Liu *et al. Cybersecurity* (2019) 2:18
https://doi.org/10.1186/s42400-019-0034-y

Cybersecurity

RESEARCH Open Access

(Identity-based) dual receiver encryption from lattice-based programmable hash functions with high min-entropy

Yanyan Liu[1,2*], Daode Zhang[1,2], Yi Deng[1,2] and Bao Li[1,2]

Abstract

Dual receiver encryption (DRE) is an important cryptographic primitive introduced by Diament et al. at CCS'04, which allows two independent receivers to decrypt a same ciphertext to obtain the same plaintext. This primitive is quite useful in designing combined public key cryptosystems and denial of service attack-resilient protocols. In this paper, we obtain some results as follows.

- Using weak lattice-based programmable hash functions (wLPHF) with high min-entropy (Crypto'16), we give a generic IND-CCA secure DRE construction in the standard model. Furthermore, we get a concrete DRE scheme by instantiating a concrete wLPHF with high min-entropy.
- For DRE notion in the identity-based setting, identity-based DRE (IB-DRE), basing on lattice-based programmable hash functions (LPHF) with high min-entropy, we give a framework of IND-ID-CPA secure IB-DRE construction in the standard model. When instantiating with concrete LPHFs with high min-entropy, we obtain five concrete IB-DRE schemes.

Keywords: Dual receiver encryption, Identity-based dual receiver encryption, Lattice-based programmable hash functions with high min-entropy

Introduction

Dual receiver encryption, which was proposed by Diament, Lee, Keromytis and Yung (Diament et al. 2004), is a special kind of public-key encryption which allows two independent users to decrypt a ciphertext to obtain the same plaintext by using their own secret keys. 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. This primitive is quite useful in designing combined public key cryptosystems and denial of service attack-resilient protocols. Ten years later, S. Chow, Franklin and Zhang (Chow et al. 2014) refined the notion of DRE and appended some appealing features for DRE. Zhang et al. (2016a) extended the DRE in public-key setting to the identity-based setting: identity-based dual receiver encryption (IB-DRE), so as to handle the difficulty of certificate management.

Many constructions from pairings and lattices have been emerged since the notions of DRE and IB-DRE was proposed.

Constructions from pairings. In Diament et al. (2004), presented the first DRE scheme by transforming the three-party one-round Diffie-Hellman key exchange scheme by Joux (2000), and also proved that it is indistinguishable secure against chosen ciphertext attacks. However, their scheme relied on the existence of random oracle heuristic, where a DRE that proven to be secure in the random oracle model (ROM) may turn into insecure one when the RO is instantiated by an actual hash function in practice. Hence, (Youn and Smith: An efficent construction of dual-receiver encryption, unpublished) began with attempting to give a provably secure DRE scheme in the standard

*Correspondence: liuyanyan@iie.ac.cn
[1]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

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 (Chow et al. 2014) 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 Kiltz (2006)) and a strong one-time signature scheme, as well as other DRE instantiations for non-malleable and other properties [1]. Recently, Zhang et al. (2016a) 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 (Waters 2005).

Constructions from lattices. As studied in (Chow et al. 2014; Zhang et al. 2016a), the DRE or IB-DRE can be viewed as a special instance of 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 (2013) constructed a tag-based anonymous hint system (Libert et al. 2012) 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 Libert et al. (2012). Wang et al. (2015) 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 (2010) proposed an adaptively secure IBBE scheme in the ROM, under the LWE assumption.

Our Contributions. In this paper, we pay attention to using lattice-based programmable hash function to construct the DRE and IB-DRE on lattices. Our schemes are constructed in the standard model and satisfy chosen-ciphertext or chosen-plaintext security based on the hardness of the Learning With Errors (LWE) problem. Specifically, our works are stated as follows.

- We give a generic DRE construction from weak lattice-based programmable hash functions (wLPHF) with high min-entropy which defined in Zhang et al. (2016b). The construction is indistinguishable against chosen-ciphertext attacks (IND-CCA) in the standard model. When instantiating with a wLPHF with high min-entropy, we get a concrete DRE scheme. We also compare our DRE scheme with the existing lattice-based DRE schemes. Please see more details in Table 1.
- We also give a framework of IB-DRE from lattice-based programmable hash functions (LPHF) with high min-entropy. The construction is secure against chosen-plaintext and adaptively chosen-identity attacks (IND-ID-CPA). When instantiating with five concrete LPHFs with high min-entropy, we obtain five concrete IB-DRE schemes. The differences between our IB-DRE schemes and the existing lattice-based IB-DRE schemes are described in Table 2.

Remark 1. This work is relevant to Zhang et al. (2018b) in which we constructed DRE_{ABB} and $\text{IB-DRE}_{\text{ABB}}$ directly from the identity-based encryption scheme in Agrawal et al. (2010), and it is a concrete case of our generic construction. As our growing understanding, we find that DRE_{ABB} (or, $\text{IB-DRE}_{\text{ABB}}$) can be explained by using wLPHFs or LPHFs with high min-entropy. So, in this paper, we present a generic DRE (IB-DRE) construction from wLPHFs (LPHFs) with high min-entropy.

Preliminaries

Notations. Let λ be the security parameter, $\mathsf{poly}(\lambda)$ denotes the function $f(\lambda) = \mathcal{O}(\lambda^c)$ for some constant c and $\mathsf{negl}(\lambda)$ represents a negligible function. For positive integer $n \in \mathbb{N}$, $[n]$ represents the set $\{1, \cdots, n\}$. $\mathbb{Z}_q$ denotes the ring of integer modulo q for integer $q \geq 2$. Matrices are written as bold capital letters such as $\mathbf{A}, \mathbf{B}$, and column vectors are written as bold lowercase letters such as $\mathbf{x}, \mathbf{y}$. The transpose of the matrix $\mathbf{A}$ stands for $\mathbf{A}^\top$ and $[\mathbf{A}|\mathbf{B}]$ represents the matrix by concatenating $\mathbf{A}$ and $\mathbf{B}$. $(\mathbf{a})_i$ and $(\mathbf{A})_i$ signify i-th element of $\mathbf{a}$ and the i-th column of $\mathbf{A}$. $\mathbf{I}_n$ and $\mathbf{Inv}_n$ stand for the $n \times n$ identity matrix and the set consists of invertible matrices in $\mathbb{Z}_q^{n\times n}$, respectively.

Dual Receiver Encryption

Definition 1 (Dual receiver encryption (DRE) (Chow et al. 2014)) *A dual receiver encryption scheme* $\mathcal{DRE} = (\mathsf{CGen}_{\mathsf{DRE}}, \mathsf{Gen}_{\mathsf{DRE}}, \mathsf{Enc}_{\mathsf{DRE}}, \mathsf{Dec}_{\mathsf{DRE}})$ *is defined as follows:*

- $\mathsf{CGen}_{\mathsf{DRE}}(1^\lambda) \to \mathsf{crs}$. *The randomized common reference string (CRS) generation algorithm on input a security parameter* λ, *output a CRS* crs.
- $\mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs}) \to (pk, sk)$. *The randomized key generation algorithm on input* crs, *output a pair of public key and secret key* (pk, sk). *Run the* $\mathsf{Gen}_{\mathsf{DRE}}$ *twice independently to generate the key pairs* (pk_1, sk_1) *and* (pk_2, sk_2) *for two independent users. Without loss of generality, assume* pk_1 *and* pk_2 *are ordered based on lexicographic order.*
- $\mathsf{Enc}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, M) \to c$. *The randomized encryption algorithm takes* crs, *two public keys* pk_1 *and* pk_2 *(such that* $pk_1 <^d pk_2$*) and a message* M *as input, outputs a ciphertext* c.
- $\mathsf{Dec}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, sk_j, c) \to M$. *The deterministic decryption algorithm on input two public keys* pk_1 *and* pk_2, *one secret keys* sk_j *(*$j \in \{1, 2\}$*), and a ciphertext* c, *output a message* M *or* $\perp$.

Table 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|*	Assumption	Security	Other primitives
Geo'13† (Georgescu 2013)	–	–	–	RLWE	IND-CCA	PKE, OTS
WWW'15 (Wang et al. 2015)	1	1	1	LWE	IND-CPA	
Ours: $\mathsf{DRE}_{\mathsf{ABB}}$	1	1	4	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 know how to show the detail of |pk|, |sk| and |c| about Geo'13 scheme

Correctness. For all $\mathsf{crs} \leftarrow \mathsf{CGen}_{\mathsf{DRE}}(1^\lambda)$, all $(pk_1, sk_1) \leftarrow \mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs})$ and all $(pk_2, sk_2) \leftarrow \mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs})$, and $c \leftarrow \mathsf{Enc}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, M)$, the following holds:

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

Security. $\mathcal{DRE}$ is said to be IND-CCA secure if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, its advantage denoted as

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

is negligible in λ, where $\mathsf{Exp}^{\mathsf{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda)$ is defined in Table 3.

Identity-Based Dual Receiver Encryption

Definition 2 (Identity-based dual receiver encryption (IB-DRE) (Zhang et al. 2016a)) *An identity-based dual receiver encryption scheme $\mathcal{IB}$-$\mathcal{DRE}$ = (*$\mathsf{Setup}_{\mathsf{ID}}$, $\mathsf{KeyGen}_{\mathsf{ID}}$, $\mathsf{Enc}_{\mathsf{ID}}$, $\mathsf{Dec}_{\mathsf{ID}}$*) is defined as follows:*

- $\mathsf{Setup}_{\mathsf{ID}}(1^\lambda) \rightarrow (PP, Msk)$. *The setup algorithm on inputs a security parameter 1^λ, outputs a pair of public parameters and master secret key (PP, Msk).*
- $\mathsf{KeyGen}_{\mathsf{ID}}(PP, Msk, id_{1st}, id_{2nd} \in \mathcal{ID}) \rightarrow sk_{id_{1st}}, sk_{id_{2nd}}$. *The key generation algorithm on inputs the public parameters PP, master secret key Msk, and two identities id_{1st}, id_{2nd}, outputs $sk_{id_{1st}}$ and $sk_{id_{2nd}}$ as the secret keys for the first receiver id_{1st} and the second receiver id_{2nd}, respectively.*
- $\mathsf{Enc}_{\mathsf{ID}}(PP, id_{1st}, id_{2nd}, M) \rightarrow c$. *The encryption algorithm on inputs the public parameters PP, two identities id_{1st} and id_{2nd}, and a message M, outputs a ciphertext c.*
- $\mathsf{Dec}_{\mathsf{ID}}(PP, c, sk_{id_j}) \rightarrow M$. *The decryption algorithm on inputs the public parameters PP, a ciphertext c, and one secret key sk_{id_j}, $j \in \{1st, 2nd\}$, outputs a message M or $\perp$.*

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

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

Security. An IB-DRE scheme is said to be IND-ID-CPA secure if for any PPT adversary $\mathcal{A}$, its advantage denoted as

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

Table 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|*	Assumption	Security	Standard model ?
WB'10 (Wang and Bi 2010)	1	1	3	LWE	IND-ID-CPA	ROM
Ours:						
$\mathsf{IB-DRE}_{\mathsf{ABB}}$	$\mathcal{O}(n)$	1	3	LWE	IND-ID-CPA	✓
$\mathsf{IB-DRE}_{\mathsf{ZCZ}}$	$\mathcal{O}(\log Q)$	1	3	LWE	IND-ID-CPA	✓
$\mathsf{IB-DRE}_{\mathsf{Yam}}$	$\omega(\sqrt{n})$	1	3	LWE	IND-ID-CPA	✓
$\mathsf{IB-DRE}_{\mathsf{MAH}}$	$\omega(\log^2 n)$	1	3	LWE	IND-ID-CPA	✓
$\mathsf{IB-DRE}_{\mathsf{AFF}}$	$\omega(\log n)$	1	3	LWE	IND-ID-CPA	✓

∗, |PP|, |Msk| and |c| show the size of public parameters, master secret key and ciphertext, respectively. Q is the number bound of the secret key queries

Table 3 IND-CCA security for DRE

Experiment $\mathsf{Exp}^{\mathsf{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda)$:

$\mathsf{crs} \xleftarrow{\$} \mathsf{CGen}_{\mathsf{DRE}}(1^\lambda)$;

$(pk_j, sk_j) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs})$ for $j \in \{1,2\}$;

$(M_0, M_1, s) \xleftarrow{\$} \mathcal{A}^{\mathsf{Dec}_{\mathsf{DRE}}(sk_j,c)}(\mathsf{crs}, pk_1, pk_2)$;

$b \xleftarrow{\$} \{0,1\}, c^\star \xleftarrow{\$} \mathsf{Enc}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, M_b)$;

$b' \xleftarrow{\$} \mathcal{A}^{\mathsf{Dec}_{\mathsf{DRE}}(sk_j,c)\wedge c\neq c^\star}(c^\star, s)$;

if $b' = b$ then return 1 else return 0.

is negligible in λ, where $\mathsf{Exp}^{\mathsf{ind-id-cpa}}_{\mathcal{IB-DRE},\mathcal{A}}(1^\lambda)$ is defined in Table 4.

Lattice-Based Programmable Hash Function with High Min-Entropy

Let $\ell, \overline{m}, m, n, q, \nu$ be some polynomials in the security parameter λ. A hash function $\mathcal{H} : \mathcal{X} \to \mathbb{Z}_q^{n\times m}$ contains two algorithms $(\mathcal{H}.\mathsf{Gen}, \mathcal{H}.\mathsf{Eval})$, where the PPT key generation algorithm $\mathcal{H}.\mathsf{Gen}(1^\lambda)$ takes the security parameter λ as input and outputs a key K, namely, $K \leftarrow \mathcal{H}.\mathsf{Gen}\left(1^\lambda\right)$, and the efficiently deterministic evaluation algorithm $\mathcal{H}.\mathsf{Eval}(K, X)$ takes $X \in \mathcal{X} = \{0,1\}^\ell$ as input and outputs a hash value $\mathbf{Z} \in \mathbb{Z}_q^{n\times m}$, namely, $\mathbf{Z} = \mathcal{H}.\mathsf{Eval}(K, X)$.

