Quantum-resistant Anonymous IBE with Traceable Identities

Zi-Yuan Liu
Department of Computer Science
National Chengchi University
Taipei 11605, Taiwan
zyliu@cs.nccu.edu.tw

Yi-Fan Tseng
Department of Computer Science
National Chengchi University
Taipei 11605, Taiwan
yftseng@cs.nccu.edu.tw

Raylin Tso*
Department of Computer Science
National Chengchi University
Taipei 11605, Taiwan
raylin@cs.nccu.edu.tw

Masahiro Mambo
Institute of Science and Engineering
Kanazawa University
Kanazawa 920-1192, Japan
mambo@ec.t.kanazawa-u.ac.jp

Yu-Chi Chen
Department of Computer Science
and Engineering
Yuan Ze University
Taoyuan 32000, Taiwan
wycchen@saturn.yzu.edu.tw

ABSTRACT

Identity-based encryption (IBE), introduced by Shamir in 1984, eliminates the need for public-key infrastructure. The sender can simply encrypt a message by using the recipient's identity (such as their email or IP address) without needing to look up the public key. In particular, when ciphertexts of an IBE scheme do not reveal the identity of the recipient, this scheme is known as an anonymous IBE scheme. Recently, Blazy *et al.* (ARES'19) analyzed the trade-off between public safety and unconditional privacy in anonymous IBE and introduced a new notion that incorporates traceability into anonymous IBE, called anonymous IBE with traceable identities (AIBET). However, their construction is based on the discrete logarithm assumption, which is insecure in the quantum era. In this paper, we first formalize the consistency of tracing key of the AIBET scheme to ensure that no adversary can obtain information with the use of wrong tracing keys. Subsequently, we present a generic formulation concept that can be used to transform structure-specific lattice-based anonymous IBE schemes into an AIBET scheme. Finally, we apply this concept to Katsumata and Yamada's compact anonymous IBE scheme (Asiacrypt'16) to obtain the first quantum-resistant AIBET scheme that is secure under the ring learning with errors assumption.

KEYWORDS

anonymous, identity-based encryption, lattice, traceable identity, quantum-resistant

1 INTRODUCTION

Identity-based encryption (IBE) enables a sender to encrypt a message by using the recipient's identity (such as their email or IP address) instead of public keys as in public-key encryption. Because a user's identity is identifiable, the sender does not need to look up the recipient's public key or verify their public-key certificate; moreover, the recipient does not need to distribute public-key certificates. The first actual implementation of IBE was proposed in 2001 by Boneh and Franklin [8] and Cocks [11], although the concept was proposed as early as 1984 by Shamir [27]. Additionally, Boneh and Franklin [8] formalized the security model of IBE, which ensures that no adversary can obtain any plaintext information from the ciphertext. Furthermore, in 2005, Abdalla *et al.* [1] proposed an "anonymous" IBE scheme according to the concept in [5]. Specifically, a secure IBE scheme can be considered to be anonymous if the ciphertext not only fails to disclose plaintext, but also fails to disclose the recipient's information.

However, public safety may be compromised if the recipient's information is always hidden or has unconditional privacy. This is because we cannot monitor the frequency of malicious people's encrypted communication in such contexts and prevent potential threats in advance. For example, the government cannot keep track of the ciphertext for some specified recipients, such as criminals. To achieve an optimal trade-off between public safety and privacy, Blazy *et al.* [6] recently introduced a new cryptography primitive called anonymous IBE with traceable identities (AIBET). This scheme, in contrast to the anonymous IBE scheme, has an additional party called a tracker that enables the filtering of ciphertext for a specific identity through a trace key generated by a trusted key generation center. Blazy *et al.* also formulated a selectively secure AIBET based on Boneh and Franklin's IBE [8], and they further presented a generic AIBET scheme transformed from any affine message authentication code [7]. Through the generic transformation, they obtained the first adaptively secure AIBET scheme under the standard model.

However, although Blazy *et al.* formulated a generic approach to achieving AIBET, the generic approach requires the aid of pairing computation and thus the security of their schemes relies on the discrete logarithm assumption. As reported by Shor [28, 29], there exists quantum algorithm can violate the integer factoring and discrete logarithm assumptions in polynomial-time complexity. In other words, as quantum computing matures, the AIBET scheme of Blazy *et al.* [6] becomes increasingly insecure against quantum attacks. In particular, with the advent of multiqubit quantum computers—such as Sycamore and Jiuzhang proposed by Arute *et al.* [4] and Zhong *et al.* [34] respectively—most existing cryptographic protocol are expected to soon be compromised. This raises the following question:

Is it possible to build a more secure AIBET resist against future quantum attacks?

*Corresponding author.

1.1 Our Contribution

The purpose of this paper is to address the aforementioned question. Accordingly, the contributions of this paper are twofold:

1.1.1 Consistency. Blazy *et al.* [6] considered only the correctness of AIBET, which is whether the recipient's identity can be traced by using a correct tracing key, which does not guarantee that no information is leaked even with the use of wrong tracing keys. In contrast, in this paper, we further formalize the *consistency* of tracing key of the AIBET to ensure that the recipient's identity cannot be traced using wrong tracing keys. Accordingly, we increase the security of the AIBET scheme.

1.1.2 Lattice-based Construction. To construct a quantum-resistant AIBET scheme, we first introduce a novel concept that can be applied to incorporate traceability into structure-specific lattice-based anonymous IBE. Furthermore, we obtain a lattice-based AIBET scheme by applying our concept to Katsumata and Yamada's compact anonymous IBE [19]. According to our findings, our scheme is secure under the ring learning with errors (RLWE) assumption; therefore, our scheme is the first quantum-resistant AIBET.

1.2 Organization of the Paper

The remainder of this paper is organized as follows. Section 2 presents some preliminaries, specifically our notations and the explanation about lattices. Section 3 provides a review of the definition and security requirements of AIBET. In Section 4, we introduce our concept and present our quantum-resistant AIBET. Section 5 provides a security proof of our proposed scheme. Finally, Section 6 concludes the paper and provides future research directions.

2 PRELIMINARIES

2.1 Notation

We adpot the following notations for convenience. First, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ denotes sets of natural numbers, integers, and real numbers, respectively. Nonitalic bold lowercase (e.g., $\mathbf{a}$) and uppercase (e.g., $\mathbf{A}$) letters denote vectors and matrices, respectively, where each entry is some number in $\mathbb{R}$; italic bold lowercase (e.g., $\boldsymbol{a}$) and uppercase (e.g., $\boldsymbol{A}$) letters denote vectors and matrices, respectively, where each entry is an element of a ring or number field. For a vector $\mathbf{a} \in \mathbb{R}^n$, $\|\mathbf{a}\|_p$ denotes the L_p-norm of $\mathbf{a}$. For a matrix $\mathbf{A} \in \mathbb{R}^{n\times n}$, $\|\mathbf{A}\|_{\mathrm{GS}}$ and $s_1(\mathbf{A})$ denote the longest column of the Gram-Schmidt orthogonalization and the largest singular value of $\mathbf{A}$, respectively. We use $[\cdot|\cdot]$ to denote the horizontal concatenation of vectors and matrices. For two random variables X and Y with support Σ, the statistical distance of X and Y is defined as $\Delta(X,Y) := \frac{1}{2}\sum_{s\in\Sigma}\left|\Pr[s=X]-\Pr[s=Y]\right|$. For two integers $a, b \in \mathbb{N}$, where $a \le b$, we use $[a, b]$ to denote the set $\{a, a+1, \cdots, b-1, b\}$. In addition, for a (quotient) polynomial ring R over $\mathbb{Z}$, $[-a, a]_R \subseteq R$ denotes the set of elements in R with all coefficients in the interval $[-a, a]$. We use the standard notations, $O, \tilde{O}, o$, and ω to classify the growth of functions. The notation $\mathrm{negl}(n)$ denotes as an arbitrary function f being *negligible* in n, where $f(n) = o(n^{-c})$ for every fixed constant c. The notation $\mathrm{poly}(n)$ denotes an arbitrary function $f(n) = O(n^c)$ for some constant c. PPT is short for "probabilistic polynomial-time." For a vector or matrix, a superscript $\top$ denotes its transpose. Finally, let D be a distribution over some finite set S; accordingly, $x \hookleftarrow D$ signifies that x is chosen from the distribution D, and $x \hookleftarrow U(S)$ signifies that x is uniformly sampled at random from S.

2.2 Lattices

This section introduces the basic concept of lattices, which is used in our scheme. An m-dimensional lattice Λ is an additive discrete subgroup of $\mathbb{R}^m$, which can be defined as follows:

Definition 2.1 (Lattice). An m-dimensional lattice Λ generated by a basis $\mathbf{B} = [\mathbf{b}_1|\cdots|\mathbf{b}_n] \in \mathbb{R}^{m\times n}$ can be defined as follows:

$$\Lambda(\mathbf{B}) = \Lambda(\mathbf{b}_1, \cdots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} \mathbf{b}_i a_i \,\middle|\, a_i \in \mathbb{Z} \right\},$$

where $\mathbf{b}_1, \cdots, \mathbf{b}_n \in \mathbb{R}^m$ are n linearly independent vectors.

