Anonymous Lattice Identity-Based Encryption with Traceable Identities

Anonymous Lattice Identity-Based Encryption with Traceable Identities

Xavier Boyen[1], Ernest Foo[2], and Qinyi Li[2⋆]

[1] QUT, Brisbane, Australia
[2] Griffith University, Brisbane, Australia
qinyi.li@griffith.edu.au

Abstract. An anonymous identity-based encryption with tracing identities (AIBET) system enjoys that same strong privacy for receivers as a normal anonymous identity-based encryption system. Additionally, an AIBET system offers an identity tracing mechanism, which allows a tracer, who has an identity-associated tracing key, to uncover the recipient's identity from the ciphertext. In this paper, we present an AIBET system based on plain lattices by exploiting a hierarchical power of lattice trapdoors in a novel way. We prove the security of the system under the conservative learning-with-errors assumption in the standard model. This is the first AIBET system provably secure under quantum-resistant assumptions. Our construction's efficiency is comparable to the state-of-the-art lattice anonymous identity-based encryption system.

Keywords: Identity-based Encryption · Anonymity · Lattice.

1 Introduction

Identity-based encryption (IBE) is a type of public-key encryption in which a user's public key is its identity, such as an identity number or an email address. Users' private identity keys are issued by a trusted authority called key generation centre (KGC). Encryption can be done using the recipient's identity rather than using certified public keys, which simplifies public key management of traditional public-key encryption where dedicated infrastructures need to be maintained.

Anonymous identity-based encryption offers an additional privacy guarantee to standard identity-based encryption. Anonymous IBE hides the recipient's identity from those who do not have the corresponding private identity key. Although such strong privacy is attractive and benign from an individual's point of view, it can potentially become a dangerous means for unlawful parties to hide communications against public safety or interest. For example, in an email filtering system (a typical scenario where anonymous IBE systems are used), the gateway may need to filter out all encrypted emails sent to a user who has misbehaved. Standard anonymous IBE prevents the gateway from implementing such

⋆ Corresponding author

filtering since the gateway cannot identify the recipients from ciphertexts. Therefore, an additional traceability function, which enables the recipients' identities to be revealed from the ciphertext, needs to be incorporated into anonymous IBE systems to enable such filtering.

Blazy et al. [4] first formalised and constructed anonymous identity-based encryption with traceable identities (AIBET).[3] In addition to all components of an anonymous IBE system, an AIBET system allows a tracer, who is given identity-associated tracing keys, to test if a given ciphertext is destined for a particular recipient. Two security notions are formally defined for AIBET systems in [4]. The notion of anonymity requires that given a ciphertext, the recipient's identity remains hidden from someone without the corresponding private identity key and tracing key. The notion of indistinguishability requires that for given a ciphertext *and* a tracing key with the same identity, no one can distinguish between a ciphertext that encapsulates the session key and a random string from the ciphertext space. Such a formalisation highlights the importance that data confidentiality (protected by the session key) should be preserved even if privacy is lost (by the identity traceability). Note that the KGC and a tracer are separated entities in [4] which reflects that a tracer, which has significantly less power than KGC, may function as a gateway, and the system will retain confidentiality even if tracers are corrupted.

Blazy et al. [4] provide two constructions of AIBET using pairing-friendly cyclic groups in the standard model. The first construction, based on Boyen's standard-model anonymous IBE system [8], offers selective security (with a polynomial-time reduction, or adaptive security using the complexity leveraging technique [6]). The second construction, is based on Blazy et al.'s affine-MAC IBE [5], and directly enjoys adaptive security. However, both constructions' security is ultimately based on the hardness of computing the discrete logarithms of the groups, which would be insecure under quantum computers. To the best of our knowledge, no AIBET systems are known *with provable security* based on non-discrete-log-type and quantum-resistant assumptions. [4]

Our contribution and approach. Motivated by extending the constructions of AIBET system from different, especially quantum-resistant computational assumptions, we construct an AIBET system using plain lattices, which is provably secure under the conservative and (conjectured) quantum-resistant learning-with-errors assumption, in the standard model.

An AIBET system has three levels of secret, the master private key, private identity keys, and tracing keys. Being of the highest privilege, the master private key can be used to generate private identity keys and tracing keys while the reverse is computationally infeasible. Private identity keys can be used to decrypt

[3] Instead of full-fledged encryption, Blazy et al. actually consider anonymous identity-based *key encapsulation mechanism* with tracing identities.

[4] We note that Lin et al. [14] propose a construction of AIBET system based on the anonymous IBE system of Katsumata and Yamada [12]. However, the work does not address the notion of indistinguishability which is what differentiates an AIBET system from a standard anonymous IBE system.

corresponding ciphertexts, recovering the messages (in the case of encryption) or the session keys (in the case of a key encapsulation mechanism), and revealing the recipients' identities from the ciphertexts, whereas tracing keys only reveals the recipients' identities but cannot affect the confidentiality of the messages or encapsulated session keys. We implement a hierarchical relation based on Agrawal et al.'s anonymous IBE system [2] by exploiting the hierarchical power of lattice trapdoors.

Technically, a (nearly) uniformly random matrix $\mathbf{F} \in \mathbb{Z}_q^{n \times m}$ where $m = O(n \log q)$, defines a so-called q-ary lattice (see Section 2.1). A strong trapdoor of $\mathbf{F}$ is a matrix $\mathbf{R}$ with an invertible square matrix $\mathbf{H}$ such that $\mathbf{F} = [\mathbf{A}|\mathbf{AR}+\mathbf{HG}]$, where $\mathbf{G}$ allows efficient low norm solutions to $\mathbf{GX} = \mathbf{0}$. A trapdoor of $\mathbf{F}$ is a low norm $\mathbf{T} \in \mathbb{Z}^{m \times m}$ such that $\mathbf{FT} = \mathbf{0}$ where all columns are linearly independent (i.e., $\mathbf{T}$ is a low norm basis for the q-ary lattice defined by $\mathbf{F}$). A weak trapdoor for $\mathbf{F}$ with respect to a random matrix $\mathbf{U} \in \mathbb{Z}_q^{n \times \ell}$ is a low norm matrix $\mathbf{D} \in \mathbb{Z}_q^{n \times \ell}$ such that $\mathbf{FD} = \mathbf{U}$. Established by a series of works on lattice trapdoors [11, 2, 9, 15], a strong trapdoor $\mathbf{R}$ can be used to efficiently generate a trapdoor $\mathbf{T}$, which in turn can be used to efficiently generates a weak trapdoor $\mathbf{D}$. With such mathematical relations, our construction essentially uses $\mathbf{R}$, $\mathbf{T}$, and $\mathbf{D}$ as the master private key, a private identity key, and a tracing key. The ciphertext of our system, like most standard model lattice encryption systems, is the dual-Regev ciphertext [17, 11]:

$$\mathbf{c}_0^\intercal = \mathbf{s}^\intercal \mathbf{F} + \mathbf{e}_0^\intercal \quad ; \quad \mathbf{c}_1^\intercal = \mathbf{s}^\intercal \mathbf{U} + \mathbf{e}_1^\intercal + \mu \cdot \lfloor q/2 \rfloor$$

where the superscript $\intercal$ denotes the vector/matrix transpose, $\mathbf{F} \in \mathbb{Z}_q^{n \times (m+w)}$ with $m, w = O(n \log q)$, $\mathbf{U} \in \mathbb{Z}_q^{\lambda}$, and $\mathbf{e}_0$ and $\mathbf{e}_1$ are low-norm vectors. Decryption requires recovering $\mathbf{s}$, which can be done by using $\mathbf{T}$, and identity tracing requires recovering μ, which can be done by using $\mathbf{D}$. Anonymity is retained when none of these trapdoors are present, since $\mathbf{c}_0$, $\mathbf{c}_1$ are samples of the LWE problem. Confidentiality is retained even given a tracing key $\mathbf{D}$ since it does not help recovering $\mathbf{s}$. To allow tracing identity id, a tracing key associated with id is created that is able to partial decrypt a given ciphertext. Extra partial decryption verification information is provided along with the ciphertext to allow verification of the partial decryption. If the partial decryption verifies, the tracer can be ensure that the recipient's identity for the ciphertext is id.

2 Preliminary

Let $\mathbf{R}$ be a matrix in $\mathbb{Z}^{m \times k}$. We use $\|\mathbf{R}\|$ to denote ℓ_2 norm of the longest column of $\mathbf{R}$, and $\|\mathbf{R}\|_\infty$ to denote the largest magnitude of the entries in $\mathbf{R}$. Let $s_1(\mathbf{R})$ denote the operator norm of $\mathbf{R}$, i.e., $s_1(\mathbf{R}) = \sup_{\|\mathbf{x}\|=1} \|\mathbf{Rx}\|$. We denote by $x \leftarrow X$ the process of sampling x according to the distribution X. Let $x \sim X$ denote sample x satisfies distribution X. We use $U(X)$ to denote the uniform distribution over the set X. We will be using standard asymptotic notations, e.g., O, Ω, ω. Let $\lambda \in \mathbb{N}$, the function $f : \mathbb{N} \to \mathbb{R}$ is said to be negligible if $f(\lambda) = \lambda^{-\omega(1)}$ and is written as $f(\lambda) = \mathsf{negl}(\lambda)$.

Let X and Y be two random variables over some finite set S. The statistical distance between X and Y is defined as $\Delta(X,Y) = \frac{1}{2}\sum_{s\in S}\left|\Pr[X=s] - \Pr[Y=s]\right|$. Let X_λ and Y_λ be ensembles of random variables indexed by the security parameter λ. We say that X and Y are $\mathsf{negl}(\lambda)$-statistically close (or simply statistically close) if $\Delta(X_\lambda, Y_\lambda) = \mathsf{negl}(\lambda)$.

For any integer q, $x \in \mathbb{Z}_q$, the algorithm $\mathsf{Round}(x)$ returns 0 if x is closer to 0 than to $\lfloor q/2 \rfloor$ modulo q. Otherwise, it returns 1. The algorithm naturally extends component-wise to vectors.

2.1 Lattices, Discrete Gaussians, and Trapdoors

Lattice. Let q be a prime, $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{u} \in \mathbb{Z}_q^n$. A q-ary lattice and its shift are defined as $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = \mathbf{0} \pmod q\}$ and $\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = \mathbf{u} \pmod q\}$. A basis for lattice $\Lambda_q^\perp(\mathbf{A})$ is a m-by-m matrix $\mathbf{T}$ with linearly independent column vectors in $\Lambda_q^\perp(\mathbf{A})$. By definition we have $\mathbf{AT} = \mathbf{0} \in \mathbb{Z}_q^{n\times m}$.