Definition 3 (Lattice-based programmable hash functions (LPHF) (Zhang et al. 2016b)) *A hash function $\mathcal{H} : \mathcal{X} \to \mathbb{Z}_q^{n\times m}$ is a $(1, \nu, \beta, \gamma, \delta)$-LPHF if there exist a PPT trapdoor key generation algorithm $\mathcal{H}.\mathsf{TrapGen}$ and a PPT deterministic trapdoor evaluation algorithm $\mathcal{H}.\mathsf{TrapEval}$ such that the following properties hold:*

Syntax : *Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times\overline{m}}$ and a (public) trapdoor matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$, the PPT algorithm $\mathcal{H}.\mathsf{TrapGen}$ outputs a key K' along with a trapdoor td. i.e., $(K', td) \leftarrow \mathcal{H}.\mathsf{TrapGen}\left(1^\lambda, \mathbf{A}, \mathbf{B}\right)$. Moreover, given td, K' and $X \in \mathcal{X}$, the deterministic algorithm $\mathcal{H}.\mathsf{TrapEval}$ returns $\mathbf{R}'_X \in \mathbb{Z}_q^{\overline{m}\times m}$ and $\mathbf{S}'_X \in \mathbb{Z}_q^{n\times n}$, i.e., $(\mathbf{R}'_X, \mathbf{S}'_X) = \mathcal{H}.\mathsf{TrapEval}(td, K', X)$, such that $s_1(\mathbf{R}'_X) \le \beta$ and $\mathbf{S}'_X \in \mathbf{Inv}_n \cup \{\mathbf{0}\}$ with overwhelming probability over the trapdoor td generated together with K', where $s_1(\cdot)$ is defined in Appendix A, and $\mathbf{Inv}_n$ denotes the set of invertible matrices in $Z_q^{n\times n}$.*

Table 4 IND-ID-CPA security for IB-DRE

Experiment $\mathsf{Exp}^{\mathsf{ind-id-cpa}}_{\mathcal{IB-DRE},\mathcal{A}}(1^\lambda)$:

$(PP, Msk) \xleftarrow{\$} \mathsf{Setup}_{\mathsf{ID}}(1^\lambda)$

$(id^\star_{1st}, id^\star_{2nd}, M_0, M_1, s) \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyGen}_{\mathsf{ID}}(PP,Msk,id_{1st},id_{2nd})}(PP)$;

$b \xleftarrow{\$} \{0,1\}, c^\star \xleftarrow{\$} \mathsf{Enc}_{\mathsf{ID}}(PP, id^\star_{1st}, id^\star_{2nd}, M_b)$;

$b' \xleftarrow{\$} \mathcal{A}^{\mathsf{KeyGen}_{\mathsf{ID}}(PP,Msk,id_{1st},id_{2nd})\wedge id_j\neq id^\star_{j=1st,2nd}}(c^\star, s)$;

if $b' = b$ then return 1 else return 0.

Correctness : *For all $(K', td) \leftarrow \mathcal{H}.\mathsf{TrapGen}\left(1^\lambda, \mathbf{A}, \mathbf{B}\right)$, all $X \in \mathcal{X}$ and $(\mathbf{R}'_X, \mathbf{S}'_X) = \mathcal{H}.\mathsf{TrapEval}(td, K', X)$, it holds that $\mathcal{H}.\mathsf{Eval}(K', X) = \mathbf{A}\mathbf{R}'_X + \mathbf{S}'_X\mathbf{B}$.*

Statistically close trapdoor keys : *For all $\left(K', td\right) \leftarrow \mathcal{H}.\mathsf{TrapGen}(1^\lambda, \mathbf{A}, \mathbf{B})$, and all $K \leftarrow \mathcal{H}.\mathsf{Gen}\left(1^\lambda\right)$, the statistical distance between $\left(\mathbf{A}, K'\right)$ and $(\mathbf{A}, K)$ is at most γ.*

Well-distributed hidden matrices : *For all $\left(K', td\right) \leftarrow \mathcal{H}.\mathsf{TrapGen}\left(1^\lambda, \mathbf{A}, \mathbf{B}\right)$, any inputs $X^*, X_1, \cdots, X_\nu$ where $X^* \neq X_j$ for any $j \in [\nu]$, it holds that*

$$\Pr[\,\mathbf{S}'_{X^*} = \mathbf{0} \wedge \mathbf{S}'_{X_1}, \cdots, \mathbf{S}'_{X_\nu} \in \mathbf{Inv}_n] \ge \delta,$$

where $(\mathbf{R}'_{X^*}, \mathbf{S}'_{X^*}) \leftarrow \mathcal{H}.\mathsf{TrapEval}(td, K', X^*)$ and $\left(\mathbf{R}'_{X_j}, \mathbf{S}'_{X_j}\right) \leftarrow \mathcal{H}.\mathsf{TrapEval}(td, K', X_j)$ for $j \in [\nu]$, and the probability is over the trapdoor td generated together with K'.

A weak LPHF (wLPHF) is a relaxed version of LPHF with only a little difference that the $\mathcal{H}.\mathsf{TrapGen}$ additionally takes X^* as input. i.e., $(K', td) \leftarrow \mathcal{H}.\mathsf{TrapGen}(1^\lambda, \mathbf{A}, \mathbf{G}, X^*)$.

Definition 4 (Lattice-based programmable hash functions with high min-entropy (Zhang et al. 2016b)) *Assume the hash function $\mathcal{H} : \mathcal{X} \to \mathbb{Z}_q^{n\times m}$ is a $(1, \nu, \beta, \gamma, \delta)$-LPHF where $\gamma = \mathsf{negl}(\lambda)$ and noticeable $\delta > 0$. The key space of $\mathcal{H}$ is $\mathcal{K}$, and $\mathcal{H}.\mathsf{TrapGen}$ and $\mathcal{H}.\mathsf{TrapEval}$ are the corresponding trapdoor generation and trapdoor evaluation algorithms. $\mathcal{H}$ is called as a LPHF with high min-entropy if for uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times\overline{m}}$ and a (public) trapdoor matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$, the following condition holds:*

- *For any $(K', td) \leftarrow \mathcal{H}.\mathsf{TrapGen}(1^\lambda, \mathbf{A}, \mathbf{B})$, any $X \in \mathcal{X}$ and $(\mathbf{R}'_X, \mathbf{S}'_X) = \mathcal{H}.\mathsf{TrapEval}(td, K', X)$, the distributions*

$$(\mathbf{A}, K', \mathbf{v}, \mathbf{u}) \text{ and } \left(\mathbf{A}, K', \mathbf{v}, (\mathbf{R}'_X)^\top\mathbf{v}\right)$$

are statistically close, where $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m, \mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^{\overline{m}}$.

In a similar way, wLPHF with high min-entropy can be defined.

Definition 5 (Weak lattice-based programmable hash functions with high min-entropy) *Assume the hash function $\mathcal{H} : \mathcal{X} \to \mathbb{Z}_q^{n\times m}$ is a $(1, \nu, \beta, \gamma, \delta)$-wLPHF where $\gamma = \mathsf{negl}(\lambda)$ and noticeable $\delta > 0$. The corresponding trapdoor generation and trapdoor evaluation algorithms are $\mathcal{H}.\mathsf{TrapGen}$ and $\mathcal{H}.\mathsf{TrapEval}$. $\mathcal{H}$ is called as a wLPHF with high min-entropy if for uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times\overline{m}}$ and a (public) trapdoor matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$:*

- *For any $(K', td) \leftarrow \mathcal{H}.\mathsf{TrapGen}\left(1^\lambda, \mathbf{A}, \mathbf{B}, X^*\right)$, and the corresponding $(\mathbf{R}'_{X^*}, \mathbf{S}'_{X^*}) = \mathcal{H}.\mathsf{TrapEval}(td, K', X^*)$,*

the distributions

$$(\mathbf{A}, K', \mathbf{v}, \mathbf{u}) \text{ and } \left(\mathbf{A}, K', \mathbf{v}, (\mathbf{R}'_{X^*})^\top \mathbf{v}\right)$$

are statistically close, where $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m, \mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^{\overline{m}}$.

Dual Receiver Encryption Construction

In this section, we will give the generic construction of DRE using the weak lattice-based programmable hash function with high min-entropy, and give the parameter selection and the security proof of the scheme.

In order to obtain the IND-CCA security, we require two primitives: a strong one-time signature scheme $\mathcal{OTS} = (\mathsf{Gen}_{\mathsf{OTS}}, \mathsf{Sig}_{\mathsf{OTS}}, \mathsf{Vrf}_{\mathsf{OTS}})$ which defined in Definition 6 in Appendix B and a $(1, \nu, \beta, \gamma, \delta)$-wLPHF $\mathcal{H} : \{0,1\}^\lambda \to \mathbb{Z}_q^{n\times m}$ with high min-entropy, where γ is negligible and $\delta > 0$ is noticeable. Let integers n, m, q, ν, β be polynomials in the security parameter λ, and set $\overline{m} = m$. Assume the message space $\mathcal{M} \in \{0,1\}^n$ and the size of verification key is λ bits , 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 Correctness and Parameter Selection as below. Then choose a uniformly random matrix $\mathbf{U} \in \mathbb{Z}_q^{n\times n}$. Finally, output a CRS $\mathsf{crs} = (n, m, q, \mathbf{U})$.
- $\mathsf{Gen}_{\mathsf{DRE}}(\mathsf{crs})$: Generate a pair of matrices $(\mathbf{A}_i, \mathbf{T}_{\mathbf{A}_i}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times m}$ by using $\mathsf{TrapGen}(1^n, 1^m, q)$, and compute $K_i \xleftarrow{\$} \mathcal{H}.\mathsf{Gen}(1^\lambda)$ twice independently for $i \in \{1,2\}$. Finally, output $pk_i = (\mathbf{A}_i, K_i)$ and $sk_i = \mathbf{T}_{\mathbf{A}_i}$.
- $\mathsf{Enc}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, \mathbf{m} \in \{0,1\}^n)$: Generate a pair $(\mathsf{vk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{OTS}}(1^\lambda)$ and compute $\mathbf{C}_1 = [\mathbf{A}_1 | \mathcal{H}.\mathsf{Eval}(K_1, \mathsf{vk})] \in \mathbb{Z}_q^{n\times 2m}$, $\mathbf{C}_2 = [\mathbf{A}_2 | \mathcal{H}.\mathsf{Eval}(K_2, \mathsf{vk})] \in \mathbb{Z}_q^{n\times 2m}$. Then, pick $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n, \widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, 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, compute and return the ciphertext $\mathbf{c} = (\mathsf{vk}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \rho)$, where $\rho = \mathsf{Sig}_{\mathsf{OTS}}(\mathsf{sk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2))$ and

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

- $\mathsf{Dec}_{\mathsf{DRE}}(\mathsf{crs}, pk_1, pk_2, sk_1, \mathbf{c})$: To decrypt a ciphertext $\mathbf{c} = (\mathsf{vk}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \rho)$ with a private key $sk_1 = \mathbf{T}_{\mathbf{A}_1}$, the algorithm $\mathsf{Dec}_{\mathsf{DRE}}$ does as follows:
  - Run $\mathsf{Vrf}_{\mathsf{OTS}}(\mathsf{vk}), (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \rho)$, outputs $\perp$ if $\mathsf{Vrf}_{\mathsf{OTS}}$ rejects;
  - For $i \in [n]$, run $(\mathbf{E}_1)_i \leftarrow \mathsf{SampleLeft}(\mathbf{A}_1, \mathcal{H}.\mathsf{Eval}(K_1, \mathsf{vk}), (\mathbf{U})_i, \mathbf{T}_{\mathbf{A}_1}, \sigma)$. Then obtain $\mathbf{E}_1 \in \mathbb{Z}_q^{2m\times n}$ such that $\mathbf{C}_1 \cdot \mathbf{E}_1 = \mathbf{U}$;
  - Compute $\mathbf{b} = \mathbf{c}_0 - \mathbf{E}_1^\top \mathbf{c}_1$ and treat each element of $\mathbf{b} = ((\mathbf{b})_1, \cdots, (\mathbf{b})_n)^\top$ as an integer in $\mathbb{Z}$, and set $(\mathbf{m})_i = 1$ if $\left|(\mathbf{b})_i - \lceil \frac{q}{2} \rceil\right| < \lceil \frac{q}{4} \rceil$, else $(\mathbf{m})_i = 0$, where $i \in [n]$;
  - Finally, it returns the plaintext $\mathbf{m} = ((\mathbf{m})_1, \cdots, (\mathbf{m})_n)^\top$.

Correctness and Parameter Selection

To make sure the correctness and the security proof works, we need to satisfy the following:

- For $i \in [n]$, the corresponding error terms are less than $q/4$ with overwhelming probability (i.e. $\alpha q\sqrt{m} + 2\alpha'\sigma mq < q/4$)

$$|(\mathbf{e}_0)_i - (\mathbf{E}_1)_i^\top \cdot \begin{bmatrix} \mathbf{e}_{1,1} \\ \mathbf{e}_{1,2} \end{bmatrix}| \le |(\widetilde{\mathbf{e}}_0)_i| + |(\mathbf{E}_1)_i^\top \cdot \begin{bmatrix} \mathbf{e}_{1,1} \\ \mathbf{e}_{1,2} \end{bmatrix}|$$
$$\le \alpha q\sqrt{m} + \sigma\sqrt{2m} \cdot \alpha' q\sqrt{2m} < q/4.$$

- TrapGen algorithm can works (i.e. $m \ge 6n\log q$).
- SampleLeft algorithms can operate (i.e., $\sigma \ge \|\widetilde{\mathbf{T}_{\mathbf{A}_i}}\| \cdot \omega\left(\sqrt{\log m}\right) = \mathcal{O}\left(\sqrt{n\log q}\right) \cdot \omega\left(\sqrt{\log m}\right)$.
- SampleRight algorithms can operate(i.e. $\sigma \ge \|\widetilde{\mathbf{T}_{\mathbf{G}}}\| \cdot s_1\left(\mathbf{R}'_{\mathsf{vk}}\right) \cdot \omega\left(\sqrt{\log m}\right)$ and $\sigma \ge \|\widetilde{\mathbf{T}_{\mathbf{G}}}\| \cdot s_1\left(\mathbf{R}''_{\mathsf{vk}}\right) \cdot \omega\left(\sqrt{\log m}\right)$, where $s_1\left(\mathbf{R}'_{\mathsf{vk}}\right) \le \beta$ and $s_1\left(\mathbf{R}''_{\mathsf{vk}}\right) \le \beta$).
- ReRand algorithm can works (i.e., $\alpha'/2\alpha > s_1(\mathbf{V}_i)$ for $i = 1, 2$, where $s_1(\mathbf{V}_1) = s_1\left([\mathbf{I}_m | \mathbf{R}'_{\mathsf{vk}^*}]^\top\right) \le 1 + s_1\left(\mathbf{R}'_{\mathsf{vk}^*}\right) \le 1 + \beta$ and $s_1(\mathbf{V}_2) \le 1 + \beta$ respectively, and $\alpha q > \max\left\{\omega\left(\sqrt{\log m}\right), \omega\left(\sqrt{\log 2m}\right)\right\} = \omega\left(\sqrt{\log 2m}\right)\Big)$.
- The worst case to average case reduction works (i.e. $\alpha q > 2\sqrt{2n}$).