In addition, for a prime q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, we can define the following three sets [2, 16]:

- $\Lambda_q := \{\mathbf{e} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}^n \text{ where } \mathbf{A}\mathbf{s} = \mathbf{e} \bmod q\}$.
- $\Lambda_q^{\perp} := \{\mathbf{e} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{e} = 0 \bmod q\}$.
- $\Lambda_q^{\mathbf{u}} := \{\mathbf{e} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{e} = \mathbf{u} \bmod q\}$.

2.3 Discrete Gaussian Distributions

For any vector $\mathbf{c} \in \mathbb{R}^n$ and any positive real number s, we can define the following:

- $\rho_{s,\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi\frac{\|\mathbf{x}-\mathbf{c}\|^2}{s^2}\right)$.
- $\rho_{s,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in\Lambda} \rho_{s,\mathbf{c}}(\mathbf{x})$.

The discrete Gaussian distribution over the lattice Λ with center $\mathbf{c}$ and parameter s can then be defined as $\mathcal{D}_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \rho_{s,\mathbf{c}}(\mathbf{x})/\rho_{s,\mathbf{c}}(\Lambda)$ for any $\mathbf{x} \in \Lambda$. Notably, $\mathbf{c}$ is usually omitted if it is 0. Additionally, the discrete Gaussian distribution over a (quotient) polynomial ring R in X over $\mathbb{R}$ can be defined as $\mathcal{D}^{\mathrm{coeff}}_{\Lambda,s,\mathbf{c}}$. For a distribution $a = \sum_{i=0}^{n-1} \alpha_i X^i \in R$ sampled from $\mathcal{D}^{\mathrm{coeff}}_{\Lambda,s}$, the coefficient vector $[\alpha_0, \cdots, \alpha_{n-1}] \in \mathbb{R}^n$ is sampled from $\mathcal{D}_{\Lambda,s}$.

We use the following lemmas, introduced in [19], in our correctness and security proofs.

Lemma 2.2 (Noise Rerandomization (Lemma 1 of [19])). *Let q, ℓ, and m be positive integers, and let r be a positive real number satisfying $r > \max\left(\omega(\sqrt{\log m}), \omega(\sqrt{\log \ell})\right)$. Let $\mathbf{b} \in \mathbb{Z}_q^m$ be arbitrary, and let $\mathbf{x}$ be chosen from $\mathcal{D}_{\mathbb{Z}^m,r}$. Then for any $\mathbf{V} \in \mathbb{Z}^{m\times\ell}$ and positive real number $\sigma > s_1(\mathbf{V})$, there exists a PPT algorithm* $\mathsf{ReRand}(\mathbf{V}, \mathbf{b}+\mathbf{x}, r, \sigma)$ *that outputs $\mathbf{b}' = \mathbf{b}\mathbf{V} + \mathbf{x}' \in \mathbb{Z}_q^{\ell}$ where $\mathbf{x}'$ is distributed statistically close to $\mathcal{D}_{\mathbb{Z}^{\ell},2r\sigma}$.*

Lemma 2.3 (Lemma 4.4 of [24]). *For any n-dimensional lattice Λ, real number $\epsilon \in (0,1)$, and $s \ge \eta_\epsilon(\Lambda)$, we derive the following:*

$$\Pr\left[\|\mathbf{x}\| > s\sqrt{n} \,\middle|\, \mathbf{x} \hookleftarrow \mathcal{D}_{\Lambda,s\omega(\sqrt{\log n})}\right] \le \frac{1+\epsilon}{1-\epsilon}\cdot 2^{-n}.$$

Lemma 2.4 (Discrete Gaussian Error Bound (Lemma 20 of [19])). *Let $\mathbf{e}$ be some vector in $\mathbb{Z}^n$ and let $\mathbf{x} \hookleftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$ for some $\alpha q > \omega(\sqrt{\log n})$. Then the quantity $|\mathbf{e}\mathbf{x}^{\top}|$ treated as an integer in $[0, \cdots, q-1]$ satisfies $|\mathbf{e}\mathbf{x}^{\top}| \le \|\mathbf{e}\|_2\alpha q\omega(\sqrt{\log n})$ with overwhelming probability.*

2.4 Rings and Ideal Lattices

This section briefly introduces the concepts of a ring and ideal lattice as formulated in previous studies [21, 22]. In particular, because our scheme is based on Katsumata and Yamada's IBE scheme [19], we recapitulate some useful functions posited in [19]. Please refer to [19] for further information.

Let n be a power of 2. The ring can then be defined as $R = \mathbb{Z}[X]/\Phi_m(X)$, where $\Phi_m(X) = X^n + 1$ is the mth cyclotomic polynomial and $m = 2n$. Furthermore, for some integer q, we use R_q to denote $R/qR = \mathbb{Z}[X]/(q, \Phi_m(X))$. Because we can consider the coefficients in R to be elements in $\mathbb{Z}^n$, for convenience, a coefficient-embedding function $\phi : \mathbb{R} \rightarrow \mathbb{Z}^n$ is posited, which maps a ring $a = \sum_{i=0}^{n-1} \alpha_i X^i \in R$ to a vector $[\alpha_0, \alpha_1, \cdots, \alpha_{n-1}] \in \mathbb{Z}^n$. Furthermore, the coefficient-embedding function can be extended naturally to vectors and matrices. We posit the ring homomorphism $\mathrm{rot} : R \rightarrow \mathbb{Z}^{n\times n}$; it sends $a \in R$ to a matrix in $\mathbb{Z}^{n\times n}$ such that the ith row in $\mathbb{Z}^{n\times n}$ is $\phi\left(a \cdot X^{i-1} \bmod \Phi_m(X)\right) \in \mathbb{Z}^n$. Similarly, the definition of rot can be extended to vectors and matrices. Additionally, for a matrix $\boldsymbol{R} \in R^{s\times t}$, the largest singular value of $\boldsymbol{R}$ is defined as $s_1(\boldsymbol{R}) := \max_{\|\mathbf{z}\|_2=1} \|\mathbf{z} \cdot \mathrm{rot}(\boldsymbol{R})\|_2$. Finally, for a vector $\boldsymbol{a} \in R^k$, we can consider $\boldsymbol{a}$ to be short if $\|\phi(\boldsymbol{a})\|_2$ is small.

A random matrix chosen from $[-\rho, \rho]_R^{s\times t}$ can be bounded by Lemma 2.5. Furthermore, Lemma 2.6 pertains to ring-based lattice regularity.

Lemma 2.5 (Lemma 2 of [19]). *Let ρ be a positive integer, and let $\boldsymbol{R}$ be an $s \times t$ matrix chosen uniformly at random from $[-\rho, \rho]_R^{s\times t}$. Then, there exists a universal constant $C(\approx 1/\sqrt{2\pi})$ such that*

$$\Pr\left[s_1(\mathbf{R}) \geq C \cdot \rho\sqrt{n} \cdot \left(\sqrt{s} + \sqrt{t} + \omega(\sqrt{\log n})\right)\right] = \mathsf{negl}(n).$$

Lemma 2.6 (Regularity Lemma (Lemma 4 of [19])). *Let n be a power of 2; let q be a prime larger than $4n$ such that $q \equiv 3 \bmod 8$; and let ℓ, k', k, and ρ be positive integers satisfying $\ell, lk' \geq 1, k \geq 2$, and $\rho < \frac{1}{2}\sqrt{q/n}$, respectively. Consider the family of hash functions $\mathcal{H} = \{h_{\mathbf{A}}(\mathbf{x}) : [-\rho, \rho]_R^k \rightarrow R_q^{k'}\}$, where $h_{\boldsymbol{A}}(\boldsymbol{x}) = \boldsymbol{A}\boldsymbol{x}$ for $\boldsymbol{A} \in R_q^{k'\times k}$ and $\boldsymbol{x} \in R_q^k$. Then, $\mathcal{H}$ is a universal hash family. Additionally, for $\boldsymbol{A} \hookleftarrow R_q^{k'\times k}$ and $\boldsymbol{X} \hookleftarrow U([-\rho, \rho]_R^{k\times\ell})$, we derive the following:*

$$\Delta\left((\boldsymbol{A}, \boldsymbol{A}\boldsymbol{X}); \left(\boldsymbol{A}, U(R_q^{k'\times\ell})\right)\right) \leq \frac{\ell}{2} \cdot \sqrt{\left(\frac{q^{k'}}{(2\rho+1)^k}\right)^n}.$$

The security of our construction is based on the famous lattice hard assumption, namely the RLWE assumption, which was first posited by Lybashevsky *et al.* [21, 22].

Definition 2.7 (RLWE Assumption (Definition 1 of [19])). Let λ be a security parameter. Given $n = n(\lambda), k = k(n)$, a prime integer $q = q(n) > 2$, an error distribution $\chi = \chi(n)$ over R_q, we can determine an advantage for the RLWE problem of $\mathcal{A}$ as follows:

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{RLWE}_{n,k,q,\chi}} = \left|\Pr\left[\mathcal{A}\left(\{a_i, v_i\}_{i=1}^k\right) \rightarrow 1\right] - \Pr\left[\mathcal{A}\left(\{a_i, a_i s + e_i\}_{i=1}^k\right) \rightarrow 1\right]\right|,$$

where $a_1, \cdots, a_k, v_1, \cdots, v_k, s \hookleftarrow U(R_q)$ and $e_1, \cdots, e_k \hookleftarrow \chi$. We suggest that the $\mathsf{RLWE}_{n,k,q,\chi}$ assumption holds if for all PPT $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{RLWE}_{n,k,q,\chi}}$ is negligible.

