Lattice-Based Dual Receiver Encryption and More

Daode Zhang[1,2], Kai Zhang[3,(✉)], Bao Li[1,2], Xianhui Lu[1,2], Haiyang Xue[1,2], and Jie Li [1,2]

1 School of Cyber Security, University of Chinese Academy of Sciences.
2 Data Assurances and Communications Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China.
3 Department of Information Security, Shanghai University of Electric Power, Shanghai, China.
zhangdaode@iie.ac.cn, kzhang@shiep.edu.cn, {libao, luxianhui, xuehaiyang,lijie}@iie.ac.cn

Abstract. Dual receiver encryption (DRE), proposed by Diament et al. at ACM CCS 2004, is a special extension notion of public-key encryption, which enables two independent receivers to decrypt a ciphertext into a same plaintext. This primitive is quite useful in designing combined public key cryptosystems and denial of service attack-resilient protocols. Up till now, a series of DRE schemes are constructed from bilinear pairing groups and lattices. In this work, we introduce a construction of lattice-based DRE. Our scheme is indistinguishable against chosen-ciphertext attacks (IND-CCA) from the standard Learning with Errors (LWE) assumption with a public key of bit-size about $2nm \log q$, where m and q are small polynomials in n. Additionally, for the DRE notion in the identity-based setting, identity-based DRE (IB-DRE), we also give a lattice-based IB-DRE scheme that achieves chosen-plaintext and adaptively chosen identity security based on the LWE assumption with public parameter size about $(2\ell + 1)nm \log q$, where ℓ is the bit-size of the identity in the scheme.

Keywords: Lattices, Dual Receiver Encryption, Identity-Based Dual Receiver Encryption, Learning with Errors, Provable Security.

1 Introduction

The notion of dual receiver encryption (DRE), formlized by Diament, Lee, Keromytis and Yung [8] at ACM CCS 2004, is an extension version of public key encryption, in which a ciphertext can be decrypted into the same plaintext by two independent users. More precisely, in a DRE scheme, the encryption algorithm takes as input a message M and two receivers' independently generated public keys pk_1 and pk_2 and produces a ciphertext c. Once the receivers receive the ciphertext c, either of them can decrypt c and obtain the message M using their respective secret key. With such a DRE primitive, one can obtain a combined public key cryptosystem or design a denial of service attack-resilient protocol [8]. A decade later, in CT-RSA 2014, Chow, Franklin, and

Zhang [6] refined the syntax of DRE and appended some appealing features for DRE. Recently, to simplify the difficulty of certificate management in traditional certificate-based DRE schemes, Zhang et al. [24] extended the DRE concept into the identity-based setting by introducing the identity-based dual receiver encryption (IB-DRE) notion.

There exist many DRE and IB-DRE constructions from pairings and lattices, which are described as follows.

- **From pairings.** In [8], Diament et al. presented the first DRE scheme by transforming the three-party one-round Diffie-Hellman key exchange scheme by Joux [12], and also proved that it is indistinguishable secure against chosen ciphertext attacks (IND-CCA). However, their scheme relied on the existence of random oracle heuristic (RO), where a DRE that proven to be secure in the RO model may turn into insecure one when the RO is instantiated by an actual hash function in practice. Hence, Youn and Smith [23] began with attempting to give a provably secure DRE scheme in the standard model by combining an adaptively CCA secure encryption scheme and a non-interactive zero-knowledge protocol, while suffered low efficiency due to the prohibitively huge proof size. Later on, Chow, Franklin, and Zhang [6] proposed a CCA secure DRE scheme via combining a selective-tag weakly CCA-secure tag-based DRE (based on the tag-based encryption scheme in [14]) and a strong one-time signature scheme, as well as other DRE instantiations for non-malleable and other properties [1]. Recently, Zhang et al. [24] constructed two provably secure IB-DRE schemes against adaptively chosen plaintext or ciphertext and chosen identity attacks based on an identity-based encryption scheme in [22].
- **From lattices.** As studied in [6, 24], the DRE or IB-DRE can be viewed as a special instance of a broadcast encryption (BE, for short) or identity-based broadcast encryption (IBBE, for short) primitive which supports multiple recipients in an encryption system. So a construction of BE or IBBE implies a construction of DRE or IB-DRE. Georgescu [10] constructed a tag-based anonymous hint system [15] under the ring learning with errors (RLWE) assumption. Combining an IND-CCA secure public key encryption (PKE) scheme and a strongly unforgeable one-time signature (OTS), we can get an IND-CCA secure BE scheme which is a conclusion in [15]. Wang et al. [20] presented a construction of BE which is indistinguishable against adaptively chosen plaintext attacks (IND-CPA), based on the LWE problem. As for IBBE constructions, Wang and Bi [21] proposed an adaptively secure IBBE scheme in the random oracle model (ROM), under the LWE assumption.

[1] Note that Chow, Franklin, and Zhang [6] also gave two generic DRE constructions: one is combining Naor-Yung "two-key" paradigm [16] with Groth-Sahai proof system [11], the other is from lossy trapdoor functions [17].

Fig. 1. Comparison of DRE Schemes from Lattices.

Schemes	# of $\mathbb{Z}_q^{n\times m}$ matrix |pk|	# of $\mathbb{Z}_q^{m\times m}$ matrix |sk|	# of $\mathbb{Z}_q^{m}$ vector |c|	Assumptions	Security	Other primitives needed
Geo′13† [10]	–	–	–	RLWE	IND-CCA	PKE, OTS
WWW'15 [20]	1	1	1	LWE	IND-CPA	
Ours:						
Section 3	1	1	2	LWE	IND-CCA	OTS

|pk|,|sk| and |c| show the size of public key, secret key and ciphertext, respectively.
†, Because of the usage of an IND-CCA secure PKE scheme from lattices, we do not konw how to show the detail of |pk|, |sk| and |c| about Geo'13 scheme.

Fig. 2. Comparison of IB-DRE Schemes from Lattices.

Schemes	# of $\mathbb{Z}_q^{n\times m}$ matrix |PP|	# of $\mathbb{Z}_q^{m\times m}$ matrix |Msk|	# of $\mathbb{Z}_q^{m}$ vector |c|	Assumptions	Security	Standard model ?
WB'10 [21]	1	1	3	LWE	IND-ID-CPA	ROM
Ours:						
Section 4	$2n+1$	1	3	LWE	IND-ID-CPA	✓
Section 4.3	$2n/\log n+1$	1	3	LWE	IND-ID-CPA	✓
Section 4.3	$2n/\log^2 n+1$	1	3	LWE	IND-ID-CPA	✓

|PP|,|Msk| and |c| show the size of public parameters, master secret key and ciphertext, respectively.

1.1 Our Contributions

In this paper, we pay attention to the construction of DRE and IB-DRE from lattices. Our two schemes are constructed in the standard model and satisfy chosen-ciphertext or chosen-plaintext security, which are based on the hardness of the Learning With Errors (LWE) problem. Specifically, based on the beautiful work of Agrawal, Boneh and Boyen [1], our works are stated as follows.

- We construct a secure DRE scheme against chosen-ciphertext attacks from the standard Learning with Errors assumption with a public key of bit-size about $2nm\log q$, where m and q are small polynomials in n. In order to encrypt a n-bit message, the ciphertext consists of two parts: one is a $(n+4m)\log q$-bit ciphertext which is an encryption of the message, the other is a one-time signature of the first part. Please see more details in Figure 1.
- Additionally, we construct a secure IB-DRE scheme against chosen-plaintext and adaptively chosen-identity attacks from the same assumption . As a result, the public parameter of our IB-DRE achieves $(2\ell+1)nm\log q$ bit-size, where ℓ is the bit-size of the identity. In order to encrypt a n-bit message, the bit-size of ciphertext will become $(n+3m)\log q$. Note that one can still

get two IB-DRE schemes with more compact public parameters via relying on other lattice-based IBE works that achieved short public parameter sizes, which is formally discussed in Section 4.3. We also present the comparison of IB-DRE schemes from lattices in Figure 2.

Remarks. This work has been accepted at the conference of ACISP'2018.

Organization. The rest of this paper is organized as follows. In Appendix A and Section 2, we recall some lattice background, dual-receiver encryption and identity-based dual-receiver encryption. Our DRE construction and its proof are presented in Section 3, and IB-DRE construction along with its proof are described in Section 4. In Section 5, we give a conclusion.

2 Preliminaries

Notations. Let λ be the security parameter, and all other quantities are implicitly dependent on λ. Let $\mathsf{negl}(\lambda)$ denote a negligible function and $\mathsf{poly}(\lambda)$ denote unspecified function $f(\lambda) = \mathcal{O}(\lambda^c)$ for a constant c. For $n \in \mathbb{N}$, we use $[n]$ to denote a set $\{1, \cdots, n\}$. And for integer $q \geq 2$, $\mathbb{Z}_q$ denotes the quotient ring of integer modulo q. We use bold capital letters to denote matrices, such as $\mathbf{A}, \mathbf{B}$, and bold lowercase letters to denote column vectors, such as $\mathbf{x}, \mathbf{y}$. The notations $\mathbf{A}^\top$ and $[\mathbf{A}|\mathbf{B}]$ denote the transpose of the matrix $\mathbf{A}$ and the matrix of concatenating $\mathbf{A}$ and $\mathbf{B}$, respectively. Additionally, we use $(\mathbf{a})_i$, $(\mathbf{A})_i$ to denote the i-th element, column of $\mathbf{a}$, $\mathbf{A}$. $\mathbf{I}_n$ denotes the $n \times n$ identity matrix and $\mathbf{Inv}_n$ denotes the set of invertible matrices in $\mathbb{Z}_q^{n \times n}$.

2.1 Encoding Vectors into Matrices

In [7], Cramer et al. described an encoding function $\mathcal{H}_{t,\mathbb{F}}$ that maps a domain $\mathbb{F}^t$ to matrices in $\mathbb{F}^{t \times t}$ with certain, strongly injective properties, where $\mathbb{F}$ is a field. For a polynomial $g \in \mathbb{F}[X]$ of degree less than $t-1$, $\mathsf{coeff}(g) \in \mathbb{F}^t$ is the t-vector of coefficients of g. Let f be a polynomial of degree t in $\mathbb{F}[X]$ that is irreducible. Then for $g \in \mathbb{F}[X]$, the polynomial $g \mod f$ has degree at most $t-1$, so $\mathsf{coeff}(g \mod f) \in \mathbb{F}^t$. Now, for an input $\mathbf{h} = (h_0, h_1, \cdots, h_{t-1})^\top \in \mathbb{F}^t$ define the polynomial $g_{\mathbf{h}}(X) = \sum_{i=0}^{t-1} h_i x^i \in \mathbb{F}[X]$. Define $\mathcal{H}_{t,\mathbb{F}}(\mathbf{h})$ as

$$\mathcal{H}_{t,\mathbb{F}}(\mathbf{h}) := \begin{pmatrix} \mathsf{coeff}(g_{\mathbf{h}} \mod f)^\top \\ \mathsf{coeff}(x \cdot g_{\mathbf{h}} \mod f)^\top \\ \vdots \\ \mathsf{coeff}(x^{t-1} \cdot g_{\mathbf{h}} \mod f)^\top \end{pmatrix} \in \mathbb{F}^{t \times t}.$$

From here on, we take $\mathbb{F} := \mathbb{Z}_q$ for a prime q. As stated in [4], it is easy to verify that $\mathcal{H}_{t,q} : \mathbb{Z}_q^t \to \mathbb{Z}_q^{t \times t}$ obeys the following properties:

- $\mathcal{H}_{t,q}(a\mathbf{h}_1 + b\mathbf{h}_2) = a \cdot \mathcal{H}_{t,q}(\mathbf{h}_1) + b \cdot \mathcal{H}_{t,q}(\mathbf{h}_2)$ for any $a, b \in \mathbb{Z}_q, \mathbf{h}_1, \mathbf{h}_2 \in \mathbf{Z}_q^t$.