Discrete Gaussians. Let $m \in \mathbb{Z}$ be a positive integer and $\Lambda \subset \mathbb{Z}^m$. For any real vector $\mathbf{c} \in \mathbb{R}^m$ and positive parameter $\sigma \in \mathbb{R}_{>0}$, let the Gaussian function $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi\|\mathbf{x}\|^2/\sigma^2\right)$ on $\mathbb{R}^m$ with center $\mathbf{0}$ and parameter σ. Define the discrete Gaussian distribution over Λ with center $\mathbf{0}$ and parameter σ as $D_{\Lambda,\sigma} = \rho_\sigma(\mathbf{y})/\rho_\sigma(\Lambda)$ for $\forall \mathbf{y} \in \Lambda$, where $\rho_\sigma(\Lambda) = \sum_{\mathbf{x}\in\Lambda}\rho_\sigma(\mathbf{x})$. The following lemma bounds the length of a discrete Gaussian vector.

Lemma 1 ([16]). *For any lattice Λ of integer dimension m, and parameter $\sigma \geq \omega(\sqrt{\log m})$, $\Pr[\|\mathbf{x}\| > \sigma\sqrt{m} : \mathbf{x} \leftarrow D_{\Lambda,\sigma}] \leq \mathsf{negl}(m)$.*

The following lemmas about the property of discrete Gaussians are useful for arguing the security of our construction.

Lemma 2 ([12], Lemma 1). *Let n, q, ℓ, m be positive integers and r a positive real satisfying $r \geq \omega(\sqrt{\log n})$. Let $\mathbf{b} \in \mathbb{Z}_q^m$ be arbitrary and $\mathbf{z} \leftarrow D_{\mathbb{Z}^m,r}$. Then there exists an efficient algorithm ReRand such that for any $\mathbf{D} \in \mathbb{Z}^{m\times\ell}$ and positive real $\sigma \geq s_1(\mathbf{D})$, the output of $\mathsf{ReRand}(\mathbf{D}, \mathbf{b}^\intercal + \mathbf{z}^\intercal, r, \sigma)$ is distributed as $\mathbf{b'}^\intercal = \mathbf{b}^\intercal\mathbf{D} + \mathbf{z'}^\intercal \in \mathbb{Z}_q^\ell$ where the distribution of $\mathbf{z'}$ is statistically close to $D_{\mathbb{Z}^\ell, 2r\sigma}$.*

Lemma 3 ([15], Lemma 2.9). *Let $h > 0$, $w > 0$ be integers and $s > 0$. For $\mathbf{R} \leftarrow D_{\mathbb{Z},s}^{h\times w}$, $s_1(\mathbf{R}) \leq s \cdot O(\sqrt{h} + \sqrt{w})$ with all but probability $2^{-\Omega(h+w)}$.*

Lemma 4 ([11], Lemma 5.2). *For prime q and integer $b \geq 2$, let $m \geq n\log q + \omega(\log n)$. For $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n\times m})$, $\mathbf{r} \leftarrow D_{\mathbb{Z}^m,s}$ with $s \geq \omega(\sqrt{\log n})$, the distribution of $\mathbf{Ar} \in \mathbb{Z}_q^n$ is statistically close to $U(\mathbb{Z}_q^n)$ with overwhelming probability. Moreover, the distribution of $\mathbf{r}$ conditioned on $\mathbf{Ar} = \mathbf{u} \in \mathbb{Z}_q^n$ is $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),s}$.*

Learning with Errors Assumption. The security of our constructions is based on the earning-with-errors (LWE) problem introduced by Regev [17]. Below we follow the work [13] for the formulation of the LWE problem. We note that this formulation is equivalent to the standard formulation, and has been used in literature in lattice-based cryptosystems [13, 1].

Definition 1 (LWE). *For integers $q = q(n) \geq 2$ and an error distribution $\chi = \chi(n)$ over $\mathbb{Z}_q$, the advantage of an adversary $\mathcal{A}$ for the learning with errors problem $\mathsf{LWE}_{n,m,q,\chi}$ is defined as*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LWE}_{n,m,q,\chi}}(\lambda) = |\Pr[\mathcal{A}(\mathbf{A}, \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal) = 1] - \Pr[\mathcal{A}(\mathbf{A}, \mathbf{b}^\intercal + \mathbf{e}^\intercal) = 1]|$$

where $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^m$ and $\mathbf{b} \leftarrow \mathbb{Z}_q^n$. We say $\mathsf{LWE}_{n,m,q,\chi}$ assumption holds if for all p.p.t adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LWE}_{n,m,q,\chi}} \leq negl(n)$.

Regev [17] shows that for $\alpha q \geq \sqrt{n}$ is as hard as approximating some traditional worst-case lattice problems, e.g., SIVP problem. We refer to [17] for details.

Lattice Trapdoors. Let $n \geq 1$, $q \geq 2$ and $p \leq q$. Let $w = n\lceil \log q \rceil$, we use the n-by-w gadget matrix ([15]) defined as $\mathbf{G} = \mathbf{I}_n \otimes [1, 2, 4, ..., 2^{k-1}] \in \mathbb{Z}_q^{n\times w}$. One useful property of $\mathbf{G}$ is that the q-ary lattice it defines, i.e., $\Lambda_q^\perp(\mathbf{G})$ has a publicly known basis $\mathbf{T_G} \in \mathbb{Z}^{w\times w}$ with low norm $\|\mathbf{T_G}\| \leq \sqrt{5}$ (see [15], Proposition 4.2).

[15] shows how to use matrix $\mathbf{G}$ to sample a nearly uniformly random matrix $\mathbf{F} \in \mathbb{Z}_q^{n\times(m+w)}$ along with "strong" trapdoor for the lattice $\Lambda_q^\perp(\mathbf{F})$: (1) Pick $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n\times m})$, $\mathbf{R} \leftarrow D_{\mathbb{Z},\omega(\sqrt{\log n})}^{m\times w}$, any n-by-n matrix $\mathbf{H}$ invertible over $\mathbb{Z}_q^{n\times n}$; (2) Return $\mathbf{F} = [\mathbf{A}|\mathbf{AR} + \mathbf{HG}]$ and gadget trapdoor $\mathbf{R}$. The Gaussian $\mathbf{R}$ is "strong" in the sense that whereas it is not a basis of lattice $\Lambda_q^\perp(\mathbf{F})$, it does everything that a low-norm basis does, and it can be used to efficiently generate low-norm basis for $\Lambda_q^\perp(\mathbf{F})$. The following lemmas, collected from [2, 15] states this property which will be extensively used in our construction.

Lemma 5 ([2], Theorem 10, and [15], Theorem 5.1). *Let $q > 2$, $m > n$, $k \geq 1$, and $\sigma > 5 \cdot s_1(\mathbf{R}) \cdot \omega(\sqrt{\log n})$, $\mathbf{U} \in \mathbb{Z}_q^{n\times k}$, there exists an efficient algorithm $\mathsf{SampleRight}(\mathbf{R}, \mathbf{F}, \mathbf{H}, \mathbf{U}, \sigma)$ that outputs a matrix $\mathbf{D} \in \mathbb{Z}^{(m+w)\times k}$ distributed statistically close to $D_{\Lambda_q^{\mathbf{U}}(\mathbf{F}),s}$.*

In particular, there exist an efficient algorithm $\mathsf{SampBasisRight}(\mathbf{R}, \mathbf{F}, \mathbf{H}, s)$ that outputs a matrix $\mathbf{T} \in \mathbb{Z}^{(m+w)\times(m+w)}$, distributed statistically close to $D_{\Lambda_q^\perp}(\mathbf{F}, s)$, which is a basis of lattice $\Lambda_q^\perp(\mathbf{F})$, i.e., $\mathbf{FT} = \mathbf{0}$ and the column vectors of $\mathbf{T}$ are linearly independent.

We note that $\mathsf{SampBasisRight}$ basically runs $\mathsf{SampleRight}(\mathbf{R}, \mathbf{F}, \mathbf{H}, \mathbf{0}, \sigma)$ for $\mathbf{0} \in \mathbb{Z}^n$ many times until the output vectors are all linearly independent, forming a basis. By [3], sampling $2(m + w)$ such vectors using $\mathsf{SampleRight}$ would be enough to get one basis on expectation.

The following lemma shows that a short basis of $\mathbf{A}$ can be used to solve learning with errors (LWE) problem defined by $\mathbf{A}$.

Lemma 6. *Let* $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n\times m})$ *where* $m > 2n$. *Let* $\mathbf{T} \in \mathbb{Z}^{m\times m}$ *be a basis of lattice* $\Lambda_q^{\perp}(\mathbf{A})$. *Given* $\mathbf{y}^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal$ *where* $\mathbf{s} \in \mathbb{Z}_q^n$, $\mathbf{e} \in \mathbb{Z}^m$ *with* $\|\mathbf{e}^\intercal\mathbf{T}\|_\infty < q$. *Then there exists an efficient algorithm* $\mathsf{Invert}(\mathbf{A}, \mathbf{T}, \mathbf{y})$ *outputs* $\mathbf{s}$ *and* $\mathbf{e}$ *with overwhelming probability.*

Basically, the algorithm works by computing $\mathbf{y}^\intercal \bmod q = \mathbf{e}^\intercal\mathbf{T} \bmod q$. Since $\|\mathbf{e}^\intercal\mathbf{T}\|_\infty < q$, $\mathbf{e}^\intercal\mathbf{T} \bmod q = \mathbf{e}^\intercal\mathbf{T} \in \mathbb{Z}^m$. As $\mathbf{T}$ has linearly independent columns (by the definition of lattice basis), one can use Gaussian elimination to recover $\mathbf{e}$ and then $\mathbf{s}^\intercal\mathbf{A}$. Finally, since a $\mathbf{A}$ has at least n linearly independent column vectors, $\mathbf{s}$ can be recovered by Gaussian elimination.

2.2 Definition

In this section, we give definitions for AIBET systems. As in [4], we define AIBET systems in the form of a key encapsulation mechanism instead of a full-fledged encryption.[5] An anonymous identity-based key encapsulation mechanism replaces the encryption algorithm by a key encapsulation algorithm which uses the target identity to produce a session key (with bit-length as the security parameter) and a ciphertext. The decryption algorithm is replaced by a key decapsulation algorithm which applies the private identity key to the ciphertext to recover the session key. In practice, such a key encapsulation mechanism is used with a symmetric-key cipher to encrypt bulky data.

An AIBET with session key space $\mathcal{K}$, identity space $\mathcal{ID}$, and ciphertext space $\mathcal{C}$, consist of six efficient algorithms. The key generation centre (KGC), trusted by all users, runs $\mathsf{Setup}(1^\lambda)$ which takes as input a security parameter λ and returns the public parameters Pub and a master private key Msk. To obtain a private identity key, a user submits its identity id to the KGC. After verifying id, KGC runs $\mathsf{Extract}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$ which produces an identity private key $\mathsf{Sk}_{\mathsf{id}}$. The KGC runs the tracing key generation algorithm $\mathsf{TskGen}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$ generates an identity tracing key for a given identity id. The sender runs the encapsulation algorithm $\mathsf{Encap}(\mathsf{Pub}, \mathsf{id})$ to generate a session key $\mathsf{K} \in \mathcal{K}$ (which may be used with a symmetric-key cipher to encrypt the actual data), and generates a ciphertext Ct that encapsulates K. Upon receiving the ciphertext Ct, the receiver runs the key decapsulation algorithm $\mathsf{Decap}(\mathsf{Pub}, \mathsf{Sk}_{\mathsf{id}}, \mathsf{Ct})$ which recovers a session key K or return $\perp$, indicating decapsulation is failed. A tracer runs the tracing algorithm $\mathsf{TkVer}(\mathsf{Td}_{\mathsf{id}}, \mathsf{id}, \mathsf{Ct})$ to check whether a ciphertext Ct is for the given identity id. TkVer returns 1 if Ct is for the user with identity id, or 0, otherwise.