Theorem 2.8 (Theorem 1 of [19]). *Let α be a positive real number, let m be a power of 2, let ℓ be an integer, let $\Phi_m(X) = X^n+1$ be the mth cyclotomic polynomial where $m = 2n$, let $R = \mathbb{Z}[X]/(\Phi_m(X))$, let $q \equiv 3 \bmod 8$ be a prime such that there exists another prime $p \equiv 1 \bmod m$ satisfying $p \leq q \leq 2p$, and let also $\alpha q \geq n^{3/2}k^{1/4}\omega(\log^{9/4} n)$. Accordingly, there exists a probabilistic polynomial-time quantum reduction from an $\tilde{O}(\sqrt{n}/\alpha)$-approximate SIVP (or SVP) to $\mathsf{RLWE}_{n,k,q,\chi}$ with $\chi = \mathcal{D}_{\mathbb{Z}^n,\alpha q}^{\mathsf{coeff}}$.*

2.5 Trapdoor for Rings

Before presenting some useful functions in this section, we define the gadget matrix. Let $\boldsymbol{g}_b = [1|b|\cdots|b^{k'-1}|\mathbf{0}] \in R_q^k$ be a gadget matrix for $b \in \mathbb{N}$ and $k \geq k' = \lfloor\log_b q\rfloor$, and let $\boldsymbol{g}_b^{-1}(\cdot)$ be a deterministic polynomial time algorithm [23] that takes the input $\boldsymbol{u} \in R_q^k$ and outputs $\boldsymbol{R} \in [-b, b]_R^{k\times k}$ such that $\boldsymbol{g}_b\boldsymbol{R} = \boldsymbol{u}$.

The following paragraphs provides a recapitulation of a key trapdoor function and key sampler functions in the "ring setting" defined in Lemma 5 of [19]; these functions are used in our construction.

Let n be a power of 2 an q be a prime larger than $4n$ such that $q \equiv 3 \bmod 8$; moreover, consider some $b, \rho \in \mathbb{Z}^+$ satisfying $\rho < \frac{1}{2}\sqrt{q/n}$. In addition, let $\log_1(\cdot) := \log_2(\cdot)$. According, we derive the following lemmas.

Lemma 2.9 (TrapGen) [23]). *There exists a randomized polynomial time algorithm $\mathsf{TrapGen}(1^n, 1^k, q, \rho)$ that outputs a vector $\boldsymbol{a} \in R_q^k$ and a matrix $\boldsymbol{T_a} \in R^{k\times k}$ when $k \geq 2\log_\rho q$. Here, $\mathrm{rot}(\boldsymbol{a}^\top)^\top \in \mathbb{Z}_q^{n\times nk}$ is a full-rank matrix and $\mathrm{rot}(\boldsymbol{T_a}) \in \mathbb{Z}_q^{nk\times nk}$ is a basis for $\Lambda^\perp(\mathrm{rot}(\boldsymbol{a}^\top)^\top)$. Furthermore, $\boldsymbol{a}$ is $\mathsf{negl}(n)$-close to uniform and $\|\mathrm{rot}(\boldsymbol{T_a})\|_{\mathrm{GS}} = O\left(b\rho \cdot \sqrt{n\log_\rho q}\right)$.*

Lemma 2.10 (SampleLeft [9]). *Consider $\boldsymbol{a}, \boldsymbol{b} \in R_q^k$ where $\mathrm{rot}(\boldsymbol{a}^\top)^\top, \mathrm{rot}(\boldsymbol{b}^\top)^\top \in \mathbb{Z}_q^{n\times nk}$ are full-rank matrices; an element $u \in R_q$, a matrix $\boldsymbol{T_a} \in R^{k\times k}$ such that $\mathrm{rot}(\boldsymbol{T_a}) \in \mathbb{Z}^{nk\times nk}$ is a basis for $\Lambda^\perp(\mathrm{rot}(\boldsymbol{a}^\top)^\top)$, and a Gaussian parameter $\sigma > \|\mathrm{rot}(\boldsymbol{T_a})\|_{\mathrm{GS}} \cdot \omega(\sqrt{\log nk})$. Accordingly, there exists a randomized polynomial time algorithm $\mathsf{SampleLeft}(\boldsymbol{a}, \boldsymbol{b}, u, \boldsymbol{T_a}, \sigma)$ that outputs a vector $\boldsymbol{e} \in R^{2k}$ sampled from a distribution that is $\mathsf{negl}(n)$-close to $\mathcal{D}_{\Lambda_{\phi(u)}^\perp([\mathrm{rot}(\boldsymbol{a}^\top)^\top|\mathrm{rot}(\boldsymbol{b}^\top)^\top]),\sigma}^{\mathsf{coeff}}$.*

Lemma 2.11 (SampleRight [3]). *Consider $\boldsymbol{a}, \boldsymbol{g}_b \in R_q^k$ where $\mathrm{rot}(\boldsymbol{a}^\top)^\top, \mathrm{rot}(\boldsymbol{g}_b) \in \mathbb{Z}_q^{n\times nk}$ are full-rank matrices; the elements $y \in R_q^*$ and $u \in R_q$; a matrix $\boldsymbol{R} \in R^{k\times k}$, a matrix $\boldsymbol{T}_{\boldsymbol{g}_b} \in R^{k\times k}$ such that $\mathrm{rot}(\boldsymbol{T}_{\boldsymbol{g}_b})) \in \mathbb{Z}^{nk\times nk}$ is a basis for $\Lambda^\perp(\mathrm{rot}(\boldsymbol{g}_b))$; and a Gaussian parameter $\sigma > \|\mathrm{rot}(\boldsymbol{T}_{\boldsymbol{g}_b})\|_{\mathrm{GS}} \cdot \omega(\sqrt{\log nk})$. Accordingly, there exists a randomized polynomial time algorithm $\mathsf{SampleLeft}(\boldsymbol{a}, \boldsymbol{g}_b, \boldsymbol{R}, y, u, \boldsymbol{T}_{\boldsymbol{g}_b}), \sigma)$ that outputs a vector $\boldsymbol{e} \in R^{2k}$ sampled from a distribution that is $\mathsf{negl}(n)$-close to $\mathcal{D}_{\Lambda_{\phi(u)}^\perp([\mathrm{rot}(\boldsymbol{a}^\top)^\top|\mathrm{rot}(\boldsymbol{b}^\top)^\top]),\sigma}^{\mathsf{coeff}}$, where $\boldsymbol{b} = \boldsymbol{a}\boldsymbol{R} + y\boldsymbol{g}_b$.*

Lemma 2.12 (Invertible Gadget Algorithm [23]). *Let $k \geq \lceil\log_b q\rceil$. There exists a publicly known matrix $\boldsymbol{T}_{\boldsymbol{g}_b}$ such that*

$\mathrm{rot}(\boldsymbol{T}_{\boldsymbol{g}_b}) \in \mathbb{Z}^{nk\times nk}$ *is a basis for the lattice* $\Lambda^{\perp}(\mathrm{rot}(\boldsymbol{g}_b))$ *and* $\|\mathrm{rot}(\boldsymbol{T}_{\boldsymbol{g}_b})\|_{\mathrm{GS}} \leq \sqrt{b^2+1}$.

2.6 Homomorphic Computation

We apply the $\mathsf{PubEval}_d : (R_q^k)^d \to R_q^k$ function presented in [19] in our construction to hash identities to R_q^k. Let $d \in \mathbb{N}$, and let $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_d \in R_q^k$. This function can be defined as follows:

$$\mathsf{PubEval}_d(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_d) = \begin{cases} \boldsymbol{b}_1 & \text{if } d = 1; \\ \boldsymbol{b}_1 \cdot \boldsymbol{g}_b^{-1}\left(\mathsf{PubEval}_{d-1}(\boldsymbol{b}_2, \cdots, \boldsymbol{b}_d)\right) & \text{if } d \geq 2. \end{cases}$$

Lemma 2.13 (Lemma 6 of [19]). *Let* $y_1, \cdots, y_d$ *be elements in* R*; let* $\boldsymbol{a}, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_d$ *be vectors in* R_q^k*; and let* $\boldsymbol{R}_1, \cdots, \boldsymbol{R}_d$ *be matrices in* $R^{k\times k}$ *such that* $\boldsymbol{b}_i = \boldsymbol{a}\boldsymbol{R}_i + y_i \boldsymbol{g}_b$ *for* $i \in [d]$*. Furthermore, we assume that* $s_1(\boldsymbol{R}_i) \leq B$, $\|\phi(y_i)\|_1 \leq \delta$ *for* $i \in [d]$*. Then, there exists an efficient algorithm* $\mathsf{TrapEval}_d$ *that takes* $\boldsymbol{R}_1, \cdots, \boldsymbol{R}_d, y_1, \cdots, y_d$ *as inputs and outputs* $\boldsymbol{R}' \in R^{k\times k}$ *such that*

$$\mathsf{PubEval}_d\left(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_d\right) = \boldsymbol{a}\boldsymbol{R}' + y_1 \cdots y_d \boldsymbol{g}_b \in R_q^k,$$

and $s_1(\boldsymbol{R}') \leq B\delta^{d-1} + Bbnk\left(\frac{\delta^{d-1}-1}{\delta-1}\right)$.