To satisfy the above requirements, we set the parameters as follows:

$$\lambda = n, \ell = n, m = \mathcal{O}(n\log q),$$
$$\sigma = \sqrt{5} \cdot \beta \cdot \omega\left(\sqrt{\log m}\right),$$
$$\alpha q = 3\sqrt{n}, \alpha' q = 6(1+\beta) \cdot \sqrt{n},$$
$$q = 12\sqrt{mn} + 48\sqrt{5}\left(\beta + \beta^2\right) \cdot m\sqrt{n} \cdot \omega\left(\sqrt{\log m}\right).$$

Security Proof

Theorem 1 *Let $n, q, m \in \mathbb{Z}$, and $\alpha, \beta \in \mathbb{R}$ be polynomials in the security parameter λ. For large enough $\nu = \mathsf{poly}(n)$, let $\mathcal{H} = (\mathcal{H}.\mathsf{Gen}, \mathcal{H}.\mathsf{Eval})$ be any $(1, \nu, \beta, \gamma, \delta)$-wLPHF with high min-entropy from $\{0,1\}^\lambda$ to $\mathbb{Z}_q^{n\times m}$, where $\nu = \mathsf{poly}(n)$ is large enough, $\gamma = \mathsf{negl}(\lambda)$ and $\delta > 0$ is noticeable. Then, if $\mathcal{OTS}$ is a strongly existential unforgeable one-time signature scheme and the $\mathsf{DLWE}_{q,n,n+2m,\alpha}$ assumption holds, then the generic DRE scheme $\mathcal{DRE}$ is IND-CCA secure.*

Proof (of Theorem 1). Assume $\mathcal{A}$ is a PPT adversary against $\mathcal{DRE}$ in a chosen-ciphertext attack. The ciphertext $\mathbf{c} = (\mathsf{vk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \rho)$ is valid if $\mathsf{Vrf}_{\mathsf{OTS}}(\mathsf{vk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \rho) = 1$. The challenge ciphertext is $\mathbf{c}^* = (\mathsf{vk}^*, (\mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*), \rho^*)$ during the experiment, and Forge is the event that $\mathcal{A}$ submits a valid ciphertext $\mathbf{c} = (\mathsf{vk}^*, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \rho)$ to the decryption oracle during the query phase (assume that vk^* is chosen at the outer of the experiment). Note that

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

By the security of $\mathcal{OTS}$ defined in Definition 6 in Appendix B, $\Pr[\,\mathsf{Forge}]$ is negligible. So in order to complete the proof of Theorem 1, we only need to prove the following lemma.

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

Proof (of Lemma 1). We will prove the lemma by a sequences of games. We show that if there is a PPT adversary $\mathcal{A}$ can breaks our $\mathcal{DRE}$ scheme with a non-negligible advantage ϵ (i.e. the success probability is $\frac{1}{2}+\epsilon$), then there exists a reduction can break the $\mathsf{DLWE}_{q,n,n+2m,\alpha}$ assumption with an advantage $\delta^2\epsilon$. For simplicity, we set the trapdoor matrix $\mathbf{B} = \mathbf{G} \in \mathbb{Z}_q^{n\times m}$ throughout the proof. Assume that the adversary $\mathcal{A}$ makes Q_1 and Q_2 times queries for $Dec(sk_1, \cdot)$ and $Dec(sk_2, \cdot)$, respectively, and $\nu = Q_1 + Q_2$. In the following, define X_i as the event that the challenger outputs 1 in $\mathbf{Game}_i$ for $i \in \{1, 2, 3, 4, 5, 6, 7\}$.

Game$_1$ This game is the same as the original experiment $\mathsf{Exp}^{\mathsf{ind-cca}}_{\mathcal{DRE},\mathcal{A}}(1^\lambda)$ as described in Table 3 except that when the adversary $\mathcal{A}$ submits a valid ciphertext $(\mathsf{vk}^*, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \rho)$ to the decryption oracle, namely, the Forge event happens, $\mathcal{C}$ aborts and outputs a random bit. It is easy to see that

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

Game$_2$ This game is identical to the **Game$_1$** except that $\mathcal{C}$ changes the generation of the public keys and the challenge ciphertext, and the way that the decrypt oracle answered.

Setup phase: For $i = 1, 2$, generate a pair of matrices $(\mathbf{A}_i, \mathbf{T}_{\mathbf{A}_i}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, and generate the key of the wLPHF as $(K_i', td_i) \leftarrow \mathcal{H}.\mathsf{TrapGen}(1^\lambda, \mathbf{A}_i, \mathbf{G}, \mathsf{vk}^*)$.

Decryption queries: When $\mathcal{A}$ submits a valid ciphertext $(\mathsf{vk} \neq \mathsf{vk}^*, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \rho)$, the challenger generates $\mathbf{E}_1$ or $\mathbf{E}_2$ as follows:

$$(\mathbf{E}_1)_j \leftarrow \mathsf{SampleLeft}\left(\mathbf{A}_1, \mathbf{A}_1\mathbf{R}'_{\mathsf{vk}} + \mathbf{S}'_{\mathsf{vk}}\mathbf{G}, (\mathbf{U})_j, \mathbf{T}_{\mathbf{A}_1}, \sigma\right)$$

$$(\mathbf{E}_2)_j \leftarrow \mathsf{SampleLeft}\left(\mathbf{A}_2, \mathbf{A}_2\mathbf{R}''_{\mathsf{vk}} + \mathbf{S}''_{\mathsf{vk}}\mathbf{G}, (\mathbf{U})_j, \mathbf{T}_{\mathbf{A}_2}, \sigma\right)$$

for $j \in [n]$, where $\mathcal{H}.\mathsf{TrapEval}(td_1, K_1', \mathsf{vk}) = \left(\mathbf{R}'_{\mathsf{vk}}, \mathbf{S}'_{\mathsf{vk}}\right)$ and $\mathcal{H}.\mathsf{TrapEval}\left(td_2, K_2', \mathsf{vk}\right) = \left(\mathbf{R}''_{\mathsf{vk}}, \mathbf{S}''_{\mathsf{vk}}\right)$.

Challenge phase: Generate $\left(\mathbf{R}'_{\mathsf{vk}^*}, \mathbf{S}'_{\mathsf{vk}^*}\right)$ and $\left(\mathbf{R}''_{\mathsf{vk}^*}, \mathbf{S}''_{\mathsf{vk}^*}\right)$ using $\mathcal{H}.\mathsf{TrapEval}$ algorithm as in Decryption queries phase, and set $\mathbf{C}_1 = \left[\mathbf{A}_1 | \mathbf{A}_1\mathbf{R}'_{\mathsf{vk}^*} + \mathbf{S}'_{\mathsf{vk}^*}\mathbf{G}\right]$, $\mathbf{C}_2 = \left[\mathbf{A}_2 | \mathbf{A}_2\mathbf{R}''_{\mathsf{vk}^*} + \mathbf{S}''_{\mathsf{vk}^*}\mathbf{G}\right]$. By the well-distribution hidden matrices property of wLPHF,

$$\Pr[\,\mathbf{S}'_{\mathsf{vk}^*} = \mathbf{0} \wedge_{i=1}^{Q_1} \mathbf{S}'_{\mathsf{vk}_i} \in \mathbf{Inv}_n] \ge \delta,$$

$$\Pr[\,\mathbf{S}''_{\mathsf{vk}^*} = \mathbf{0} \wedge_{i=1}^{Q_2} \mathbf{S}''_{\mathsf{vk}_i} \in \mathbf{Inv}_n] \ge \delta.$$

Thus, with noticeable probability δ^2, $(\mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*)$ in the challenge ciphertext are as follows:

$$\mathbf{c}_0^* = \mathbf{U}^\top\mathbf{s} + \widetilde{\mathbf{e}}_0 + \mathbf{m}_b \cdot \left\lceil \frac{q}{2} \right\rceil,$$

$$\mathbf{c}_1^* = \begin{bmatrix} (\mathbf{A}_1)^\top \\ (\mathbf{R}'_{\mathsf{vk}^*})^\top(\mathbf{A}_1)^\top \end{bmatrix}\mathbf{s} + \begin{bmatrix} \mathbf{e}_{1,1} \\ \mathbf{e}_{1,2} \end{bmatrix},$$

$$\mathbf{c}_2^* = \begin{bmatrix} (\mathbf{A}_2)^\top \\ (\mathbf{R}''_{\mathsf{vk}^*})^\top(\mathbf{A}_2)^\top \end{bmatrix}\mathbf{s} + \begin{bmatrix} \mathbf{e}_{2,1} \\ \mathbf{e}_{2,2} \end{bmatrix}.$$

Game$_3$ This game is identical to the **Game$_2$** except that $\mathcal{C}$ chooses the matrices $\mathbf{A}_1$ and $\mathbf{A}_2$ uniformly random from $\mathbb{Z}_q^{n\times m}$ instead of generated by TrapGen, and generate the matrices $\mathbf{E}_1$ and $\mathbf{E}_2$ using SampleRight instead of SampleLeft. i.e., for $j \in [n]$,

$$(\mathbf{E}_1)_j \leftarrow \mathsf{SampleRight}\left(\mathbf{A}_1, \mathbf{G}, \mathbf{R}'_{\mathsf{vk}}, \mathbf{S}'_{\mathsf{vk}}, (\mathbf{U})_j, \mathbf{T}_{\mathbf{G}}, \sigma\right),$$

$$(\mathbf{E}_2)_j \leftarrow \mathsf{SampleRight}\left(\mathbf{A}_2, \mathbf{G}, \mathbf{R}''_{\mathsf{vk}}, \mathbf{S}''_{\mathsf{vk}}, (\mathbf{U})_j, \mathbf{T}_{\mathbf{G}}, \sigma\right),$$

where $\mathcal{H}.\mathsf{TrapEval}\left(td_1, K_1', \mathsf{vk}\right) = \left(\mathbf{R}'_{\mathsf{vk}}, \mathbf{S}'_{\mathsf{vk}}\right)$ and $\mathcal{H}.\mathsf{TrapEval}(td_2, K_2', \mathsf{vk}) = \left(\mathbf{R}''_{\mathsf{vk}}, \mathbf{S}''_{\mathsf{vk}}\right)$.

Game$_4$ This game is identical to the **Game$_3$** except that we change the way that the challenge ciphertext is generated. Pick $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, and $\widetilde{\mathbf{e}}_{1,1}, \widetilde{\mathbf{e}}_{2,1} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$, and set $\mathbf{w} = \mathbf{U}^\top\mathbf{s} + \widetilde{\mathbf{e}}_0$, $\mathbf{b}_1 = \mathbf{A}_1^\top\mathbf{s} + \widetilde{\mathbf{e}}_{1,1}$, $\mathbf{b}_2 = \mathbf{A}_2^\top\mathbf{s} + \widetilde{\mathbf{e}}_{2,1}$. Then compute

$$\mathbf{c}_0^* = \mathbf{U}^\top\mathbf{s} + \widetilde{\mathbf{e}}_0 + \mathbf{m}_b \cdot \left\lceil \frac{q}{2} \right\rceil,$$

$$\mathbf{c}_1^* = \mathsf{ReRand}\left(\begin{bmatrix} \mathbf{I}_m \\ (\mathbf{R}'_{\mathsf{vk}^*})^\top \end{bmatrix}, \mathbf{b}_1, \alpha q, \frac{\alpha'}{2\alpha}\right),$$

$$\mathbf{c}_2^* = \mathsf{ReRand}\left(\begin{bmatrix} \mathbf{I}_m \\ (\mathbf{R}''_{\mathsf{vk}^*})^\top \end{bmatrix}, \mathbf{b}_2, \alpha q, \frac{\alpha'}{2\alpha}\right).$$

Game$_5$ This game is identical to the **Game$_4$** except that the challenge ciphertext generated as follows. The challenger $\mathcal{C}$ first picks $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{b}}_1 \xleftarrow{\$} \mathbb{Z}_q^m$, $\widetilde{\mathbf{b}}_2 \xleftarrow{\$} \mathbb{Z}_q^m$, and $\widetilde{\mathbf{e}}_{1,1}, \widetilde{\mathbf{e}}_{2,1} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$, 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

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

Game$_6$ In this game, the challenge ciphertext generated as follows: $\mathcal{C}$ picks $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{b}}_1 \xleftarrow{\$} \mathbb{Z}_q^m$, $\widetilde{\mathbf{b}}_2 \xleftarrow{\$} \mathbb{Z}_q^m$, and $\mathbf{e}_{1,1}, \mathbf{e}_{2,1}, \mathbf{e}_{1,2}, \mathbf{e}_{2,2} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$. Then it computes

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

Game$_7$ In this game, $(\mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*)$ in the challenge ciphertext $\mathbf{c}^* = (\mathsf{vk}^*, (\mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*), \rho^*)$ is chosen from $\mathbb{Z}_q^n \times \mathbb{Z}_q^{2m} \times \mathbb{Z}_q^{2m}$ uniform randomly. At this time, ρ^* is a signature on a random message. In this cases, the adversary $\mathcal{A}$ has no more advantage than random guess. Thus, $\Pr[X_7] = \frac{1}{2}$.

Analysis of Games.

Lemma 2 $|\Pr[X_2] - \frac{1}{2}| = \delta^2 |\Pr[X_1] - \frac{1}{2}| + \mathsf{negl}(\lambda)$.