We consider correctness and soundness of AIBET systems. For all $\lambda \in \mathbb{N}$, all pairs of $(\mathsf{Pub}, \mathsf{Msk}) \leftarrow \mathsf{Setup}(1^\lambda)$, all identities $\mathsf{id} \in \mathcal{ID}$, all $\mathsf{Sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$, and all $\mathsf{Td}_{\mathsf{id}} \leftarrow \mathsf{TskGen}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$, the correctness of AIBET requires that

$$\Pr\left[(\mathsf{Decap}(\mathsf{Pub}, \mathsf{Sk}_{\mathsf{id}}, \mathsf{Ct}) = \mathsf{k}) \wedge (\mathsf{TkVer}(\mathsf{Td}_{\mathsf{id}}, \mathsf{id}, \mathsf{Ct}) = 1)\right] \geq 1 - \mathsf{negl}(\lambda)$$

[5] In this paper, we use the acronym AIBET for both anonymous identity-based encryption with traceable identities and anonymous identity-based key encapsulation mechanism with traceable identities.

and the soundness of AIBET requires

$$\Pr[\mathsf{Decap}(\mathsf{Pub}, \mathsf{Sk}_{\mathsf{id}}, \mathsf{Ct}) = \perp \mid \mathsf{TkVer}(\mathsf{Td}_{\mathsf{id}}, \mathsf{id}, \mathsf{Ct}) = 0] \geq 1 - \mathsf{negl}(\lambda)$$

where the probability is taken over the randomness of all the algorithms of the AIBET system.

Following [4], we give the definitions of anonymity and ciphertext indistinguishability for AIBET. Anonymity essentially states a ciphertext of an AIBET system is computationally indistinguishable from a random string from the ciphertext space, provided the efficient adversary does not have the tracing key of the ciphertext identity. Ciphertext indistinguishability ensures that given a ciphertext and a session key, it is computationally infeasible for to tell whether the session key is valid (i.e. correctly encapsulated in the ciphertext) or a random string, even with the tracing key associated with the identity of the ciphertext.

Definition 2. *Let $\lambda \in \mathbb{N}$ be the security parameter. We say an AIBET system $\Pi = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encap}, \mathsf{TskGen}, \mathsf{Decap}, \mathsf{TkVer})$, with session key space $\mathcal{K}$, identity space $\mathcal{ID}$, and ciphertext space $\mathcal{C}$, has ciphertext anonymity (or is anonymous) against selective-identity attack and chosen-plaintext attack if*

$$\mathsf{Adv}^{\mathrm{anon}}_{\Pi,\mathcal{A}}(\lambda) = \left| \Pr[\mathsf{Exp}^{\mathrm{anon}}_{\Pi,\mathcal{A}}(\lambda) = 1] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

where the experiment $\mathsf{Exp}^{\mathrm{anon}}_{\Pi,\mathcal{A}}(\lambda)$ is defined in Figure 1, in which the challenge identity id^* is not allowed to query oracles $\mathcal{O}_{\mathsf{Extract}}(\cdot)$ and $\mathcal{O}_{\mathsf{TskGen}}(\cdot)$.

Experiment $\mathsf{Exp}^{\mathrm{anon}}_{\Pi,\mathcal{A}}\lambda)$:

1. $\mathsf{id}^* \leftarrow \mathcal{A}(1^\lambda)$ with $\mathsf{id}^* \in \mathcal{ID}$
2. $(\mathsf{Pub}, \mathsf{Msk}) \leftarrow \mathsf{Setup}(1^\lambda)$
3. $\mathsf{state} \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Extract}}(\cdot),\mathcal{O}_{\mathsf{TskGen}}(\cdot)}(\mathsf{Pub})$
4. $(\mathsf{K}, \mathsf{Ct}^*_0) \leftarrow \mathsf{Encap}(\mathsf{Pub}, \mathsf{id}^*)$
5. $\mathsf{Ct}^*_1 \leftarrow U(\mathcal{C})$, $b \leftarrow U(\{0,1\})$
6. $b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Extract}}(\cdot),\mathcal{O}_{\mathsf{TskGen}}(\cdot)}(\mathsf{state}, \mathsf{Ct}^*_b)$
7. Return 1 if $b' = b$; Otherwise, 0

Oracle $\mathcal{O}_{\mathsf{Extract}}(\mathsf{id})$: // $\mathsf{id} \neq \mathsf{id}^*$

1. Return $\mathsf{Sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$

Oracle $\mathcal{O}_{\mathsf{TskGen}}(\mathsf{id})$: // $\mathsf{id} \neq \mathsf{id}^*$

1. Return $\mathsf{Td}_{\mathsf{id}} \leftarrow \mathsf{TskGen}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$

Fig. 1: Anonymity Experiment of AIBET.

Definition 3. *Let λ be the security parameter. We say an AIBET system $\Pi = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encap}, \mathsf{TskGen}, \mathsf{Decap}, \mathsf{TkVer})$, with session key space $\mathcal{K}$, identity space $\mathcal{ID}$, and ciphertext space $\mathcal{C}$, has ciphertext indistinguishability against selective-identity attack and chosen-plaintext attack if*

$$\mathsf{Adv}^{\mathrm{ind-sid-cpa}}_{\Pi,\mathcal{A}}(\lambda) = \left| \Pr[\mathsf{Exp}^{\mathrm{ind-sid-cpa}}_{\Pi,\mathcal{A}}(\lambda) = 1] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

where the experiment $\mathsf{Exp}^{\mathrm{ind-sid-cpa}}_{\Pi,\mathcal{A}}(\lambda)$ *is defined in Figure 2 and the challenge identity* id^* *is allowed for* $\mathcal{O}_{\mathsf{TskGen}}(\cdot)$ *but not allowed for* $\mathcal{O}_{\mathsf{Extract}}(\cdot)$.

Experiment $\mathsf{Exp}^{\mathrm{ind-sid-cpa}}_{\Pi,\mathcal{A}}\lambda)$:

1. $\mathsf{id}^* \leftarrow \mathcal{A}(1^\lambda)$ with $\mathsf{id}^* \in \mathcal{ID}$
2. $(\mathsf{Pub}, \mathsf{Msk}) \leftarrow \mathsf{Setup}(1^\lambda)$
3. $\mathsf{state} \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Extract}}(\cdot),\mathcal{O}_{\mathsf{TskGen}}(\cdot)}(\mathsf{Pub})$
4. $(\mathsf{K}^*_0, \mathsf{Ct}^*) \leftarrow \mathsf{Encap}(\mathsf{Pub}, \mathsf{id}^*)$
5. $\mathsf{K}^*_1 \leftarrow U(\mathcal{K})$, $b \leftarrow U(\{0,1\})$
6. $b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Extract}}(\cdot),\mathcal{O}_{\mathsf{TskGen}}(\cdot)}(\mathsf{state}, \mathsf{Ct}^*, \mathsf{K}^*_b)$
7. Return 1 if $b' = b$; Otherwise, 0

Oracle $\mathcal{O}_{\mathsf{Extract}}(\mathsf{id})$: // $\mathsf{id} \neq \mathsf{id}^*$

1. Return $\mathsf{Sk}_{\mathsf{id}} \leftarrow \mathsf{Extract}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$

Oracle $\mathcal{O}_{\mathsf{TskGen}}(\mathsf{id})$:

1. Return $\mathsf{Td}_{\mathsf{id}} \leftarrow \mathsf{TskGen}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$

Fig. 2: Ciphertext Indistinguishability Experiment of AIBET.

2.3 Construction

Parameters. Let λ be the security parameter. We assume that all parameters are functions of λ. The construction uses a set of public known parameters $(n, q, m, w, H, s, r, \alpha, \sigma)$ that we specify here. We assume all algorithms of the system implicitly take this parameter set as input.

- Let $n \geq 2$, prime $q \geq 2$, $w = n\lceil \log q \rceil$, and $m \geq n \log q + \omega(\log n)$. The identity space is $\mathcal{ID} = \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$.
- Let $H : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n \times n}$ be a full-rank difference encoding (FRD) (see [2]). It has a property that for $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n$ where $\mathbf{x} \neq \mathbf{y}$, $H(\mathbf{x}) - H(\mathbf{y})$ is invertible over $\mathbb{Z}_q^{n \times n}$. In particular, $H(\mathbf{x})$ is invertible over $\mathbb{Z}_q^{n \times n}$ for non-zero $\mathbf{x}$.
- Set $s = O(\sqrt{m}) \cdot \omega(\log n)$, $r = \alpha q$, $\alpha = \left(\omega(\log^{1.5} n) \cdot O(m^{2.5})\right)^{-1}$, and $\sigma \geq \omega(\log^{1.5} n) \cdot O(m^{2.5})$ large enough for correctness and security.

In our construction, we assume each identity id can only be given exactly one tracing key $\mathsf{Td}_{\mathsf{id}}$. If the same identity is used to request a tracing key more than once, the same tracing key will be returned. We note such a restriction has happened in existing IBE systems, e.g., Gentry's IBE system [10], and a pseudorandom function (PRF) can simply make the system stateless.

Algorithm descriptions. We recall that for integer $q > 2$, $x \in \mathbb{Z}_q$, the algorithm $\mathsf{Round}(x)$ returns 0 if x is closer to 0 than to $\lfloor q/2 \rfloor$ modulo q. Otherwise, it returns 1. The algorithm naturally extends component-wise to vectors. In the construction $\oplus$ denotes the XOR operation. The construction of the AIBET system Π is described as follows.

- $\mathsf{Setup}(1^\lambda)$:

1. Sample $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n\times m})$, $\mathbf{R} \leftarrow D^{m\times w}_{\mathbb{Z},\omega(\sqrt{\log n})}$.
2. Set $\mathbf{A}_1 \leftarrow \mathbf{AR}$ and $\mathbf{U}, \mathbf{U}_1 \leftarrow U(\mathbb{Z}_q^{n\times\lambda})$.
3. Output $\mathsf{Pub} = (\mathbf{A}, \mathbf{A}_1, \mathbf{U}, \mathbf{U}_1)$ and $\mathsf{Msk} = \mathbf{R}$.

– $\mathsf{Extract}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$:
1. Set $\mathbf{F}_{\mathsf{id}} \leftarrow [\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}]$.
2. Sample $\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{SampBasisRight}(\mathbf{A}, \mathbf{F}_{\mathsf{id}}, \mathbf{R}, H(\mathsf{id}), s) \in \mathbb{Z}^{(m+w)\times(m+w)}$
3. Return $\mathsf{Sk}_{\mathsf{id}} \leftarrow \mathbf{T}_{\mathsf{id}}$.