3 ANONYMOUS IBE WITH TRACEABLE IDENTITIES

In this section, we consider the system definition and security model of AIBET provided by Blazy *et al.* [6]. However, Blazy *et al.* considered only the correctness requirement in AIBET. Therefore, we cannot guarantee that no information is leaked with the use of wrong tracing keys. Hence, in this paper, we further formalize the *consistency* requirement of AIBET to ensure that there exists no adversary who can obtain any information of the recipient's identity with the use of wrong tracing keys.

Definition 3.1. The AIBET scheme comprises six algorithms $(\mathsf{Setup}, \mathsf{USK_G}, \mathsf{TSK_G}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{TVerify})$ along with an identity space $\mathcal{ID}$, which are described as follows:

- $\mathsf{Setup}(1^\lambda)$: Given a security parameter λ, the *setup* algorithm outputs a master public key mpk and master secret key msk.
- $\mathsf{USK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$: Given a master public key mpk, a master secret key msk, and an identity $\mathsf{id} \in \mathcal{ID}$, the *secret key generation* algorithm outputs a secret key $\mathsf{usk_{ID}}$ for an identity id.
- $\mathsf{TSK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$: Given a master public key mpk, a master secret key msk, and an identity $\mathsf{id} \in \mathcal{ID}$, the *tracing key generation* algorithm outputs a tracing key $\mathsf{tsk_{id}}$ for identity id.
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mathsf{M})$: Given a master public key, an identity id, and a message M, the *encryption* algorithm outputs a ciphertext C.
- $\mathsf{Dec}(\mathsf{usk_{id}}, \mathsf{C})$: Given a user's secret key $\mathsf{usk_{id}}$ and a ciphertext C, the *decryption* algorithm outputs a message M.
- $\mathsf{TVerify}(\mathsf{tsk_{id}}, \mathsf{C})$: Given a user's tracing key $\mathsf{tsk_{id}}$ and a ciphertext C, the *trace verification* algorithm checks whether the ciphertext C is targeted for the identity id. If yes, it outputs 1; otherwise, it outputs 0.

Definition 3.2 (Correctness). Consider all security parameters λ; all pairs $(\mathsf{mpk}, \mathsf{msk})$ generated by $\mathsf{Setup}(1^\lambda)$; all messages M; all identities $\mathsf{id} \in \mathcal{ID}$; all $\mathsf{usk_{id}}$ and $\mathsf{tsk_{id}}$ generated by $\mathsf{USK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$ and $\mathsf{TSK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$, respectively; and all ciphertexts C generated by $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mathsf{M})$. Accordingly, we derive the following:

$$\Pr[\mathsf{Dec}(\mathsf{usk_{id}}, \mathsf{C}) = \mathsf{M} \wedge \mathsf{TVerify}(\mathsf{tsk_{id}}, \mathsf{C}) = 1] \geq 1 - \mathsf{negl}(\lambda).$$

Definition 3.3 (Consistency). Consider all security parameters λ; all pairs $(\mathsf{mpk}, \mathsf{msk})$ generated by $\mathsf{Setup}(1^\lambda)$; all messages M, all identities $\mathsf{id}, \mathsf{id}' \in \mathcal{ID}$, where $\mathsf{id} \neq \mathsf{id}'$; all $\mathsf{usk_{id}}$, $\mathsf{usk_{id'}}$, $\mathsf{tsk_{id}}$, and $\mathsf{tsk_{id'}}$ generated by $\mathsf{USK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$, $\mathsf{USK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}')$, $\mathsf{TSK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$, and $\mathsf{TSK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}')$, respectively; and all ciphertexts C generated by $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mathsf{M})$. Accordingly, we derive the following:

$$\Pr\left[\mathsf{TVerify}(\mathsf{tsk_{id'}}, \mathsf{C}) = 0\right] \geq 1 - \mathsf{negl}(\lambda).$$

The security requirement of the AIBET scheme is almost the same as that of the anonymous IBE scheme. The only difference is that adversary is allowed to query the tracing key on any identity except for the challenged identity. We present the following game to model this security between an adversary $\mathcal{A}$ and challenger $\mathcal{B}$ for AIBET scheme Π.

Game - IND-ANON-ID-CPA:

- **Setup.** The challenger $\mathcal{B}$ runs $\mathsf{Setup}(1^\lambda)$ to generate $(\mathsf{mpk}, \mathsf{msk})$ and give mpk to $\mathcal{A}$.
- **Phase 1.** $\mathcal{A}$ is allowed to adaptively query the secret key generation and tracing key generation oracles as follows:
  - $\mathcal{O}^{\mathsf{USK_G}}$: After receiving an identity $\mathsf{id} \in \mathcal{ID}$ submitted by $\mathcal{A}$, $\mathcal{B}$ returns $\mathsf{usk_{id}} \hookleftarrow \mathsf{USK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$.
  - $\mathcal{O}^{\mathsf{TSK_G}}$: After receiving an identity $\mathsf{id} \in \mathcal{ID}$ submitted by $\mathcal{A}$, $\mathcal{B}$ returns $\mathsf{tsk_{id}} \hookleftarrow \mathsf{USK_G}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$.
- **Challenge.** After **Phase 1**, $\mathcal{A}$ outputs a challenge message M and an identity $\mathsf{id}^* \in \mathcal{ID}$ to $\mathcal{B}$, where id has not been queried to oracles. $\mathcal{B}$ picks a random coin $\mathrm{b} \hookleftarrow U(\{0,1\})$ and a random ciphertext C from the ciphertext space. If $b = 0$, then $\mathcal{B}$ outputs a ciphertext $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*, \mathsf{M}) \to \mathsf{C}^*$; otherwise, $\mathcal{B}$ sets $\mathsf{C}^* = \mathsf{C}$. Subsequently, $\mathcal{B}$ returns C^* as a challenge to $\mathcal{A}$.
- **Phase 2.** $\mathcal{A}$ can continue to query the oracles as executed in *Phase 1.* The only restriction is that $\mathcal{A}$ cannot query these oracles on the challenge identity id^*
- **Guess.** Finally, $\mathcal{A}$ outputs a guess b'. If $b' = b$, $\mathcal{A}$ wins the game. The advantage of $\mathcal{A}$ winning the game can be defined as follows:
$$\mathsf{Adv}_{\mathcal{A},\Pi}^{\mathsf{AIBET}} = \left|\Pr[b' = b] - \frac{1}{2}\right|.$$

Definition 3.4 (IND-ANON-ID-CPA for AIBET). For all PPT adversaries $\mathcal{A}$, we suggest that AIBET scheme Π is IND-ANON-ID-CPA secure if $\mathsf{Adv}_{\mathcal{A},\Pi}^{\mathsf{AIBET}}$ is negligible.

4 OUR CONCEPT AND CONSTRUCTION

This section presents our concept and the AIBET scheme that is secure under the RLWE assumption.

4.1 Overview of Our Concept

Before introducing our concept, we provide an overview of the framework presented in [2]; this is because the current standard model secure lattice-based anonymous IBE [3, 9, 19, 20, 30, 32, 33] follows this framework. Consider the single-bit selectively secure anonymous IBE scheme presented in [2] as an example. Let $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}$, and u be public parameters; let a user's identity id be associated with the matrix $[\mathbf{A}|\mathsf{H}(\mathsf{id})]$; let the user's secret $\mathsf{USK}_{\mathsf{id}}$ be generate from the SampleLeft function; and let $F_{\mathsf{id}} \cdot \mathsf{USK}_{\mathsf{id}} = u$, where $F_{\mathsf{id}} = [\mathbf{A}_0|\mathbf{A}_1 + H(\mathsf{id}) \cdot \mathbf{B}]$. The ciphertext has two parts $\mathsf{C} = \left\{ c_0 = us + x + b\lfloor \frac{q}{2} \rfloor, \mathbf{c}_1 = F_{\mathsf{id}}s + \begin{bmatrix} y \\ z \end{bmatrix} \right\}$, where c_0 is related to the message b and $\mathbf{c}_1$ is related to the identity. If the parameters are set correctly, the message can be recovered by computing $c_0 - \mathsf{USK}_{\mathsf{id}} \cdot \mathbf{c}_1$.

To incorporate traceability into lattice-based IBE, an intuitive approach is to generate another formal part of the ciphertext; that is, $c_0' = u's + x' + b'\lfloor \frac{q}{2} \rfloor$ according to the original scheme. Here, let u' be an added public parameter with the same distribution as u. The tracing key USK_{id} is generated in a manner similar to that of the user's secret key, except that $F_{\mathsf{id}} \cdot \mathsf{TSK}_{\mathsf{id}} = u'$. If b' can be recovered by computing $c_0' - \mathsf{TSK}_{id} \cdot \mathbf{c}_1$, then the recipient can be considered to be id. However, in this approach, if the sender wishes to hide the recipient's identity, they may randomly generate c_0' such that the tracker cannot trace the recipient of the ciphertext even if the tracker has the tracing key.

