots, \bar{R}_{p,j_p}^k).\end{aligned}$$

Based on Lemma 3, we have

$$\begin{aligned}\|\hat{R}_{\mathcal{ID}_{k,1}}\| &= \|R_0 + \hat{R}_{\mathcal{ID}_{k,1}}\| \leq \|R_0\| + \sum_{(j_1, \dots, j_p) \in \mathcal{F}(\mathcal{ID}_{k,1})} \|\text{TrapEval}_p(R_{1,j_1}^k, \dots, R_{p,j_p}^k)\| \\ &\leq m + nmp(pn^c)^{p-1} = m(1 + p^p n^{cp-c+1}).\end{aligned}\quad (27)$$

$\|\hat{R}_{\mathcal{ID}_{k,2}}\|$ is the same as $\|\hat{R}_{\mathcal{ID}_{k,1}}\|$.

Then define $R_{\mathcal{ID}_{k,i'}} = \hat{R}_{\mathcal{ID}_{1,i'}} | \dots | \hat{R}_{\mathcal{ID}_{k,i'}} \in \mathbb{Z}_q^{m \times km}$ where $i' \in \{1, 2\}$. We have $\|R_{\mathcal{ID}_{k,i'}}\| \leq km(1 + p^p n^{cp-c+1})$.

Game₃. In this game, we change the way A_0 is generated. The challenger chooses a random matrix $A_0 \in \mathbb{Z}_q^{n \times m}$ instead of using the TrapGen algorithm. For the secret key queries, the challenger responds by the SampleRight instead of SampleLeft. By the definition of $R_{\mathcal{ID}_k}$, we have

$$\begin{aligned}\mathcal{H}(\mathcal{ID}_{k,1}) &= A_0 \cdot (\hat{R}_{\mathcal{ID}_{1,1}} + h_{id_{1,1}} G) | \dots | A_0 \cdot (\hat{R}_{\mathcal{ID}_{k,1}} + h_{id_{k,1}} G), \\ \mathcal{H}(\mathcal{ID}_{k,2}) &= A_0 \cdot (\hat{R}_{\mathcal{ID}_{1,2}} + h_{id_{1,2}} G) | \dots | A_0 \cdot (\hat{R}_{\mathcal{ID}_{k,2}} + h_{id_{k,2}} G).\end{aligned}$$

Therefore for $i' \in \{1, 2\}$,

$$F_{\mathcal{ID}_{k,i'}} = A_0 | \mathcal{H}(\mathcal{ID}_{k,i'}) = A_0 | A_0 (R_{\mathcal{ID}_{k,i'}} + G_{\mathcal{ID}_{k,i'}}) \quad (28)$$

where $R_{\mathcal{ID}_{k,i'}} = \hat{R}_{\mathcal{ID}_{1,i'}} | \dots | \hat{R}_{\mathcal{ID}_{k,i'}}$ and $G_{\mathcal{ID}_{k,i'}} = h_{id_{1,i'}} G | \dots | h_{id_{k,i'}} G$.

If $H(\mathcal{ID}_{k,1}) = 0$ or $H(\mathcal{ID}_{k,2}) = 0$, the challenger aborts and returns a random bit. Otherwise, it returns E_1 and E_2 to $\mathcal{A}$ where

$$E_1 \leftarrow \text{SampleBasisRight}(A_0, G_{\mathcal{ID}_{k,1}}, R_{\mathcal{ID}_{k,1}}, T_G, \sigma_k)$$

$$E_2 \leftarrow \text{SampleBasisRight}(A_0, G_{\mathcal{ID}_{k,2}}, R_{\mathcal{ID}_{k,2}}, T_G, \sigma_k)$$

In particular, the challenger checks if the challenge identity $(\mathcal{ID}_{k,1}^*, \mathcal{ID}_{k,2}^*)$ satisfies $H(\mathcal{ID}_{k,1}^*) = 0$ and $H(\mathcal{ID}_{k,2}^*) = 0$. If not, the game aborts as in **Game₁**.