- For any vector $\mathbf{h} \neq \mathbf{0}$, $\mathcal{H}_{t,q}(\mathbf{h})$ is invertible, and $\mathcal{H}_{t,q}(\mathbf{0}) = \mathbf{0}$.

In [1], according to function $\mathcal{H}_{t,q}$, Agrawal et al. defined the following equation $\mathcal{H}_{\mathrm{ABB}} : \mathbb{Z}_q^\ell \to \mathbb{Z}^{n\times n}$: For $\mathbf{x} = (x_1, \cdots, x_\ell)^\top \in \mathbb{Z}_q^\ell$,

$$\mathcal{H}_{\mathrm{ABB}}(\mathbf{x}) = \mathbf{I}_n + \sum_{i=1}^{\ell} x_i \cdot \mathcal{H}_{t,q}(\mathbf{h}_i) \otimes \mathbf{I}_{n/t},$$

where $\mathbf{h}_i \xleftarrow{\$} \mathbf{Z}_q^t$ for $i \in \{1, \cdots, \ell\}$, and assume that n is a multiple of t. Then, they implicitly presented the following lemma. However, they did not give a complete proof.

Lemma 1. *For any integers ℓ, t, n, and a prime q, let $\mathcal{H}_{\mathrm{ABB}}$ be the hash function family defined as above. Then for any fixed set $\mathcal{S} \subseteq \mathbb{Z}_q^\ell, |\mathcal{S}| \leq Q$, and any $\mathbf{x} \in \mathbb{Z}_q^\ell \backslash \mathcal{S}$, we have*

$$\Pr\left[\mathcal{H}_{\mathrm{ABB}}(\mathbf{x}) = \mathbf{0} \wedge (\forall \mathbf{x}' \in \mathcal{S}, \mathcal{H}_{\mathrm{ABB}}(\mathbf{x}') \in \mathbf{Inv}_n)\right] \in \left(\frac{1}{q^t}(1 - \frac{Q}{q^t}), \frac{1}{q^t}\right).$$

Proof. For a vector $\mathbf{e}_1 = (1, 0, \cdots, 0)^\top \in \mathbb{Z}_q^t$, we have $\mathcal{H}_{t,q}(\mathbf{e}_1) = \mathbf{I}_t$. For $\mathbf{x} = (x_1, \cdots, x_\ell)^\top \in \mathbb{Z}_q^\ell$, let $\mathcal{S}_0$ be the set of functions in $\mathcal{H}_{\mathrm{ABB}}$ such that $\mathcal{H}_{\mathrm{ABB}}(\mathbf{x}) = \mathbf{0}$. It is straightforward to verify that the following equation holds:

$$\begin{aligned}\mathcal{H}_{\mathrm{ABB}}(\mathbf{x}) =& \mathbf{I}_n + \sum_{i=1}^{\ell} x_i \cdot \mathcal{H}_{t,q}(\mathbf{h}_i) \otimes \mathbf{I}_{n/t} = \left(\mathbf{I}_t + \sum_{i=1}^{\ell} x_i \cdot \mathcal{H}_{t,q}(\mathbf{h}_i)\right) \otimes \mathbf{I}_{n/t} \\ =& \left(\mathcal{H}_{t,q}(\mathbf{e}_1) + \sum_{i=1}^{\ell} x_i \cdot \mathcal{H}_{t,q}(\mathbf{h}_i)\right) \otimes \mathbf{I}_{n/t} = \mathcal{H}_{t,q}\left(\mathbf{e}_1 + \sum_{i=1}^{\ell} x_i \mathbf{h}_i\right) \otimes \mathbf{I}_{n/t}.\end{aligned}$$

By a simple observation, we have $\mathcal{H}_{\mathrm{ABB}}(\mathbf{x}) = \mathbf{0}$ if and only if $\sum_{i=1}^{\ell} x_i \mathbf{h}_i = -\mathbf{e}_1$. As a result, we can get $|\mathcal{S}_0| = q^{(\ell-1)t}$. In the same way, we can get $|\mathcal{S}_i'| = q^{(\ell-1)t}$, where $\mathcal{S}_i'$ is the set of functions $\mathcal{H}_{\mathrm{ABB}}$ such that $\mathcal{H}_{\mathrm{ABB}}(\mathbf{x}_i') = \mathbf{0}$ for $\mathbf{x}_i' \in \mathcal{S} = \{\mathbf{x}_1', \cdots, \mathbf{x}_{|\mathcal{S}|}'\}$. Moreover, $|\mathcal{S}_0 \cap \mathcal{S}_i'| \leq q^{(\ell-2)t}$ for $i \in \{1, \cdots, |\mathcal{S}|\}$. The set of functions in $\mathcal{H}_{\mathrm{ABB}}$ such that $\mathcal{H}_{\mathrm{ABB}}(\mathbf{x}) = \mathbf{0}$ and $\forall \mathbf{x}' \in \mathcal{S}, \mathcal{H}_{\mathrm{ABB}}(\mathbf{x}') \in \mathbf{Inv}_n$ is exactly $\widetilde{\mathcal{S}} = \mathcal{S}_0 \setminus \{\mathcal{S}_1' \cup \cdots \cup \mathcal{S}_{|\mathcal{S}|}'\}$. Now, we have

$$\left|\widetilde{\mathcal{S}}\right| = \left|\mathcal{S}_0 \setminus \{\mathcal{S}_1' \cup \cdots \cup \mathcal{S}_{|\mathcal{S}|}'\}\right| \geq |\mathcal{S}_0| - \sum_{i=1}^{|\mathcal{S}|} |\mathcal{S}_0 \cap \mathcal{S}_i'| \geq q^{(\ell-1)t} - Qq^{(\ell-2)t}.$$

Therefore the above probability holds with $|\widetilde{\mathcal{S}}|/q^{t\ell}$ is at least $\frac{1}{q^t}(1 - \frac{Q}{q^t})$. And the probability is at most $\frac{1}{q^t}$ since $|\widetilde{\mathcal{S}}| \leq |\mathcal{S}_0| = q^{(\ell-1)t}$. □

2.2 (Identity-Based) Dual Receiver Encryption

Dual Receiver Encryption [8]. A DRE scheme consists of the following four algorithms:

- $\mathsf{CGen}_{\mathsf{DRE}}(1^\lambda) \to \mathsf{crs}$: The randomized common reference string (CRS) generation algorithm takes as input a security parameter λ and outputs a CRS crs.
- $\mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs}) \to (pk, sk)$: The randomized key generation algorithm takes as input crs and outputs a public/secret key pair (pk, sk). We regard (pk_1, sk_1) and (pk_2, sk_2) as the key pairs of two independent users. Without loss of generality, we assume $pk_1 <^d pk_2$, where $<^d$ is a "less-than" operator based on lexicographic order throughout this paper.
- $\mathsf{Enc}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, M) \to c$: The randomized encryption algorithm takes as input crs, two public keys pk_1 and pk_2 (such that $pk_1 <^d pk_2$) and a message M, and outputs a ciphertext c.
- $\mathsf{Dec}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, sk_j, c) \to M$: The deterministic decryption algorithm takes two public keys pk_1 and pk_2 (such that $pk_1 <^d pk_2$), one of the secret keys sk_j ($j \in \{1, 2\}$), and a ciphertext c as input, and outputs a message M (which may be the special symbol $\perp$).

Correctness. For consistency, we require that, if $\mathsf{crs} \leftarrow \mathsf{CGen}_{\mathsf{DRE}}(1^\lambda)$, $(pk_1, sk_1) \leftarrow \mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs})$ and $(pk_2, sk_2) \leftarrow \mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs})$, and $c \leftarrow \mathsf{Enc}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, M)$, then we have the probability

$$\Pr\left[\mathsf{Dec}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, sk_1, c) = \mathsf{Dec}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, sk_2, c) = M\right] = 1 - \mathsf{negl}(\lambda).$$

Security. A DRE scheme is said to be indistinguishable against chosen-ciphertext attacks (IND-CCA) if for any PPT adversary $\mathcal{A}$,

$$\mathbf{Adv}^{\mathsf{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda) = \left|\Pr\left[\mathsf{Exp}^{\mathsf{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda) = 1\right] - \frac{1}{2}\right|$$

is negligible in λ.

Identity-Based Dual Receiver Encryption [24]. An IB-DRE scheme consists of the following four algorithms:

- $\mathsf{Setup}_{\mathsf{ID}}(1^\lambda) \to (PP, Msk)$. The setup algorithm takes in a security parameter 1^λ as input. It outputs public parameters PP and a master secret key Msk.
- $\mathsf{KeyGen}_{\mathsf{ID}}(PP, Msk, id_{1st}, id_{2nd} \in ID) \to sk_{id_{1st}}, sk_{id_{2nd}}$. The key generation algorithm takes public parameters PP, master secret key Msk, and two identities id_{1st}, id_{2nd} as input. It outputs $sk_{id_{1st}}$ as the secret key for the first receiver id_{1st}, and $sk_{id_{2nd}}$ for the second receiver id_{2nd}.
- $\mathsf{Enc}_{\mathsf{ID}}(PP, id_{1st}, id_{2nd}, M) \to c$. The encryption algorithm takes in public parameters PP, two identities id_{1st} and id_{2nd}, and a message M as input. It outputs a ciphertext c.

Fig. 3. IND-CCA security for DRE and IND-ID-CPA security for IB-DRE

$$\begin{array}{|l|}\hline \textbf{Experiment } \mathsf{Exp}^{\mathsf{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda): \\ \quad \mathsf{crs} \xleftarrow{\$} \mathsf{CGen}_{\mathsf{DRE}}(1^\lambda); \\ \quad (pk_j, sk_j) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs}) \text{ for } j \in 1,2; \\ \quad (M_0, M_1, s) \xleftarrow{\$} \mathcal{A}^{\mathsf{Dec}_{\mathsf{DRE}}(sk_j,c)}(\mathsf{crs}, pk_1, pk_2); \\ \quad b \xleftarrow{\$} \{0,1\},\ c^\star \xleftarrow{\$} \mathsf{Enc}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, M_b); \\ \quad b' \xleftarrow{\$} \mathcal{A}^{\mathsf{Dec}_{\mathsf{DRE}}(sk_j,c)\wedge c\neq c^\star}(c^\star, s); \\ \quad \text{if } b' = b \text{ then return 1 else return 0.} \\ \hline \textbf{Experiment } \mathsf{Exp}^{\mathsf{ind-id-cpa}}_{\mathcal{IB}-\mathcal{DRE},\mathcal{A}}(1^\lambda): \\ \quad (PP, Msk) \xleftarrow{\$} \mathsf{Setup}_{\mathsf{ID}}(1^\lambda) \\ \quad (id^\star_{1st}, id^\star_{2nd}, M_0, M_1, s) \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyGen}_{\mathsf{ID}}(PP,Msk,id_{1st},id_{2nd})}(PP); \\ \quad b \xleftarrow{\$} \{0,1\}, c^\star \xleftarrow{\$} \mathsf{Enc}_{\mathsf{ID}}(PP, id^\star_{1st}, id^\star_{2nd}, M_b); \\ \quad b' \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyGen}_{\mathsf{ID}}(PP,Msk,id_{1st},id_{2nd})\wedge id_j\neq id^\star_{j,j=1st,2nd}}(c^\star, s); \\ \quad \text{if } b' = b \text{ then return 1 else return 0.} \\ \hline \end{array}$$

- $\mathsf{Dec}_{\mathsf{ID}}(PP, c, sk_{id_j}) \rightarrow M$. The decryption algorithm takes in public parameters PP, a ciphertext c, and one secret key sk_{id_j} as input, where $j \in \{1st, 2nd\}$. It outputs a message M.