To solve the aforementioned problem, c_0 must connect to c_0'; thus, we can carefully make the following two adjustments: (1) each user's secret key $\mathsf{USK}_{\mathsf{id}}$ is sampled to satisfy $F_{\mathsf{id}} \cdot \mathsf{USK}_{\mathsf{id}} = (u + u')$ and $c_0' = u's + x'$; (2) to recover the message, the decryptor must compute $\widetilde{c_0} = c_0 + c_0'$. If the tracker can obtain 0 by computing $c_0' - F_{\mathsf{id}}\mathbf{c}_1$, then the recipient is traced. Nevertheless, through this adjustment, if the ciphertext cannot be traced, then the ciphertext cannot be decrypted.

At a high level, compared with the approach in [2], our approach has only one additional public parameter u', and the means through which a secret key is generated is changed (the parameter of SampleLeft is changed to $u + u'$). Specifically, this heuristic can be directly incorporated into pre-existing anonymous IBE schemes [3, 9, 19, 20, 30, 32, 33] based on [2].[1]

4.2 Lattice-based AIBET

To achieve efficiency and security, we apply our concept to Katsumata and Yamada's anonymous IBE [19], which was proven to be IND-ANON-ID-CPA secure under the standard model.

Let the identity space of our proposed scheme be $\mathcal{ID} \subseteq \{0,1\}^\kappa$ for some $\kappa \in \mathbb{N}$, and let the message space be $\{0,1\}^n \subset R$. In addition, we use an efficiently computable injetive map S to map the identity $\mathsf{id} \in \{0,1\}^\kappa$ to a subset $S(\mathsf{id})$ of $[1,\ell]^d$, where $\ell = \lceil \kappa^{1/d} \rceil$ and $d \in \mathbb{N}$. The parameters of the scheme are $n = n(\lambda), b = b(n), \rho = \rho(n), m = 2n, q = q(n), k = k(n), \ell = \ell(n), \alpha = \alpha(n), \alpha' = \alpha'(n)$ and $\sigma = \sigma(n)$. This choice of parameters is justified in Section 4.4.

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$:
  (1) Compute $\boldsymbol{a} \in R_q^k$ associated with its trapdoor $\boldsymbol{T_a} \in R^{k\times k}$, where $(\boldsymbol{a}, \boldsymbol{T}) \hookleftarrow \mathsf{TrapGen}(1^n, 1^k, q, \rho)$.
  (2) Sample two uniformly random polynomials $u_1, u_2 \hookleftarrow U(R_q)$, and a polynomial vector $\boldsymbol{b}_0 \hookleftarrow U(R_q^k)$.
  (3) For $(i,j) \in [d] \times [\ell]$, sample random polynomial vectors $\boldsymbol{b}_{i,j} \hookleftarrow U(R_q^k)$.
  (4) Define a deterministic function $\mathsf{H} : \mathcal{ID} \to R_q^k$:
  $$\mathsf{H}(\mathsf{id}) = \boldsymbol{b}_0 + \sum_{(j_1,\cdots,j_d)\in S(\mathsf{id})} \mathsf{PubEval}_d(\boldsymbol{b}_{1,j_1}, \boldsymbol{b}_{2,j_2}, \cdots, \boldsymbol{b}_{d,j_d}) \in R_q^k.$$
  (5) Output $\mathsf{mpk} := (\boldsymbol{a}, u_1, u_2, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d]\times[\ell]}, \mathsf{H})$ and $\mathsf{msk} := \boldsymbol{T_a}$.
- $\mathsf{USK_G}(\mathsf{mpk} = (\boldsymbol{a}, u_1, u_2, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d]\times[\ell]}, \mathsf{H}), \mathsf{msk} = \boldsymbol{T_a}, \mathsf{id} \in \mathcal{ID}) \to \mathsf{usk_{id}}$:
  (1) Compute $\boldsymbol{e} \hookleftarrow \mathsf{SampleLeft}(\boldsymbol{a}, \mathsf{H}(\mathsf{id}), u_1 + u_2, \boldsymbol{T_a}, \sigma)$.
  (2) Output $\mathsf{usk_{id}} := \boldsymbol{e} \in R^{2k}$.
- $\mathsf{TSK_G}(\mathsf{mpk} = (\boldsymbol{a}, u_1, u_2, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d]\times[\ell]}, \mathsf{H}), \mathsf{msk} = \boldsymbol{T_a}, \mathsf{id} \in \mathcal{ID}) \to \mathsf{tsk_{id}}$:
  (1) Compute $\boldsymbol{f} \hookleftarrow \mathsf{SampleLeft}(\boldsymbol{a}, \mathsf{H}(\mathsf{id}), u_2, \boldsymbol{T_a}, \sigma)$.
  (2) Output $\mathsf{tsk_{id}} := \boldsymbol{f} \in R^{2k}$.
- $\mathsf{Enc}(\mathsf{mpk} = (\boldsymbol{a}, u_1, u_2, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d]\times[\ell]}, \mathsf{H}), \mathsf{id}, \mathsf{M} \in \{0,1\}^n \subset R) \to \mathsf{C}$:
  (1) Sample $s \hookleftarrow U(R_q), x_{0,1}, x_{0,2} \hookleftarrow \mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}$.
  (2) Sample $\boldsymbol{x}_1, \boldsymbol{x}_2 \hookleftarrow \left(\mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha'}\right)^k$
  (3) Compute $c_{0,1} = su_1 + x_{0,1} + \lfloor q/2 \rceil \mathsf{M}$, $c_{0,2} = su_2 + x_{0,2}$, and $\boldsymbol{c}_1 = s[\boldsymbol{a}|\mathsf{H}(\mathsf{id})] + [\boldsymbol{x}_1|\boldsymbol{x}_2]$.
  (4) Output $\mathsf{C} := (c_{0,1}, c_{0,2}, \boldsymbol{c}_1) \in R_q \times R_q \times R_q^{2k}$.
- $\mathsf{Dec}(\mathsf{usk_{id}} = \boldsymbol{e}, \mathsf{C} = (c_{0,1}, c_{0,2}, \boldsymbol{c}_1)) \to \mathsf{M}$:
  (1) Compute $c_0 = c_{0,1} + c_{0,2} \in R_q$.
  (2) Compute $w = \left(\lfloor (2/q) \cdot \phi(c_0 - \boldsymbol{c}_1\boldsymbol{e}^\top) \rceil \bmod 2\right)$, where the rounding function $\lfloor \cdot \rceil$ is applied component-wise.
  (3) Output $\mathsf{M} := w$.
- $\mathsf{TVerify}(\mathsf{tsk_{id}} = \boldsymbol{f}, \mathsf{C} = (c_{0,1}, c_{0,2}, \boldsymbol{c}_1)) \to 1/0$:
  (1) Compute $w = \left(\lfloor (2/q) \cdot \phi(c_{0,2} - \boldsymbol{c}_1\boldsymbol{f}^\top) \rceil \bmod 2\right) \in \{0,1\}^n$, where the rounding function $\lfloor \cdot \rceil$ is applied component-wise.
  (2) If w is 0 for all elements, output 1; otherwise, output 0.

4.3 Correctness and Consistency

Lemma 4.1 (Correctness). *Given a pair comprising a master public key and master secret key* $(\mathsf{mpk} = (\boldsymbol{a}, u_1, u_2, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d]\times[\ell]}, \mathsf{H}), \mathsf{msk} = \boldsymbol{T_a}) \hookleftarrow \mathsf{Setup}(1^\lambda)$, *given a ciphertext* $\mathsf{C} = (c_{0,1}, c_{0,2}, \boldsymbol{c}_1) \hookleftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mathsf{M})$, *given a secret key* $\mathsf{usk_{id}} = \boldsymbol{e}$, *and given a tracing key* $\mathsf{tsk_{id}} = \boldsymbol{f}$ *for user* id, *our proposed scheme is correct if the norm of the error term is bounded by* $q/5$ *with overwhelming probability.*

Proof. The correctness of our scheme is proven if $\mathsf{Dec}(\mathsf{usk_{id}}, \mathsf{C})$ and $\mathsf{TVerify}(\mathsf{tsk_{id}}, \mathsf{C})$ return the message M and 1, respectively.

[1] Notably, because the former part of the ciphertext in lattice-based anonymous IBE schemes [12, 16, 26] that are secure under random oracle model is independent from of the identity, our concept is not applicable to these schemes, which is consistent with the description in [6].

We first consider the correctness of the decryption algorithm. In the Dec algorithm, we have

$$\phi(c_0 - \boldsymbol{c}_1\boldsymbol{e}^\top) = \left\lfloor \frac{q}{2} \right\rceil \phi(\mathsf{M}) + \underbrace{\phi(x_{0,1}) + \phi(x_{0,2}) - \phi([\boldsymbol{x}_1|\boldsymbol{x}_2])\mathrm{rot}(\boldsymbol{e}^\top)}_{\text{error term}},$$

where $c_0 = c_{0,1} + c_{0,2}$.