Since in the adversary's view, **Game₂** and **Game₃** are identical (the public parameters, abort conditions, responses to private key queries and the challenge ciphertext). The advantage of the adversary $\mathcal{A}$ is identical to **Game₂**, i.e.,

$$|\Pr[W_2] - \Pr[W_3]| = \text{negl}(n).$$

Game₄. As we know, the ciphertext space is $\mathcal{C} \in \mathbb{Z}_q \times \mathbb{Z}_q^{(k+1)m} \times \mathbb{Z}_q^{(k+1)m}$. In this game, the challenger set the ciphertext as $c^* = \{c_0^*, c_1^*, c_2^*\}$ which is uniformly random in $\mathbb{Z}_q \times \mathbb{Z}_q^{(k+1)m} \times \mathbb{Z}_q^{(k+1)m}$ in the challenge phase. And the advantage of the adversary $\mathcal{A}$ is 0. As shown in Lemma

10, assuming $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$ -LWE holds, **Game**₃ and **Game**₄ are computationally indistinguishable, i.e., $|\Pr[W_3] - \Pr[W_4]| = \text{negl}(n)$. $\square$

Lemma 10. For any PPT adversary $\mathcal{A}$, there exists a challenger $\mathcal{B}$ such that

$$|\Pr[W_3] - \Pr[W_4]| \leq \text{LWE} - \text{Adv}(\mathcal{B}).$$

Proof of Lemma 10. Suppose $\mathcal{A}$ has a non-negligible advantage in distinguishing **Game**₄ and **Game**₅. We use $\mathcal{A}$ to construct an LWE algorithm denoted $\mathcal{B}$.

Recall from Definition 4 that an LWE problem instance is provided as a sampling oracle $\mathcal{O}$ which is either a truly random sampler $\mathcal{O}'_s$ or a noisy pseudo-random sampler $\mathcal{O}_s$ for a secret $s \in \mathbb{Z}_q^n$. The challenger $\mathcal{B}$ uses the adversary $\mathcal{A}$ to distinguish which the sampler it is given, and proceeds as follows:

Instance. The challenger $\mathcal{B}$ requests from $\mathcal{O}$ to obtain $(m + 1)$ LWE samples that we denote as:

$$\{(w_0, v_0), (w_1, v_1), (w_2, v_2), \dots, (w_m, v_m)\} \in (\mathbb{Z}_q^n \times \mathbb{Z}_q)$$

Setup. The challenger $\mathcal{B}$ constructs the public parameters pp as follows:

- (1) Construct a matrix $A_0 \in \mathbb{Z}_q^{n \times m}$ by assembling m LWE samples such that $A_0 = (w_1, w_2, \dots, w_m)$, and let $u = w_0$.
- (2) Choose y as in **Game**₁ and constructs the remainder of the public parameters as in **Game**₂.
- (3) Send the $pp = \{A_0, (A_{i,j}^k, \bar{A}_{i,j}^k)_{(i,j) \in [p,l], k \in [d]}, B_0, u\}$ to $\mathcal{A}$.

Queries. $\mathcal{A}$ makes secret key query. The challenger $\mathcal{B}$ computes and checks if $H(\mathcal{ID}_k) = 0$. If it holds, it aborts. Otherwise it generate the secret key for $\mathcal{A}$ as in **Game**₃.

Challenge. $\mathcal{A}$ sends a message bit $\mu^* \in \{0, 1\}$ and the target identities $((\mathcal{ID}_{k,1}^*, \mathcal{ID}_{k,2}^*))$ to $\mathcal{B}$. The challenger $\mathcal{B}$ constructs $v^* = (v_1, v_2, \dots, v_m)^\top$ where $v_0, v_1, \dots, v_m \in \mathbb{Z}_q$ is the LWE samples. Let $R_{\mathcal{ID}_{k,1}^*} = \hat{R}_{\mathcal{ID}_{1,1}^*} | \dots | \hat{R}_{\mathcal{ID}_{k,1}^*} \in \mathbb{Z}_q^{m \times km}$ and $R_{\mathcal{ID}_{k,2}^*} = \hat{R}_{\mathcal{ID}_{1,2}^*} | \dots | \hat{R}_{\mathcal{ID}_{k,2}^*} \in \mathbb{Z}_q^{m \times km}$. Then the challenge ciphertext