– $\mathsf{Encap}(\mathsf{Pub}, \mathsf{id})$:
1. Sample, $\mathbf{k}', \mathbf{k}'' \leftarrow U(\{0,1\}^\lambda)$; Set $\mathbf{k} \leftarrow \mathbf{k}' \oplus \mathbf{k}''$.
2. Sample $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$, $\mathbf{e}_0, \leftarrow D^m_{\mathbb{Z},r}$, $\mathbf{e}_1 \leftarrow D^w_{\mathbb{Z},2r\sigma}$, $\mathbf{e}_2 \leftarrow D^\lambda_{\mathbb{Z},2r\sigma}$, $\mathbf{e}_3 \leftarrow D^\lambda_{\mathbb{Z},r}$.
3. Set
$$[\mathbf{c}_0^\intercal|\mathbf{c}_1^\intercal] \leftarrow \mathbf{s}^\intercal[\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}] + [\mathbf{e}_0^\intercal|\mathbf{e}_1^\intercal]$$
and
$$[\mathbf{c}_2^\intercal|\mathbf{c}_3^\intercal] \leftarrow \mathbf{s}^\intercal[\mathbf{U}|\mathbf{U}_1] + [(\mathbf{e}_2 + \mathbf{k}'\lfloor q/2\rfloor)^\intercal|(\mathbf{e}_3 + \mathbf{k}''\lfloor q/2\rfloor)^\intercal].$$
4. Return $\mathsf{Ct} \leftarrow (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$ and $\mathsf{K} = \mathbf{k}$.

– $\mathsf{TskGen}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$
1. Set $\mathbf{F}_{\mathsf{id}} \leftarrow [\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}]$.
2. Sample $\mathbf{D}_{\mathsf{id}} \leftarrow \mathsf{SampleRight}(\mathbf{R}, \mathbf{F}_{\mathsf{id}}, H(\mathsf{id}), \mathbf{U}, s) \in \mathbb{Z}^{(m+w)\times\lambda}$.
3. Return $\mathsf{Td}_{\mathsf{id}} \leftarrow \mathbf{D}_{\mathsf{id}}$.

– $\mathsf{Decap}(\mathsf{Pub}, \mathsf{Sk}_{\mathsf{id}}, \mathsf{Ct})$
1. Parse $\mathsf{Ct} = (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$; Output $\perp$ if Ct doesn't parse.
2. Set $\mathbf{F}_{\mathsf{id}} \leftarrow [\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}]$; Recover $\mathbf{s}$ via $\mathsf{Invert}(\mathbf{T}_{\mathsf{id}}, \mathbf{F}_{\mathsf{id}}, [\mathbf{c}_0^\intercal|\mathbf{c}_1^\intercal])$.
3. Recover $\tilde{\mathbf{k}}' \leftarrow \mathsf{Round}(\mathbf{c}_2^\intercal - \mathbf{s}^\intercal\mathbf{U})$; Return $\perp$ if $\tilde{\mathbf{k}}' \neq \mathbf{k}'$.
4. Recover $\mathbf{k}'' \leftarrow \mathsf{Round}(\mathbf{c}_3 - \mathbf{s}^\intercal\mathbf{U}_1)$ and set $\mathbf{k} \leftarrow \mathbf{k}' \oplus \mathbf{k}''$.
5. Return $\mathsf{K} = \mathbf{k}$.

– $\mathsf{TkVer}(\mathsf{Pub}, \mathsf{Td}_{\mathsf{id}}, \mathsf{Ct})$
1. Parse $\mathsf{Ct} = (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$; Output $\perp$ if Ct doesn't parse.
2. Set $\mathbf{F}_{\mathsf{id}} = [\mathbf{A}|\mathbf{A}_1 + H((\mathsf{id})\mathbf{G}]$; Recover $\tilde{\mathbf{k}}' \leftarrow \mathsf{Round}(\mathbf{c}_2^\intercal - [\mathbf{c}_0^\intercal|\mathbf{c}_1^\intercal]\mathbf{D}_{\mathsf{id}})$.
3. Return 1 if $\tilde{\mathbf{k}}' = \mathbf{k}'$; Otherwise, return 0.

Correctness and soundness. First of all, $\mathsf{SampleRight}$ and $\mathsf{SampBasisRight}$ are ensured to run correctly as per Lemma 5. According to Lemma 3, we have $s_1(\mathbf{R}) = O(\sqrt{m}) \cdot \omega(\sqrt{\log n})$. So, $s = O(\sqrt{m}) \cdot \omega(\log n) \geq 5 \cdot s_1(\mathbf{R}) \cdot \omega(\sqrt{\log n})$ as required.

Second, we have $\|[\mathbf{e}_0^\intercal|\mathbf{e}_1^\intercal] \cdot \mathbf{T}_{\mathsf{id}}\|_\infty \leq \|[\mathbf{e}_0^\intercal|\mathbf{e}_1^\intercal]\| \cdot \|\mathbf{T}_{\mathsf{id}}\| \leq \|[\mathbf{e}_0^\intercal|\mathbf{e}_1^\intercal]\| \leq (2r\sigma \cdot \sqrt{m+w}) \cdot (s \cdot \sqrt{m+w}) \leq q/4$ where the third inequality is due to Lemma 1. Using Lemma 6, this means Invert under Decap runs correctly except with negligible probability. Moreover, since $\mathbf{e}_2 \sim D_{\mathbb{Z}^\lambda,2r\sigma}$ and $\mathbf{e}_2 \sim D_{\mathbb{Z}^\lambda,r}$. Applying Lemma 1 and our parameter setup, $\|\mathbf{e}_3\|_\infty \leq \|\mathbf{e}_2\|_\infty \leq \|\mathbf{e}_2\| \leq 2r\sigma\sqrt{\lambda} < q/4$. Hence, $\mathsf{Round}(\mathbf{c}_2^\intercal - \mathbf{s}^\intercal\mathbf{U}) = \mathsf{Round}((\mathbf{k}'\lfloor q/2\rfloor)^\intercal + \mathbf{e}_2^\intercal)$ and $\mathsf{Round}(\mathbf{c}_3^\intercal - \mathbf{s}^\intercal\mathbf{U}_1) = \mathsf{Round}((\mathbf{k}''\lfloor q/2\rfloor)^\intercal + \mathbf{e}_3^\intercal)$ will correctly return $\mathbf{k}'$ and $\mathbf{k}''$, respectively with all but negligible probability. Then, $\mathbf{k} = \mathbf{k}' \oplus \mathbf{k}''$ can be recovered.

For correctness of TkVer, we have $\mathsf{Round}(\mathbf{c}_2^\intercal - [\mathbf{c}_0^\intercal|\mathbf{c}_1^\intercal]\mathbf{D}_{\mathsf{id}}) = \mathsf{Round}((\mathbf{k}'\lfloor q/2\rfloor)^\intercal + [\mathbf{e}_0^\intercal|\mathbf{e}_1^\intercal] \cdot \mathbf{D}_{\mathsf{id}})$. $\mathbf{D}_{\mathsf{id}}$ has a distribution statistically close to $D_{\Lambda_q^{\mathbf{U}},s}$, and according

to Lemma 1, $\|\mathbf{D}_{\mathsf{id}}\| \leq s\sqrt{m+w}$. So, $\|[\mathbf{e}_0^\intercal|\mathbf{e}_1^\intercal] \cdot \mathbf{D}_{\mathsf{id}}\| \leq 2r\sigma\sqrt{w} \cdot s\sqrt{m+w} \leq q/4$ by the parameter we set up, and thus, TkVer runs correctly except negligible probability.

The soundness of the construction follows directly from the fact that if TkVer returns 0, Decap returns $\perp$ in its third step.

Achieving adaptive security. In the next section, we prove the security of the above construction in the so-called selective security mode, as defined in Definition 2 and Definition 3. In this mode, the adversary is required to submit the identity id^* that it wants to be challenged upon *before* seeing Pub. To achieve security in the adaptive security model in which the adversary can decide id^* for the challenge ciphertext after seeing Pub and making identity key extraction queries and tracing key queries, we can simply apply the complexity leveraging argument (let the proof guess id^*) [6] . Based on the sub-exponential hardness of LWE problem, this results in meaningful security. We note that complexity leveraging often leads to more efficient schemes than the ones with "natural" adaptive security proof, as discussed in [7]. However, it would be nice to construct an AIBET scheme from lattices or other post-quantum computational problems that has a direct proof in the adaptive security model.

3 Security Proof

We proceed with the proofs using game sequences. Each security game will output a well defined bit value. We denote by S_i the event that the ith game returns 1 (which usually indicates the adversary makes a correct guess).

3.1 Proof of Anonymity

Theorem 1. *The construction* $\Pi = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encap}, \mathsf{TskGen}, \mathsf{Decap}, \mathsf{TkVer})$ *has ciphertext anonymity under the* $\mathsf{LWE}_{n,q,m,r}$ *assumption. In particular, if there exist an adversary* $\mathcal{A}$ *that has advantage* $\mathsf{Adv}^{\mathrm{anon}}_{\Pi,\mathcal{A}}(\lambda)$ *against* Π*, we have* $\mathsf{Adv}^{\mathrm{anon}}_{\Pi,\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{LWE}_{n,q,m+\lambda,r}}_{\mathcal{B}}(\lambda) + \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$*.*

Proof. The proof starts from the first security game Game 0, which is the real security experiment defined in Figure 2, and gradually modifies Game 0 towards the final security game Game 3, in which the adversary has no advantage. The modifications are either statistically indistinguishable (based on information-theoretical arguments) or computationally indistinguishable under the LWE assumption.

Game 0. Game 0 is identical to $\mathsf{Exp}^{\mathrm{anon}}_{\Pi,\mathcal{A}}(\lambda)$ in which real algorithms specified in our construction are run. To construct the challenge ciphertexts of identity id^*, the game constructs $(\mathsf{K}, \mathsf{Ct}_0^*) \leftarrow \mathsf{Encap}(\mathsf{Pub}, \mathsf{id}^*)$ and samples Ct_1^* uniformly at random from the ciphertext space $\mathcal{C}$. Then, the adversary is given Ct_b^* for a

random coin $b \leftarrow U(\{0,1\})$. Eventually, the adversary outputs $b' \in \{0,1\}$. The game returns 1 if $b' = b$, or 0, otherwise. By definition, we have

$$\Pr[S_0] = \Pr[\mathsf{Exp}^{\mathrm{anon}}_{\Pi,\mathcal{A}}(\lambda) = 1] \tag{1}$$

Game 1. Game 1 modifies Game 0 in construction of Pub and responding private identity key extraction queries and tracing key queries. To construct Pub, Game 1 uses the challenge identity id^* supplied by the adversary $\mathcal{A}$ and does:

1. Sample $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n\times m})$, $\mathbf{R} \leftarrow D^w_{\mathbb{Z}^m,\omega(\sqrt{\log n})}$, $\tilde{\mathbf{R}} \leftarrow D^\lambda_{\mathbb{Z}^m,\omega(\sqrt{\log n})}$.
2. Set $\mathbf{A}_1 \leftarrow \mathbf{AR} - H(\mathsf{id}^*)\mathbf{G}$, $\mathbf{U} \leftarrow \mathbf{A}\tilde{\mathbf{R}}$, $\mathbf{U}_1 \leftarrow U(\mathbb{Z}_q^{n\times\lambda})$.
3. Output $\mathsf{Pub} = (\mathbf{A}, \mathbf{A}_1, \mathbf{U}, \mathbf{U}_1)$ and $\mathsf{Msk} = \mathbf{R}$.