Proof This lemma can be proved by the the statistically close trapdoor keys and well-distributed hidden matrices properties of the wLPHF.

Lemma 3 Game$_3$ *and* **Game$_2$** *are statistically indistinguishable, namely,* $|\Pr[X_3] - \Pr[X_2]| \leq \mathsf{negl}(\lambda)$.

Proof By the first, second and third items in Lemma 16, the matrix $\mathbf{A}$ that generated by $\mathsf{TrapGen}$ is statistically close to uniform in $\mathbb{Z}_q^{n\times m}$, and the vectors generated by $\mathsf{SampleLeft}$ and $\mathsf{SampleRight}$ are statistically close. Those changes only make negligible difference, $|\Pr[X_3] - \Pr[X_2]| \leq \mathsf{negl}(\lambda)$.

Lemma 4 Game$_4$ *and* **Game$_3$** *are statistically indistinguishable, namely,* $|\Pr[X_4] - \Pr[X_3]| \leq \mathsf{negl}(\lambda)$.

Proof This lemma can be proved by using the property of ReRand in Lemma 17.

Lemma 5 *Assume that the* $\mathsf{DLWE}_{n,q,n+2m,\alpha}$ *assumption holds, then* **Game$_5$** *and* **Game$_4$** *are computationally indistinguishable, namely,* $|\Pr[X_5] - \Pr[X_4]| \leq \mathsf{DLWE}_{n,q,n+2m,\alpha}$.

Proof Suppose there exists an adversary $\mathcal{A}$ can distinguish **Game$_4$** and **Game$_5$** with non-negligible advantage, then we can construct an reduction $\mathcal{B}$ who can break the DLWE assumption as follows.

The simulator $\mathcal{B}$ is given the LWE instance: $\left(\mathbf{U}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{w} = \widetilde{\mathbf{w}} + \widetilde{\mathbf{e}}_0, \mathbf{b}_1 = \widetilde{\mathbf{b}}_1 + \widetilde{\mathbf{e}}_{1,1}, \mathbf{b}_2 = \widetilde{\mathbf{b}}_2 + \widetilde{\mathbf{e}}_{2,1}\right) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n \times \mathbb{Z}_q^m \times \mathbb{Z}_q^m$ where $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, $\widetilde{\mathbf{e}}_{1,1}, \widetilde{\mathbf{e}}_{2,1} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$. The task of $\mathcal{B}$ is to 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 $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$ or $\widetilde{\mathbf{w}} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{b}}_1, \widetilde{\mathbf{b}}_2 \xleftarrow{\$} \mathbb{Z}_q^m$. Note that this subtle change from the standard LWE problem is done only for the convenience of the proof. Then it works as follows:

Setup phase: The same as in **Game$_4$**.

Decryption queries: During the game, decryption queries made by $\mathcal{A}$ are answered as in **Game$_4$**.

Challenge phase: When $\mathcal{A}$ sends two messages $\mathbf{m}_0$, $\mathbf{m}_1$, $\mathcal{B}$ generates the challenge ciphertext as follows:

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

Guess phase: After being allowed to make additional queries, $\mathcal{A}$ guesses if it interacts with the challenger in **Game$_4$** or **Game$_5$**.

It is easy to see that if $(\mathbf{U}, \mathbf{A}, \mathbf{w}, \mathbf{b})$ is a valid LWE instance, then the view of $\mathcal{A}$ is the same as in **Game$_4$**; otherwise, the view of $\mathcal{A}$ corresponds to that in **Game$_4$**. By the $\mathsf{DLWE}_{n,q,n+2m,\alpha}$ assumption, it holds that $|\Pr[X_5] - \Pr[X_4]| \leq \mathsf{DLWE}_{n,q,n+2m,\alpha}$.

Lemma 6 Game$_6$ *and* **Game$_5$** *are statistically indistinguishable, namely,* $|\Pr[X_6] - \Pr[X_5]| \leq \mathsf{negl}(\lambda)$.

Proof This lemma can be proved by property of ReRand in Lemma 17.

Lemma 7 Game$_7$ *and* **Game$_6$** *are statistically indistinguishable, namely,* $|\Pr[X_7] - \Pr[X_6]| \leq \mathsf{negl}(\lambda)$.

Proof This lemma can be obtained by the property of wLPHF with high min-entropy.

Complete the Proof of Theorem 1. By Lemmas 3-7 and the fact that $\Pr[X_7]=\frac{1}{2}$, we can get $\left|\Pr[X_2]-\frac{1}{2}\right| \leq \mathsf{DLWE}_{n,q,n+2m,\alpha} + \mathsf{negl}(\lambda)$. Note that $|\Pr[X_1]-\frac{1}{2}| + \frac{1}{2}\Pr[\mathsf{Forge}] \geq \epsilon$ and $\Pr[\mathsf{Forge}] \leq \mathsf{negl}(\lambda)$, and by Lemma 2, we obtain that $\mathsf{DLWE}_{n,q,n+2m,\alpha} \geq \delta^2\epsilon + \mathsf{negl}(\lambda)$.

Identity-Based Dual Receiver Encryption Construction

In this section, we will give the generic construction of IB-DRE using lattice-based programmable hash functions, and give the parameter selection and the security proof of the scheme.

In our IB-DRE scheme, we require that the hash function $\mathcal{H}: \{0,1\}^{\lambda} \to \mathbb{Z}_q^{n\times m}$ is a $(1,\nu,\beta,\gamma,\delta)$-LPHF with high min-entropy which is defined in Definition 4, where γ is negligible and $\delta > 0$ is noticeable. Let integers n, m, q, ν, β be polynomials in the security parameter λ. And in our concrete construction, set $\overline{m} = m$. Assume the identity space is $\mathcal{ID} = \{0,1\}^{\ell}$, and a message space $\mathcal{M} = \{0,1\}^{n}$, our IB-DRE scheme $\mathcal{IB}\text{-}\mathcal{DRE}$ is as follows:

- $\mathsf{Setup}_{\mathsf{ID}}(1^{\lambda})$: Given a security parameter λ, first set the parameters n, m, q as specified in parameter selection in Parameter selection as below. Then, obtain a pair of matrices $(\mathbf{A}, \mathbf{T_A}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times m}$ by using $\mathsf{TrapGen}(1^n, 1^m, q)$, generate K_1, K_2 by running $\mathcal{H}.\mathsf{Gen}(1^{\lambda})$ twice independently, and choose a uniformly random matrix $\mathbf{U} \in \mathbb{Z}_q^{n\times n}$. Finally, output $PP = (n, m, q, \mathbf{A}, K_1, K_2, \mathbf{U})$ and $Msk = \mathbf{T_A}$.
- $\mathsf{KeyGen}_{\mathsf{ID}}(PP, Msk, \mathbf{id}_{1st}, \mathbf{id}_{2nd} \in \mathcal{ID})$: Given public parameters PP, a master key Msk, and identities $\mathbf{id}_{1st}, \mathbf{id}_{2nd}$, first compute

$$\mathbf{A}_{\mathbf{id}_1} = \mathcal{H}.\mathsf{Eval}(K_1, \mathbf{id}_{1st}),\ \mathbf{A}_{\mathbf{id}_2} = \mathcal{H}.\mathsf{Eval}(K_2, \mathbf{id}_{2nd}).$$

  Then, for $i \in [n]$, $(\mathbf{E}_{\mathbf{id}_1})_i \leftarrow \mathsf{SampleLeft}(\mathbf{A}, \mathbf{A}_{\mathbf{id}_1}, (\mathbf{U})_i, \mathbf{T_A}, \sigma)$. Set $sk_{\mathbf{id}_{1st}} = \mathbf{E}_{\mathbf{id}_1} \in \mathbb{Z}_q^{2m\times n}$ satisfying $\left[\mathbf{A}|\mathbf{A}_{\mathbf{id}_1}\right] \cdot \mathbf{E}_{\mathbf{id}_1} = \mathbf{U}$. Similarly, obtain $sk_{\mathbf{id}_{2nd}} = \mathbf{E}_{\mathbf{id}_2}$ such that $\left[\mathbf{A}|\mathbf{A}_{\mathbf{id}_2}\right] \cdot \mathbf{E}_{\mathbf{id}_2} = \mathbf{U}$.
- $\mathsf{Enc}_{\mathsf{ID}}(PP, \mathbf{id}_{1st}, \mathbf{id}_{2nd}, \mathbf{m})$: Compute $\mathbf{A}_{\mathbf{id}_1}, \mathbf{A}_{\mathbf{id}_2}$ as above. Then, pick $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, and $\mathbf{e}_{1,1}$, $\mathbf{e}_{1,2}, \mathbf{e}_{1,3} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$. Finally, compute and return the ciphertext $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1)$, where

$$\mathbf{c}_0 = \mathbf{U}^{\top}\mathbf{s} + \mathbf{e}_0 + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m} \in \mathbb{Z}_q^n,$$
$$\mathbf{c}_1 = \begin{bmatrix} \mathbf{c_{1,1}} \\ \mathbf{c_{1,2}} \\ \mathbf{c_{1,3}} \end{bmatrix} = \begin{bmatrix} \mathbf{A}^{\top} \\ (\mathbf{A}_{\mathbf{id}_1})^{\top} \\ (\mathbf{A}_{\mathbf{id}_2})^{\top} \end{bmatrix} \mathbf{s} + \begin{bmatrix} \mathbf{e_{1,1}} \\ \mathbf{e_{1,2}} \\ \mathbf{e_{1,3}} \end{bmatrix} \in \mathbb{Z}_q^{3m}.$$

- $\mathsf{Dec}_{\mathsf{ID}}(PP, sk_{\mathbf{id}_j}, \mathbf{c})$: 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 let $\mathbf{b} = ((\mathbf{b})_1, \cdots, (\mathbf{b})_n)^{\top} \in \mathbb{Z}_q^n$. Set $(\mathbf{m})_i = 1$ if $\left|(\mathbf{b})_i - \lceil \frac{q}{2} \rceil\right| < \lceil \frac{q}{4} \rceil$; otherwise set $(\mathbf{m})_i = 0$ where $i \in \{1, \cdots, n\}$. Finally, it returns a plaintext $\mathbf{m} = ((\mathbf{m})_1, \cdots, (\mathbf{m})_n)^{\top}$.

Correctness and Parameter Selection

Parameter selection. To make sure the correctness and the security proof works, we need to satisfy the following

- For $i \in [n]$, the corresponding error term should be less than $q/4$ with overwhelming probability

$$|(\mathbf{e}_0)_i - (\mathbf{E}_{\mathbf{id}_1})_i^{\top} \cdot \begin{bmatrix} \mathbf{e}_{1,1} \\ \mathbf{e}_{1,2} \end{bmatrix}| \leq |(\mathbf{e}_0)_i| + |(\mathbf{E}_{\mathbf{id}_1})_i^{\top} \cdot \begin{bmatrix} \mathbf{e}_{1,1} \\ \mathbf{e}_{1,2} \end{bmatrix}|$$
$$\leq \alpha q\sqrt{m} + \sigma\sqrt{2m} \cdot \alpha' q\sqrt{2m} \leq q/4.$$

- the $\mathsf{TrapGen}$ algorithm can works (i.e. $m \geq 6n\log q$)
- $\mathsf{SampleLeft}$ algorithms can operate (i.e. $\sigma \geq \|\widetilde{\mathbf{T}_{\mathbf{A}}}\| \cdot \omega\left(\sqrt{\log m}\right) = \mathcal{O}\left(\sqrt{n\log q}\right) \cdot \omega\left(\sqrt{\log m}\right)$)
- $\mathsf{SampleRight}$ algorithms can operate(i.e. $\sigma \geq \|\widetilde{\mathbf{T}_{\mathbf{G}}}\| \cdot s_1\left(\mathbf{R}'_{\mathbf{id}_j^i}\right) \cdot \omega\left(\sqrt{\log m}\right) = \sqrt{5} \cdot \beta \cdot \omega\left(\sqrt{\log m}\right)$, where $s_1\left(\mathbf{R}'_{\mathbf{id}_j^i}\right) \leq \beta, i \in [Q], j = 1, 2$)
- ReRand algorithm can works (i.e. $\alpha'/2\alpha > s_1(\mathbf{V})$ where $s_1(\mathbf{V}) = s_1\left(\left(\mathbf{I}_m|\mathbf{R}'_{\mathbf{id}_1^*}|\mathbf{R}'_{\mathbf{id}_2^*}\right)^{\top}\right) \leq 1 + s_1\left(\mathbf{R}'_{\mathbf{id}_1^*}\right) + s_1\left(\mathbf{R}'_{\mathbf{id}_2^*}\right) \leq 1 + 2\beta$, and $\alpha q > \max\left\{\omega\left(\sqrt{\log m}\right), \omega\left(\sqrt{\log 3m}\right)\right\} = \omega\left(\sqrt{\log 3m}\right)$)
- the worst case to average case reduction works (i.e. $\alpha q > 2\sqrt{2n}$)

To satisfy the above requirements, we set the parameters as follows:

$$\lambda = n, \ell = n, m = \mathcal{O}(n\log q),$$
$$\sigma = \sqrt{5} \cdot \beta \cdot \omega\left(\sqrt{\log m}\right),$$
$$\alpha q = 3\sqrt{n}, \alpha' q = 6(1+2\beta) \cdot \sqrt{n}, q = 12\sqrt{mn} + 48\sqrt{5}\left(\beta + 2\beta^2\right) \cdot m\sqrt{n} \cdot \omega\left(\sqrt{\log m}\right).$$

Security Proof

Theorem 2 *Let $n, q, m \in \mathbb{Z}$, and $\alpha, \beta \in \mathbb{R}$ be polynomials in the security parameter λ. For large enough $\nu = \mathsf{poly}(n)$, let $\mathcal{H} = (\mathcal{H}.\mathsf{Gen}, \mathcal{H}.\mathsf{Eval})$ be any $(1,\nu,\beta,\gamma,\delta)$-PHF with high min-entropy from $\{0,1\}^n$ to $\mathbb{Z}_q^{n\times m}$, where $\gamma = negl(\lambda)$ and $\delta > 0$ is noticeable. Then, if the $\mathsf{DLWE}_{q,n,n+m,\alpha}$ assumption holds, then the above scheme $\mathcal{IB}\text{-}\mathcal{DRE}$ is a*

secure IB-DRE scheme against chosen-plaintext and adaptively chosen-identity attacks.