$$\begin{aligned} c_0^* &= v_0 + \mu^* \lfloor q/2 \rfloor, \\ c_1^* &= \begin{bmatrix} v^* \\ R_{\mathcal{ID}_{k,1}^*}^\top v^* \end{bmatrix}, \\ c_2^* &= \begin{bmatrix} v^* \\ R_{\mathcal{ID}_{k,2}^*}^\top v^* \end{bmatrix}. \end{aligned}$$

$\mathcal{B}$ sends the challenge ciphertext $c^* = \{c_0^*, c_1^*, c_2^*\}$ to $\mathcal{A}$.

Note that when $\mathcal{O} = \mathcal{O}_s$, the ciphertext is valid. (We just argue only when no abort happens). Since $H(\mathcal{ID}_{k,1}^*) = 0$ and $H(\mathcal{ID}_{k,2}^*) = 0$, we have $F_{\mathcal{ID}_{k,1}^*} = A_0 | \mathcal{H}(\mathcal{ID}_{k,1}^*) = A_0 | A_0 R_{\mathcal{ID}_{k,1}^*}$. The same as $F_{\mathcal{ID}_{k,1}^*}$, we have $F_{\mathcal{ID}_{k,2}^*} = A_0 | A_0 R_{\mathcal{ID}_{k,2}^*}$. By definition of $\mathcal{O}_s$, we know $v^* = A_0^\top s + x$. Then we have

$$c_0^* = v_0 + \mu^* \lfloor q/2 \rfloor = (u^\top s + x_0) + \mu^* \lfloor q/2 \rfloor \quad (29)$$

$$\begin{aligned} c_1^* &= \begin{bmatrix} v^* \\ R_{\mathcal{ID}_{k,1}^*}^\top v^* \end{bmatrix} = \begin{bmatrix} A_0^\top s + x \\ R_{\mathcal{ID}_{k,1}^*}^\top (A_0^\top s + x) \end{bmatrix} \\ &= \begin{bmatrix} A_0^\top s + x \\ [A_0 R_{\mathcal{ID}_{k,1}^*}]^\top s + R_{\mathcal{ID}_{k,1}^*}^\top x \end{bmatrix} = F_{\mathcal{ID}_{k,1}^*}^\top s + \begin{bmatrix} x \\ R_{\mathcal{ID}_{k,1}^*}^\top x \end{bmatrix} \end{aligned} \quad (30)$$

The same as c_1^*, c_2^* is also valid. It is also similar to the **Game**₃.

When $\mathcal{O} = \mathcal{O}'_s$, $v_0 \in \mathbb{Z}_q$ and $v^* \in \mathbb{Z}_q^m$ are all uniform. Therefore c_0^*, c_1^*, c_2^* are uniform in $\mathbb{Z}_q \times \mathbb{Z}_q^{(k+1)m} \times \mathbb{Z}_q^{(k+1)m}$ by the Lemma 6.

Guess. After being allowed to make additional secret key queries, $\mathcal{A}$ guesses if it is interacting with a **Game₄** or **Game₅** challenger. $\mathcal{B}$ output $\mathcal{A}$'s guess as the answer to the LWE challenge it is trying to solve. Therefore we have $\text{LWE} - \text{Adv}(\mathcal{B}) = |\Pr[W_3] - \Pr[W_4]|$. $\square$