Recall that in Game 0, $\mathbf{A}_1$ is set as $\mathbf{AR}$ where $\mathbf{R} \leftarrow D^w_{\mathbb{Z}^m,\omega(\sqrt{\log n})}$, and $\mathbf{U} \leftarrow U(\mathbb{Z}_q^{n\times\lambda})$. The identity key extraction queries and the tracing key queries are responded to using the strong trapdoor $\mathbf{R}$. We note that the adversary is not allowed to use the challenge identity id^* for queries.

– To respond to a private identity key query for $\mathsf{id} \neq \mathsf{id}^*$, the game sets

$$\mathbf{F}_{\mathsf{id}} = [\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}] = [\mathbf{A}|\mathbf{AR} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{G}].$$

By the property of full-rank difference encoding H, $H(\mathsf{id}) - H(\mathsf{id}^*)$ is invertible over $\mathbb{Z}_q^{n\times n}$. So, the game gets $\mathsf{Sk}_{\mathsf{id}} = \mathbf{T}_{\mathsf{id}}$ by

$$\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{SampBasisRight}(\mathbf{R}, \mathbf{F}_{\mathsf{id}}, H(\mathsf{id}) - H(\mathsf{id}^*), s).$$

– To respond to a tracing key query for $\mathsf{id} \neq \mathsf{id}^*$, the game sets $\mathbf{F}_{\mathsf{id}} = [\mathbf{A}|\mathbf{AR} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{G}]$, and gets $\mathsf{Td}_{\mathsf{id}} = \mathbf{D}_{\mathsf{id}}$ by

$$\mathbf{D}_{\mathsf{id}} \leftarrow \mathsf{SampleRight}(\mathbf{R}, \mathbf{F}_{\mathsf{id}}, H(\mathsf{id}) - H(\mathsf{id}^*), \mathbf{U}, \mathbf{s}).$$

Finally, the challenge ciphertext in Game 1 is constructed exactly as in Game 0.

We analyse the game. First of all, consider the adversary $\mathcal{A}$'s view of Pub *before* it launches any query. Recall the matrices $\mathbf{R} \sim D^w_{\mathbb{Z}^m,\omega(\sqrt{\log n})}$, $\tilde{\mathbf{R}} \sim D^\lambda_{\mathbb{Z}^m,\omega(\sqrt{\log n})}$, applying Lemma 4 shows that the distribution of Pub in Game 1, i.e.,

$$\mathsf{Pub} = (\mathbf{A}, \mathbf{A}_1 \leftarrow \mathbf{AR} - H(\mathsf{id}^*)\mathbf{G}, \mathbf{U} \leftarrow \mathbf{A}\tilde{\mathbf{R}}, \mathbf{U}_1 \leftarrow U(\mathbb{Z}_q^{n\times\lambda}))$$

and the distribution of Pub in Game 0, i.e.,

$$\mathsf{Pub} = \big(\mathbf{A}, \mathbf{A}_1 \leftarrow \mathbf{AR}, \mathbf{U} \leftarrow U(\mathbb{Z}_q^{n\times\lambda}), \mathbf{U}_1 \leftarrow U(\mathbb{Z}_q^{n\times\lambda})\big)$$

are both statistically close to the distribution

$$(\mathbf{A}, \mathbf{A}_1 \leftarrow U(\mathbb{Z}_q^{n\times w}), \mathbf{U} \leftarrow U(\mathbb{Z}_q^{n\times\lambda}), \mathbf{U}_1 \leftarrow U(\mathbb{Z}_q^{n\times\lambda}))$$

Next, we consider the responses to private key extraction queries and tracing key queries. Unlike Game 0, Game 1 cannot respond to queries with $\mathsf{id} = \mathsf{id}^*$

(because the strong trapdoor for $\mathbf{F}_{\mathsf{id}^*} = [\mathbf{A}|\mathbf{AR}]$ vanishes. However, no such query is allowed by the security model. For $\mathsf{id} \neq \mathsf{id}^*$, Lemma 5 shows that in both Game 0 and Game 1, $\mathsf{Sk}_{\mathsf{id}} = \mathbf{T}_{\mathsf{id}}$ has a distribution statistically close to $D_{\Lambda_q^\perp(\mathbf{F}_{\mathsf{id}}),s}$, and $\mathsf{Td}_{\mathsf{id}} = \mathbf{D}_{\mathsf{id}}$ has a distribution statistically close to $D_{\Lambda_q^{\mathbf{U}}(\mathbf{F}_{\mathsf{id}}),s}$, where the parameters s is public. Note that $\mathbf{F}_{\mathsf{id}}$, $\mathbf{U}$ are independent of $\mathbf{R}$ and $\tilde{\mathbf{R}}$, so are $\mathbf{T}_{\mathsf{id}}$ and $\mathbf{D}_{\mathsf{id}}$. Meanwhile, the challenge ciphertext does not change the adversary's view on Pub. Hence, the distributions of Pub in Game 0 and Game 1 are statistically close from the adversary's view, given all the responses to queries. Using this fact, we conclude that the distributions of $(\mathbf{F}_{\mathsf{id}}, \mathbf{U})$ in Game 0 and Game 1 are statistically close, and thus, the distributions of all query responses $\mathbf{T}_{\mathsf{id}}$ and $\mathbf{D}_{\mathsf{id}}$ in Game 0 and Game 1 are statistically close. This shows Game 0 and Game 1 are statistically indistinguishable, and

$$|\Pr[S_1] - \Pr[S_0]| \leq \mathsf{negl}(\lambda) \tag{2}$$

for some negligible function λ.

Game 2. Game 2 is identical to Game 1 except that it modifies the construction of the challenge ciphertext. In particular, given the challenge identity id^*, the game does the following to generate Ct_0^* (recall, Ct_1^* is sampled uniformly at random from the ciphertext space $\mathcal{C}$):

1. Sample $\mathbf{k}', \mathbf{k}'' \leftarrow U(\{0,1\}^n)$; Set $\mathbf{k} \leftarrow \mathbf{k}' \oplus \mathbf{k}''$.
2. Sample $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$, $\mathbf{e}_0 \leftarrow D_{\mathbb{Z},r}^m$, $\mathbf{e}_3 \leftarrow D_{\mathbb{Z},r}^\lambda$.
3. Set $\mathbf{c}_0^\intercal \leftarrow \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_0^\intercal$, $\mathbf{c}_3^\intercal \leftarrow \mathbf{s}^\intercal\mathbf{U}_1 + (\mathbf{e}_3 + \mathbf{k}''\lfloor q/2 \rfloor)^\intercal$ and
$$[\mathbf{c}_1^\intercal|\mathbf{c}_2^\intercal] \leftarrow [\mathsf{ReRand}(\mathbf{R}, \mathbf{c}_0^\intercal, r, \sigma)|\mathsf{ReRand}(\mathbf{c}_0^\intercal, \tilde{\mathbf{R}}, r, \sigma) + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal].$$
4. Return $\mathsf{Ct}_0^* \leftarrow (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$

Note the ciphertext components $\mathbf{c}_1, \mathbf{c}_2$ are constructed using $\mathbf{c}_0$. We argue that Ct_0^* is statistically close to the distribution of a real ciphertext. First, $\mathbf{c}_0$ and $\mathbf{c}_3$ are distributed exactly as they are in the real system. Using Lemma 2 with that fact $s_1(\mathbf{R})$, $s_1(\tilde{\mathbf{R}}) \leq \sigma$, and $\mathbf{A}_1 = \mathbf{AR} - H(\mathsf{id}^*)\mathbf{G}$, we get

$$\begin{aligned}\mathbf{c}_1^\intercal &= \mathsf{ReRand}(\mathbf{R}, \mathbf{c}_0^\intercal, r, \sigma) = (\mathbf{s}^\intercal\mathbf{A})\mathbf{R} + \mathbf{e}_1^\intercal \\ &= \mathbf{s}^\intercal(\mathbf{A}_1 + H(\mathsf{id}^*)\mathbf{G}) + \mathbf{e}_1\end{aligned}$$

and

$$\begin{aligned}\mathbf{c}_2^\intercal &= \mathsf{ReRand}(\tilde{\mathbf{R}}, \mathbf{c}_0^\intercal, r, \sigma) + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal = (\mathbf{s}^\intercal\mathbf{A})\tilde{\mathbf{R}} + \mathbf{e}_2^\intercal + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal \\ &= \mathbf{s}^\intercal\mathbf{U} + (\mathbf{e}_2 + \mathbf{k}'\lfloor q/2 \rfloor)^\intercal\end{aligned}$$

where the distribution of $\mathbf{e}_1$ and $\mathbf{e}_2$ are statistically close to $D_{\mathbb{Z}^w,2r\sigma}$ and $D_{\mathbb{Z}^\lambda,2r\sigma}$. So, Game 1 and Game 2 are statistically indistinguishable, and

$$|\Pr[S_2] - \Pr[S_1]| \leq \mathsf{negl}(\lambda) \tag{3}$$

for some negligible function $\mathsf{negl}(\lambda)$.

Game 3. Game 3 is identical to Game 2 except that it further modifies the way generates Ct_0^*. In particular, given the challenge identity id^*, the game does:

1. Sample $\mathbf{k}', \mathbf{k}'' \leftarrow U(\{0,1\}^n)$; Set $\mathbf{k} \leftarrow \mathbf{k}' \oplus \mathbf{k}''$.
2. Sample $\bar{\mathbf{b}} \leftarrow U(\mathbb{Z}_q^m)$, $\tilde{\mathbf{b}} \leftarrow U(\mathbb{Z}_q^\lambda)$, $\mathbf{e}_0 \leftarrow D_{\mathbb{Z}^m,r}$, and $\mathbf{e}_3 \leftarrow D_{\mathbb{Z}^\lambda,r}$.
3. Set $\mathbf{c}_0^\intercal = \bar{\mathbf{b}}^\intercal + \mathbf{e}_0^\intercal$ and $\mathbf{c}_3^\intercal = \tilde{\mathbf{b}}^\intercal + (\mathbf{e}_3 + \mathbf{k}''\lfloor q/2 \rfloor)^\intercal$.
4. Set

$$[\mathbf{c}_1^\intercal | \mathbf{c}_2^\intercal] \leftarrow [\mathsf{ReRand}(\mathbf{R}, \mathbf{c}_0^\intercal, r, \sigma) | \mathsf{ReRand}(\mathbf{c}_0^\intercal, \tilde{\mathbf{R}}, r, \sigma) + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal].$$