Correctness. For all $(PP, Msk) \xleftarrow{\$} \mathsf{Setup}_{\mathsf{ID}}(1^\lambda)$, all identities $id_j \in ID$, all messages M, all $sk_{id_j} \leftarrow \mathsf{KeyGen}_{\mathsf{ID}}(PP, Msk, id_j)$, all $c \leftarrow \mathsf{Enc}_{\mathsf{ID}}(PP, id_{1st}, id_{2nd}, M)$, we have

$$\Pr[\mathsf{Dec}_{\mathsf{ID}}(PP, sk_{id_{1st}}, c) = \mathsf{Dec}_{\mathsf{ID}}(PP, sk_{id_{2nd}}, c) = M] = 1 - \mathsf{negl}(\lambda).$$

Security. An IB-DRE scheme is said to be indistinguishable against chosen-plaintext and adaptively chosen-identity attacks (IND-ID-CPA) if for any PPT adversary $\mathcal{A}$,

$$\mathbf{Adv}^{\mathsf{ind-id-cpa}}_{\mathcal{IB}-\mathcal{DRE},\mathcal{A}}(1^\lambda) = \left|\Pr\left[\mathsf{Exp}^{\mathsf{ind-id-cpa}}_{\mathcal{IB}-\mathcal{DRE},\mathcal{A}}(1^\lambda) = 1\right] - \frac{1}{2}\right|$$

is negligible in λ.

3 Dual Receiver Encryption Construction

Our scheme relies upon a strongly unforgeable one-time signature scheme $\mathcal{OTS} = (\mathsf{Gen}_{\mathsf{OTS}}, \mathsf{Sig}_{\mathsf{OTS}}, \mathsf{Vrf}_{\mathsf{OTS}})$ whose verification key is exactly λ bits long. The description of our DRE scheme $\mathcal{DRE}$ is as follows.

- $\mathsf{CGen}_{\mathsf{DRE}}(1^\lambda)$. On input a security parameter λ, algorithm $\mathsf{CGen}_{\mathsf{DRE}}$ sets the parameters n, m, q as specified in Figure 4. Then it selects a uniformly random matrix $\mathbf{U} \in \mathbb{Z}_q^{n\times n}$. Finally it outputs a CRS $\mathsf{crs} = (n, m, q, \mathbf{U})$.

- $\mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs})$. For user $j \in \{1,2\}$, this algorithm generates a pair matrices $(\mathbf{A}_j, \mathbf{T}_{\mathbf{A}_j}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times m}$ by running $\mathsf{TrapGen}(1^n, 1^m, q)$ and selects a random matrix $\mathbf{B}_j \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$. Finally, it outputs

$$pk_j = (\mathbf{A}_j, \mathbf{B}_j) \qquad \text{and} \qquad sk_j = \mathbf{T}_{\mathbf{A}_j}.$$

- $\mathsf{Enc}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, \mathbf{m} \in \{0,1\}^n)$. It first obtains a pair $(\mathsf{vk}, \mathsf{sk})$ by running $\mathsf{Gen}_{\mathsf{OTS}}(1^\lambda)$ and computes $\mathbf{C}_1 = [\mathbf{A}_1|\mathbf{B}_1 + \mathcal{H}_{n,q}(\mathsf{vk}) \cdot \mathbf{G}] \in \mathbb{Z}_q^{n\times 2m}$,$\mathbf{C}_2 = [\mathbf{A}_2|\mathbf{B}_2 + \mathcal{H}_{n,q}(\mathsf{vk}) \cdot \mathbf{G}] \in \mathbb{Z}_q^{n\times 2m}$. Then, it picks $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, and $\mathbf{e}_{1,1}, \mathbf{e}_{2,1}, \mathbf{e}_{1,2}, \mathbf{e}_{2,2} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$. Finally, it computes and returns the ciphertext $\mathbf{c} = (\mathsf{vk}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \delta)$, where $\delta = \mathsf{Sig}_{\mathsf{OTS}}(\mathsf{sk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2))$ and

$$\mathbf{c}_0 = \mathbf{U}^\top \mathbf{s} + \widetilde{\mathbf{e}}_0 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} \in \mathbb{Z}_q^n,$$
$$\mathbf{c}_1 = \mathbf{C}_1^\top \mathbf{s} + \begin{bmatrix} \mathbf{e_{1,1}} \\ \mathbf{e_{1,2}} \end{bmatrix} \in \mathbb{Z}_q^{2m}, \mathbf{c}_2 = \mathbf{C}_2^\top \mathbf{s} + \begin{bmatrix} \mathbf{e_{2,1}} \\ \mathbf{e_{2,2}} \end{bmatrix} \in \mathbb{Z}_q^{2m}.$$

- $\mathsf{Dec}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, sk_1, \mathbf{c})$. To decrypt a ciphertext $\mathbf{c} = (\mathsf{vk}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \delta)$ with a private key $sk_1 = \mathbf{T}_{\mathbf{A}_1}$, the algorithm $\mathsf{Dec}_{\mathsf{DRE}}$ performs each of the following steps:
  (1) it runs $\mathsf{Vrf}_{\mathsf{OTS}}(\mathsf{vk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \delta)$, outputs $\perp$ if $\mathsf{Vrf}_{\mathsf{OTS}}$ rejects;
  (2) for $i \in \{1, \cdots, n\}$, it runs $\mathsf{SampleLeft}(\mathbf{A}_1, \mathbf{B}_1 + \mathcal{H}_{n,q}(\mathsf{vk}) \cdot \mathbf{G}, (\mathbf{U})_i, \mathbf{T}_{\mathbf{A}_1}, \sigma)$ to obtain $(\mathbf{E}_1)_i$, i.e., it obtains $\mathbf{E}_1 \in \mathbb{Z}_q^{2m\times n}$ such that $\mathbf{C}_1 \cdot \mathbf{E}_1 = \mathbf{U}$;
  (3) it computes $\mathbf{b} = \mathbf{c}_0 - \mathbf{E}_1^\top \mathbf{c}_1$ and treats each element of $\mathbf{b} = [(\mathbf{b})_1, \cdots, (\mathbf{b})_n]^\top$ as an integer in $\mathbb{Z}$, and sets $(\mathbf{m})_i = 1$ if $\left|(\mathbf{b})_i - \lceil \frac{q}{2} \rceil\right| < \lceil \frac{q}{4} \rceil$, else $(\mathbf{m})_i = 0$, where $i \in \{1, \cdots, n\}$.
  (4) finally, it returns the plaintext $\mathbf{m} = [(\mathbf{m})_1, \cdots, (\mathbf{m})_n]^\top$.

3.1 Correctness and Parameter Selection

In order to satisfy the correctness requirement and make the security proof work, we need that

- for $i \in \{1, \cdots, n\}$, the error term is bounded by

$$\left| (\widetilde{\mathbf{e}}_0)_i - (\mathbf{E})_i^\top \begin{bmatrix} \mathbf{e_{1,1}} \\ \mathbf{e_{1,2}} \end{bmatrix} \right| \leq \alpha q \sqrt{m} + (\sigma\sqrt{2m}) \cdot (\alpha' q \sqrt{2m}) < q/4.$$

- $\mathsf{TrapGen}$ in Lemma 12 (Item 1) can work ($m \geq 6n\lceil \log q \rceil$), and it returns $\mathbf{T}_{\mathbf{A}}$ satisfying $\|\widetilde{\mathbf{T}_{\mathbf{A}}}\| \geq \mathcal{O}(\sqrt{n \log q})$.
- the Leftover Hash Lemma in Lemma 12 (Item 4) can be applied to the security proof ($m > (n+1)\log q + \omega(\log n)$).
- $\mathsf{SampleLeft}$ in Lemma 12 (Item 2) can operate ($\sigma \geq \|\widetilde{\mathbf{T}_{\mathbf{A}}}\| \cdot \omega(\sqrt{\log m}) = \mathcal{O}(\sqrt{n \log q}) \cdot \omega(\sqrt{\log m})$).
- $\mathsf{SampleRight}$ in Lemma 12 (Item 3) can operate ($\sigma \geq \|\widetilde{\mathbf{T}_{\mathbf{G}}}\| \cdot s_1(\mathbf{R}_j) \cdot \omega(\sqrt{\log m})$, for $j = 1, 2$).

- ReRand (Lemma 13) in the security proof can operate ($\alpha q > \omega(\sqrt{\log m})$, and $\alpha' q/(2\alpha q) > s_1([\mathbf{I}_m|\mathbf{R}_j]^\top)$, where $s_1([\mathbf{I}_m|\mathbf{R}_j]^\top) \leq (1 + s_1(\mathbf{R}_j)) \leq (1 + 12\sqrt{2m})$, for $j = 1, 2$.

To satisfy the above requirements, we set the parameters in Figure 4.

Fig. 4. Parameter Selection of DRE Construction

Parameters	Description	Setting
λ	security parameter	
n	PK-matrix row number	$n = \lambda$
m	PK-matrix column number	$6n \log q$
σ	$\mathsf{SampleLeft}$,$\mathsf{SampleRight}$ width	$12\sqrt{10m} \cdot \omega(\sqrt{\log n})$
q	modulus	$96\sqrt{5}m^{3/2}n\omega(\sqrt{\log n})$
αq	error width	$2\sqrt{2n}$
$\alpha' q$	error width	$96\sqrt{mn}$

3.2 Security Proof

Theorem 1. *If $\mathcal{OTS}$ is a strongly existential unforgeable one-time signature scheme and the* $\mathrm{DLWE}_{q,n,n+2m,\alpha}$ *assumption holds, then the above scheme $\mathcal{DRE}$ is a secure DRE against chosen-ciphertext attacks.*

Proof (of Theorem 1). Assume $\mathcal{A}$ is a probabilistic polonomial time (PPT) adversary attacks $\mathcal{DRE}$ in a chosen-ciphertext attack. If $\mathsf{Vrf}_{\mathsf{OTS}}(\mathsf{vk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \delta) = 1$, we say the ciphertext $\mathbf{c} = (\mathsf{vk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \delta)$ is valid. Let $\mathbf{c}^\star$ denote the challenge ciphertext $(\mathsf{vk}^\star, (\mathbf{c}_0^\star, \mathbf{c}_1^\star, \mathbf{c}_2^\star), \delta^\star)$ received by $\mathcal{A}$ during a particular run of the experiment, and let Forge denote the event that $\mathcal{A}$ submits a valid ciphertext $(\mathsf{vk}^\star, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \delta)$ to the decryption oracle (we assume that $\mathsf{vk}^\star$ is chosen at the outer of the experiment so this well-defined even before $\mathcal{A}$ is given $\mathbf{c}^\star$.) According to the security of $\mathcal{OTS}$, $\Pr[\mathsf{Forge}]$ is negligible. We then prove the following lemma:

Lemma 2. $\left|\Pr\left[\mathsf{Exp}^{\mathrm{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda) = 1 \wedge \overline{\mathsf{Forge}}\right] + \frac{1}{2}\Pr[\mathsf{Forge}] - \frac{1}{2}\right|$ *is negligible, if assuming that the* $\mathrm{DLWE}_{q,n,n+2m,\alpha}$ *assumption holds.*

To see that this implies the theorem, note that

$$\begin{aligned}
\mathsf{Adv}^{\mathrm{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda) &= \left|\Pr\left[\mathsf{Exp}^{\mathrm{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda) = 1\right] - \frac{1}{2}\right| \\
&\leq \left|\Pr\left[\mathsf{Exp}^{\mathrm{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda) = 1 \wedge \mathsf{Forge}\right] - \frac{1}{2}\Pr[\mathsf{Forge}]\right| \\
&\quad + \left|\Pr\left[\mathsf{Exp}^{\mathrm{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda) = 1 \wedge \overline{\mathsf{Forge}}\right] + \frac{1}{2}\Pr[\mathsf{Forge}] - \frac{1}{2}\right| \\
&\leq \frac{1}{2}\Pr[\mathsf{Forge}] + \left|\Pr\left[\mathsf{Exp}^{\mathrm{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda) = 1 \wedge \overline{\mathsf{Forge}}\right] + \frac{1}{2}\Pr[\mathsf{Forge}] - \frac{1}{2}\right|.
\end{aligned}$$

Proof (of Lemma 2). We sketch the proof via a sequence of games. The games involve the challenger and an adversary $\mathcal{A}$. In the following, we define X_κ as the event that the challenger outputs 1 in $\mathbf{Game}_\kappa$, for $\kappa \in \{1,2,3,4,5\}$.