Remark 1. Note that, as in [10,11], the two schemes also can encrypt multiple message bits. To encrypt n -bits message we need to include n vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ in the public parameters pp . Let $\mathbf{U} = (\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n)$ and replace the vector $\mathbf{u}$ with $\mathbf{U}$. Then taking each element of $\mathbf{U}$ as input in the KeyGen phase in the IB-DRE scheme or the Decrypt phase in the HIB-DRE scheme such that $\mathbf{e}_{\text{id}_{i'}} \leftarrow \text{SampleLeft}(\mathbf{A}_0, \mathcal{H}(\text{id}_{i'}), \mathbf{u}_i, \mathbf{T}_{\mathbf{A}_0}), \mathbf{e}_{\text{ID}_{k,i'}} \leftarrow \text{SamplePre}(\mathbf{F}_{\text{ID}_{k,i'}}, \text{sk}_{\text{ID}_{k,i'}}, \mathbf{u}_i, \bar{\sigma}_k)$. Moreover, replace the ciphertext c_0 with $c_0 = \mathbf{U}^\top \mathbf{s} + x + \mu \lfloor q/2 \rfloor \in \mathbb{Z}_q^n$. The proof of security is basically unchanged, except that in the **Instance** phase $\mathcal{B}$ makes $m + n$ times queries of the LWE oracle instead of $m + 1$ times.

5. Performance Analysis

Here we firstly give the comparison between lattice-based IB-DRE scheme and other related IB-DRE schemes which are based on bilinear maps. As shown in Table 1, compared to [4], our scheme and [20] can resist quantum attack due to the fact that our scheme and [20] are based on the LWE problem on lattices which is proved by Regev [9] to resist quantum computing attack, but [4] is based on the decisional bilinear Diffie–Hellman (DBDH) problem which can not resist quantum computing attack. In addition, [4,20] and our scheme are all proved to be CPA secure. To lighten the pressure of KGC, we extend our scheme to the hierarchical scenario, but [4,20] can not support hierarchical scenario.

Table 1. The comparison between lattice-based identity-based device receiver encryption (IB-DRE) and bilinear maps-based IB-DRE.

Scheme	Security Assumption	Resistance to Quantum Attack	CPA/CCA	Hierarchical
[4]	DBDH	No	CPA	No
[20]	LWE	Yes	CPA	No
Ours	LWE	Yes	CPA	Yes

Next we give the comparison of storage cost, communication cost and computational cost between our construction and the first lattice-based IB-DRE scheme (next we use how Zhang18 denotes it).

Storage costs analysis. Here we give the comparison of storage costs between our construction and the first lattice-based IB-DRE scheme (next we use how Zhang18 denotes it). In Zhang18, the authors propose an adaptively secure IB-DRE scheme based on the LWE problem. In their scheme, to achieve the adaptively-ID secure, they generate $2n$ matrices in the Setup phase by using the same method of [11]. The size of public parameters is $O(n^3 \log q)$ which lead to a high storage overhead. As shown in Table 2, the suggested lattice dimension m in our scheme is smaller than [20] under the same adaptively secure model. Since p is a flexible constant which can directly affect the pp size, we give the comparison results when p takes different values. Since we introduce an injective map function in our construction, the public parameters size can be reduced from $2n + 2$ matrices to $2pn^{\frac{1}{p}} + 2$ matrices where $p (\geq 2)$ is a flexible constant. Namely, the storage cost of public parameters pp is reduced from $O(n^3 \log q)$ to $O(n^{2+\frac{1}{p}} \log q)$. Moreover, the user's secret key in our scheme is smaller than [20] and the ciphertext is equal to [20]. Figure 1 shows that when $p = 2$ and $n = 284$ according to the suggestion given by Micciancio et al. in [22], the size of public parameters in our scheme is reduced by merely 88% of Zhang et al.'s method. Not to mention when $p > 2$ or $n > 284$. In addition, from the Figure 1, with the increasing of the bit-length of identity, the size of public parameters in our scheme and [20] are also increase. It is still smaller than [20]. In addition, in our scheme, when $p = 2$, the size of the public parameters in our scheme achieves the largest of our scheme, and it is 12% of [20]. Not to mention when $p > 2$.

Table 2. The comparison between our scheme and related lattice-based scheme.