5. Return $\mathsf{Ct}_0^* \leftarrow (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$.

We first show that Game 3 and Game 2 are computationally indistinguishable under the LWE assumption. To this end, we construct an LWE adversary $\mathcal{B}$. $\mathcal{B}$ receives an $\mathsf{LWE}_{n,q,m+\lambda,r}$ problem challenge $(\mathbf{C}, \mathbf{c}^\intercal = \mathbf{b}^\intercal + \mathbf{e}^\intercal)$, where $\mathbf{C} \in \mathbb{Z}_q^{n \times (m+\lambda)}$ is random, $\mathbf{c} \in \mathbb{Z}_q^{m+\lambda}$, and $\mathbf{e} \sim D_{\mathbb{Z},r}^{m+\lambda}$. It needs to decide whether $\mathbf{b}$ is uniformly random (in which case $\mathbf{c}$ is also uniformly random), or there is a vector $\mathbf{s} \in \mathbb{Z}_q^n$ such that $\mathbf{b}^\intercal = \mathbf{s}^\intercal \mathbf{C}$. $\mathcal{B}$ receives the challenge identity id^* and proceeds to the simulation as follows:

- Set $[\mathbf{A}|\mathbf{U}_1] \leftarrow \mathbf{C}$ where $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{U}_1 \in \mathbb{Z}_q^{n \times \lambda}$.
- Pick $\mathbf{R} \leftarrow D_{\mathbb{Z},\omega(\sqrt{\log n})}^{m \times w}$, $\tilde{\mathbf{R}} \leftarrow D_{\mathbb{Z},\omega(\sqrt{\log n})}^{m \times \lambda}$; Set $\mathbf{A}_1 \leftarrow \mathbf{A}\mathbf{R} - H(\mathsf{id}^*)\mathbf{G}$, $\mathbf{U} \leftarrow \mathbf{A}\tilde{\mathbf{R}}$.
- Set $\mathsf{Pub} = (\mathbf{A}, \mathbf{A}_1, \mathbf{U}, \mathbf{U}_1)$
- Respond to the private identity key extraction queries and tracing key queries as Game 2 (Game 3 does not modify the ways that queries are responded).
- Split $\mathbf{c}^\intercal = \mathbf{b}^\intercal + \mathbf{e}^\intercal \in \mathbb{Z}_q^{m+\lambda}$ into $\bar{\mathbf{c}}^\intercal = \bar{\mathbf{b}}^\intercal + \mathbf{e}_0^\intercal \in \mathbb{Z}_q^m$ and $\tilde{\mathbf{c}}^\intercal = \tilde{\mathbf{b}}^\intercal + \mathbf{e}_3^\intercal \in \mathbb{Z}_q^\lambda$ and create the challenge ciphertext Ct_0^* by:
  1. Sample $\mathbf{k}', \mathbf{k}'' \leftarrow U(\{0,1\}^n)$; Set $\mathbf{k} \leftarrow \mathbf{k}' \oplus \mathbf{k}''$.
  2. Set $\mathbf{c}_0^\intercal \leftarrow \bar{\mathbf{c}}^\intercal$ and $\mathbf{c}_3^\intercal \leftarrow \tilde{\mathbf{c}}^\intercal + (\mathbf{k}''\lfloor q/2 \rfloor)^\intercal$.
  3. Set

$$[\mathbf{c}_1^\intercal | \mathbf{c}_2^\intercal] \leftarrow [\mathsf{ReRand}(\mathbf{R}, \mathbf{c}_0^\intercal, r, \sigma) | \mathsf{ReRand}(\mathbf{c}_0^\intercal, \tilde{\mathbf{R}}, r, \sigma) + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal].$$

  4. Return $\mathsf{Ct}_0^* \leftarrow (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$.
- Finally, return what $\mathcal{A}$ returns.

We can see that Pub that $\mathcal{B}$ creates has the correct distribution as required by Game 2 and Game 3. Moreover, $\mathcal{B}$ can respond to queries properly. When $\mathcal{B}$ receives real LWE samples, i.e., $\mathbf{b}^\intercal = \mathbf{x}^\intercal \mathbf{C}$, we have $\mathbf{c}_0^\intercal = \mathbf{s}^\intercal \mathbf{A} + \mathbf{e}_0^\intercal$ and $\mathbf{c}_3^\intercal = \mathbf{s}^\intercal \mathbf{U}_1 + \mathbf{e}_3^\intercal$, meaning that $\mathbf{c}_0, \mathbf{c}_3$ are distributed as in Game 2. Also, using Lemma 2, $\mathbf{c}_1$ and $\mathbf{c}_2$ are distributed as in Game 2. Therefore, we can see that $\mathcal{B}$ simulates Game 2 and, hence,

$$\Pr[S_3] = \Pr[\mathcal{B}(\mathbf{C}, \mathbf{s}^\intercal \mathbf{C} + \mathbf{e}^\intercal) = 1].$$

On the other hand, if $\mathcal{B}$ receives random samples, Ct_0^* distributes as in Game 3 and, thus, $\mathcal{B}$ simulates Game 3 which gives

$$\Pr[S_2] = \Pr[\mathcal{B}(\mathbf{C}, \mathbf{b}^\intercal + \mathbf{e}^\intercal) = 1].$$

for random $\mathbf{b} \in \mathbb{Z}_q^m$. So, we get

$$\begin{aligned} |\Pr[S_3] - \Pr[S_2]| &= |\Pr[\mathcal{B}(\mathbf{C}, \mathbf{x}^\intercal \mathbf{C} + \mathbf{e}^\intercal) = 1] - \Pr[\mathcal{B}(\mathbf{C}, \mathbf{b}^\intercal + \mathbf{e}^\intercal) = 1]| \\ &\leq \mathsf{Adv}_{\mathcal{B}}^{\mathsf{LWE}_{n,q,m+\lambda,r}}(\lambda) \end{aligned} \tag{4}$$

We argue that the challenge ciphertext Ct_0^* constructed in Game 3 has uniform distribution over the ciphertext space. In Game 3, $\mathsf{Pub} = (\mathbf{A} \leftarrow U(\mathbb{Z}_q^{n\times m}), \mathbf{A}_1 \leftarrow \mathbf{AR} - H(\mathsf{id}^*)\mathbf{G}, \mathbf{U} \leftarrow \mathbf{A}\tilde{\mathbf{R}}, \mathbf{U}_1 \leftarrow U(\mathbb{Z}_q^\lambda))$, and the challenge ciphertext $\mathsf{Ct}_0^* = (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$ where for random vectors $\bar{\mathbf{b}} \in \mathbb{Z}_q^m$, $\tilde{\mathbf{b}} \in \mathbb{Z}_q^\lambda$,

$$\mathbf{c}_0^\intercal = \bar{\mathbf{b}}^\intercal + \mathbf{e}_0^\intercal$$

$$\mathbf{c}_1^\intercal = \mathsf{ReRand}(\mathbf{R}, \mathbf{c}_0^\intercal, r, \sigma) = \bar{\mathbf{b}}^\intercal \mathbf{R} + \mathbf{e}_1^\intercal$$

$$\mathbf{c}_2^\intercal = \mathsf{ReRand}(\mathbf{c}_0^\intercal, \tilde{\mathbf{R}}, r, \sigma) + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal = \tilde{\mathbf{b}}^\intercal \tilde{\mathbf{R}} + \mathbf{e}_2^\intercal + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal$$

$$\mathbf{c}_3^\intercal = \tilde{\mathbf{b}}^\intercal + \mathbf{e}_3^\intercal + (\mathbf{k}''\lfloor q/2 \rfloor)^\intercal$$

Applying Lemma 2, $\mathbf{e}_1$ and $\mathbf{e}_2$ are statistically close to $D_{\mathbb{Z}^w, 2r\sigma}$ and $D_{\mathbb{Z}^\lambda, 2r\sigma}$, respectively. Using the same argument as in proving formula (2) using Lemma 5, from the adversary's view, the responses $\mathbf{T}_{\mathsf{id}} \sim D_{\Lambda_q^\perp(\mathbf{F}_{\mathsf{id}})}$, $\mathbf{D}_{\mathsf{id}} \sim D_{\Lambda_q^{\mathbf{U}}(\mathbf{F}_{\mathsf{id}})}$ (where $\mathbf{F}_{\mathsf{id}} = [\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}] = [\mathbf{A}|\mathbf{AR} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{G}]$) only depends on $\mathbf{A}$, $\mathbf{A}_1$ from Pub. On the other hand, we have already used Lemma 4 to show that $\mathbf{A}_1$ has a distribution that is statistically close to $U(\mathbb{Z}_q^{n\times w})$. Therefore, no information about $\mathbf{R}$ and $\tilde{\mathbf{R}}$ are leaked through answering private key extraction queries and tracing key queries. Therefore, applying Lemma 4 again, we get

$$\left(\begin{bmatrix}\mathbf{A}\\ \bar{\mathbf{b}}^\intercal\end{bmatrix}, \begin{bmatrix}\mathbf{A}\\ \bar{\mathbf{b}}^\intercal\end{bmatrix}\mathbf{R}, \begin{bmatrix}\mathbf{A}\\ \bar{\mathbf{b}}^\intercal\end{bmatrix}\tilde{\mathbf{R}}\right) = \left(\begin{bmatrix}\mathbf{A}\\ \bar{\mathbf{b}}^\intercal\end{bmatrix}, \begin{bmatrix}\mathbf{A}_1 - H(\mathsf{id}^*)\mathbf{G}\\ \bar{\mathbf{b}}^\intercal\mathbf{R}\end{bmatrix}, \begin{bmatrix}\mathbf{U}\\ \bar{\mathbf{b}}^\intercal\tilde{\mathbf{R}}\end{bmatrix}\right)$$

and

$$\left(\begin{bmatrix}\mathbf{A}\\ \bar{\mathbf{b}}^\intercal\end{bmatrix}, \begin{bmatrix}\mathbf{A}_1 - H(\mathsf{id}^*)\mathbf{G}\\ \mathbf{u}_1^\intercal\end{bmatrix}, \begin{bmatrix}\mathbf{U}\\ \mathbf{u}_2^\intercal\end{bmatrix}\right)$$

are statistically close, where $\mathbf{u}_1 \leftarrow U(\mathbb{Z}_q^w)$, $\mathbf{u}_2 \leftarrow U(\mathbb{Z}_q^n)$. Moreover, we know that in Game 3, $\tilde{\mathbf{b}}$ is random over $\mathbb{Z}_q^\lambda$. Hence, all components of Ct_0^* are either uniformly random (i.e., $\mathbf{k}'$) or masked by uniformly random vectors (i.e., $\bar{\mathbf{b}}$, $\mathbf{u}_1^\intercal = \bar{\mathbf{b}}^\intercal\mathbf{R}$, $\mathbf{u}_2^\intercal = \bar{\mathbf{b}}^\intercal\tilde{\mathbf{R}}$). So, both Ct_0^* and Ct_1^* have distributions statistically close to uniform distribution over the ciphertext space, and the adversary $\mathcal{A}$ has no significant advantage in wining the game, i.e.,

$$|\Pr[S_3] - 1/2| \leq \mathsf{negl}(\lambda) \tag{5}$$

for some negligible function $\mathsf{negl}(\lambda)$. Combining inequalities (1) - (5) results in

$$\mathsf{Adv}_{\Pi,\mathcal{A}}^{\mathrm{anon}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}}^{\mathsf{LWE}_{n,q,m+\lambda,r}}(\lambda) + \mathsf{negl}(\lambda)$$

for some negligible function $\mathsf{negl}(\lambda)$. This concludes the proof. □

3.2 Proof of Ciphertext Indistinguishability

Theorem 2. *The construction* $\Pi = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Encap}, \mathsf{TskGen}, \mathsf{Decap}, \mathsf{TkVer})$ *has ciphertext indistinguishability under the assumption that* $\mathsf{LWE}_{n,q,m,r}$ *is hard. In particular, if there exist an adversary* $\mathcal{A}$ *that has advantage* $\mathsf{Adv}^{\mathrm{ind-sid-cpa}}_{\Pi,\mathcal{A}}(\lambda)$ *against* Π*, we have* $\mathsf{Adv}^{\mathrm{ind-sid-cpa}}_{\Pi,\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{LWE}_{n,q,m+\lambda,r}}_{\mathcal{B}}(\lambda) + \mathsf{negl}(\lambda)$ *for some efficient algorithm* $\mathcal{B}$ *and negligible function* $\mathsf{negl}(\lambda)$*.*

Proof. The proof starts from the first security game Game 0, which is the real security experiment defined in Figure 3, and gradually modify it towards to the final security game Game 3, in which the adversary has no advantage. The modifications are either statistically indistinguishable based on information-theoretical arguments or computationally indistinguishable to under the LWE assumption. The proof is similar to the proof of Theorem 1, but it differs in dealing with answering the tracing key query on the challenge identity id^*.