$\mathbf{Game_1}$: This game is the original experiment $\mathsf{Exp}^{\mathrm{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda)$ except that when the adversary $\mathcal{A}$ submits a valid ciphertext $(\mathsf{vk}^\star,(\mathbf{c}_0,\mathbf{c}_1,\mathbf{c}_2),\delta)$ to the decryption oracle, the challenger outputs a random bit. It is easy to see that

$$\left|\Pr[X_1]-\frac{1}{2}\right| = \left|\Pr\left[\mathsf{Exp}^{\mathrm{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda)=1 \wedge \overline{\mathsf{Forge}}\right]+\frac{1}{2}\Pr[\mathsf{Forge}]-\frac{1}{2}\right|.$$

$\mathbf{Game_2}$: This game is identical to $\mathbf{Game_1}$ except that the challenger changes (1) the generation of public keys pk_1, pk_2: the challenger selects random matrices $\mathbf{A}_1,\mathbf{A}_2 \in \mathbb{Z}_q^{n\times m}$ instead of running $\mathsf{TrapGen}$, and random matrices $\mathbf{R}_1,\mathbf{R}_2 \in \{-1,1\}^{m\times m}$; then, the challenger computes $\mathbf{B}_1 = \mathbf{A}_1\mathbf{R}_1 - \mathcal{H}_{n,q}(\mathsf{vk}^\star)\mathbf{G}, \mathbf{B}_2 = \mathbf{A}_2\mathbf{R}_2 - \mathcal{H}_{n,q}(\mathsf{vk}^\star)\mathbf{G} \in \mathbb{Z}_q^{n\times m}$. (2) the decryption oracle: when $\mathcal{A}$ submits a valid ciphertext $(\mathsf{vk}\neq\mathsf{vk}^\star,(\mathbf{c}_0,\mathbf{c}_1,\mathbf{c}_2),\delta)$, the challenger can generate $\mathbf{E}_1$ by running the algorithm $\mathsf{SampleRight}(\mathbf{A}_1,\mathbf{G},\mathbf{R}_1,\mathcal{H}_{n,q}(\mathsf{vk}-\mathsf{vk}^\star),(\mathbf{U})_i,\mathbf{T}_\mathbf{G},\sigma)$ (In the similar way, the challenger obtains $\mathbf{E}_2$ by running $\mathsf{SampleRight}(\mathbf{A}_1,\mathbf{G},\mathbf{R}_2,\mathcal{H}_{n,q}(\mathsf{vk}-\mathsf{vk}^\star),(\mathbf{U})_i,\mathbf{T}_\mathbf{G},\sigma)$) instead of $\mathsf{SampleLeft}$, for $i\in\{1,\cdots,n\}$. Note that the following equation holds:

$$\mathbf{c}_0^\star = \mathbf{U}^\top\mathbf{s}+\widetilde{\mathbf{e}}_0+\left\lceil\frac{q}{2}\right\rceil\cdot\mathbf{m}_b,$$
$$\mathbf{c}_1^\star = \begin{bmatrix}(\mathbf{A}_1)^\top\mathbf{s}+\mathbf{e}_{1,1}\\ (\mathbf{R}_1)^\top(\mathbf{A}_1)^\top\mathbf{s}+\mathbf{e}_{1,2}\end{bmatrix}, \mathbf{c}_2^\star = \begin{bmatrix}(\mathbf{A}_2)^\top\mathbf{s}+\mathbf{e}_{2,1}\\ (\mathbf{R}_2)^\top(\mathbf{A}_2)^\top\mathbf{s}+\mathbf{e}_{2,2}\end{bmatrix},$$

where $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$ and $\mathbf{e_{1,1}},\mathbf{e_{1,2}},\mathbf{e_{2,1}},\mathbf{e_{2,2}} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$.

$\mathbf{Game_3}$: In this game, the challenger changes the way that the challenge ciphertext $\mathbf{c}^\star$ is created: the challenger first picks $\mathbf{s}\xleftarrow{\$}\mathbb{Z}_q^n, \widetilde{\mathbf{e}}_0\xleftarrow{\$}\mathcal{D}_{\mathbb{Z}^n,\alpha q}, \widetilde{\mathbf{e}}_{1,1},\widetilde{\mathbf{e}}_{2,1}\xleftarrow{\$}\mathcal{D}_{\mathbb{Z}^m,\alpha q}$ and sets $\mathbf{w}=\mathbf{U}^\top\mathbf{s}+\widetilde{\mathbf{e}}_0, \mathbf{b}_1=(\mathbf{A}_1)^\top\mathbf{s}+\widetilde{\mathbf{e}}_{1,1}, \mathbf{b}_2=(\mathbf{A}_2)^\top\mathbf{s}+\widetilde{\mathbf{e}}_{2,1}$. Then, it computes

$$\mathbf{c}_0^\star = \mathbf{w}+\left\lceil\frac{q}{2}\right\rceil\cdot\mathbf{m}_b,$$
$$\mathbf{c}_1^\star = \mathsf{ReRand}\left(\begin{bmatrix}\mathbf{I}_m\\ (\mathbf{R}_1)^\top\end{bmatrix},\mathbf{b}_1,\alpha q,\frac{\alpha' q}{2\alpha q}\right), \mathbf{c}_2^\star = \mathsf{ReRand}\left(\begin{bmatrix}\mathbf{I}_m\\ (\mathbf{R}_2)^\top\end{bmatrix},\mathbf{b}_2,\alpha q,\frac{\alpha' q}{2\alpha q}\right).$$

$\mathbf{Game_4}$: In this game, the challenger changes the way that the challenge ciphertext $\mathbf{c}^\star$ is created: the challenger first picks random vectors $\mathbf{w}\xleftarrow{\$}\mathbb{Z}_q^n, \widetilde{\mathbf{b}}_1\xleftarrow{\$}\mathbb{Z}_q^m, \widetilde{\mathbf{b}}_2\xleftarrow{\$}\mathbb{Z}_q^m, \widetilde{\mathbf{e}}_{1,1},\widetilde{\mathbf{e}}_{2,1}\xleftarrow{\$}\mathcal{D}_{\mathbb{Z}^m,\alpha q}$ and sets $\mathbf{b}_1=\widetilde{\mathbf{b}}_1+\widetilde{\mathbf{e}}_{1,1}, \mathbf{b}_2=\widetilde{\mathbf{b}}_2+\widetilde{\mathbf{e}}_{2,1}$. Then, it computes

$$\mathbf{c}_0^\star = \mathbf{w}+\left\lceil\frac{q}{2}\right\rceil\cdot\mathbf{m}_b,$$
$$\mathbf{c}_1^\star = \mathsf{ReRand}\left(\begin{bmatrix}\mathbf{I}_m\\ (\mathbf{R}_1)^\top\end{bmatrix},\mathbf{b}_1,\alpha q,\frac{\alpha' q}{2\alpha q}\right), \mathbf{c}_2^\star = \mathsf{ReRand}\left(\begin{bmatrix}\mathbf{I}_m\\ (\mathbf{R}_2)^\top\end{bmatrix},\mathbf{b}_2,\alpha q,\frac{\alpha' q}{2\alpha q}\right).$$

Game$_5$: In this game, the challenger changes the way that the challenge ciphertext $\mathbf{c}^\star$ is created: the challenger first picks $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^n, \widetilde{\mathbf{b}}_1 \xleftarrow{\$} \mathbb{Z}_q^m, \widetilde{\mathbf{b}}_2 \xleftarrow{\$} \mathbb{Z}_q^m, \mathbf{e}_{1,1}, \mathbf{e}_{1,2}, \mathbf{e}_{2,1}, \mathbf{e}_{2,2} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$ and computes

$$\mathbf{c}_0^\star = \mathbf{w} + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m}_b,$$
$$\mathbf{c}_1^\star = \begin{bmatrix} \widetilde{\mathbf{b}}_1 + \mathbf{e}_{1,1} \\ (\mathbf{R}_1)^\top \widetilde{\mathbf{b}}_1 + \mathbf{e}_{1,2} \end{bmatrix}, \mathbf{c}_2^\star = \begin{bmatrix} \widetilde{\mathbf{b}}_2 + \mathbf{e}_{2,1} \\ (\mathbf{R}_2)^\top \widetilde{\mathbf{b}}_2 + \mathbf{e}_{2,2} \end{bmatrix}.$$

Analysis of Games. We use the following lemmas to give a analysis between each adjacent games.

Lemma 3. **Game$_1$** *and* **Game$_2$** *are statistically indistinguishable.*

Proof Sketch. We can prove that **Game$_2$** is statistically close to **Game$_1$** using Leftover Hash Lemma (Lemma 12, item 4) and the properties of the algorithms SampleRight, TrapGen. □

Lemma 4. **Game$_2$** *and* **Game$_3$** *are identically distributed, and* **Game$_4$** *and* **Game$_5$** *are identically distributed.*

Proof. This lemma can be proved just according to the property of Rand. □

Lemma 5. *Assume the* $\mathrm{DLWE}_{q,n,n+2m,\alpha}$ *assumption holds,* **Game$_3$** *and* **Game$_4$** *are computationally indistinguishable.*

Proof. Suppose there exists an adversary $\mathcal{A}$ who has a non-negligible advantage in distinguishing **Game$_3$** and **Game$_4$**, then we can construct an adversary $\mathcal{B}$ who can break the LWE assumption as follows.

Instance. Based on the given LWE instance $(\mathbf{U}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{w}, \mathbf{b}_1, \mathbf{b}_2) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n \times \mathbb{Z}_q^m \times \mathbb{Z}_q^m$ and assume $\mathbf{w} = \widetilde{\mathbf{w}} + \widetilde{\mathbf{e}}_0$ and $\mathbf{b}_1 = \widetilde{\mathbf{b}}_1 + \widetilde{\mathbf{e}}_{1,1}, \mathbf{b}_2 = \widetilde{\mathbf{b}}_2 + \widetilde{\mathbf{e}}_{2,1}$ where $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}, \widetilde{\mathbf{e}}_{1,1}, \widetilde{\mathbf{e}}_{2,1} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$. Then $\mathcal{B}$ should distinguish whether $\widetilde{\mathbf{w}} = \mathbf{U}^\top \mathbf{s}, \widetilde{\mathbf{b}}_1 = \mathbf{A}_1^\top \mathbf{s}, \widetilde{\mathbf{b}}_2 = \mathbf{A}_2^\top \mathbf{s}$ for some $\mathbf{s} \in \mathbb{Z}_q^n$ or $\widetilde{\mathbf{w}} \xleftarrow{\$} \mathbb{Z}_q^n, \widetilde{\mathbf{b}}_1, \widetilde{\mathbf{b}}_2 \xleftarrow{\$} \mathbb{Z}_q^m$. We note this subtle change from the standard LWE problem is done only for the convenience of the proof.

Setup. The $\mathcal{B}$ constructs $\{\mathbf{B}_1, \mathbf{B}_2\}$ for $i \in \{1, \cdots, \ell\}$ as in **Game$_3$**.

Decryption Queries. The $\mathcal{B}$ answers decryption oracle as in **Game$_3$**.

Challenge ciphertext. When $\mathcal{A}$ sends two message (m_0, m_1), the reduction $\mathcal{B}$ computes the challenge ciphertext as follows

$$\mathbf{c}_0^\star = \mathbf{w} + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m}_b \in \mathbb{Z}_q^n,$$
$$\mathbf{c}_1^\star = \mathsf{ReRand}\left(\begin{bmatrix} \mathbf{I}_m \\ (\mathbf{R}_1)^\top \end{bmatrix}, \mathbf{b}_1, \alpha q, \frac{\alpha' q}{2\alpha q} \right), \mathbf{c}_2^\star = \mathsf{ReRand}\left(\begin{bmatrix} \mathbf{I}_m \\ (\mathbf{R}_2)^\top \end{bmatrix}, \mathbf{b}_2, \alpha q, \frac{\alpha' q}{2\alpha q} \right).$$

Guess. After being allowed to make additional queries, $\mathcal{A}$ guesses if it interacts with a challenger of **Game$_3$** or **Game$_4$** .