Proof (of Theorem 2) We show that if there is a PPT adversary $\mathcal{A}$ can breaks our $\mathcal{IB}$-$\mathcal{DRE}$ scheme with a non-negligible advantage ϵ (i.e. the success probability is $\frac{1}{2}+\epsilon$), then there exists a reduction that can break the LWE assumption with an advantage $\frac{\delta^2\epsilon}{3}$.

Let $Q = Q(\lambda)$ be the upper bound of the number of key queries and $I^* = \left\{(\mathbf{id}^*_{1st}, \mathbf{id}^*_{2nd}), (\mathbf{id}^i_{1st}, \mathbf{id}^i_{2nd})_{i\in[Q]}\right\}$ the set of challenge ID and ID's for key queries. We will prove the theorem by a sequences of games where the first game is the real IND-ID-CPA game in Table 4 and in the last game the adversary has advantage zero. In each game, the challenger $\mathcal{C}$ selects a uniform coin $b \xleftarrow{\$} \{0,1\}$ in the challenge phase, while finally $\mathcal{A}$ returns a guess bit b' for b to the challenger. In the first game, the challenger sets $\hat{b} = b'$, these values might be different in the latter games. We define X_i as the event that $\hat{b} = b$ in $\mathbf{Game}_i$ for $i \in \{0,1,2,3,4,5,6,7\}$. As mentioned in the proof of Lemma 1, we fix the trapdoor matrix $\mathbf{B} = \mathbf{G} \in \mathbb{Z}_q^{n\times m}$ throughout the proof.

$\mathbf{Game_0}$ This game is the real IND-ID-CPA game. By the definition, it holds that

$$\left|\Pr[X_0] - \frac{1}{2}\right| = \left|\Pr[\hat{b} = b] - \frac{1}{2}\right| = \left|\Pr[b' = b] - \frac{1}{2}\right| = \epsilon.$$

$\mathbf{Game_1}$ This game is identical to **$\mathbf{Game_0}$** except that $\mathcal{C}$ changes the setup and challenge phases.

Setup phase: Same as in **$\mathbf{Game_0}$** except that generate $(K'_i, td_i) \leftarrow \mathcal{H}.\mathsf{TrapGen}(1^\lambda, \mathbf{A}, \mathbf{G})$ for $i = 1, 2$.

Challenge phase: Generate $\mathbf{A}_{\mathbf{id}^*_1}$ and $\mathbf{A}_{\mathbf{id}^*_2}$ using $\mathcal{H}.\mathsf{TrapEval}$ instead of $\mathcal{H}.\mathsf{Eval}$. Compute $(\mathbf{R}'_{\mathbf{id}^*_1}, \mathbf{S}'_{\mathbf{id}^*_1}) \leftarrow \mathcal{H}.\mathsf{TrapEval}(K'_1, td_1, \mathbf{id}^*_{1st})$, $(\mathbf{R}'_{\mathbf{id}^*_2}, \mathbf{S}'_{\mathbf{id}^*_2}) \leftarrow \mathcal{H}.\mathsf{TrapEval}(K'_2, td_2, \mathbf{id}^*_{2nd})$, and set $\mathbf{A}_{\mathbf{id}^*_i} = \mathbf{A}\mathbf{R}'_{\mathbf{id}^*_i} + \mathbf{S}'_{\mathbf{id}^*_i}\mathbf{G}$ for $i = 1, 2$. Then, choose a random coin $b \in \{0,1\}$, pick $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, $\mathbf{e}_{1,1}, \mathbf{e}_{1,2}, \mathbf{e}_{1,3} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$. Compute the challenge ciphertext $\mathbf{c}^* = (\mathbf{c}^*_0, \mathbf{c}^*_1)$ where

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

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

$\mathbf{Game_2}$ This game is identical to **$\mathbf{Game_1}$** except that add an abort event that is independent of the adversary's view.

Guess phase: Finally, $\mathcal{A}$ outputs his guess $b' \in \{0,1\}$ of b. $\mathcal{C}$ defines the following function

$$\tau\left(\widehat{td_1}, \widehat{td_2}, \widehat{K'_1}, \widehat{K'_2}, I^*\right) = \begin{cases} 0, & \mathbf{S}'_{\mathbf{id}^*_1} = \mathbf{0} \wedge \mathbf{S}'_{\mathbf{id}^*_2} = \mathbf{0} \wedge \bigwedge_{i=1}^{Q} \mathbf{S}'_{\mathbf{id}^i_1} \in \mathbf{Inv_n} \wedge \bigwedge_{i=1}^{Q} \mathbf{S}'_{\mathbf{id}^i_2} \in \mathbf{Inv_n}, \\ 1, & \text{otherwise}, \end{cases}$$

where $\left(\mathbf{R}'_{\mathbf{id}^*_i}, \mathbf{S}'_{\mathbf{id}^*_i}\right)$, $i = 1, 2$, generated as in **$\mathbf{Game_1}$**, and $\left(\mathbf{R}'_{\mathbf{id}^i_1}, \mathbf{S}'_{\mathbf{id}^i_1}\right) \leftarrow \mathcal{H}.\mathsf{TrapEval}\left(\widehat{K'_1}, \widehat{td_1}, \mathbf{id}^i_{1st}\right)$, $\left(\mathbf{R}'_{\mathbf{id}^i_2}, \mathbf{S}'_{\mathbf{id}^i_2}\right) \leftarrow \mathcal{H}.\mathsf{TrapEval}(\widehat{K'_2}, \widehat{td_2}, \mathbf{id}^i_{2nd})$ for $i \in [Q]$.

Abort check: Let $(td_i, K'_i), i = 1, 2$ be produced at setup phase as in **$\mathbf{Game_1}$**. The challenger $\mathcal{C}$ computes $\tau(td_1, td_2, K'_1, K'_2, I^*)$. If $\tau(td_1, td_2, K'_1, K'_2, I^*) = 1$, the challenger aborts the game and sets $\hat{b} \xleftarrow{\$} \{0,1\}$ ignoring the output of $\mathcal{A}$.

Artificial abort: Given the identities set I^*, let $p = \Pr\left[\tau\left(\widehat{td_1}, \widehat{td_2}, \widehat{K'_1}, \widehat{K'_2}, I^*\right) = 0\right]$ over the random choice of $\left(\widehat{td_1}, \widehat{K'_1}\right)$ and $\left(\widehat{td_2}, \widehat{K'_2}\right)$. The challenger samples $\mathcal{O}\left(\epsilon^{-2}\log\left(\epsilon^{-1}\right)\lambda^{-1}\log\left(\lambda^{-1}\right)\right)$ times the probability p by independently running $\left(\widehat{td_i}, \widehat{K'_i}\right) \leftarrow \mathcal{H}.\mathsf{TrapGen}\left(1^\lambda, \mathbf{A}_i, \mathbf{G}\right)$ and evaluating $\tau\left(\widehat{td_1}, \widehat{td_2}, \widehat{K'_1}, \widehat{K'_2}, I^*\right)$ to compute an estimate p', where λ is the lower bound of the p for any set I^*. If $p' > \lambda$, then abort with probability $\frac{p'-\lambda}{p'}$ (and not abort with probability $\frac{\lambda}{p'}$), and set $\hat{b} \xleftarrow{\$} \{0,1\}$ ignoring the output of $\mathcal{A}$.

Finally, when receiving b' from $\mathcal{A}$, the challenger sets $\hat{b} = b'$.

$\mathbf{Game_3}$ This game is identical to **$\mathbf{Game_2}$** except that change the generation of $\mathbf{A}$ and the way that answering the key query.

Setup phase: Choose a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ instead of running the $\mathsf{TrapGen}$ algorithm.

Key query: For the i-th secret key query $\left(\mathbf{id}^i_{1st}, \mathbf{id}^i_{2nd}\right)$, $i \in [Q]$, generate $\left(\mathbf{R}'_{\mathbf{id}^i_1}, \mathbf{S}'_{\mathbf{id}^i_1}\right)$ and $\left(\mathbf{R}'_{\mathbf{id}^i_2}, \mathbf{S}'_{\mathbf{id}^i_2}\right)$ by using $\mathcal{H}.\mathsf{TrapEval}$ such that $\mathbf{A}_{\mathbf{id}^i_1} = \mathbf{A}\mathbf{R}'_{\mathbf{id}^i_1} + \mathbf{S}'_{\mathbf{id}^i_1}\mathbf{G}$ and $\mathbf{A}_{\mathbf{id}^i_2} = \mathbf{A}\mathbf{R}'_{\mathbf{id}^i_2} + \mathbf{S}'_{\mathbf{id}^i_2}\mathbf{G}$. If $\mathbf{S}'_{\mathbf{id}^i_1} = \mathbf{0}$ or $\mathbf{S}'_{\mathbf{id}^i_2} = \mathbf{0}$, abort the game and set $\hat{b} \xleftarrow{\$} \{0,1\}$ ignoring the output of $\mathcal{A}$. Otherwise, compute $\left(\mathbf{E}_{\mathbf{id}^i_\iota}\right)_j \leftarrow \mathsf{SampleRight}\left(\mathbf{A}, \mathbf{G}, \mathbf{R}'_{\mathbf{id}^i_\iota}, \mathbf{S}'_{\mathbf{id}^i_\iota}, \mathbf{T_G}, (\mathbf{U})_j, \sigma\right)$ for $\iota = 1, 2$ and $j \in [n]$, set and send $sk_{\mathbf{id}^i_1} = \mathbf{E}_{\mathbf{id}^i_1} \in \mathbb{Z}_q^{2m\times n}$ and $sk_{\mathbf{id}^i_2} = \mathbf{E}_{\mathbf{id}^i_2} \in \mathbb{Z}_q^{2m\times n}$, where $i \in [Q]$.

Challenge phase: When the adversary outputs $\mathbf{id}^*_{1st}$, $\mathbf{id}^*_{2nd}$ and two messages $\mathbf{m}_0$, $\mathbf{m}_1$, for $\left(\mathbf{R}'_{\mathbf{id}^*_i}, \mathbf{S}'_{\mathbf{id}^*_i}\right)$, $i = 1, 2$, generated as in **$\mathbf{Game_2}$**, the challenger first checks if $\mathbf{S}'_{\mathbf{id}^*_1} = \mathbf{0} \wedge \mathbf{S}'_{\mathbf{id}^*_2} = \mathbf{0}$. If not, abort the game and output a random bit $\hat{b} \xleftarrow{\$} \{0,1\}$. Thus, $\mathbf{A}_{\mathbf{id}^*_i} = \mathbf{A}\mathbf{R}'_{\mathbf{id}^*_i}$, $i = 1, 2$. Pick $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, $\mathbf{e}_{1,1}, \mathbf{e}_{1,2}, \mathbf{e}_{1,3} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$, compute and send the challenge ciphertext $\mathbf{c}^* = (\mathbf{c}^*_0, \mathbf{c}^*_1)$ where

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

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

At the guess phase, it also executes the artificial abort check.

Game$_4$ This game is identical to **Game$_3$** except that change the way that the challenge ciphertext generated. Pick $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, $\mathbf{e}_1 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$, and set $\mathbf{w} = \mathbf{U}^\top \mathbf{s} + \mathbf{e}_0, \mathbf{b}_1 = \mathbf{A}^\top \mathbf{s} + \mathbf{e}_1$. Compute

$$\mathbf{c}_0^* = \mathbf{w} + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m}_b,$$

$$\mathbf{c}_1^* = \mathsf{ReRand}\left(\begin{bmatrix} \mathbf{I}_m \\ (\mathbf{R}'_{\mathbf{id}_1^*})^\top \\ (\mathbf{R}'_{\mathbf{id}_2^*})^\top \end{bmatrix}, \mathbf{b}_1, \alpha q, \frac{\alpha'}{2\alpha} \right).$$

Game$_5$ In this game, the challenge ciphertext is generated as follows. Pick $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{b}} \xleftarrow{\$} \mathbb{Z}_q^m$, $\mathbf{e}_1 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha q}$, $\mathbf{b}_1 = \widetilde{\mathbf{b}} + \mathbf{e}_1$. Then compute

$$\mathbf{c}_0^* = \mathbf{w} + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m}_b,$$

$$\mathbf{c}_1^* = \mathsf{ReRand}\left(\begin{bmatrix} \mathbf{I}_m \\ (\mathbf{R}'_{\mathbf{id}_1^*})^\top \\ (\mathbf{R}'_{\mathbf{id}_2^*})^\top \end{bmatrix}, \mathbf{b}_1, \alpha q, \frac{\alpha'}{2\alpha} \right).$$

Game$_6$ In this game, the challenge ciphertext is generated as follows. Pick $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{b}} \xleftarrow{\$} \mathbb{Z}_q^m$, $\mathbf{e}_{1,1}, \mathbf{e}_{1,2}, \mathbf{e}_{1,3} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$. Then compute

$$\mathbf{c}_0^* = \mathbf{w} + \left\lceil \frac{q}{2} \right\rceil \cdot \mathbf{m}_b, \quad \mathbf{c}_1^* = \begin{bmatrix} \widetilde{\mathbf{b}} \\ (\mathbf{R}'_{\mathbf{id}_1^*})^\top \widetilde{\mathbf{b}} \\ (\mathbf{R}'_{\mathbf{id}_2^*})^\top \widetilde{\mathbf{b}} \end{bmatrix} + \begin{bmatrix} \mathbf{e}_{1,1} \\ \mathbf{e}_{1,2} \\ \mathbf{e}_{1,3} \end{bmatrix}$$

Game$_7$ In this game, choose the challenge ciphertext randomly uniform, namely, $\mathbf{c} = (\mathbf{c}_0^*, \mathbf{c}_1^*) \xleftarrow{\$} \mathbb{Z}_q^n \times \mathbb{Z}_q^{3m}$. In this game, the advantage of the adversary is zero. Namely, $\Pr[X_7] = \frac{1}{2}$. By the definition of Γ_7, we have $\Gamma_7 = 0$.

Analysis of Games.

Lemma 8 *If $\mathcal{H}$ is a LPHF with high min-entropy, then* $|\Pr[X_1] - \Pr[X_0]| \leq \mathsf{negl}(\lambda)$.