Game 0. Game 0 is identical to $\mathsf{Exp}^{\mathrm{ind-sid-cpa}}_{\Pi,\mathcal{A}}(\lambda)$ in which real algorithms specified in our construction are run. In the game, the adversary supplies the challenge identity id^* before seeing Pub. To construct the challenge ciphertext and session key under the selected identity id^*, the game runs $(\mathsf{K}^*_0, \mathsf{Ct}^*) \leftarrow \mathsf{Encap}(\mathsf{Pub}, \mathsf{id}^*)$, sample a random session key $\mathsf{K}^*_1 \leftarrow U(\{0,1\}^n)$, flips a random coin $b \leftarrow U(\{0,1\})$, and passes on $(\mathsf{K}^*_b, \mathsf{Ct}^*)$ to the adversary $\mathcal{A}$. The adversary can make identity key extraction queries on any identity $\mathsf{id} \neq \mathsf{id}^*$ as well as tracing key queries on any identity id including id^*. Eventually, the adversary $\mathcal{A}$ returns $b' \in \{0,1\}$ and the game outputs 1 if $b' = b$, or 0, otherwise. By definition,

$$\Pr[S_0] = \Pr[\mathsf{Exp}^{\mathrm{ind-sid-cpa}}_{\Pi,\mathcal{A}}(\lambda) = 1] \tag{6}$$

Game 1. Game 1 modifies Game 0 in the ways that how Pub is generated and how the key extraction queries and tracing key queries are answered. Using the challenge identity id^* supplied by the adversary, the game does the following to generate Pub:

1. Sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{R} \leftarrow D^w_{\mathbb{Z}^m,\omega(\sqrt{\log n})}$, $\mathbf{D}_1 \leftarrow D^\lambda_{\mathbb{Z}^m,s}$, $\mathbf{D}_2 \leftarrow D^\lambda_{\mathbb{Z}^w,s}$.
2. Set $\mathbf{A}_1 \leftarrow \mathbf{AR} - H(\mathsf{id}^*)\mathbf{G}$, $\mathbf{U} \leftarrow \mathbf{AD}_1 + (\mathbf{AR}) \cdot \mathbf{D}_2$; Sample $\mathbf{U}_1 \leftarrow \mathbb{Z}_q^{n\times\lambda}$.
3. Return $\mathsf{Pub} = (\mathbf{A}, \mathbf{A}_1, \mathbf{U}, \mathbf{U}_1)$, $\mathsf{Msk} = \mathbf{R}$, and $\mathbf{D}_1, \mathbf{D}$

The game passes on Pub to the adversary and keeps $\mathbf{R}$, $\mathbf{D}_1$, and $\mathbf{D}_2$.

The game responds to queries from the adversary as follows:

1. For a private identity key query on $\mathsf{id} \neq \mathsf{id}^*$, the game sets

$$\mathbf{F}_{\mathsf{id}} = [\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}] = [\mathbf{A}|\mathbf{AR} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{G}]$$

   By the property of full-rank difference encoding H, $H(\mathsf{id}) - H(\mathsf{id}^*)$ is invertible over $\mathbb{Z}_q^{n\times n}$. The game obtains $\mathsf{Sk}_{\mathsf{id}} = \mathbf{T}_{\mathsf{id}}$ by

$$\mathbf{T}_{\mathsf{id}} \leftarrow \mathsf{SampBasisRight}(\mathbf{R}, \mathbf{F}_{\mathsf{id}}, H(\mathsf{id}) - H(\mathsf{id}^*), s).$$

2. For a tracing key query on $\mathsf{id} \neq \mathsf{id}^*$, the game again sets

$$\mathbf{F}_{\mathsf{id}} = [\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}] = [\mathbf{A}|\mathbf{AR} + (H(\mathsf{id}) - H(\mathsf{id}^*))\mathbf{G}],$$

and obtains $\mathsf{Td}_{\mathsf{id}} = \mathbf{D}_{\mathsf{id}}$ by

$$\mathbf{D}_{\mathsf{id}} \leftarrow \mathsf{SampleRight}(\mathbf{R}, \mathbf{F}_{\mathsf{id}}, H(\mathsf{id}) - H(\mathsf{id}^*), \mathbf{U}, \mathbf{s}).$$

3. To respond to the tracing key query for id^*,[6] the game sets

$$\mathbf{D}_{\mathsf{id}^*} = \begin{bmatrix} \mathbf{D}_1 \\ \mathbf{D}_2 \end{bmatrix} \in \mathbb{Z}^{(m+w)\times n}$$

and returns $\mathsf{Td}_{\mathsf{id}^*} = \mathbf{D}_{\mathsf{id}^*}$ (Recall $\mathbf{D}_1$, $\mathbf{D}_2$ have been generated with Pub.).

Finally, Ct^* and $(\mathsf{K}_0^*, \mathsf{K}_1^*)$ in Game 1 are constructed as in Game 0.

We note that the only difference between Game 1 in this proof and Game 1 in the security proof of Theorem 2 is how $\mathbf{U}$ is constructed. So, first we can use the same argument from the proof of Theorem 2 to show that the distributions of $(\mathbf{A}, \mathbf{A}_1, \mathbf{U}_1)$ (and particularly the matrix $\mathbf{F}_{\mathsf{id}} = [\mathbf{A}|\mathbf{A}_1 + H(\mathsf{id})\mathbf{G}]$) and $\mathbf{T}_{\mathsf{id}}$ in Game 0 and Game 1 are statistically close. It remains to show that the distributions of $\mathbf{U}$, $\mathbf{D}_{\mathsf{id}}$ (including $\mathbf{D}_{\mathsf{id}^*}$) in the two games are statistically close.

Recall that $\mathbf{F}_{\mathsf{id}^*} = [\mathbf{A}|\mathbf{AR}]$ is statistically close to $U(\mathbb{Z}_q^{n\times(m+w)})$ according to Lemma 4. So, the columns of $\mathbf{F}_{\mathsf{id}^*}$ generates $\mathbb{Z}_q^n$ with overwhelming probability. Therefore, applying Lemma 4 shows that for $s \geq \omega\sqrt{\log n}$ the distributions $\mathbf{U} = \mathbf{F}_{\mathsf{id}}\mathbf{D}_{\mathsf{id}}$ is statistically close to $U(\mathbb{Z}_q^\lambda)$. Moreover, for $\mathsf{id} \neq \mathsf{id}^*$, $\mathbf{D}_{\mathsf{id}}$ is generated by $\mathsf{SampleRight}$ which has a distribution statistically close to $D^n_{\Lambda_q^{\mathbf{U}}(\mathbf{F}_{\mathsf{id}}),s}$ according to Lemma 5. Using Lemma 4, $\mathbf{D}_{\mathsf{id}^*}$ has a distribution $D^\lambda_{\mathbb{Z}^{m+w},s}$ conditioned on $\mathbf{F}_{\mathsf{id}}\mathbf{D}_{\mathsf{id}} = \mathbf{U}$ which is precisely $D_{\Lambda_q^{\mathbf{U}}(\mathbf{F}_{\mathsf{id}^*}),s}$. Finally, we note that our AIBET system issues only one tracing key to each identity. The same tracing key (i.e., $\mathsf{Td}_{\mathsf{id}^*} = \mathbf{D}_{\mathsf{id}^*}$) will be replied for multiple tracing key queries for id^*. So, the adversary does not gain more information by making tracing key queries.

The challenge ciphertexts in Game 0 and Game 1 are generated in the same way, so Game 0 and Game 1 are statistically indistinguishable, and

$$|\Pr[S_1] - \Pr[S_0]| \leq \mathsf{negl}(\lambda) \tag{7}$$

for some negligible function $\mathsf{negl}(\lambda)$.

Game 2. Game 2 is identical to Game 1 except it modifies the construction of the challenge ciphertext from Game 1. In particular, given the challenge identity id^*, Game 2 uses Pub to do:

1. Sample $\mathbf{k}_0^*, \mathbf{k}' \leftarrow U(\{0,1\}^\lambda)$; Set $\mathbf{k}'' \leftarrow \mathbf{k}_0^* \oplus \mathbf{k}'$.

[6] Recall the adversary is allowed to make a tracing key query for id^* and such a tracing key should not allow the adversary to distinguish a session key generated by the real encapsulation algorithm or a random session key.

2. Sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e}_0 \leftarrow D_{\mathbb{Z}^m,r}$, $\mathbf{e}_3 \leftarrow D_{\mathbb{Z}^\lambda,r}$.
3. Set $\mathbf{c}_0^\intercal \leftarrow \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_0^\intercal$, $\mathbf{c}_3^\intercal \leftarrow \mathbf{s}^\intercal\mathbf{U}_1 + \mathbf{e}_3^\intercal + (\mathbf{k}''\lfloor q/2 \rfloor)$, and

$$[\mathbf{c}_1^\intercal|\mathbf{c}_2^\intercal] \leftarrow [\mathsf{ReRand}(\mathbf{R}, \mathbf{c}_0^\intercal, r, \sigma)|\mathsf{ReRand}(\mathbf{c}_0^\intercal, \mathbf{D}_1 + \mathbf{R}\mathbf{D}_2, r, \sigma) + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal].$$

4. Return $\mathsf{Ct}^* \leftarrow (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$ and $\mathsf{K}_0^* = \mathbf{k}^*$

It also selects a random session key $\mathsf{K}_1^* \leftarrow U(\{0,1\}^n)$, a random coin $b \leftarrow U(\{0,1\})$, and returns $(\mathsf{K}_b^*, \mathsf{Ct}^*)$ to the adversary.