It can be easily seen that if $(\mathbf{U}, \mathbf{A}, \mathbf{w}, \mathbf{b})$ is a valid LWE sample, the view of $\mathcal{A}$ corresponds to $\mathbf{Game}_3$; otherwise, the view of $\mathcal{A}$ corresponds to that of $\mathbf{Game}_4$. We complete the proof of this lemma. □

Complete the Proof of Theorem 1. It is obvious that $\Pr[X_5] = \frac{1}{2}$, this is because the challenge bit b is independent of the $\mathcal{A}$'s view. From Lemma 3 to Lemma 5, we know that

$$\Pr[X_1] \approx \Pr[X_2], \Pr[X_2] = \Pr[X_3], \Pr[X_4] = \Pr[X_5].$$

From Lemma 5, we know that

$$|\Pr[X_3] - \Pr[X_4]| = \left|\Pr[X_4] - \frac{1}{2}\right| \leq \mathrm{DLWE}_{q,n,n+2m,\alpha},$$

which implies $\left|\Pr[X_1] - \frac{1}{2}\right| \leq \mathrm{DLWE}_{q,n,n+2m,\alpha} - \mathsf{negl}(\lambda)$. □□

4 Identity-Based Dual Receiver Encryption Construction

Assume an identity space $\mathcal{ID} = \{-1, 1\}^\ell$ (In general, IB-DRE needs to support n-bit length identity, i.e., $\ell = n$) and a message space $\mathcal{M} = \{0, 1\}^n$, our IB-DRE scheme $\mathcal{IB}\text{-}\mathcal{DRE}$ consists of the following four algorithms:

- $\mathsf{Setup}_{\mathsf{ID}}(1^\lambda) \rightarrow (PP, Msk)$: On input a security parameter λ, it sets the parameters n, m, q as specified in Figure 5. Then it obtains a pair matrices $(\mathbf{A}, \mathbf{T}_\mathbf{A}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times m}$ by running $\mathsf{TrapGen}(1^n, 1^m, q)$ and selects a uniformly random matrix $\mathbf{U} \in \mathbb{Z}_q^{n\times n}, \mathbf{A}_i^1, \mathbf{A}_i^2 \in \mathbb{Z}_q^{n\times m}$, where $i \in \{1, \cdots, n\}$. Finally it outputs $PP = (n, m, q, \mathbf{A}, \mathbf{A}_i^1, \mathbf{A}_i^2, \mathbf{U})$ and $Msk = \mathbf{T}_\mathbf{A}$.
- $\mathsf{KeyGen}_{\mathsf{ID}}(PP, Msk, \mathbf{id}_{1st}, \mathbf{id}_{2nd} \in \mathcal{ID}) \rightarrow sk_{\mathbf{id}_{1st}}, sk_{\mathbf{id}_{2nd}}$: On input public parameters PP, a master key Msk, and identities $\mathbf{id}_{1st}, \mathbf{id}_{2nd}$, it first computes $\mathbf{A}_{\mathbf{id}_1} = \sum_{i=1}^n (\mathbf{id}_{1st})_i \cdot \mathbf{A}_i^1 + \mathbf{G}, \mathbf{A}_{\mathbf{id}_2} = \sum_{i=1}^n (\mathbf{id}_{2nd})_i \cdot \mathbf{A}_i^2 + \mathbf{G}$. Then for $i \in \{1, \cdots, n\}$, it runs $\mathsf{SampleLeft}(\mathbf{A}, \mathbf{A}_{\mathbf{id}_1}, (\mathbf{U})_i, \mathbf{T}_\mathbf{A}, \sigma)$ to obtain $(\mathbf{E}_{\mathbf{id}_1})_i$ and sets $sk_{\mathbf{id}_{1st}} = \mathbf{E}_{\mathbf{id}_1} \in \mathbb{Z}_q^{2m\times n}$. Similarly, it can obtain $sk_{\mathbf{id}_{2nd}} = \mathbf{E}_{\mathbf{id}_2}$ such that $[\mathbf{A}|\mathbf{A}_{\mathbf{id}_2}] \cdot \mathbf{E}_{\mathbf{id}_2} = \mathbf{U}$.
- $\mathsf{Enc}_{\mathsf{ID}}(PP, \mathbf{id}_{1st}, \mathbf{id}_{2nd}, \mathbf{m}) \rightarrow \mathbf{c}$. It computes $\mathbf{A}_{\mathbf{id}_1}, \mathbf{A}_{\mathbf{id}_2}$ as above. Then, it picks $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, and $\mathbf{e}_{1,1}, \mathbf{e}_{2,1}, \mathbf{e}_{1,2}, \mathbf{e}_{2,2} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$. Finally, it computes and returns the ciphertext $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1)$, where

$$\mathbf{c}_0 = \mathbf{U}^\top \mathbf{s} + \mathbf{e}_0 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} \in \mathbb{Z}_q^n,$$

$$\mathbf{c}_1 = \begin{bmatrix} \mathbf{c_{1,1}} \\ \mathbf{c_{1,2}} \\ \mathbf{c_{1,3}} \end{bmatrix} = \begin{bmatrix} \mathbf{A}^\top \\ (\mathbf{A}_{\mathbf{id}_1})^\top \\ (\mathbf{A}_{\mathbf{id}_2})^\top \end{bmatrix} \mathbf{s} + \begin{bmatrix} \mathbf{e_{1,1}} \\ \mathbf{e_{1,2}} \\ \mathbf{e_{1,3}} \end{bmatrix} \in \mathbb{Z}_q^{3m},$$

- $\mathsf{Dec}_{\mathsf{ID}}(PP, sk_{\mathbf{id}_j}, \mathbf{c}) \rightarrow \mathbf{m}$. To decrypt a ciphertext $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1)$ with a private key $sk_{\mathbf{id}_{1st}} = \mathbf{E}_{\mathbf{id}_1}$, it computes $\mathbf{b} = \mathbf{c}_0 - \mathbf{E}_{\mathbf{id}_1}^\top \cdot \begin{bmatrix} \mathbf{c}_{1,1} \\ \mathbf{c}_{1,2} \end{bmatrix}$ and regards each coordinate of $\mathbf{b} = [(\mathbf{b})_1, \cdots, (\mathbf{b})_n]^\top$ as an integer in $\mathbb{Z}$, and sets $(\mathbf{m})_i = 1$ if $\left|(\mathbf{b})_i - \lceil \frac{q}{2} \rceil\right| < \lceil \frac{q}{4} \rceil$; otherwise sets $(\mathbf{m})_i = 0$ where $i \in \{1, \cdots, n\}$. Finally, it returns a plaintext $\mathbf{m} = [(\mathbf{m})_1, \cdots, (\mathbf{m})_n]^\top$.

4.1 Correctness and Parameter Selection

In order to satisfy the correctness requirement and make the security proof work (which is very similar to Subsection 3.1), we set the parameters in Figure 5.

Fig. 5. Parameter Selection of IB-DRE Construction

Parameters	Description	Setting
λ	security parameter	
n	PK-matrix row number	$n = \lambda$
m	PK-matrix column number	$6n \log q$
ℓ	length of identity	n
σ	SampleLeft,SampleRight width	$12\sqrt{10mn} \cdot \omega(\sqrt{\log n})$
q	modulus	$\mathcal{O}(m^2 n^{5/2} \omega(\sqrt{\log n}))$
αq	error width	$2\sqrt{2n}$
$\alpha' q$	error width	$192 n^{3/2} \sqrt{m}$

4.2 Security Proof

Theorem 2. *If the* $\mathrm{DLWE}_{q,n,n+m,\alpha}$ *assumption holds, then the above scheme* $\mathcal{IB}$-$\mathcal{DRE}$ *is a secure IB-DRE scheme against chosen-plaintext and adaptively chosen-identity attacks.*

Proof (of Theorem 2). We prove the theorem with showing that if a PPT adversary $\mathcal{A}$ can break our $\mathcal{IB}$-$\mathcal{DRE}$ scheme with a non-negligible advantage ϵ (i.e., success probability $\frac{1}{2} + \epsilon$), then there exists a reduction that can break the $\mathrm{DLWE}_{q,n,n+m,\alpha}$ assumption with an advantage $\mathrm{poly}(\epsilon) - \mathrm{negl}(1^\lambda)$. Let $Q = Q(\lambda)$ be the upper bound of the number of $\mathsf{KeyGen}_{\mathsf{ID}}$ queries and $I^* = \{(\mathbf{id}^*_{1st}, \mathbf{id}^*_{2nd}), (\mathbf{id}^\jmath_{1st}, \mathbf{id}^\jmath_{2nd})_{\jmath \in [Q]}\}$ be the challenge ID along with the queried ID's.

We formally give the proof via a sequence of games and define X_κ as the event that the challenger outputs 1 in $\mathbf{Game}_\kappa$, for $\kappa \in \{0, 1, 2, 3, 4, 5, 6\}$.

$\mathbf{Game_0}$: This game is the original experiment $\mathsf{Exp}^{\mathrm{ind-id-cpa}}_{\mathcal{IB}-\mathcal{DRE},\mathcal{A}}(1^\lambda)$ in Figure 3. It is easy to see that

$$\epsilon = \left| \Pr[X_0] - \frac{1}{2} \right| = \left| \Pr\left[\mathsf{Exp}^{\mathrm{ind-id-cpa}}_{\mathcal{IB}-\mathcal{DRE},\mathcal{A}}(1^\lambda) = 1 \right] - \frac{1}{2} \right|.$$

$\mathbf{Game_1}$: This game is as same as $\mathbf{Game_0}$ except that we add an abort event that is independent of the adversary's view. Let n, ℓ, q be the parameters as in the scheme's setup algorithm and the challenger selects $t = \lceil \log_q(2Q/\epsilon) \rceil$, hence we have $q^t \geq 2Q/\epsilon \geq q^{t-1}$. Then the challenger chooses $2n$ random integer

vectors $\mathbf{h}_i^1, \mathbf{h}_i^2 \in \mathbb{Z}_q^t$ and defines two functions $\mathcal{H}_{\mathrm{ABB}}^1, \mathcal{H}_{\mathrm{ABB}}^2 : \mathcal{ID} \to \mathbb{Z}_q^{n\times n}$ as follows: $\forall \mathbf{id} \in \mathcal{ID}$,

$$\mathcal{H}_{\mathrm{ABB}}^1(\mathbf{id}) = \mathbf{I}_n + \sum_{i=1}^{n} (\mathbf{id})_i \cdot \mathcal{H}(\mathbf{h}_i^1) \otimes \mathbf{I}_{n/t}, \mathcal{H}_{\mathrm{ABB}}^2(\mathbf{id}) = \mathbf{I}_n + \sum_{i=1}^{n} (\mathbf{id})_i \cdot \mathcal{H}(\mathbf{h}_i^2) \otimes \mathbf{I}_{n/t}.$$

We then describe how the challenger behaves in $\mathbf{Game_1}$ as follows:

- **Setup** : The same as $\mathbf{Game_0}$ except that the challenger keeps the hash functions $\mathcal{H}_{\mathrm{ABB}}^1$ and $\mathcal{H}_{\mathrm{ABB}}^2$ passed from the experiment.
- **Secret key and ciphertext query:** The challenger responds to secret key queries for identities and challenge ciphertext query (with a random bit $b \in \{0,1\}$) as same as that in $\mathbf{Game_0}$.
- **Gauss:** When the adversary returns a bit b', the challenger checks if

$$\mathcal{H}_{\mathrm{ABB}}^2(\mathbf{id}_{1st}^\star) = \mathbf{0}, \mathcal{H}_{\mathrm{ABB}}^2(\mathbf{id}_{1st}^\jmath) \in \mathbf{Inv}_n$$

$$\mathcal{H}_{\mathrm{ABB}}^2(\mathbf{id}_{2nd}^\star) = \mathbf{0}, \mathcal{H}_{\mathrm{ABB}}^2(\mathbf{id}_{2nd}^\jmath) \in \mathbf{Inv}_n$$

for $\jmath \in \{1, \cdots, Q\}$ where $\mathbf{Inv}_n$ denotes invertible matrices in $\mathbf{Z}_q^{n\times n}$. If the condition does not hold, the challenger outputs a random bit $b \in \{0,1\}$, namely we say the challenger aborts the game.