We next analyze the norm of the error term by following the analogue of the Proof of Lemma 10 in [19]. Because $x_{0,1}$ and $x_{0,2}$ are chosen from $\mathcal{D}^{\mathrm{coeff}}_{\mathbb{Z}^n,\alpha q}$, the vectors $\phi(x_{0,1})$ and $\phi(x_{0,2})$ are subgaussians with the parameter αq. Thus, let each jth entry of $\phi(x_{0,1}), \phi(x_{0,2})$, $|\phi(x_{0,1})_j|, |\phi(x_{0,2})_j|$ be less than $\alpha q\omega(\sqrt{\log n})$ with overwhelming probability. Similarly, because $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are chosen from $\left(\mathcal{D}^{\mathrm{coeff}}_{\mathbb{Z}^n,\alpha'}\right)^k$, we have $\phi([\boldsymbol{x}_1|\boldsymbol{x}_2]) \hookleftarrow \mathcal{D}_{\mathbb{Z}^{2nk},\alpha'}$. In addition, according to the definition of the rot function, the norm of each column of $\mathrm{rot}(\boldsymbol{e}^\top)$ is $\|\phi(\boldsymbol{e})\|_2$, where $\phi(\boldsymbol{e}) \hookleftarrow \mathcal{D}_{\Lambda^\perp_{\phi(u_1+u_2)}([\mathrm{rot}(\boldsymbol{a}^\top)^\top|\mathrm{rot}(\mathsf{H}(\mathsf{id})^\top)^\top]),\sigma}$. According to Lemmas 2.3 and 2.4, we have, for each jth column, $|\phi([\boldsymbol{x}_1|\boldsymbol{x}_2])\mathrm{rot}(\boldsymbol{e}^\top)_j| \leq \|\phi(\boldsymbol{e})\|_2 \cdot \alpha'\omega(\sqrt{\log nk}) \leq \sqrt{nk}\alpha'\sigma\omega(\sqrt{\log nk})$ with overwhelming probability.

Hence, we can conclude that each jth entry of the error term is bounded as $\left|\phi(x_{0,1}) + \phi(x_{0,2}) - \phi([\mathbf{x}_1|\mathbf{x}_2])\mathrm{rot}(\mathbf{e}^\top)\right| \leq 2\alpha q\omega\left(\sqrt{\log n} + \sqrt{nk}\alpha'\sigma\omega(\sqrt{\log nk})\right)$ with overwhelming probability. If the assumption holds, i.e., $2\alpha q\omega\left(\sqrt{\log n} + \sqrt{nk}\alpha'\sigma\omega(\sqrt{\log nk})\right) \leq q/5$, then we can obtain the message M correctly with overwhelming probability.

Subsequently, we analyze the correctness of the trace verification algorithm. In the TVerify algorithm, we have

$$\phi(c_{0,2} - \boldsymbol{c}_1\boldsymbol{f}^\top) = \underbrace{\phi(x_{0,2}) - \phi([\boldsymbol{x}_1|\boldsymbol{x}_2])\mathrm{rot}(\boldsymbol{f}^\top)}_{\text{error term}}.$$

Using the preceding steps of the proof, we can also deduce that each jth entry of the error term is bounded as $\left|\phi\left(x_{0,2} - \phi([\mathbf{x}_1|\mathbf{x}_2])\mathrm{rot}(\mathbf{f}^\top)\right)\right| \leq \alpha q\omega\left(\sqrt{\log n} + \sqrt{nk}\alpha'\sigma\omega(\sqrt{\log nk})\right)$ with overwhelming probability. If the assumption holds (i.e., $\alpha q\omega\left(\sqrt{\log n} + \sqrt{nk}\alpha'\sigma\omega(\sqrt{\log nk})\right) \leq q/5$), then we can trace the identity of the recipient correctly with overwhelming probability. □

Lemma 4.2 (Consistency). *Consider a pair comprising a master public key and master secret key* ($\mathsf{mpk} = (\boldsymbol{a}, u_1, u_2, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d]\times[\ell]}, \mathsf{H}), \mathsf{msk} = \boldsymbol{T_a}) \hookleftarrow \mathsf{Setup}(1^\lambda)$*; a ciphertext* $\mathsf{C} = (c_{0,1}, c_{0,2}, \boldsymbol{c}_1) \hookleftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mathsf{M})$*; a secret key* $\mathsf{usk}_{\mathsf{id}'} = \boldsymbol{e}'$*; and a tracing key* $\mathsf{tsk}_{\mathsf{id}'} = \boldsymbol{f}'$ *for the user* id'*, where* $\mathsf{id} \neq \mathsf{id}'$*. Accordingly, our proposed scheme is consistent if the norm of the error term is bounded by* $q/5$ *with overwhelming probability.*

Proof. The proof of consistency is analogous to the proof of Lemma 4.1. Specifically, consistency is proven if $\mathsf{TVerify}(\mathsf{tsk}_{\mathsf{id}'}, \mathsf{C})$ returns 0.

Consider the process of the trace verification algorithm. In the TVerify algorithm, we have

$$\phi(c_{0,2} - \boldsymbol{c}_1\boldsymbol{f'}^\top) = \phi(su_2) - \phi(s[\boldsymbol{a}|\mathsf{H}(\mathsf{id})])\mathrm{rot}(\boldsymbol{f'}^\top) + \underbrace{\phi(x_{0,2}) - \phi([\boldsymbol{x}_1|\boldsymbol{x}_2])\mathrm{rot}(\boldsymbol{f'}^\top)}_{\text{error term}}.$$

According to the aforementioned assumption, the error term is bounded only by $q/5$. Because $u_2 \in R_q$, $\boldsymbol{a} \in R_q^k$, and $\mathsf{H}(\mathsf{id}) \in R_q^k$, the term $\phi(su_2) - \phi(s[\boldsymbol{a}|\mathsf{H}(\mathsf{id})])\mathrm{rot}(\boldsymbol{f}^\top)$ cannot be eliminated. The result of TVerify is not composed solely of 0 elements, so the algorithm outputs 0. Therefore, if the assumption holds, the tracker cannot trace the identity of the recipient correctly with overwhelming probability. □

4.4 Parameter Selection

To satisfy the algorithms (TrapGen and SampleLeft), the security proofs, and the requirement for the norm of error term to be less than $q/5$ (for correctness and consistency to hold), the following requirements must be satisfied.

- the norms of the error terms $\alpha q\omega(\sqrt{\log n}) + \sqrt{nk}\alpha'\sigma\omega(\sqrt{\log nk})$ and $2\alpha q\omega(\sqrt{\log n}) + \sqrt{nk}\alpha'\sigma\omega(\sqrt{\log nk})$ are less than $q/5$ with overwhelming probability (required by Lemma 4.1 and 4.2),
- $\rho < \frac{1}{2}\sqrt{q/n}$ and $k \geq 2\log_\rho q$ to ensure that TrapGen can function correctly (required by Theorem 2.9).
- $k \geq \lceil \log_b q \rceil$ such that the gadget matrix $\mathbf{g}_b$ can be defined (required by Theorem 2.12),
- $\sigma > O\left(b\rho \cdot \sqrt{n\log_\rho q}\right) \cdot \omega(\sqrt{\log nk})$ and $\sigma > s_1(\boldsymbol{R})\sqrt{b^2+1} \cdot \omega(\sqrt{\log n})$ such that the algorithms SampleLeft and SampleRight function correctly (required by Theorem 2.10 and 2.11). Here, $s_1(\boldsymbol{R}) \leq C'' \cdot \kappa\rho\sqrt{n}\left(\sqrt{k} + \omega(\sqrt{\log n})\right)\left((cn)^{d-1} + bnk\frac{(cn)^{d-1}-1}{cn-1}\right)$ for some absolute constant C'',
- $\frac{k}{2}\left(\frac{q^2}{(2\rho+1)^k}\right)^{n/2} = \mathrm{negl}(n)$ such that regularity lemma can be applied in the security proof (required by Lemma 2.6),
- $\alpha q \geq n^{3/2}k^{1/4}\omega(\log^{9/4} n)$ such that a worst-case-to-average-case reduction is achieved (required by Theorem 2.8),
- $\alpha' > 2\alpha q(s_1(\boldsymbol{R}) + 1)$ and $\alpha q > \omega(\sqrt{\log nk})$ such that the ReRand algorithm works correctly in the security proof (required by Lemma 2.2).

In [19], the author provided two candidate parameter sets, and the reader can consult that study for more details.

5 SECURITY PROOF

This section demonstrates that our above proposed scheme is adaptively IND-ANON-ID-CPA secure. Because our scheme is based on Katsumata and Yamada's IBE [19], we use the formulation they described for their security proof to implement the following proof.

Theorem 5.1. *Our proposed AIBET scheme is adaptively IND-ANON-ID-CPA secure assuming that* $\mathsf{RLWE}_{n,k+2,q,\mathcal{D}^{\mathrm{coeff}}_{\mathbb{Z}^n,\alpha q}}$ *is hard, where the ciphertext space is* $C = R_q \times R_q \times R_q^{2k}$.

Proof. Let $\mathcal{A}$ be a PPT adversary, $\epsilon = \epsilon(n)$ be the advantage of $\mathcal{A}$, and $Q = Q(n)$ be the upper bound of the number of secret key generation and tracing key generation oracles. Because $\mathcal{A}$ is a PPT adversary and $n = O(\lambda^{\delta})$, where δ is a constant, we have $4(dQ + 1) \leq n^{\varphi}$ for all elements n that are sufficiently large, where $\varphi \in \mathbb{N}$. Similarly, suppose that $\mathcal{A}$ breaks the security of our proposed scheme. Accordingly, we have $2\epsilon \geq n^{-\psi}$ for infinitely many elements n, where $\psi \in \mathbb{N}$. Therefore, for infinitely many $n \in \mathbb{N}$, we have

$$4dQ \leq n^{\xi} \text{ for all } n \in \mathbb{N} \text{ and } \frac{\epsilon}{2(dQ+1)} \geq \frac{1}{n^{\xi}}, \qquad (1)$$

where $\xi = \varphi + \psi$. Because ξ and d are constants, assuming that $d(\xi - 1) < n$, the aforementioned statement holds if n is sufficiently large.