Proof This lemma can be proved by the statistically close trapdoor keys property of LPHF in definition 3.

For $i \in \{2,3,4,5,6,7\}$, let $\widetilde{p}_i$ be the probability that the challenger does not abort in the abort check stage in **Game**$_i$, and the probability in the artificial abort stage in **Game**$_i$ is defined as $p_i = \Pr\left[\tau\left(\widehat{td_1}, \widehat{td_2}, \widehat{K'_1}, \widehat{K'_2}, I^*\right) = 0\right]$. Since the adversary might obtain some information of td_1 and td_2 from the challenge ciphertext, the probability $\widetilde{p}_i$ might not be equal to p_i. Formally, let Γ_i be the difference between $\widetilde{p}_i$ and p_i, i.e. $\Gamma_i = |\widetilde{p}_i - p_i|$.

Lemma 9 *If $\mathcal{H}$ is a $(1, \nu, \beta, \gamma, \delta)$-LPHF, and $Q \leq \nu$, then* $|\Pr[X_2] - \frac{1}{2}| \geq \frac{1}{2}\epsilon(\delta^2 - \Gamma_2)$.

So as not to interrupt the proof of Theorem 2, we skip the proof of Lemma 9 for time being.

Lemma 10 *If $\mathcal{H}$ is a $(1, \nu, \beta, \gamma, \delta)$-LPHF, and $Q \leq \nu$, then* $|\Pr[X_3] - \Pr[X_2]| \leq \mathsf{negl}(\lambda)$ *and* $|\Gamma_3 - \Gamma_2| \leq \mathsf{negl}(\lambda)$.

Proof Note that abort check and the artificial abort in **Game$_2$** and in **Game$_3$** are identical. By the item 1, item 2 and item 3 of Lemma 16, those changes that generating the matrix $\mathbf{A}$ using $\mathsf{TrapGen}$ and secret key $sk_{\mathbf{id}_j^i}$, $i \in [Q], j = 1,2$, using $\mathsf{SampleRight}$ instead of $\mathsf{SampleLeft}$ make only negligible difference. In conclusion, $|\Pr[X_3] - \Pr[X_2]| \leq \mathsf{negl}(\lambda)$ and $|\Gamma_3 - \Gamma_2| \leq \mathsf{negl}(\lambda)$.

Lemma 11 *If $\mathcal{H}$ is a $(1, \nu, \beta, \gamma, \delta)$-LPHF, and $Q \leq \nu$, then* $|\Pr[X_4] - \Pr[X_3]| \leq \mathsf{negl}(\lambda)$ *and* $|\Gamma_4 - \Gamma_3| \leq \mathsf{negl}(\lambda)$.

Proof This lemma can be proved by the property of ReRand in Lemma 17.

Lemma 12 *Assume that the* $\mathsf{DLWE}_{n,q,n+m,\alpha}$ *assumption holds, then* $|\Pr[X_5] - \Pr[X_4]| \leq \mathsf{DLWE}_{n,q,n+m,\alpha}$ *and* $|\Gamma_5 - \Gamma_4| \leq \mathsf{DLWE}_{n,q,n+m,\alpha}$.

Proof we can construct an adversary $\mathcal{B}$ to against the $\mathsf{DLWE}_{n,q,n+m,\alpha}$ problem using the ability of $\mathcal{A}$, where $\mathcal{A}$ is an adversary in **Game$_4$** or **Game$_5$**. The simulator $\mathcal{B}$ is given the LWE instance: $(\mathbf{A}', \mathbf{u}' = \mathbf{b}' + \mathbf{e}') \in \mathbb{Z}_q^{n \times (n+m)} \times \mathbb{Z}_q^{n+m}$ where $\mathbf{e}' \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^{n+m},\alpha q}$. And the task of $\mathcal{B}$ is to distinguish whether $\mathbf{b}' = (\mathbf{A}')^\top \mathbf{s}$ for $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$ or $\mathbf{b}' \xleftarrow{\$} \mathbb{Z}_q^{n+m}$. Note that this subtle change from the standard LWE problem is done only for the convenience of the proof. Then works as follows:

Setup phase: Let the first n columns of $\mathbf{A}'$ be the matrix $\mathbf{U} \in \mathbb{Z}_q^{n \times n}$ and the last m columns the matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times n}$. The rest is the same as in **Game$_4$**.

Key query: During the game, key extraction queries made by $\mathcal{A}$ are answered as in **Game$_4$** without knowing $\mathbf{T}_\mathbf{A}$.

Challenge phase: For $\left(\mathbf{R}'_{\mathbf{id}_i^*}, \mathbf{S}'_{\mathbf{id}_i^*}\right)$, $i = 1,2$, generated as in **Game$_4$**, first check if $\mathbf{S}'_{\mathbf{id}_1^*} = \mathbf{0} \wedge \mathbf{S}'_{\mathbf{id}_2^*} = \mathbf{0}$. If not,

abort the game as in **Game$_4$**. Otherwise, $\mathbf{A}_{\mathbf{id}_1^*} = \mathbf{AR}'_{\mathbf{id}_1^*}$, $\mathbf{A}_{\mathbf{id}_2^*} = \mathbf{AR}'_{\mathbf{id}_2^*}$. Pick a random coin $b \xleftarrow{\$} \{0,1\}$. Let the first n coefficients of $\mathbf{u}'$ be $\mathbf{w} \in \mathbb{Z}_q^n$, and the last m coefficients $\mathbf{b}_1 \in \mathbb{Z}_q^m$. Then the challenge ciphertext generated as follows:

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

If $\mathbf{b}' = (\mathbf{A}')^\top \mathbf{s}$ for $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, then $(\mathbf{A}', \mathbf{u}' = \mathbf{b}' + \mathbf{e}' = (\mathbf{U}, \mathbf{A})^\top \mathbf{s} + \mathbf{e}')$ is a valid LWE sample, the view of the adversary $\mathcal{A}$ is the same as in **Game$_4$**. And if $\mathbf{b}' \xleftarrow{\$} \mathbb{Z}_q^{n+m}$, then the view of the adversary $\mathcal{A}$ is the same as in **Game$_5$**. So the advantage of $\mathcal{B}$ is $|\Pr[X_5] - \Pr[X_4]|$, by the DLWE assumption, it holds that $|\Pr[X_5] - \Pr[X_4]| \leq \mathsf{DLWE}_{n,q,n+m,\alpha}$ and $|\Gamma_5 - \Gamma_4| \leq \mathsf{DLWE}_{n,q,n+m,\alpha}$.

Lemma 13 $|\Pr[X_6] - \Pr[X_5]| \leq \mathsf{negl}(\lambda)$ *and* $|\Gamma_6 - \Gamma_5| \leq \mathsf{negl}(\lambda)$.

Proof This lemma can be proved just according to the property of ReRand in Lemma 17.

Lemma 14 *If $\mathcal{H}$ is LPHF with high min-entropy, then* $|\Pr[X_7] - \Pr[X_6]| \leq \mathsf{negl}(\lambda)$ *and* $|\Gamma_7 - \Gamma_6| \leq \mathsf{negl}(\lambda)$.

Proof This lemma can be obtained by the property of LPHF with high min-entropy in definition 4.

Complete the proof of Theorem 2. By Lemmas 9-14 and the fact that $\Pr[X_7] = \frac{1}{2}$, it holds that

$$\mathsf{DLWE}_{n,q,n+m,\alpha} \geq \frac{1}{2}\epsilon(\delta^2 - \Gamma_2) - \mathsf{negl}(\lambda).$$

And by Lemmas 10-14 again, we can obtain that $\Gamma_2 \leq \mathsf{DLWE}_{n,q,n+m,\alpha} + \mathsf{negl}(\lambda)$. Thus, $\mathsf{DLWE}_{n,q,n+m,\alpha} \geq \frac{\delta^2\epsilon}{3} - \mathsf{negl}(\lambda)$.

In order to complete the proof of Theorem 2, we need to prove the Lemma 9 by using the Lemma 28 in the full vision of Agrawal et al. (2010), which is described as follows.

Lemma 15 (Lemma 28 in Agrawal et al. (2010)) *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 $\eta(I^*)$ the probability that an abort does not happen in* **Game$_2$**. *Let $\eta_{max} = \max \eta(I^*)$ and $\eta_{min} = \min \eta(I^*)$. For $i = 1, 2$, we set X_i be the event that $\hat{b} = b$ at the end of* **Game$_1$**. *Then*

$$\left|\Pr[X_2] - \frac{1}{2}\right| \geq \eta_{min}\left|\Pr[X_1] - \frac{1}{2}\right| - \frac{1}{2}(\eta_{max} - \eta_{min}).$$

Lemma 9: If $\mathcal{H}$ is a $(1, \nu, \beta, \epsilon, \delta)$-LPHF, and $Q \leq \nu$, then $|\Pr[X_2] - \frac{1}{2}| \geq \frac{1}{2}\epsilon(\delta^2 - \Gamma_2)$.

Proof (of Lemma 9) As the generations of $(\widehat{td}_1, \widehat{K}'_1)$ and $(\widehat{td}_2, \widehat{K}'_2)$ are independent, by the well-distributed hidden matrices property of the $\mathcal{H}$, it holds that

$$\begin{aligned} p &= \Pr\left[\mathbf{S}'_{\mathbf{id}_1^*} = \mathbf{0} \wedge \mathbf{S}'_{\mathbf{id}_2^*} = \mathbf{0} \wedge_{i=1}^{Q} \mathbf{S}'_{\mathbf{id}_1^i} \in \mathbf{Inv_n} \wedge_{i=1}^{Q} \mathbf{S}'_{\mathbf{id}_2^i} \in \mathbf{Inv_n}\right] \\ &= \Pr\left[\mathbf{S}'_{\mathbf{id}_1^*} = \mathbf{0} \wedge_{i=1}^{Q} \mathbf{S}'_{\mathbf{id}_1^i} \in \mathbf{Inv_n}\right] \cdot \Pr[\mathbf{S}'_{\mathbf{id}_2^*} = \mathbf{0} \wedge_{i=1}^{Q} \mathbf{S}'_{\mathbf{id}_2^i} \in \mathbf{Inv_n}] \\ &\geq \delta \cdot \delta = \delta^2 = \lambda. \end{aligned}$$

According to Lemma 15, we only need to evaluate η_{max}, η_{min} and $\eta_{max} - \eta_{min}$. By the definition of $\widetilde{p_2}$ and p_2 in **Game$_2$**, it holds that $\eta(I^*) = \widetilde{p_2}\frac{\lambda}{p'}$, where p' is an estimate of p_2. Since the challenger always samples $\mathcal{O}\left(\epsilon^{-2}\log\left(\epsilon^{-1}\right)\lambda^{-1}\log\left(\lambda^{-1}\right)\right)$ times p_2 to compute p', according to the Chernoff bounds, we have $\Pr\left[p' \geq p_2\left(1 + \frac{\epsilon}{8}\right)\right] \leq \lambda\frac{\epsilon}{8}$ and $\Pr\left[p' \leq p_2\left(1 - \frac{\epsilon}{8}\right)\right] \leq \lambda\frac{\epsilon}{8}$. Then,

$$\begin{aligned} \eta_{max} &\leq \left(1 - \lambda\frac{\epsilon}{8}\right)\widetilde{p_2}\frac{\lambda}{p_2\left(1 - \frac{\epsilon}{8}\right)}, \\ \eta_{min} &\geq \left(1 - \lambda\frac{\epsilon}{8}\right)\widetilde{p_2}\frac{\lambda}{p_2(1 + \frac{\epsilon}{8})} \geq \frac{7\lambda\widetilde{p_2}}{9p_2} \\ \eta_{max} - \eta_{min} &\leq \left(1 - \lambda\frac{\epsilon}{8}\right)\frac{\lambda\epsilon\widetilde{p_2}}{4(1 - \frac{\epsilon^2}{64})p_2} \leq \frac{16\lambda\epsilon\widetilde{p_2}}{63p_2} \end{aligned}$$

Substitute them and the value of λ into the inequality in Lemma 15, we can get

$$\begin{aligned} \left|\Pr[X_2] - \frac{1}{2}\right| &\geq \frac{7\lambda\widetilde{p_2}}{9p_2} \cdot \epsilon - \frac{1}{2} \cdot \frac{16\lambda\epsilon\widetilde{p_2}}{63p_2} \\ &\geq \frac{\lambda\epsilon(p_2 - \Gamma_2)}{2p_2} \geq \frac{1}{2}\epsilon(\lambda - \Gamma_2) = \frac{1}{2}\epsilon\left(\delta^2 - \Gamma_2\right). \end{aligned}$$

Instantiation of Generic DRE construction

As said in Zhang et al. (2016b), the selectively secure IBE in Agrawal et al. (2010) implies a weak LPHF with high min-entropy, thus we can use this weak LPHF to instantiate our IND-CCA secure DRE scheme.

The wLPHF $\mathcal{H}_{\mathrm{ABB}} : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times m}$ in Agrawal et al. (2010) consists of two algorithms ($\mathcal{H}_{\mathrm{ABB}}$.Gen, $\mathcal{H}_{\mathrm{ABB}}$.Eval) which are defined as follows:

- $\mathcal{H}_{\mathrm{ABB}}.\mathsf{Gen}(1^\lambda) \to K$: $\mathbf{A}_0 \xleftarrow{\$} \mathcal{K} = \mathbb{Z}_q^{n\times m}$, and output $K = \mathbf{A}_0$.
- $\mathcal{H}_{\mathrm{ABB}}.\mathsf{Eval}(K, X) \to \mathbf{Z} \in \mathbb{Z}_q^{n\times m}$: For $X \in \mathbb{Z}_q^n$, an FRD encoding function $H_{n,q} : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$ which was introduced in Zhang et al. (2018b), output $\mathbf{Z} = \mathbf{A}_0 + H_{n,q}(X)\mathbf{G}$.