Schemes	Lattice Dimension m	pp	sk_{id}	Ciphertext	$1/\alpha$ for LWE Assumption	Selective/adaptive
Zhang18 [20]	$6n \log q$	$O(n^3 \log q)$	$2mn \log q$	$O(n^3 \log q)$	Fixed $\text{poly}(n)$	Adaptive
Ours IB-DRE	$3n \log q$	$O(n^{2+\frac{1}{p}} \log q)$ $p(\geq 2)$	$2m \log q$	$O(n^3 \log q)$	All $\text{poly}(n)$	Adaptive

Fixed $\text{poly}(n)$: a scheme is proven secure under the LWE assumption with $1/\alpha$ being some fixed polynomial (e.g., n^3).
 All $\text{poly}(n)$: a scheme is proven secure under the LWE assumption with $1/\alpha$ being all polynomial.

Figure 1. The number of the matrices in public parameters.

Communication costs analysis. There are four algorithms in our scheme and in Zhang18 [20]. During the operation of the algorithm, three transmissions of public parameters, two transmissions of ciphertext and at least two transmissions of user's secret key are required. According to the comparison results of Table 2 and Figure 1, under the same transmission bandwidth, it is obvious that communication costs of our public parameters and user's secret key are faster than in Zhang18 [20]. Communication cost of the ciphertext is equal to Zhang18 [20].

Computational costs analysis. As shown in Table 3, we compared our scheme with Zhang18 on computational costs. The computational cost of encryption in our construction is equal to the related lattice-based IB-DRE scheme in [20]. As for the computational cost of KeyGen, in [20] the user's secret key is a $2m \times n$ matrix while it is a $2m$ dimensions vector in our scheme. Thus, the computational cost of KeyGen in [20] is larger than our scheme. Due to the fact that the size of user's secret in [20] is n times larger than us, the computational cost is also larger than us.

Table 3. The comparison of computational cost.

Scheme	KeyGen	Encryption	Decryption
Zhang18 [20]	$O(n^2 m^2)$	$O(n^2 m)$	$O(n m^2)$
Ours	$O(n m^2)$	$O(n^2 m)$	$O(m^2)$

6. Conclusions

Different from the standard cryptographic primitive of public key encryption by which a ciphertext can usually be decrypted by the private-key holders only, dual receiver encryption enables a ciphertext to be decrypted to the same plaintext by two different but dual receivers. In this paper, we propose two more efficient constructions of (hierarchical) identity-based dual receiver encryption schemes from lattices which can resist quantum attack. By combining an injective map and a homomorphic computation technique, the size of public parameters is remarkably reduced from $2n + 2$ matrices to $2pn^{\frac{1}{p}} + 2$ matrices where $p(\geq 2)$ is a flexible constant. Compared to the only related work—Zhang18, about 88% = (1–12%) storage cost is saved by using our method. Under the

intractability assumption of the learning with errors problem over lattices, our proposal was proved to be semantically secure against adaptively chosen identity and plaintext attacks.