Note that $\mathcal{A}$ never sees the random hash functions $\mathcal{H}_{\mathrm{ABB}}^1$ and $\mathcal{H}_{\mathrm{ABB}}^2$, and has no idea if an abort event took place. While it is convenient to describe the abort action at the end of the game, nothing would change if the challenger aborts the game as soon as the abort condition becomes true.

$\mathbf{Game_2}$: This game is as same as $\mathbf{Game_1}$ except that we slightly change the way that the challenger generates the matrices $\mathbf{A}_i^1, \mathbf{A}_i^1$ for $i \in \{1, \cdots, n\}$. Taking t as $t = \lceil \log_q 2Q/\epsilon \rceil$, we thus have $q^t \geq 2Q/\epsilon \geq q^{t-1}$. Assume n is a multiple of t. For $i = 1, \cdots, n$, the challenger chooses $2n$ random integer vectors $\mathbf{h}_i^1, \mathbf{h}_i^2 \in \mathbb{Z}_q^t$ and random matrices $\mathbf{R}_i^1, \mathbf{R}_i^2 \in \{-1,1\}^{m\times m}$. Then it sets $\mathbf{A}_i^1 = \mathbf{A}\mathbf{R}_i^1 + (\mathcal{H}_{t,q}(\mathbf{h}_i^1) \otimes \mathbf{I}_{n/t}) \cdot \mathbf{G}, \mathbf{A}_i^2 = \mathbf{A}\mathbf{R}_i^2 + (\mathcal{H}_{t,q}(\mathbf{h}_i^2) \otimes \mathbf{I}_{n/t}) \cdot \mathbf{G}$.

$\mathbf{Game_3}$: This game is identical to $\mathbf{Game}_2$ except that the challenger chooses a random matrix $\mathbf{A}$ instead of running $\mathsf{TrapGen}$ and responds to private key queries by involving the algorithm $\mathsf{SampleRight}$ instead of $\mathsf{SampleLeft}$. To respond to a private key query for $\mathbf{id}_{1st}, \mathbf{id}_{2nd}$, the challenger needs short vectors $(\mathbf{E}_{\mathbf{id}_1})_i \in \wedge_q^{(\mathbf{U})_i}([\mathbf{A}|\mathbf{A}_{\mathbf{id}_1}])$ and $(\mathbf{E}_{\mathbf{id}_2})_i \in \wedge_q^{(\mathbf{U})_i}([\mathbf{A}|\mathbf{A}_{\mathbf{id}_2}])$, where

$$\mathbf{A}_{\mathbf{id}_1} = \sum_{i=1}^{n} (\mathbf{id}_{1st})_i \cdot \mathbf{A}_i^1 + \mathbf{G} = \mathbf{A}\left(\sum_{i=1}^{n} (\mathbf{id}_{1st})_i \cdot \mathbf{R}_i^1\right) + \mathcal{H}_{\mathrm{ABB}}^1(\mathbf{id}_{1st}) \cdot \mathbf{G};$$

$$\mathbf{A}_{\mathbf{id}_2} = \sum_{i=1}^{n} (\mathbf{id}_{2nd})_i \cdot \mathbf{A}_i^2 + \mathbf{G} = \mathbf{A}\left(\sum_{i=1}^{n} (\mathbf{id}_{2nd})_i \cdot \mathbf{R}_i^2\right) + \mathcal{H}_{\mathrm{ABB}}^2(\mathbf{id}_{2nd}) \cdot \mathbf{G}.$$

If $\mathcal{H}_{\mathrm{ABB}}^1(\mathbf{id}_{1st}) \notin \mathbf{Inv}_n$ or $\mathcal{H}_{\mathrm{ABB}}^2(\mathbf{id}_{2nd}) \notin \mathbf{Inv}_n$, the challenger aborts this game and returns a random bit. Otherwise, the challenger responds the pri-

vate key query by running

$$\mathsf{SampleRight}(\mathbf{A},\mathbf{G},\sum_{i=1}^{n}(\mathbf{id}_{1st})_i\,\mathbf{R}_i^1,\mathcal{H}^1_{\mathrm{ABB}}(\mathbf{id}_{1st}),(\mathbf{U})_i,\mathbf{T}_{\mathbf{G}},\sigma),\ \text{to get}\ \mathbf{E}_{\mathbf{id}_1},$$

$$\mathsf{SampleRight}(\mathbf{A},\mathbf{G},\sum_{i=1}^{n}(\mathbf{id}_{2nd})_i\,\mathbf{R}_i^2,\mathcal{H}^2_{\mathrm{ABB}}(\mathbf{id}_{2nd}),(\mathbf{U})_i,\mathbf{T}_{\mathbf{G}},\sigma),\ \text{to get}\ \mathbf{E}_{\mathbf{id}_2},$$

for $i \in \{1,\cdots,n\}$. Since $\mathcal{H}^1_{\mathrm{ABB}}(\mathbf{id}^\star_{1st}) = \mathbf{0}, \mathcal{H}^2_{\mathrm{ABB}}(\mathbf{id}^\star_{2nd}) = \mathbf{0}$, it holds:

$$\mathbf{c}_0^\star = \mathbf{U}^\top\mathbf{s} + \widetilde{\mathbf{e}}_0 + \left\lceil\frac{q}{2}\right\rceil\cdot\mathbf{m}_b, \mathbf{c}_1^\star = \begin{bmatrix}\mathbf{A}^\top\mathbf{s}+\mathbf{e}_{\mathbf{1},\mathbf{1}}\\ \left(\sum_{i=1}^n(\mathbf{id}^\star_{1st})_i\cdot\mathbf{R}_i^1\right)^\top\mathbf{A}^\top\mathbf{s}+\mathbf{e}_{\mathbf{1},\mathbf{2}}\\ \left(\sum_{i=1}^n(\mathbf{id}^\star_{2nd})_i\cdot\mathbf{R}_i^2\right)^\top\mathbf{A}^\top\mathbf{s}+\mathbf{e}_{\mathbf{1},\mathbf{2}}\end{bmatrix},$$

where $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}, \mathbf{e}_{\mathbf{1},\mathbf{1}}, \mathbf{e}_{\mathbf{1},\mathbf{2}}, \mathbf{e}_{\mathbf{1},\mathbf{3}} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$.

Game$_4$: In this game, the challenge ciphertext is generated as follows: it chooses $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n, \widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}, \widetilde{\mathbf{e}}_1 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$ and sets $\mathbf{w} = \mathbf{U}^\top\mathbf{s} + \widetilde{\mathbf{e}}_0, \mathbf{b} = \mathbf{A}^\top\mathbf{s} + \widetilde{\mathbf{e}}_1$. Then, it computes

$$\mathbf{c}_0^\star = \mathbf{w} + \left\lceil\frac{q}{2}\right\rceil\cdot\mathbf{m}_b, \mathbf{c}_1^\star = \mathsf{ReRand}\left(\begin{bmatrix}\mathbf{I}_m\\ \left(\sum_{i=1}^n(\mathbf{id}^\star_{1st})_i\cdot\mathbf{R}_i^1\right)^\top\\ \left(\sum_{i=1}^n(\mathbf{id}^\star_{2nd})_i\cdot\mathbf{R}_i^2\right)^\top\end{bmatrix}, \mathbf{b}, \alpha q, \frac{\alpha' q}{2\alpha q}\right).$$

Game$_5$: In this game, the challenge ciphertext is generated as follows: it first picks random vectors $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^n, \widetilde{\mathbf{b}} \xleftarrow{\$} \mathbb{Z}_q^m, \widetilde{\mathbf{e}}_1 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$ and sets $\mathbf{b} = \widetilde{\mathbf{b}} + \widetilde{\mathbf{e}}_1$. Then, it computes

$$\mathbf{c}_0^\star = \mathbf{w} + \left\lceil\frac{q}{2}\right\rceil\cdot\mathbf{m}_b, \mathbf{c}_1^\star = \mathsf{ReRand}\left(\begin{bmatrix}\mathbf{I}_m\\ \left(\sum_{i=1}^n(\mathbf{id}^\star_{1st})_i\cdot\mathbf{R}_i^1\right)^\top\\ \left(\sum_{i=1}^n(\mathbf{id}^\star_{2nd})_i\cdot\mathbf{R}_i^2\right)^\top\end{bmatrix}, \mathbf{b}, \alpha q, \frac{\alpha' q}{2\alpha q}\right).$$

Game$_6$: In this game, the challenge ciphertext is generated as follows: it first picks $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^n, \widetilde{\mathbf{b}} \xleftarrow{\$} \mathbb{Z}_q^m$ and $\mathbf{e}_{1,1}, \mathbf{e}_{1,2}, \mathbf{e}_{1,3} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$ and computes

$$\mathbf{c}_0^\star = \mathbf{w} + \left\lceil\frac{q}{2}\right\rceil\cdot\mathbf{m}_b, \mathbf{c}_1^\star = \begin{bmatrix}\widetilde{\mathbf{b}}+\mathbf{e}_{1,1}\\ (\sum_{i=1}^n(\mathbf{id}^\star_{1st})_i\cdot\mathbf{R}_i^1)^\top\widetilde{\mathbf{b}}+\mathbf{e}_{1,2}\\ (\sum_{i=1}^n(\mathbf{id}^\star_{2nd})_i\cdot\mathbf{R}_i^2)^\top\widetilde{\mathbf{b}}+\mathbf{e}_{1,3}\end{bmatrix}.$$

Analysis of Games. We use the following lemmas to give a analysis between each adjacent games.

The only difference between **Game$_1$** and **Game$_0$** is the abort event. We use Lemma 28 in [1] to argue that the adversary still has a non-negligible advantage in **Game$_1$** even though the abort event happens.

Lemma 6 ([1]). *Let I^* be a $(Q+1)$-ID tuple $\{id^*, \{id_j\}_{j\in[Q]}\}$ denoted the challenge ID along with the queried ID's, and $\eta(I^*)$ be the probability that an abort event does not happen in* $\mathbf{Game_1}$. *Let $\eta_{max} = \max\ \eta(I^*)$ and $\eta_{min} = \min\ \eta(I^*)$. For $i = 0, 1$, we let X_i be the event that the challenger returns 1 as the output of* $\mathbf{Game}_i$. *Then, we have*

$$\left|\Pr[X_1] - \frac{1}{2}\right| \geq \eta_{min}\left|\Pr[X_0] - \frac{1}{2}\right| - \frac{1}{2}(\eta_{max} - \eta_{min}).$$

Lemma 7. *Let $\epsilon = \left|\Pr[X_0] - \frac{1}{2}\right|$, then $\left|\Pr[X_1] - \frac{1}{2}\right| \geq \frac{\epsilon^3}{64q^2Q^2}$.*

Proof. As the selections of $\mathbf{h}_i^1, \mathbf{h}_i^2$ are independent, then according to Lemma 1 we have

$$\begin{aligned}
&\Pr\left[\mathcal{H}^1_{\mathrm{ABB}}(id_1^\star) = \mathbf{0}, \mathcal{H}^1_{\mathrm{ABB}}(id_i) \in \mathbf{Inv}_n \wedge \mathcal{H}^2_{\mathrm{ABB}}(id_2^\star) = \mathbf{0}, \mathcal{H}^2_{\mathrm{ABB}}(id_i) \in \mathbf{Inv}_n\right] \\
=&\Pr\left[\mathcal{H}^1_{\mathrm{ABB}}(id_1^\star) = \mathbf{0}, \mathcal{H}^1_{\mathrm{ABB}}(id_i) \in \mathbf{Inv}_n\right] \cdot \Pr\left[\mathcal{H}^2_{\mathrm{ABB}}(id_2^\star) = \mathbf{0}, \mathcal{H}^2_{\mathrm{ABB}}(id_i) \in \mathbf{Inv}_n\right] \\
\in&\left(\frac{1}{q^{2t}}(1 - \frac{Q}{q^t})^2, \frac{1}{q^{2t}}\right).
\end{aligned}$$