The associating algorithms $\mathcal{H}_{\mathrm{ABB}}$.TrapGen and $\mathcal{H}_{\mathrm{ABB}}$.TrapEval are defined as follows:

- $\mathcal{H}_{\mathrm{ABB}}.\mathsf{TrapGen}(1^\lambda, \mathbf{A}, \mathbf{G}, X^*) \to (K', td)$: Randomly choose $\mathbf{R} \xleftarrow{\$} \{-1,1\}^{m\times m}$, and set $\mathbf{A}_0 = \mathbf{AR} - H_{n,q}(X^*)\mathbf{G}$, and output $K' = \mathbf{A}_0$ and $td = \{\mathbf{R}\}$.
- $\mathcal{H}_{\mathrm{ABB}}.\mathsf{TrapEval}(td, K', X) \to (\mathbf{R}_X, \mathbf{S}_X)$: For $X \in \mathbb{Z}_q^n$, $\mathbf{Z} = \mathbf{AR} + (H_{n,q}(X) - H_{n,q}(X^*))\mathbf{G}$, where $\mathbf{R}_X = \mathbf{R}$ and $\mathbf{S}_X = H_{n,q}(X) - H_{n,q}(X^*)$.

The above function $\mathcal{H}_{\mathrm{ABB}}$ is a $(1, \nu, \mathcal{O}(\ell\sqrt{m}), \mathsf{negl}(\lambda), 1)$-wLPHF with high min-entropy (Zhang et al. 2016b), and using it to instantiate our generic DRE construction, we can get the concrete $\mathrm{DRE}_{\mathrm{ABB}}$ scheme in Table 5.

Instantiations of Generic IB-DRE construction

As mentioned in Zhang et al. (2019), the adaptively secure and anonymous IBE schemes in Agrawal et al. (2010); Yamada (2016); Yamada (2017) naturally imply instantiations of LPHFs with high min-entropy. In this section, we will use them to instantiate our generic IB-DRE constructions.

IB-DRE construction from LPHF $\mathcal{H}_{\mathrm{ABB}}$

$\mathcal{H}_{\mathrm{ABB}} : \{-1,1\}^\ell \to \mathbb{Z}_q^{n\times m}$ in Agrawal et al. (2010) consists of two algorithms $(\mathcal{H}.\mathsf{Gen}, \mathcal{H}.\mathsf{Eval})$ are defined as follows:

- $\mathcal{H}_{\mathrm{ABB}}.\mathsf{Gen}(1^\lambda) \to K$: Randomly choose $\mathbf{A}_1, \cdots, \mathbf{A}_\ell \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, and output $K = (\{\mathbf{A}_i\}_{i\in[\ell]})$.
- $\mathcal{H}_{\mathrm{ABB}}.\mathsf{Eval}(K, X) \to \mathbf{Z} \in \mathbb{Z}_q^{n\times m}$: For $X \in \{-1,1\}^\ell$, $\mathbf{Z} = \mathbf{G} + \sum_{i=1}^{l}(X)_i \cdot \mathbf{A}_i \in \mathbb{Z}_q^{n\times m}$.

Table 5 $\mathrm{DRE}_{\mathrm{ABB}}$ scheme

$\mathsf{CGen}_{\mathrm{DRE}}(1^\lambda)$: $\mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$, output $\mathrm{crs} = \mathbf{U}$.

$\mathsf{Gen}_{\mathrm{DRE}}(\mathrm{crs})$: $(\mathbf{A}_i, \mathbf{T}_{\mathbf{A}_i}) \xleftarrow{\$} \mathsf{TrapGen}(1^n, 1^m, q)$, $\mathbf{B}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i = 1, 2$. Output $pk_i = (\mathbf{A}_i, \mathbf{B}_i)$, $sk_i = \mathbf{T}_{\mathbf{A}_i}$.

$\mathsf{Enc}_{\mathrm{DRE}}(\mathrm{crs}, pk_1, pk_2, \mathbf{m} \in \{0,1\}^n)$:

1. Generate $(\mathrm{vk}, \mathrm{sk}) \leftarrow \mathsf{Gen}_{\mathrm{OTS}}(1^\lambda)$.
2. Compute $\mathbf{C}_1 = (\mathbf{A}_1|\mathbf{B}_1 + H_{n,q}(\mathrm{vk}) \cdot \mathbf{G})$, $\mathbf{C}_2 = \left(\mathbf{A}_2|\mathbf{B}_2 + H_{n,q}(\mathrm{vk}) \cdot \mathbf{G}\right)$.
3. Pick $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\widetilde{\mathbf{e}}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, and $\mathbf{e}_{1,1}, \mathbf{e}_{2,1}, \mathbf{e}_{1,2}, \mathbf{e}_{2,2} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$, compute and return the ciphertext $\mathbf{c} = (\mathrm{vk}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \rho)$, where

$$\rho = \mathsf{Sig}_{\mathrm{OTS}}(\mathrm{sk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2)) \text{ and}$$

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

$$\mathbf{c}_1 = \mathbf{C}_1^\top\mathbf{s} + \begin{bmatrix} \mathbf{e}_{1,1} \\ \mathbf{e}_{1,2} \end{bmatrix} \in \mathbb{Z}_q^{2m}, \quad \mathbf{c}_2 = \mathbf{C}_2^\top\mathbf{s} + \begin{bmatrix} \mathbf{e}_{2,1} \\ \mathbf{e}_{2,2} \end{bmatrix} \in \mathbb{Z}_q^{2m}.$$

$\mathsf{Dec}_{\mathrm{DRE}}(\mathrm{crs}, pk_1, pk_2, sk_1, \mathbf{c})$:

1. Run $\mathsf{Vrf}_{\mathrm{OTS}}(\mathrm{vk}, (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2), \rho)$, outputs $\perp$ if $\mathsf{Vrf}_{\mathrm{OTS}}$ rejects;
2. $(\mathbf{E}_1)_i \leftarrow \mathsf{SampleLeft}(\mathbf{A}_1, \mathbf{B}_1 + H_{n,q}(\mathrm{vk}) \cdot \mathbf{G}, (\mathbf{U})_i, \mathbf{T}_{\mathbf{A}_1}, \sigma)$, $i \in [n]$, to obtain $\mathbf{E}_1 \in \mathbb{Z}_q^{2m\times n}$ such that $\mathbf{C}_1 \cdot \mathbf{E}_1 = \mathbf{U}$;
3. Compute $\mathbf{b} = \mathbf{c}_0 - \mathbf{E}_1^\top\mathbf{c}_1 = ((\mathbf{b})_1, \cdots, (\mathbf{b})_n)^\top \in \mathbb{Z}^n$. Set $(\mathbf{m})_i = 1$ if $\left|(\mathbf{b})_i - \lceil \tfrac{q}{2} \rceil\right| < \lceil \tfrac{q}{4} \rceil$, else $(\mathbf{m})_i = 0$, $i \in [n]$.
4. Return the plaintext $\mathbf{m} = ((\mathbf{m})_1, \cdots, (\mathbf{m})_n)^\top$.

The associating algorithms $\mathcal{H}_{\mathrm{ABB}}.\mathsf{TrapGen}$ and $\mathcal{H}_{\mathrm{ABB}}.\mathsf{TrapEval}$ are defined as follows:

- $\mathcal{H}_{\mathrm{ABB}}.\mathsf{TrapGen}(1^\lambda, \mathbf{A}, \mathbf{G}) \to (K', td)$: Randomly choose $\mathbf{R}_1, \cdots, \mathbf{R}_\ell \xleftarrow{\$} \{-1,1\}^{m\times m}$, and set $\mathbf{A}_i = \mathbf{AR}_i + H_{t,q}(\mathbf{h}_i) \otimes \mathbf{I}_{n/t} \cdot \mathbf{G}$, where $H_{t,q} : \mathbb{Z}_q^t \to \mathbb{Z}_q^{t\times t}$ is a FRD function introduced in Zhang et al. (2018b), and $\mathbf{h}_i \xleftarrow{\$} \mathbb{Z}_q^t$, $i \in [\ell]$. Output $K' = (\{\mathbf{A}_i\}_{i\in[\ell]})$ and $td = (\{\mathbf{h}_i\}_{i\in[\ell]}, \{\mathbf{R}_i\}_{i\in[\ell]})$.
- $\mathcal{H}_{\mathrm{ABB}}.\mathsf{TrapEval}(td, K', id) \to (\mathbf{R}_{\mathbf{id}}, \mathbf{S}_{\mathbf{id}})$: For $id \in \{-1,1\}^\ell$,

$$\mathbf{Z} = \mathbf{A}\sum_{i=1}^{l} id_i\mathbf{R}_i + (\mathbf{I}_n + \sum_{i=1}^{l} id_i \cdot H_{t,q}(\mathbf{h}_i) \otimes \mathbf{I}_{n/t})\mathbf{G}, \text{ where}$$

$$\mathbf{R}_{id} = \sum_{i=1}^{l} id_i\mathbf{R}_i \text{ and } \mathbf{S}_{id} = \mathbf{I}_n + \sum_{i=1}^{l} id_i \cdot H_{t,q}(\mathbf{h}_i) \otimes \mathbf{I}_{n/t}.$$

$\mathcal{H}_{\mathrm{ABB}}$ can be proved as a $(1, \nu, \mathcal{O}(\ell\sqrt{m}), \mathsf{negl}(\lambda), \frac{1}{q^t}(1 - \frac{Q}{q^t}))$-LPHF with high min-entropy (Zhang et al. 2016b), where t is the smallest integer satisfying $q^t > 2\nu$. And using it to instantiate our generic IB-DRE construction, we can get our concrete $\text{IB-DRE}_{\mathrm{ABB}}$ scheme in Table 6.

IB-DRE constructions from other LPHFs with high min-entropy

In this section, we plug the LPHFs with high min-entropy corresponding to the adaptively secure IBE schemes in Zhang et al. (2016b); Yamada (2016); Yamada (2017) into our generic IB-DRE construction, and obtain some

Table 6 $\text{IB-DRE}_{\mathrm{ABB}}$ scheme

$\mathsf{Setup}_{\mathrm{ID}}(1^\lambda)$: $(\mathbf{A}, \mathbf{T}_{\mathbf{A}}) \xleftarrow{\$} \mathsf{TrapGen}(1^n, 1^m, q)$, $\mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$, $\mathbf{A}_i^1, \mathbf{A}_i^2 \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [\ell]$. Output $PP = \left(\mathbf{A}, \{\mathbf{A}_i^1\}_{i\in\ell}, \{\mathbf{A}_i^2\}_{i\in\ell}, \mathbf{U}\right)$ and $Msk = \mathbf{T}_{\mathbf{A}}$.

$\mathsf{KeyGen}_{\mathrm{ID}}(PP, Msk, \mathbf{id}_{1st}, \mathbf{id}_{2nd} \in \mathcal{ID})$:

1. Compute $\mathbf{A}_{\mathbf{id}_1} = \mathbf{G} + \sum_{i=1}^{l}(\mathbf{id}_{1st})_i\mathbf{A}_i^1$, $\mathbf{A}_{\mathbf{id}_2} = \mathbf{G} + \sum_{i=1}^{l}(\mathbf{id}_{2nd})_i\mathbf{A}_i^2$.
2. $\left(\mathbf{E}_{\mathbf{id}_1}\right)_i \leftarrow \mathsf{SampleLeft}\left(\mathbf{A}, \mathbf{A}_{\mathbf{id}_1}, (\mathbf{U})_i, \mathbf{T}_{\mathbf{A}}, \sigma\right)$ for $i \in [n]$ and sets $sk_{\mathbf{id}_{1st}} = \mathbf{E}_{\mathbf{id}_1}$. Similarly, it obtain $sk_{\mathbf{id}_{2nd}} = \mathbf{E}_{\mathbf{id}_2}$ such that $\left[\mathbf{A}|\mathbf{A}_{\mathbf{id}_2}\right] \cdot \mathbf{E}_{\mathbf{id}_2} = \mathbf{U}$.
3. Output the secret key $sk_{\mathbf{id}_{1st}} = \mathbf{E}_{\mathbf{id}_1} \in \mathbb{Z}_q^{2m\times n}$ and $sk_{\mathbf{id}_{2nd}} = \mathbf{E}_{\mathbf{id}_2} \in \mathbb{Z}_q^{2m\times n}$.

$\mathsf{Enc}_{\mathrm{ID}}(PP, \mathbf{id}_{1st}, \mathbf{id}_{2nd}, \mathbf{m})$:

Compute $\mathbf{A}_{\mathbf{id}_1}, \mathbf{A}_{\mathbf{id}_2}$ as above. Pick $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e}_0 \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, $\mathbf{e}_{1,1}, \mathbf{e}_{1,2}, \mathbf{e}_{1,3} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z}^m,\alpha' q}$.

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

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

$\mathsf{Dec}_{\mathrm{ID}}(PP, sk_{\mathbf{id}_j}, \mathbf{c})$: Compute $\mathbf{b} = \mathbf{c}_0 - \mathbf{E}_{\mathbf{id}_1}^\top \cdot \begin{bmatrix} \mathbf{c}_{1,1} \\ \mathbf{c}_{1,2} \end{bmatrix}$

$= ((\mathbf{b})_1, \cdots, (\mathbf{b})_n)^\top \in \mathbb{Z}^n$. Set $(\mathbf{m})_i = 1$ if $\left|(\mathbf{b})_i - \lceil \tfrac{q}{2} \rceil\right| < \lceil \tfrac{q}{4} \rceil$; otherwise sets $(\mathbf{m})_i = 0$ where $i \in [n]$. Finally, output a plaintext $\mathbf{m} = ((\mathbf{m})_1, \cdots, (\mathbf{m})_n)^\top$.

concrete IB-DRE schemes on lattice in the standard model. Please see more details in Table 7.

Conclusion

In this paper, we give the frameworks of the DRE and IB-DRE by using the (weak) LPHFs with high min-entropy on lattice. The constructions are based on the learning with error assumption in the standard model and have adaptively secure. And when instantiating with the concrete (w)LPHFs with high min-entropy, we get a concrete DRE scheme and five concrete IB-DRE schemes.

Endnote

[1] Note that Chow et al. (2014) also gave two generic DRE constructions: one is combining Naor-Yung "two-key" paradigm (Naor and Yung 1990) with Groth-Sahai proof system (Groth and Sahai 2008), the other is from lossy trapdoor functions (Peikert and Waters 2011).