Author Contributions: Conceptualization, X.S. and L.L.; investigation, L.L.; formal analysis and scheme design, Y.L. and X.S.; secure proof and performance analysis, Y.L. and L.W.; methodology, Y.L. and L.W.; writing—original draft preparation, Y.L.; writing—review and editing, X.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Shandong Provincial Key Research and Development Program of China (2018CXGC0701), the National Natural Science Foundation of China (NSFC) (No. 61972050), and the BUPT Excellent Ph.D. Students Foundation (Grant Nos. CX2019119 and CX2019233).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Diament, T.; Lee, H.K.; Keromytis, A.D.; Yung, M. The dual receiver cryptosystem and its applications. In Proceedings of the 11th ACM Conference on Computer and Communications Security 2004 (CCS'04), Washington, DC, USA, 25–29 October 2004; pp. 330–343.
2. Chow, S.S.M.; Franklin, M.; Zhang, H. Practical dual-receiver encryption. In Proceedings of the Cryptographers' Track at the RSA Conference (CT-RSA'14), San Francisco, CA, USA, 25–28 February 2014; pp. 85–105.
3. Dodis, Y.; Katz, J.; Smith, A.; Walfish, S. Composability and on-line deniability of authentication. In Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography 2009 (TCC'09), San Francisco, CA, USA, 15–17 March 2009; pp. 146–162.
4. Zhang, K.; Chen, W.; Li, X.; Chen, J.; Qian, H.F. New application of partitioning methodology: Identity-based dual receiver encryption. *Secur. Commun. Netw.* **2016**, *9*, 5789–5802. [[CrossRef](#)]
5. Waters, B. Efficient identity-based encryption without random oracles. In Proceedings of the Advances in Cryptology-Eurocrypt 2005, Aarhus, Denmark, 22–26 May 2005; pp. 114–127.
6. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [[CrossRef](#)]
7. Ajtai, M.; Dwork, C. A public-key cryptosystem with worst-case/average-case equivalence. In Proceedings of the 29th Annual ACM Symposium on Theory of Computing (STOC'97), El Paso, TX, USA, 9–11 May 1997; pp. 284–293.
8. Ajtai, M. Generating hard instances of lattice problems. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC'96), Philadelphia, PA, USA, 21–23 May 1996; pp. 99–108.
9. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. In Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC'05), Baltimore, MD, USA, 22–24 May 2005; pp. 84–93.
10. Gentry, C.; Peikert, C.; Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. In Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC'08), Victoria, BC, Canada, 17–20 May 2008; pp. 197–206.
11. Agrawal, S.; Boneh, D.; Boyen, X. Efficient lattice (H)IBE in the standard model. In Proceedings of the Advances in Cryptology-Eurocrypt'10, French Riviera, France, 30 May–3 June 2010; pp. 553–572.
12. Agrawal, S.; Boneh, D.; Boyen, X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In Proceedings of the Advances in Cryptology-Crypto'10, Santa Barbara, CA, USA, 15–19 August 2010; pp. 98–115.
13. Singh, K.; Pandurangan, C.; Banerjee, A.K. Adaptively secure efficient lattice (H)IBE in standard model with short public parameters. In Proceedings of the Second International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE'12), Chennai, India, 3–4 November 2012; pp. 153–172.
14. Yamada, S. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In Proceedings of the Advances in Cryptology-Eurocrypt'16, Vienna, Austria, 8–12 May 2016; pp. 32–62.
15. Agrawal, S.; Boyen, X.; Vaikuntanathan, V.; Voulgaris, P. Functional encryption for threshold functions (or Fuzzy IBE) from lattices. In Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography (PKC'12), Darmstadt, Germany, 18–20 May 2012; pp. 280–297.

16. Boyen, X. Attribute-based functional encryption on lattices. In Proceedings of the 10th Theory of Cryptography Conference (TCC'13), Tokyo, Japan, 3–6 March 2013; pp. 122–142.
17. Gorbunov, S.; Vaikuntanathan, V.; Wee, H. Attribute-based encryption for circuits. In Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC'13), Palo Alto, CA, USA, 1–4 June 2013; pp. 545–554.
18. Boneh, D.; Gentry, C.; Gorbunov, S.; Halevi, S. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuit. In Proceedings of the Advances in Cryptology-Eurocrypt'14, Copenhagen, Denmark, 11–15 May 2014; pp. 533–556.
19. Liu, Y.; Wang, L.; Li, L.; Yan, X. Security and efficient multi-authority attribute-based encryption scheme from lattices. *IEEE Access* **2019**, *7*, 3665–3674. [[CrossRef](#)]
20. Zhang, D.; Zhang, K.; Li, B.; Lu, X.; Xue, H.; Li, J. Lattice-based dual receiver encryption and more. In *ACISP2018: Information Security and Privacy*; Springer: Cham, Switzerland, 2018; pp. 520–538.
21. Alwen, J.; Peikert, C. Generating shorter bases for hard random lattices. In proceedings of the 26th Symposium on Theoretical Aspects of Computer Science (STACS'09), Freiburg, Germany, 26–28 February 2009; pp. 75–86.
22. Micciancio, D.; Peikert, C. Trapdoors for lattices: Simpler, tighter, faster, smaller. In proceedings of the Advances in Cryptology-Eurocrypt'12, Cambridge, UK, 15–19 April 2012; pp. 700–718.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).