Since $t = \lceil \log_q 2Q/\epsilon \rceil$, we have $q^t \geq 2Q/\epsilon \geq q^{t-1}$, $\frac{1}{q^t} \geq \frac{\epsilon}{2qQ}$ and $Q < 0.5\epsilon q^t$. According to Lemma 6, we hence have

$$\begin{aligned}
\left|\Pr[X_1] - \frac{1}{2}\right| \geq& \eta_{min}\left|\Pr[X_0] - \frac{1}{2}\right| - \frac{1}{2}(\eta_{max} - \eta_{min}) \\
=&\frac{1}{q^{2t}}(1 - 0.5\epsilon)^2\epsilon - \frac{1}{2q^{2t}}(\epsilon - 0.25\epsilon^2) \qquad (1)\\
\geq&\frac{9\epsilon}{16q^{2t}} - \frac{\epsilon}{2q^{2t}} \geq \frac{\epsilon}{16q^{2t}} \geq \frac{\epsilon^3}{64q^2Q^2}.
\end{aligned}$$

□

Lemma 8. $\mathbf{Game_1}$ *and* $\mathbf{Game_2}$ *are statistically indistinguishable.*

Proof. We show that $\mathbf{Game_2}$ is statistically close to $\mathbf{Game_1}$ using Leftover Hash Lemma (Lemma 12, item 4). Note that the only difference between the two games is how the matrices $\mathbf{A}_i^1, \mathbf{A}_i^2$ were generated. According to Leftover Hash Lemma,

$$\left(\mathbf{A}, \{\mathbf{A}_i^1\}, \{\mathbf{A}_i^2\}\right) \approx \left(\mathbf{A}, \{\mathbf{AR}_i^1\}, \{\mathbf{AR}_i^2\}\right),$$

where $\mathbf{A}_i^1, \mathbf{A}_i^2 \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$. Then, we have

$$\left(\mathbf{A}, \left\{\mathbf{A}_i^1\right\}, \left\{\mathbf{A}_i^2\right\}\right) \approx \left(\mathbf{A}, \left\{\mathbf{AR}_i^1 + \mathcal{H}_{t,q}(\mathbf{h}_i^1) \otimes \mathbf{I}_{n/t} \cdot \mathbf{G}\right\}, \left\{\mathbf{AR}_i^2 + \mathcal{H}_{t,q}(\mathbf{h}_i^2) \otimes \mathbf{I}_{n/t} \cdot \mathbf{G}\right\}\right).$$

Therefore, $\mathbf{Game_1}$ and $\mathbf{Game_2}$ are statistically indistinguishable. □

Lemma 9. $\mathbf{Game_2}$ *and* $\mathbf{Game_3}$ *are statistically indistinguishable.*

Proof. We prove that $\mathbf{Game_2}$ and $\mathbf{Game_3}$ are statistically indistinguishable by using Lemma 12, items $1, 2, 3$. Note that in $\mathbf{Game_2}$, the matrix $\mathbf{A}$ is generated by using algorithm $\mathsf{TrapGen}$, and secret key queries are answered by using $\mathsf{SampleLeft}$. While in $\mathbf{Game_3}$, the matrix $\mathbf{A}$ is generated by uniformly selecting from $\mathbb{Z}_q^{n\times m}$, and secret key queries are answered by using $\mathsf{SampleRgiht}$.

According to Lemma 12, item 1, $\mathbf{A}$ is statistically close to an uniform distribution over $\mathbb{Z}_q^{n\times m}$ as in $\mathbf{Game_3}$. As we set Gaussian parameter σ in subsection 4.1, the output of $\mathsf{SampleRgiht}$ is identically distributed to the output of $\mathsf{SampleLeft}$ according to Lemma 12, items 2 and 3. Therefore, $\mathbf{Game_2}$ and $\mathbf{Game_3}$ are statistically indistinguishable. □

Lemma 10. $\mathbf{Game_3}$ *and* $\mathbf{Game_4}$ *are identically distributed, and* $\mathbf{Game_5}$ *and* $\mathbf{Game_6}$ *are identically distributed.*

Proof. This lemma can be proved just according to the property of Rand. □

Lemma 11. *Assume the* $\mathrm{DLWE}_{q,n,n+m,\alpha}$ *assumption holds,* $\mathbf{Game_4}$ *and* $\mathbf{Game_5}$ *are computationally indistinguishable.*

Proof. Suppose there exists an adversary $\mathcal{A}$ who has a non-negligible advantage in distinguishing $\mathbf{Game_4}$ and $\mathbf{Game_5}$, then we can construct an adversary $\mathcal{B}$ who can break the LWE assumption as follows.

Instance. Based on the given LWE instance $(\mathbf{U}, \mathbf{A}, \mathbf{w}, \mathbf{b}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n \times \mathbb{Z}_q^m$ and assume $\mathbf{w} = \widetilde{\mathbf{w}} + \widetilde{\mathbf{e}}_0$ and $\mathbf{b} = \widetilde{\mathbf{b}} + \widetilde{\mathbf{e}}_1$ where $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}, \widetilde{\mathbf{e}}_1 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$. Then $\mathcal{B}$ should distinguish whether $\widetilde{\mathbf{w}} = \mathbf{U}^\top \mathbf{s}, \widetilde{\mathbf{b}} = \mathbf{A}^\top \mathbf{s}$ for some $\mathbf{s} \in \mathbb{Z}_q^n$ or $\widetilde{\mathbf{w}} \xleftarrow{\$} \mathbb{Z}_q^n, \widetilde{\mathbf{b}} \xleftarrow{\$} \mathbb{Z}_q^m$. We note this subtle change from the standard LWE problem is done only for the convenience of the proof.

Setup. The $\mathcal{B}$ constructs $\{\mathbf{A}_i^1, \mathbf{A}_i^2\}$ for $i \in \{1, \cdots, \ell\}$ as in $\mathbf{Game}_3$. Then it sets $PP = (\mathbf{A}, \mathbf{A}_i^1, \mathbf{A}_i^2, \mathbf{U})$.

Queries. The $\mathcal{B}$ answers identity queries as in $\mathbf{Game}_3$ including aborting the simulation if needed.

Challenge ciphertext. When $\mathcal{A}$ sends identities $(id_1^\star, id_2^\star)$ and message (m_0, m_1), the reduction $\mathcal{B}$ computes the challenge ciphertext as follows

$$\mathbf{c}_0^\star = \mathbf{w} + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} \in \mathbb{Z}_q, \mathbf{c}_1^\star = \mathsf{ReRand}\left(\begin{bmatrix} \mathbf{I}_m \\ (\sum_{i=1}^{\ell} (id_1^\star)_i \mathbf{R}_i^1)^\top \\ (\sum_{i=1}^{\ell} (id_2^\star)_i \mathbf{R}_i^2)^\top \end{bmatrix}, \mathbf{b}, \alpha q, \frac{\alpha' q}{2\alpha q} \right) \in \mathbb{Z}_q^{3m}.$$

Guess. After being allowed to make additional queries, $\mathcal{A}$ guesses if it interacts with a challenger of $\mathbf{Game}_4$ or $\mathbf{Game}_5$.

It can be easily seen that if $(\mathbf{U}, \mathbf{A}, \mathbf{w}, \mathbf{b})$ is a valid LWE sample, the view of $\mathcal{A}$ corresponds to $\mathbf{Game}_4$; otherwise, the view of $\mathcal{A}$ corresponds to that of $\mathbf{Game}_5$. We complete the proof of this lemma. □

Complete the Proof of Theorem 2. It is obvious that $\Pr[X_6] = \frac{1}{2}$, this is because the challenge bit b is independent of the $\mathcal{A}$'s view. From Lemma 7 to Lemma 10, we know that

$$\Pr[X_1] \approx \Pr[X_2], \Pr[X_2] \approx \Pr[X_3], \Pr[X_3] = \Pr[X_4], \Pr[X_5] = \Pr[X_6]. \quad (2)$$

From Lemma 11, we know that

$$|\Pr[X_4] - \Pr[X_5]| = \left|\Pr[X_4] - \frac{1}{2}\right| \leq \mathrm{DLWE}_{q,n,n+m,\alpha},$$

which implies $\mathrm{DLWE}_{q,n,n+m,\alpha} \geq \frac{\epsilon^3}{64q^2Q^2} - \mathsf{negl}(\lambda)$, according to Equations 1 and 2. □□

4.3 Extension: IB-DRE with More Compact Parameters.

As mentioned above, our IB-DRE scheme is based on the beautiful work of Agrawal, Boneh and Boyen [1], i.e., an adaptively secure identity-based encryption (IBE) scheme. However, one drawback of Agarwal et al.'s adaptive secure IBE scheme [1] is the large public parameter sizes: namely, the public parameters contain $\ell + 1$ matrices composed of $n \times m$ elements, where ℓ is the size of the bit-string representing identities. As a result, the public parameters in our IB-DRE scheme contain $2 \cdot \ell + 1$ matrices composed of $n \times m$ elements.

In [19], Singh, Pandurangan and Banerjee considered identities as one chunk rather than bit-by-bit. In fact, the maximum of the above chunk is a number in $\mathbb{Z}_q$, so that they can reduce the number of the matrices in the scheme by a factor at most $\log q$, while encryption and decryption are almost as efficient as that in [1]. Applying their technique (they called "Blocking Technique") to our construction, we can get an IB-DRE scheme with more compact public parameter sizes. More precisely, we can get a more efficient IB-DRE scheme in which there exist only $2 \cdot \frac{\ell}{\log q} + 1$ matrices composed of $n \times m$ elements, or about $\mathcal{O}(\frac{n}{\log n})$ matrices (since $l = n$ and q is a polynomial of n).

Based the IBE schemes in [1, 19], Apon, Fan and Liu [4] proposed an identity-based encryption scheme which only needs $\mathcal{O}(\frac{n}{\log^2 n})$ public matrices to support n-bit length identity. The reason why the number of the matrices in their scheme is less about $\log n$ times than that of the IBE scheme in [19] is that they used a different gadget matrix $\widehat{\mathbf{G}}$ and flattening function $\widehat{\mathbf{G}}^{-1}$ in logarithmic ($\log n$) base instead of the usual gadget matrix $\mathbf{G}$ and flattening function $\mathbf{G}^{-1}$ in 2 base. Note that the encryption and decryption of the IBE scheme in [4] are less efficient than that in [1, 19], this is because the flattening function $\widehat{\mathbf{G}}^{-1}$ is much slower than $\mathbf{G}^{-1}$. Applying their technique to our construction, we can get a more efficient IB-DRE scheme in which there exist about $\mathcal{O}(\frac{n}{\log^2 n})$ matrices.

Overall, we can further obtain more compact IB-DRE schemes from the IBE schemes in [19, 4].

5 Conclusion

The learning with errors (LWE) problem is a promising cryptographic primitive that is believed to be resistant to attacks by quantum computers. Under this assumption, we construct a dual-receiver encryption scheme with a CCA security. Additionally, for the DRE notion in the identity-based setting, namely IB-DRE, we also give a lattice-based IB-DRE scheme that achieves IND-ID-CPA security.

6 Acknowledgments

We thank the anonymous ACISP'2018 reviewers for their helpful comments. This work is supported by the National Natural Science Foundation of China (No.61772515, No.61602473, No.61571191), the National Basic Research Program of China (973 project, No.2014CB340603), the National Cryptography Development Fund (No. MMJJ20170116), the Dawn Program of Shanghai Education Commission (No. 16SG21) and the Open Foundation of Co-Innovation Center for Information Supply & Assurance Technology (No. ADXXBZ201701).