Appendix A: Lattice Background

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

Let $\mathbf{S} = \{\mathbf{s}_1, \cdots, \mathbf{s}_n\}$ be a set of vectors in $\mathbb{R}^m$. The Gram-Schmidt orthogonalization of the vectors $\mathbf{s}_1, \cdots, \mathbf{s}_n$ is denoted as $\widetilde{\mathbf{S}} = \{\widetilde{\mathbf{s}}_1, \cdots, \widetilde{\mathbf{s}}_n\}$. $\|\mathbf{S}\|$:= the length of the longest vector in $\mathbf{S}$. For a real matrix $\mathbf{R}$, let $s_1(\mathbf{R}) = \max_{\|\mathbf{u}\|=1} \|\mathbf{R}\mathbf{u}\|$ (respectively, $\|\mathbf{R}\|_\infty = \max \|\mathbf{r}_i\|_\infty$).

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

Learning with Errors Assumption. The learning with errors (LWE) problem was introduced by Regev (2005). For integer $n, m = m(n)$, a prime integer $q > 2$, an error rate $\alpha \in (0,1)$, the LWE problem $\mathsf{LWE}_{q,n,m,\alpha}$ is to distinguish $\{\mathbf{A}, \mathbf{A}^\top\mathbf{s} + \mathbf{e}\}$ 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 (2005) showed that for $\alpha q > 2\sqrt{2n}$, solving the decisional version $\mathsf{LWE}_{q,n,m,\alpha}$ ($\mathsf{DLWE}_{q,n,m,\alpha}$) problem is (quantumly) as hard as approximating the SIVP and GapSVP problems within $\widetilde{\mathcal{O}}(n/\alpha)$ factors in the worst case.

Lemma 16 *Let p, q, n, m be positive integers with $q \geq p \geq 2$ and q prime, the following holds:*

- *(*Ajtai (1999); Alwen and Peikert (2009)*): When $m \geq 6n\lceil\log q\rceil$, the randomized algorithm* $\mathsf{TrapGen}(1^n, 1^m, q)$ *outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ which is statistically close to uniform in $\mathbb{Z}_q^{n\times m}$, and a matrix $\mathbf{T}_\mathbf{A} \in \mathbb{Z}^{m\times m}$ which is a basis of $\Lambda_q^\perp(\mathbf{A})$, satisfying $\|\widetilde{\mathbf{T}_\mathbf{A}}\| \leq \mathcal{O}(\sqrt{n\log q})$ with overwhelming probability.*
- *(*Cash et al. (2010)*): The randomized algorithm* $\mathsf{SampleLeft}(\mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{T}_\mathbf{A}, \sigma)$ *on inputs 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 $\mathbf{T}_\mathbf{A}$ of $\Lambda_q^\perp(\mathbf{A})$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$ and $\sigma \geq \|\widetilde{\mathbf{T}_\mathbf{A}}\| \cdot \omega(\sqrt{\log m})$, outputs a vector $\mathbf{r} \in \mathbb{Z}_q^{2m}$ which is distributed statistically close to $\mathcal{D}_{\Lambda_q^\mathbf{u}(\mathbf{F}),\sigma}$ where $\mathbf{F} = [\mathbf{A}|\mathbf{B}]$.*
- *(*Agrawal et al. (2010)*): The randomized algorithm* $\mathsf{SampleRight}(\mathbf{A}, \mathbf{G}, \mathbf{R}, \mathbf{S}, \mathbf{u}, \mathbf{T}_\mathbf{G}, \sigma)$ *on inputs 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 $\sigma \geq \|\widetilde{\mathbf{T}_\mathbf{G}}\| \cdot s_1(\mathbf{R}) \cdot \omega(\sqrt{\log m})$, outputs a vector $\mathbf{r} \in \mathbb{Z}_q^{2m}$ which is statistically close to $\mathcal{D}_{\Lambda_q^\mathbf{u}(\mathbf{F}),\sigma}$ where $\mathbf{F} = [\mathbf{A}|\mathbf{A}\mathbf{R} + \mathbf{S}\mathbf{G}]$.*
- *(**Gadget Matrix** Micciancio and Peikert (2012)): When $m > n\lceil\log q\rceil$, there exists a full-rank matrix $\mathbf{G} \in \mathbb{Z}_q^{n\times m}$ which is called gadget matrix, satisfies that*

Table 7 IB-DRE schemes from other LPHF with high min-entropy

Schemes	# of $\mathbb{Z}_q^{n\times m}$ matrix |PP|*	Modulus q	Sample width σ	Error width $\alpha' q$	Error width αq	Reduction cost
IB-DRE$_{ZCZ16}$	$\mathcal{O}(\log Q)$	$\mathcal{O}(n^{6.5+7.5\eta+4c})$	$\mathcal{O}(n^{2.5+3.5\eta+2c})$	$\mathcal{O}(n^{3+3\eta+2c})^\dagger$	$\mathcal{O}\left(n^{0.5}\right)$	$\mathcal{O}\left(\frac{\epsilon}{\ell^2 Q^4}\right)$
IB-DRE$_{Yam16}$	$\omega(\sqrt{n})$	$\mathcal{O}(n^{5.5+3.5\eta+2c})$	$\mathcal{O}(n^{2+1.5\eta+c})$	$\mathcal{O}(n^{2.5+\eta+c})\ddagger$	$\mathcal{O}\left(n^{0.5}\right)$	$\mathcal{O}\left(\frac{\epsilon^5}{\ell^2 Q^4}\right)$
IB-DRE$_{MAH}$	$\omega(\log^2 n)$	$\mathcal{O}(n^{6.5+7.5\eta})$	$\mathcal{O}(n^{2+3.5\eta})$	$\mathcal{O}(n^{2.5+3\eta})$	$\mathcal{O}\left(n^{0.5}\right)$	$\mathcal{O}\left(\frac{\epsilon^{2\varphi+1}}{Q^{2\varphi}}\right)\S$
IB-DRE$_{AFF}$	$\omega(\log n)$	poly(n)	poly(n)	poly(n)	$\mathcal{O}\left(n^{0.5}\right)$	$\mathcal{O}\left(\frac{\epsilon^3}{\ell^4 Q^2}\right)$

*, |PP|, |Msk| and |c| show the size of public parameters, master secret key and ciphertext, respectively. ℓ is the length of identity and Q is the bound of secret key queries.
† Assume that η such that $n^\eta > \lceil\log q\rceil = \mathcal{O}(\log n)$, and c is the smallest integer satisfying that $n^c \geq Q + 1$.
‡ $c = c_1 + c_2$ where c_1, c_2 satisfying $\frac{n^{c_1}}{2} \geq Q + 1$ and $n^{-c_2} \leq \epsilon$
§ $\varphi > 1$ is the constant which satisfying $s = 1 - 2^{-\frac{1}{\epsilon}}$, where $s \in \{0, 1\}$ is the relative distance of the underlying error correcting code. We can take φ as close to 1 as one wants

the lattice $\Lambda_q^{\perp}(\mathbf{G})$ *has a public known basis* $\mathbf{T_G} \in \mathbb{Z}_q^{m\times m}$ *with* $\|\widetilde{\mathbf{T_G}}\| \leq \sqrt{5}$.

In Katsumata and Yamada (2016), 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 17 (Noise Rerandomization (Katsumata and Yamada 2016)) *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 6 (Signature Scheme) *A signature scheme* $\mathcal{S}\rangle\} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *is defined as follows:*

- $\mathsf{Gen}(1^\lambda)$*: given the security parameter* λ*, output a pair of verification key and signing key* (vk, sk).
- $\mathsf{Sign}(sk, \mu)$*: given* sk *and a message* $\mu \in \{0,1\}^\star$, *output a signature* $\sigma \in \{0,1\}^\star$.
- $\mathsf{Ver}(vk, \mu, \sigma)$*: output either accept if the signature* σ *is the signature of message* μ *under vk or reject.*

Correctness. *For any message* $\mu \in \mathcal{M}$, *any* $(vk, sk) \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$, *and* $\sigma \xleftarrow{\$} \mathsf{Sign}(sk; \mu)$, $\Pr[\mathsf{Ver}(vk, \mu, \sigma)\ accept] = 1 - \mathsf{negl}(\lambda)$.

Security. *In our construction IND-CCA DRE construction, we need the signature scheme satisfies strong existential unforgeability under one-time chosen message attack. The game between the challenger* $\mathcal{C}$ *and the forger* $\mathcal{S}$ *is as follows: generate* $(vk, sk) \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$ *and give vk to* $\mathcal{S}$; $\mathcal{S}$ *outputs a message* μ; *generate and send* $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, \mu)$ *to* $\mathcal{S}$. $\mathcal{S}$ *wins if it outputs* $(\mu^\star, \sigma^\star) \neq (\mu, \sigma)$ *such that* $\mathsf{Ver}(vk, \mu^\star, \sigma^\star)$ *accepts. The signature scheme is secure if for every PPT adversary* $\mathcal{S}$, $\Pr[\mathcal{S}\ wins] = \mathsf{negl}(\lambda)$.

Acknowledgements
Not applicable.

Funding
This work was supported by National Natural Science Foundation of China (Grant No. 61379141 and No. 61772521), Key Research Program of Frontier Sciences, CAS (Grant No. QYZDB-SSW-SYS035), and the Open Project Program of the State Key Laboratory of Cryptology.

Availability of data and materials
Not applicable.

Authors' contributions
The first author conceived the idea of the study and wrote the paper; all authors discussed the results and revised the final manuscript. All authors read and approved the final manuscript.

Publisher's Note

Received: 11 December 2018 Accepted: 29 April 2019
Published online: 13 June 2019

References

Agrawal S., Boneh D., Boyen X. (2010) Efficient lattice (H)IBE in the standard model. In: Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings. pp 553–572. https://doi.org/10.1007/978-3-642-13190-5_28

Ajtai M. (1999) Generating hard instances of the short basis problem. In: ICALP 1999. pp 1–9

Alwen J., Peikert C. (2009) Generating shorter bases for hard random lattices. In: STOCS 2009. pp 75–86

Cash D., Hofheinz D., Kiltz E., Peikert C. (2010) Bonsai trees, or how to delegate a lattice basis. In: EUROCRYPT 2010. pp 523–552

Chow SSM, Franklin MK, Zhang H (2014) Practical dual-receiver encryption - soundness, complete non-malleability, and applications. In: Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings. pp 85–105. https://dblp.org/rec/bib/conf/ctrsa/ChowFZ14

Diament T, Lee HK, Keromytis AD, Yung M (2004) The dual receiver cryptosystem and its applications. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004. pp 330–343. https://dblp.org/rec/bib/conf/ccs/DiamentLKY04

Georgescu A (2013) Anonymous lattice-based broadcast encryption. In: Information and Communicatiaon Technology - International Conference, ICT-EurAsia 2013, Yogyakarta, Indonesia, March 25-29, 2013. Proceedings. pp 353–362. https://dblp.org/rec/bib/conf/ict-eurasia/Georgescu13

Groth J, Sahai A (2008) Efficient non-interactive proof systems for bilinear groups. In: Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings. pp 415–432. https://dblp.org/rec/bib/conf/eurocrypt/GrothS08

Joux A (2000) 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. pp 385–394. https://dblp.org/rec/bib/conf/ants/Joux00

Katsumata S, Yamada S (2016) Partitioning via non-linear polynomial functions: More compact ibes from ideal lattices and bilinear maps. In: Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II. pp 682–712. http://dblp.uni-trier.de/rec/bib/conf/asiacrypt/Katsumata016

Kiltz E (2006) Chosen-ciphertext security from tag-based encryption. In: Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings. pp 581–600. https://dblp.org/rec/bib/conf/tcc/Kiltz06

Libert B, Paterson KG, Quaglia EA (2012) 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. pp 206–224. https://dblp.org/rec/bib/conf/pkc/LibertPQ12

Micciancio D, Peikert C (2012) Trapdoors for lattices: Simpler, tighter, faster, smaller. In: Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings. pp 700–718. http://dblp.uni-trier.de/rec/bib/conf/eurocrypt/MicciancioP12

Naor M, Yung M (1990) Public-key cryptosystems provably secure against chosen ciphertext attacks. In: Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, STOC 1990, May 13-17, 1990, Baltimore, Maryland, USA. pp 427–437. https://dblp.org/rec/bib/conf/stoc/NaorY90

Peikert C, Waters B (2011) Lossy trapdoor functions and their applications. SIAM J Comput 40(6):1803–1844

Regev O (2005) On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing, STOC 2005, Baltimore, MD, USA, May 22-24, 2005. pp 84–93. http://dblp.uni-trier.de/rec/bib/conf/stoc/Regev05

Wang J, Bi J (2010) Lattice-based identity-based broadcast encryption scheme. IACR Cryptology ePrint Archive 2010:288
Wang F, Wang XA, Wang C (2015) Lattice-based dynamical and anonymous broadcast encryption scheme for wireless ad hoc networks. J Interconnection Netw 15(3-4):1–14
Waters B (2005) Efficient identity-based encryption without random oracles. In: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings. pp 114–127. https://dblp.org/rec/bib/conf/eurocrypt/Waters05
Yamada S (2016) Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In: Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II. pp 32–62. http://dblp.uni-trier.de/rec/bib/conf/eurocrypt/Yamada16
Yamada, S (2017) Asymptotically compact adaptively secure lattice ibes and verifiable random functions via generalized partitioning techniques. In: Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III. pp 161–193. http://dblp.org/rec/bib/conf/crypto/Yamada17
Zhang K, Chen W, Li X, Chen J, Qian H (2016a) New application of partitioning methodology: identity-based dual receiver encryption. Secur Commun Netw 9(18):5789–5802
Zhang J, Chen Y, Zhang Z (2016b) Programmable hash functions from lattices: Short signatures and ibes with small key sizes. In: Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III. pp 303–332. http://dblp.uni-trier.de/rec/bib/conf/crypto/ZhangCZ16
Zhang D., Li J., Li B., Lu X., Xue H., Jia D., Liu Y. (2019) Deterministic Identity-Based Encryption from Lattice-Based Programmable Hash Functions with High Min-Entropy Vol. 2019. pp 1816393:1–1816393:12. https://doi.org/10.1155/2019/1816393
Zhang D, Zhang K, Li B, Lu X, Xue H, Li J (2018b) Lattice-based dual receiver encryption and more. In: ACISP 2018. pp 520–538. https://dblp.org/rec/bib/conf/acisp/ZhangZLLXL18