We argue that Ct^* statistically distributed as the challenge ciphertext in Game 1. First of all, we can see that $\mathbf{c}_0$ and $\mathbf{c}_3$ are distributed exactly as the ones in Game 1. Recall that the game (like in Game 1) generates the public matrix $\mathbf{U}$ in Pub by sampling $\mathbf{D}_1 \sim D^\lambda_{\mathbb{Z}^m,s}$, $\mathbf{D}_2 \sim D^\lambda_{\mathbb{Z}^w,s}$ and computes $\mathbf{U} \leftarrow \mathbf{A}\mathbf{D}_1 + (\mathbf{A}\mathbf{R})\mathbf{D}_2$. Since the singular value $s_1(\mathbf{D}_1 + \mathbf{R}\mathbf{D}_2) \leq \sigma$, using Lemma 2, we have

$$\begin{aligned}\mathbf{c}_1^\intercal &= \mathsf{ReRand}(\mathbf{R}, \mathbf{c}_0^\intercal, r, \sigma) = (\mathbf{s}^\intercal\mathbf{A})\mathbf{R} + \mathbf{e}_1^\intercal \\ &= \mathbf{s}^\intercal(\mathbf{A}_1 + H(\mathsf{id}^*)\mathbf{G}) + \mathbf{e}_1\end{aligned}$$

and

$$\begin{aligned}\mathbf{c}_2^\intercal &= \mathsf{ReRand}(\mathbf{D}_1 + \mathbf{R}\mathbf{D}_2, \mathbf{c}_0^\intercal, r, \sigma) + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal \\ &= (\mathbf{s}^\intercal\mathbf{A})(\mathbf{D}_1 + \mathbf{R}\mathbf{D}_2) + \mathbf{e}_2^\intercal + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal \\ &= \mathbf{s}^\intercal\mathbf{U} + (\mathbf{e}_2 + \mathbf{k}'\lfloor q/2 \rfloor)^\intercal\end{aligned}$$

where the distribution of $\mathbf{e}_1$ and $\mathbf{e}_2$ are statistically close to $D_{\mathbb{Z}^w,2r\sigma}$ and $D_{\mathbb{Z}^\lambda,2r\sigma}$, as required. This shows that Game 1 and Game 2 are statistically indistinguishable. Hence,

$$|\Pr[S_2] - \Pr[S_1]| \leq \mathsf{negl}(\lambda) \tag{8}$$

for some negligible function $\mathsf{negl}(\lambda)$.

Game 3. Game 3 is identical to Game 2 except it further modifies that way that generates Ct^* from Game 2. In particular, given the challenge identity id^*, the game does:

1. Sample $\mathbf{k}^*, \mathbf{k}' \leftarrow U(\{0,1\}^n)$; Set $\mathbf{k}'' \leftarrow \mathbf{k} \oplus \mathbf{k}'$.
2. Sample $\bar{\mathbf{b}} \leftarrow U(\mathbb{Z}_q^m)$, $\tilde{\mathbf{b}} \leftarrow U(Z_q^\lambda)$, $\mathbf{e}_0 \leftarrow D_{\mathbb{Z}^m,r}$, $\mathbf{e}_3 \leftarrow D_{\mathbb{Z}^\lambda,r}$.
3. Set $\mathbf{c}_0^\intercal \leftarrow \bar{\mathbf{b}}^\intercal + \mathbf{e}_0^\intercal$ and $\mathbf{c}_3^\intercal \leftarrow \tilde{\mathbf{b}} + \mathbf{e}_3^\intercal(\mathbf{k}''\lfloor q/2 \rfloor)^\intercal$, and

$$[\mathbf{c}_1^\intercal|\mathbf{c}_2^\intercal] \leftarrow [\mathsf{ReRand}(\mathbf{R}, \mathbf{c}_0^\intercal, r, \sigma)|\mathsf{ReRand}(\mathbf{D}_1 + \mathbf{R}\mathbf{D}_2, \mathbf{c}_0^\intercal, r, \sigma) + (\mathbf{k}'\lfloor q/2 \rfloor)^\intercal].$$

4. Return $\mathsf{Ct}_0^* \leftarrow (\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{k}')$.

Since the only change we make from Game 2 is to replace $\mathbf{c}_0^\intercal = \mathbf{s}^\intercal\mathbf{A} + \mathbf{e}_0^\intercal$ to $\mathbf{c}_0^\intercal = \bar{\mathbf{b}}^\intercal\mathbf{A} + \mathbf{e}_0^\intercal$ and $\mathbf{c}_3^\intercal = \mathbf{s}^\intercal\mathbf{U}_1 + \mathbf{e}_3^\intercal + (\mathbf{k}''\lfloor q/2 \rfloor)^\intercal$ to $\mathbf{c}_3^\intercal = \tilde{\mathbf{b}}^\intercal + \mathbf{e}_3^\intercal + (\mathbf{k}''\lfloor q/2 \rfloor)^\intercal$. By

using the same argument of proof of formula (4), we can use the LWE assumption to show Game 2 and Game 3 are computationally indistinguishable, i.e.,

$$|\Pr[S_3] - \Pr[S_2]| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathsf{LWE}_{n,q,m+\lambda,r}}(\lambda) \tag{9}$$

for some efficient adversary $\mathcal{B}$.

We can see that, in Game 3, $\mathbf{c}_3$ is distributed uniformly random over $\mathbb{Z}_q^\lambda$, because $\tilde{\mathbf{b}} \leftarrow U(\mathbb{Z}_q^\lambda)$. Therefore, from the adversary's view, the ciphertext is independent of $\mathbf{k}''$. That is the value of $\mathsf{K}_0^* = \mathbf{k} = \mathbf{k}' \oplus \mathbf{k}''$, the same as K_1^*, is uniformly random over $\{0,1\}^\lambda$ under $\mathcal{A}$'s view. Hence, the adversary has no advantage in winning the security game and

$$|\Pr[S_3]| = 1/2. \tag{10}$$

Combining inequalities (6)-(10) using triangle inequality shows that

$$\mathsf{Adv}_{\Pi,\mathcal{A}}^{\mathrm{ind-sid-cpa}}(\lambda) \leq \mathsf{Adv}_{\Pi,\mathcal{A}}^{\mathsf{LWE}_{n,q,m+\lambda,r}}(\lambda) + \mathsf{negl}(\lambda)$$

for some negligible function $\mathsf{negl}(\lambda)$. This completes the proof. □

4 Conclusion and Discussion

In this paper, we have presented the first construction of anonymous identity-based encryption (key encapsulation mechanism) with traceable identities (AIBET) using quantum-resistant assumptions. Specifically, the security of our construction is given in the standard model based on the conservative learning with errors assumption.

Our construction exploits the hierarchical power of different lattice trapdoors to implement the hierarchical relations among the master private key, private identity keys, and the tracing keys. Our construction incorporates identity traceability into Agrawal et al.'s anonymous IBE system [2] by adding a small overhead to parameters. In Table 1, we compare our construction with the anonymous IBE system in [2], in terms of LWE hardness parameter α (also known as the the modulus-to-noise ratio), public key size, ciphertext size, as well as anonymity and traceability. A smaller α means relying on a stronger LWE assumption. To make the comparison fair, we use a variant of Agrawal at al.'s IBE system [2] which is based on the Micciancio-Peikert (strong) gadget trapdoor, as our construction. The variant encrypts λ-bit messages (thus can be seen as an IBKEM that encapsulates λ-bit keys). In the table, λ is the security parameter, $m = 2w = 2n \log q$, and $\tilde{O}$ ignores the logarithmic factor in O notation.

We can see from Table 1 that our construction performs asymptotically similar to Agrawal et al.'s anonymous IBE system [2] in terms of public key size and ciphertext size. The extra overhead of our construction comes from the need to encode the two λ-bit shares of the actual session key. We can also see that our system has smaller parameter α meaning that our system needs to rely on a slightly stronger LWE assumption. This comes from simulating the tracing

	Param. α	$\lvert\mathsf{Pk}\rvert$	$\lvert\mathsf{Ct}\rvert$	Anonymity	Traceability
ABB10 [2]	$\tilde{O}(n^{-1.5})$	$3n\log^2 q + n\lambda \log q$	$3\log^2 q + \lambda \log q$	YES	NO
Ours	$\tilde{O}(n^{-2.5})$	$3n\log^2 q + 2n\lambda \log q$	$3\log^2 q + 2\lambda \log q + \lambda$	YES	YES

Table 1: Comparison with ABB10 Anonymous IBE

key in the indistinguishability proof. On the other hand, our system does enjoy identity traceability with quantum resistance. Our construction achieves selective security with a polynomial time reduction and is also adaptively secure using the complexity leveraging argument [6]. We leave constructing an AIBET system from lattice assumptions or other quantum-resistant assumptions that is directly adaptively secure as a future work.

References

1. Shweta Agrawal, Sanjay Bhattacherjee, Duong Hieu Phan, Damien Stehlé, and Shota Yamada. Efficient public trace and revoke from standard assumptions. In *CCS 2017*, pages 2277–2293, 2017.
2. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In *EUROCRYPT 2010*, LNCS 6110, pages 553–572. Springer, 2010.
3. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In *CRYPTO 2010*, LNCS 6223, pages 98–115. Springer, 2010.
4. Olivier Blazy, Laura Brouilhet, and Duong Hieu Phan. Anonymous identity based encryption with traceable identities. In *ARES 2019*, pages 1–10, 2019.
5. Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (Hierarchical) identity-based encryption from affine message authentication. In *CRYPTO 2014*, LNCS 8616, pages 408–425. Springer, 2014.
6. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *EUROCRYPT 2004*, LNCS 3027, pages 223–238. Springer, 2004.
7. Xavier Boyen and Qinyi Li. Towards tightly secure lattice short signature and id-based encryption. In *ASIACRYPT 2016*, LNCS 10032, pages 404–434. Springer, 2016.
8. Xavier Boyen and Brent Waters. Anonymous hierarchical identity-based encryption (without random oracles). In *CRYPTO 2006*, LNCS 4117, pages 290–307. Springer, 2006.
9. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of Cryptology*, 25(4):601–639, 2012.
10. Craig Gentry. Practical identity-based encryption without random oracles. In *EUROCRYPT 2006*, LNCS 4004, pages 445–464. Springer, 2006.
11. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC 2008*, pages 197–206, ACM, 2008.

12. Shuichi Katsumata and Shota Yamada. Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps. In *ASIACRYPT 2016*, LNCS 10032, pages 682–712. Springer, 2016.
13. Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa. Tighter security proofs for GPV-IBE in the quantum random oracle model. In *ASIACRYPT* 2018, LNCS 11273, pages 253–282. Springer, 2018.
14. Zi-Yuan Liu, Yi-Fan Tseng, Raylin Tso, Masahiro Mambo, and Yu-Chi Chen. Quantum-resistant anonymous IBE with traceable identities. Cryptology ePrint Archive, Report 2021/033, 2021. https://eprint.iacr.org/2021/033.
15. Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *EUROCRYPT 2012*, LNCS 7237, pages 700–718. Springer, 2012.
16. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.*, 37(1):267–302, April 2007.
17. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC 2005*, pages 84–93, ACM, 2005.