To perform the proof, we execute a sequence of games in which the first game is identical to the IND-ANON-ID-CPA game defined in Section 3 and $\mathcal{A}$ has no advantage in the last game. In addition, we define X_i to be the event that $\mathcal{A}$ wins Game$_i$.

Game$_0$: This game is identical to the real IND-ANON-ID-CPA game. Suppose $\mathcal{A}$ outputs a guess $\bar{b}$ at the end of the game, by the definition of the advantage of $\mathcal{A}$, we have

$$\left|\Pr[X_0] - \tfrac{1}{2}\right| = \left|\Pr[\bar{b} = b] - \tfrac{1}{2}\right| = \epsilon.$$

Game$_1$: This game is similar to the previous game, except that at the end of the game, $\mathcal{B}$ performs additional steps, which are described as follows:

(1) $\mathcal{B}$ picks $\boldsymbol{y} = (y_0, \{y_{i,j}\}_{(i,j)\in[d,\ell]})$, where $y_0 \hookleftarrow U([-\kappa(\xi n)^d, -1]_{R,(\xi-1)d+1})$ and $y_{i,j} \hookleftarrow U([1,n]_{R,\xi})$. Here, for two integers $v_0, v_1 \in \mathbb{Z}$, where $v_0 \leq v_1$, the positive integer $w \in \mathbb{N}$, $[v_0, v_1]_{R,w}$ is denoted as

$$[v_0, v_1]_{R,w} := \left\{ \sum_{i=0}^{w-1} a_i X^i | a_i \in [v_0, v_1] \text{ for all } i \in [0, w-1] \right\} \subseteq R.$$

(2) Let id* be the challenged identity and $\mathsf{id}_1, \cdots \mathsf{id}_Q$ be the identities queried on the secret key generation and tracing key generation oracles, $\mathcal{B}$ then checks whether the following condition is satisfied:

$$\mathsf{F}_{\boldsymbol{y}}(\mathsf{id}^*) = 0 \wedge \mathsf{F}_{\boldsymbol{y}}(\mathsf{id}_1) \in R_q^* \wedge \cdots \wedge \mathsf{F}_{\boldsymbol{y}}(\mathsf{id}_Q) \in R_q^*,$$

where $\mathsf{F}_{\boldsymbol{y}} : \mathcal{ID} \to R_q$ is defined as:

$$\mathsf{F}_{\boldsymbol{y}}(\mathsf{id}) = y_0 + \sum_{(j_1,\cdots,j_d)\in S(\mathsf{id})} y_{1,j_1} \cdots y_{d,j_d}.$$

If this condition does not hold, $\mathcal{B}$ aborts the game and sets $\mathcal{A}$'s guess to $b' \hookleftarrow \{0,1\}$. Otherwise, $\mathcal{B}$ sets $b' = \bar{b}$.

Lemma 5.2. *For any adversary $\mathcal{A}$, we have*

$$\left|\Pr[X_1] - \tfrac{1}{2}\right| \geq \tfrac{1}{(\kappa\xi^d n^d)^{(\xi-1)d+1}} \left(\tfrac{\epsilon}{2} - \tfrac{dQ}{n^{\xi}}\right).$$

Proof. The proof is executed in a similar manner to the proof of Lemma 11 in [19]. Due to space constraints, please refer to [19] for more details. □

Game$_2$: This game is differs only slightly from the previous game, with the difference being the manner of choosing $\boldsymbol{b}_0, \boldsymbol{b}_{i,j}$. Specifically, in place of choosing $\boldsymbol{b}_0, \boldsymbol{b}_{i,j} \hookleftarrow U(R_q^k)$, $\boldsymbol{b}_0, \boldsymbol{b}_{i,j}$ are chosen as follows:

$$\boldsymbol{b}_0 = \boldsymbol{a}\boldsymbol{R}_0 + y_0\boldsymbol{g}_b, \boldsymbol{b}_{i,j} = \boldsymbol{a}\mathbf{R}_{i,j} + y_{i,j}\boldsymbol{g}_b,$$

for $(i,j) \in [d] \times [\ell]$. According to regularity lemma (Lemma 2.6), the distributions of $(\boldsymbol{a}, \boldsymbol{b}_0, \boldsymbol{b}_{i,j})$ in Game$_1$ and Game$_2$ are negl-close. Therefore, we have $|\Pr[X_1] - \Pr[X_2]| = \mathsf{negl}(n)$.

Game$_3$: In the previous games, when the condition

$$\mathsf{F}_{\boldsymbol{y}}(\mathsf{id}^*) = 0 \wedge \mathsf{F}_{\boldsymbol{y}}(\mathsf{id}_1) \in R_q^* \wedge \cdots \wedge \mathsf{F}_{\boldsymbol{y}}(\mathsf{id}_Q) \in R_q^*,$$

is not satisfied, $\mathcal{B}$ aborts at the end of the game. In the current game, $\mathcal{B}$ moves the abort time forward. In other words, as long as the condition is not satisfied, $\mathcal{B}$ aborts the game. Because no actual change occurs between Game$_2$ and Game$_3$, we have $\Pr[X_2] = \Pr[X_3]$.

Before moving to the next game, we define and provide the following results. First, we can define $\boldsymbol{R}_{\mathsf{id}}$ for an identity as follows:

$$\boldsymbol{R}_{\mathsf{id}} = \boldsymbol{R}_0 + \sum_{(j_1,\cdots,j_d)\in S(\mathsf{id})} \mathsf{TrapEval}_d(\boldsymbol{R}_{1,j_1}, \cdots, \boldsymbol{R}_{d,j_d}, y_{1,j_1}, \cdots, y_{d,j_d}).$$

Additionally, according to the definition of $\boldsymbol{R}_{\mathsf{id}}$, $\mathsf{H}(\mathsf{id})$, PubEval, and Lemma 2.13, we have

$$\begin{aligned}\mathsf{H}(\mathsf{id}) &= \boldsymbol{b}_0 + \sum_{(j_1,\cdots,j_d)\in S(\mathsf{id})} \mathsf{PubEval}_d(\boldsymbol{b}_{1,j_1}, \cdots, \boldsymbol{b}_{d,j_d}) \\ &= \boldsymbol{a}\boldsymbol{R}_{\mathsf{id}} + \mathsf{F}_{\boldsymbol{y}}(\mathsf{id})\boldsymbol{g}_b.\end{aligned}$$

Furthermore, we consider the bound of $s_1(\boldsymbol{R}_{\mathsf{id}})$. First, because $y_{i,j}$ is chosen from $[1,n]_{R,\xi}$, we have $\|y_{i,j}\|_1 \leq \xi n$. Then, according to Lemma 2.5, we have $s_1(\boldsymbol{R}_0), s_1(\boldsymbol{R}_{i,j}) \leq B$ with all but negligible probability because $\boldsymbol{R}_0$ and $\boldsymbol{R}_{i,j}$ are chosen from $[-\rho,\rho]_R^{k\times k}$, where $B = C' \cdot \rho\sqrt{n}(\sqrt{k} + \omega(\sqrt{\log n}))$. Therefore, we have

$$\begin{aligned} s_1(\boldsymbol{R}_{\mathsf{id}}) \leq s_1(\boldsymbol{R}_0) &+ \sum_{(j_1,\cdots,j_d)\in S(\mathsf{id})} \\ &s_1\left(\mathsf{TrapEval}_d(\boldsymbol{R}_{1,j_1}, \cdots, \boldsymbol{R}_{d,j_d}, y_{1,j_1}, \cdots, y_{d,j_d})\right) \\ &\leq B\left(1 + \kappa(\xi n)^{d-1} + \kappa bnk\frac{(\xi n)^{d-1} - 1}{\xi n - 1}\right), \end{aligned} \qquad (2)$$

for any id $\in \mathcal{ID}$ with all but negligible probability.