References

1. S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *EUROCRYPT 2010*, pages 553–572, 2010.
2. M. Ajtai. Generating hard instances of the short basis problem. In *ICALP 1999*, pages 1–9, 1999.
3. J. Alwen and C. Peikert. Generating shorter bases for hard random lattices. In *STACS 2009*, pages 75–86, 2009.
4. D. Apon, X. Fan, and F. Liu. Compact identity based encryption from lwe. *IACR Cryptology ePrint Archive*, 2016:125, 2016.
5. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In *EUROCRYPT 2010*, pages 523–552, 2010.
6. S. S. M. Chow, M. K. Franklin, and H. Zhang. Practical dual-receiver encryption - soundness, complete non-malleability, and applications. In *CT-RSA 2014*, pages 85–105, 2014.
7. R. Cramer and I. Damgård. On the amortized complexity of zero-knowledge protocols. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, pages 177–191, 2009.
8. T. Diament, H. K. Lee, A. D. Keromytis, and M. Yung. The dual receiver cryptosystem and its applications. In *CCS 2004*, pages 330–343, 2004.
9. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.
10. A. Georgescu. Anonymous lattice-based broadcast encryption. In *Information and Communicatiaon Technology - International Conference, ICT-EurAsia 2013*, pages 353–362, 2013.
11. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT 2008*, pages 415–432, 2008.

12. A. Joux. A one round protocol for tripartite diffie-hellman. In *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*, pages 385–394, 2000.
13. S. Katsumata and S. Yamada. Partitioning via non-linear polynomial functions: More compact ibes from ideal lattices and bilinear maps. In *ASIACRYPT 2016*, pages 682–712, 2016.
14. E. Kiltz. Chosen-ciphertext security from tag-based encryption. In *TCC 2006*, pages 581–600, 2006.
15. B. Libert, K. G. Paterson, and E. A. Quaglia. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, pages 206–224, 2012.
16. M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC 1990*, pages 427–437, 1990.
17. C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In *STOC 2008*, pages 187–196, 2008.
18. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC 2005*, pages 84–93, 2005.
19. K. Singh, C. P. Rangan, and A. K. Banerjee. Adaptively secure efficient lattice (H)IBE in standard model with short public parameters. In *SPACE 2012*, pages 153–172, 2012.
20. F. Wang, X. A. Wang, and C. Wang. Lattice-based dynamical and anonymous broadcast encryption scheme for wireless ad hoc networks. *Journal of Interconnection Networks*, 15(3-4):1–14, 2015.
21. J. Wang and J. Bi. Lattice-based identity-based broadcast encryption scheme. *IACR Cryptology ePrint Archive*, 2010:288, 2010.
22. B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT 2005*, pages 114–127, 2005.
23. Y. Youn and A. Smith. An efficient construction of dual-receiver encryption. *unpublished*, 2008.
24. K. Zhang, W. Chen, X. Li, J. Chen, and H. Qian. New application of partitioning methodology: identity-based dual receiver encryption. *Security and Communication Networks*, 9(18):5789–5802, 2016.

Appendix A: Lattice Background

For positive integers q, n, m, and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the m-dimensional integer lattices are defined as: $\Lambda_q(\mathbf{A}) = \{\mathbf{y} : \mathbf{y} = \mathbf{A}^\top \mathbf{s} \text{ for some } \mathbf{s} \in \mathbb{Z}^n\}$ and $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{y} : \mathbf{A}\mathbf{y} = \mathbf{0} \mod q\}$.

Let $\mathbf{S}$ be a set of vectors $\mathbf{S} = \{\mathbf{s}_1, \cdots, \mathbf{s}_n\}$ in $\mathbb{R}^m$. We use $\widetilde{\mathbf{S}} = \{\widetilde{\mathbf{s}}_1, \cdots, \widetilde{\mathbf{s}}_n\}$ to denote the Gram-Schmidt orthogonalization of the vectors $\mathbf{s}_1, \cdots, \mathbf{s}_n$ in that order, and $\|\mathbf{S}\|$ to denote the length of the longest vector in $\mathbf{S}$. For a real-valued matrix $\mathbf{R}$, let $s_1(\mathbf{R}) = \max_{\|\mathbf{u}\|=1} \|\mathbf{R}\mathbf{u}\|$ (respectively, $\|\mathbf{R}\|_\infty = \max \|\mathbf{r}_i\|_\infty$) denote the operator norm (respectively, infinity norm) of $\mathbf{R}$.

For $\mathbf{x} \in \Lambda$, define the Gaussian function $\rho_{s,\mathbf{c}}(\mathbf{x})$ over $\Lambda \subseteq \mathbb{Z}^m$ centered at $\mathbf{c} \in \mathbb{R}^m$ with parameter $s > 0$ as $\rho_{s,\mathbf{c}}(\mathbf{x}) = \exp(-\pi||\mathbf{x} - \mathbf{c}||/s^2)$. Let $\rho_{s,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in\Lambda} \rho_{s,\mathbf{c}}(\mathbf{x})$, and define the discrete Gaussian distribution over Λ as $\mathcal{D}_{\Lambda,s,\mathbf{c}}(\mathbf{x}) =$

$\frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}$, where $\mathbf{x} \in \Lambda$. For simplicity, $\rho_{s,\mathbf{0}}$ and $\mathcal{D}_{\Lambda,s,\mathbf{0}}$ are abbreviated as ρ_s and $\mathcal{D}_{\Lambda,s}$, respectively.

Learning with Errors Assumption. The learning with errors problem, denoted by $\mathrm{LWE}_{q,n,m,\alpha}$, was first proposed by Regev [18]. For integer $n, m = m(n)$, a prime integer $q > 2$, an error rate $\alpha \in (0,1)$, the LWE problem $\mathrm{LWE}_{q,n,m,\alpha}$ is to distinguish the following pairs of distributions: $\{\mathbf{A}, \mathbf{A}^\top\mathbf{s} + \mathbf{e}\}$ and $\{\mathbf{A}, \mathbf{u}\}$, where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n, \mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m$ and $\mathbf{e} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$. Regev [18] showed that solving decisional $\mathrm{LWE}_{q,n,m,\alpha}$ (denoted by $\mathrm{DLWE}_{q,n,m,\alpha}$) for $\alpha q > 2\sqrt{2n}$ is (quantumly) as hard as approximating the SIVP and GapSVP problems to within $\widetilde{\mathcal{O}}(n/\alpha)$ factors in the worst case.

Lemma 12. *Let p, q, n, m be positive integers with $q \geq p \geq 2$ and q prime. There exists PPT algorithms such that*

- *([2, 3]):* $\mathsf{TrapGen}(1^n, 1^m, q)$ *a randomized algorithm that, when $m \geq 6n\lceil \log q \rceil$, outputs a pair $(\mathbf{A}, \mathbf{T_A}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}^{m\times m}$ such that $\mathbf{A}$ is statistically close to uniform in $\mathbb{Z}_q^{n\times m}$ and $\mathbf{T_A}$ is a basis of $\Lambda_q^\perp(\mathbf{A})$, satisfying $\|\widetilde{\mathbf{T_A}}\| \leq \mathcal{O}(\sqrt{n \log q})$ with overwhelming probability.*
- *([5]):* $\mathsf{SampleLeft}(\mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{T_A}, \sigma)$ *a randomized algorithm that, given a full rank matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$, a basis $\mathbf{T_A}$ of $\Lambda_q^\perp(\mathbf{A})$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$ and $\sigma \geq \|\widetilde{\mathbf{T_A}}\| \cdot \omega(\sqrt{\log m})$, then outputs a vector $\mathbf{r} \in \mathbb{Z}_q^{2m}$ distributed statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{F}),\sigma}$ where $\mathbf{F} = [\mathbf{A}|\mathbf{B}]$.*
- *([1]):* $\mathsf{SampleRight}(\mathbf{A}, \mathbf{G}, \mathbf{R}, \mathbf{S}, \mathbf{u}, \mathbf{T_G}, \sigma)$ *a randomized algorithm that, given a full rank matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a matrix $\mathbf{R} \in \mathbb{Z}_q^{m\times m}$, an invertible matrix $\mathbf{S} \in \mathbb{Z}_q^{n\times n}$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$ and $\sigma \geq \|\widetilde{\mathbf{T_G}}\| \cdot s_1(\mathbf{R}) \cdot \omega(\sqrt{\log m})$, then it outputs a vector $\mathbf{r} \in \mathbb{Z}_q^{2m}$ statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{F}),\sigma}$ where $\mathbf{F} = [\mathbf{A}|\mathbf{AR} + \mathbf{SG}]$.*
- *(Generalized Leftover Hash Lemma [1, 9]): For $m > (n+1)\log q + \omega(\log n)$ and prime $q > 2$, let $\mathbf{R} \xleftarrow{\$} \{-1, 1\}^{m\times k}$ and $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}, \mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{n\times k}$ be uniformly random matrices. Then the distribution $(\mathbf{A}, \mathbf{AR}, \mathbf{R}^\top\mathbf{w})$ is $\mathsf{negl}(n)$-close to the distribution $(\mathbf{A}, \mathbf{B}, \mathbf{R}^\top\mathbf{w})$ for all vector $\mathbf{w} \in \mathbb{Z}_q^m$. When $\mathbf{w}$ is always $\mathbf{0}$, this lemma is called Leftover Hash Lemma.*

In [13], Katsuamta and Yamada introduced the "Noise Rerandomization" lemma which plays an important role in the security proof because of creating a well distributed challenge ciphertext.

Lemma 13 (Noise Rerandomization [13]). *Let q, w, m be positive integers and r a positive real number with $r > \max\{\omega(\sqrt{\log m}), \omega(\sqrt{\log w})\}$. For arbitrary column vector $\mathbf{b} \in \mathbb{Z}_q^m$, vector $\mathbf{e}$ chosen from $\mathcal{D}_{\mathbb{Z}^m,r}$, any matrix $\mathbf{V} \in \mathbb{Z}^{w\times m}$ and positive real number $\sigma > s_1(\mathbf{V})$, there exists a PPT algorithm $\mathsf{ReRand}(\mathbf{V}, \mathbf{b} + \mathbf{e}, r, \sigma)$ that outputs $\mathbf{b}' = \mathbf{Vb} + \mathbf{e}' \in \mathbb{Z}^w$ where $\mathbf{e}'$ is distributed statistically close to $\mathcal{D}_{\mathbb{Z}^w,2r\sigma}$.*

Appendix B: Signature

Definition 1 (Signature Scheme). *A signature scheme is a triple of probabilistic polynomial-time algorithms as follows:*

- $\mathsf{Gen}(1^\lambda)$ *outputs a verification key* vk *and a signing key* sk.
- $\mathsf{Sign}(sk, \mu)$, *given* sk *and a message* $\mu \in \{0,1\}^\star$, *outputs a signature* $\sigma \in \{0,1\}^\star$.
- $\mathsf{Ver}(vk, \mu, \sigma)$ *either accepts or rejects the signature* σ *for message* μ.

The correctness requirement is: for any message $\mu \in \mathcal{M}$, and for $(vk, sk) \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$, $\sigma \xleftarrow{\$} \mathsf{Sign}(sk; \mu)$, $\mathsf{Ver}(vk, \mu, \sigma)$ should accept with overwhelming probability (over all the randomness of the experiment).

The notion of security that we require for our IND-CCA DRE construction is strong existential unforgeability under a one-time chosen-message attack. The attack is defined as follows: generate $(vk, sk) \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$ and give vk to the adversary $\mathcal{A}$, then $\mathcal{A}$ outputs a message μ. Generate $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, \mu)$ and give σ to $\mathcal{A}$. The advantage of $\mathcal{A}$ in the attack is the probability that it outputs some $(\mu^\star, \sigma^\star) \neq (\mu, \sigma)$ such that $\mathsf{Ver}(vk, \mu^\star, \sigma^\star)$ accepts. We say that the signature scheme is secure if for every PPT adversary $\mathcal{A}$, its advantage in the attack is $\mathsf{negl}(\lambda)$.