Game$_4$: In this game, instead of generating $\boldsymbol{a}$ using the TrapGen algorithm, $\mathcal{B}$ picks $\boldsymbol{a} \hookleftarrow U(R_q^k)$. According to Lemma 2.9, $\boldsymbol{a}$ is $\mathsf{negl}(n)$-close to uniform; thus, the difference is only negligible. In addition, how the challenger answers the oracles is changed. Specifically, instead of answering the user's secret key usk $= \boldsymbol{e} \hookleftarrow \mathsf{SampleLeft}(\boldsymbol{a}, \mathsf{H}(\mathsf{id}), u_1 + u_2, \boldsymbol{T_a}, \sigma)$ and tracing key tsk $= \boldsymbol{f} \hookleftarrow \mathsf{SampleLeft}(\boldsymbol{a}, \mathsf{H}(\mathsf{id}), u_2, \boldsymbol{T_a}, \sigma)$ for the identity id $\in \mathcal{ID}$ and $\mathsf{F}_{\boldsymbol{y}}(\mathsf{id}) \in R_q^*$, $\mathcal{B}$ answers them as follows: For any identity id $\in \mathcal{ID}$, if $\mathsf{F}_{\boldsymbol{y}}(\mathsf{id}) \notin R_q^*$, $\mathcal{B}$ aborts it. Otherwise, $\mathcal{B}$ first computes $\boldsymbol{R}_{\mathsf{id}}$ and then returns the secret key by computing usk $= \boldsymbol{e} \hookleftarrow \mathsf{SampleRight}(\boldsymbol{a}, \boldsymbol{g}_b, \boldsymbol{R}_{\mathsf{id}}, \mathsf{F}_{\boldsymbol{y}}(\mathsf{id}), u_1 + u_2, \boldsymbol{T}_{\boldsymbol{g}_b}, \sigma)$ and returns the tracing key by computing tsk $= \boldsymbol{f} \hookleftarrow \mathsf{SampleRight}(\boldsymbol{a}, \boldsymbol{g}_b, \boldsymbol{R}_{\mathsf{id}}, \mathsf{F}_{\boldsymbol{y}}(\mathsf{id}), u_2, \mathbf{T}_{\mathbf{g}_b}, \sigma)$, depending on which oracle was queried by $\mathcal{A}$. Therefore, according to the proper choice of σ and according to Eq. (2), Theorem 2.10, and Theorem

2.11, the output distribution of SampleRight is $\mathsf{negl}(n)$-close to the distribution of SampleLeft. Hence, from the perspective of $\mathcal{A}$, the change is negligible. We have $|\Pr[X_3]-\Pr[X_4]| = \mathsf{negl}(n)$.

Game$_5$: In the preceding game, when $b = 0$, $\mathcal{B}$ generates the challenged ciphertext following the real scheme. In the current game, if the game does not abort and $b = 0$, $\mathcal{B}$ creates the challenged ciphertext as follows. First, $\mathcal{B}$ picks $s \hookleftarrow U(R_q)$ and picks $\mathbf{x} \hookleftarrow \left(\mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}\right)^k$ before computing $\boldsymbol{v} = s\boldsymbol{a} + \boldsymbol{x} \in R^k$. Additionally, according to Lemma 2.2, $\mathcal{B}$ computes $\mathbf{c} \hookleftarrow \mathsf{ReRand}\left(\mathsf{rot}([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{id}^*}]), \phi(\boldsymbol{v}), \alpha q, \frac{\alpha'}{2\alpha q}\right) \in \mathbb{Z}_q^{2nk}$, where $\boldsymbol{I}_k \in R^{k\times k}$ is the identity matrix of size $k\times k$. $\mathcal{B}$ then picks $x_{0,1}, x_{0,2} \hookleftarrow \mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}$, and sets the challenged ciphertext to be

$$\mathsf{C}^* = (c_{0,1} = v_{0,1} + \lfloor q/2 \rceil \cdot \mathsf{M}, c_{0,2} = v_{0,2}, \boldsymbol{c}_1 = \phi^{-1}(\mathbf{c})) \in R_q \times R_q^{2k},$$

where $v_{0,1} = su_1 + x_{0,2}, v_{0,2} = su_2 + x_{0,2}$ and M is the challenge message chosen by $\mathcal{A}$.

In the following paragraphs, we show that, the change is negligible from the perspective of $\mathcal{A}$. Since $\phi(\boldsymbol{v}) = \phi(s\boldsymbol{a}+\boldsymbol{x}) = \phi(s)\mathsf{rot}(\boldsymbol{a})+\phi(\boldsymbol{x}) \in \mathbb{Z}_k^n$, where $\phi(\boldsymbol{x})$ has the distribution $\phi(\boldsymbol{x}) \hookleftarrow \mathcal{D}_{\mathbb{Z}^{nk},\alpha q}$, with the proper choices of α and α' and according to the property of ReRand, we have

$$\begin{aligned}\mathbf{c} &= (\phi(s)\mathsf{rot}(\boldsymbol{a})) \cdot \mathsf{rot}([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{id}^*}]) + \boldsymbol{x}' \\ &= \phi(s) \cdot \mathsf{rot}([\boldsymbol{a}|\mathsf{H}(\mathsf{id}^*)]) + \boldsymbol{x}' \\ &= \phi(s[\boldsymbol{a}|\mathsf{H}(\mathsf{id}^*)]) + \boldsymbol{x}' \\ &= \phi(s[\boldsymbol{a}|\boldsymbol{a}\boldsymbol{R}_{\mathsf{id}^*}]) + \boldsymbol{x}'.\end{aligned}$$

Thus, according to Lemma 2.2, the distribution of $\boldsymbol{x}'$ is $\mathsf{negl}(n)$-close to $\mathcal{D}_{\mathbb{Z}^{2nk},\alpha'}$. From the perspective of $\mathcal{A}$, the distribution of $\mathbf{c}_1$ between Game$_4$ and Game$_5$ is statistically close. Therefore, $|\Pr[X_4] - \Pr[X_5]| = \mathsf{negl}(n)$.

Game$_6$: This game continues to change how the challenged ciphertext is generated when $b = 0$ and when the game is not aborted. In this game, $\mathcal{B}$ picks $v_{0,1}, v_{0,2} \hookleftarrow U(R_q), \mathbf{v}' \hookleftarrow U(R_q^k)$, and $\mathbf{x} \hookleftarrow \left(\mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}\right)^k$. Then, $\mathcal{B}$ computes $\mathbf{c} \hookleftarrow \mathsf{ReRand}\left(\mathsf{rot}([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{id}^*}]), \phi(\boldsymbol{v}), \alpha q, \frac{\alpha'}{2\alpha q}\right) \in \mathbb{Z}_q^{2nk}$, where $\boldsymbol{v} = \boldsymbol{v}' + \boldsymbol{x}$. Finally, the challenged ciphertext is set to be

$$\mathsf{C}^* = (c_{0,1} = v_{0,1}, c_{0,2} = v_{0,2}, \boldsymbol{c}_1 = \phi^{-1}(\mathbf{c})) \in R_q \times R_q \times R_q^{2k},$$

where $s \hookleftarrow U(R_q)$ and $x_{0,2} \hookleftarrow \mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}$.

Lemma 5.3. *For any adversary $\mathcal{A}$, we have $|\Pr[X_5] - \Pr[X_6]| = \mathsf{negl}(n)$ under the $\mathsf{RLWE}_{n,k+2,q,\mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}}$ assumption.*

Proof. Suppose that there exists an adversary $\mathcal{A}$ that can distinguish between Game$_5$ and Game$_6$ with a nonnegligible advantage. Accordingly, there exists an another algorithm $\mathcal{B}$ that can solve $\mathsf{RLWE}_{n,k+2,q,\mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}}$ assumption with a nonnegligible advantage.

Instance. Before the **Setup** phase, $\mathcal{B}$ is given an RLWE instance: $(\{a_i, v_i\}_{i=0}^{k+1}) \in (R_q \times R_q)^{k+2}$. Without loss of generality, we assume that $v_i = v_i' + x_i$ for $x_i \hookleftarrow \mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}$. The target of $\mathcal{B}$ is to distinguish whether $v_i' = a_i s$ for some $s \in R_q$ or $v_i' \hookleftarrow U(R_q)$.

Setup. $\mathcal{B}$ first picks $u_1 \hookleftarrow U(R_q)$, and sets $u_2 = a_0 - u_1$, $\boldsymbol{a} := (a_2, \cdots, a_{k+1}), v_{0,1} := v_0$, and $v_{0,2} := v_1$, $\boldsymbol{v} := (v_2, \cdots, v_{k+1})$. In addition, $\mathcal{B}$ picks $\boldsymbol{y}$ as in Game$_1$; picks $\boldsymbol{R}_0, \boldsymbol{R}_{i,j}$ as in Game$_2$, sets $\boldsymbol{b}_0$ and $\boldsymbol{b}_{i,j}$ as in Game$_2$, and defines a function H as in Game$_2$. Finally, $\mathcal{B}$ outputs $\mathsf{mpk} = (\boldsymbol{a}, u_1, u_2, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d,\ell]}, \mathsf{H})$ to $\mathcal{A}$.

Phase 1 and Phase 2. The secret key generation and tracing key generation oracles are answered as in Game$_4$. That is, the keys are generated by $\boldsymbol{R}_0$ and $\boldsymbol{R}_{i,j}$.

Challenge. In this phase, $\mathcal{A}$ submits a challenge identity id^* and message M to $\mathcal{B}$. If $\mathsf{F}_{\boldsymbol{y}}(\mathsf{id}^*) \neq 0$, $\mathcal{B}$ aborts and sets $b' \hookleftarrow U(\{0,1\})$. Otherwise, $\mathcal{B}$ first randomly picks $b \hookleftarrow U(\{0,1\})$. Then, if $b = 0$, $\mathcal{B}$ computes $\boldsymbol{R}_{\mathsf{id}^*}$ and $\mathbf{c}$ as in Game$_6$. Subsequently, $\mathcal{B}$ sets the challenged ciphertext C^* as in Game$_5$. If $b = 1$, $\mathcal{B}$ picks $c_{0,1}, c_{0,2} \hookleftarrow U(R_q)$, picks $\boldsymbol{c}_1 \hookleftarrow U(R_q^{2k})$, and sets $\mathsf{C}^* = (c_{0,1}, c_{0,2}, \boldsymbol{c}_1)$. Finally, $\mathcal{B}$ returns C^* to $\mathcal{A}$.

Guess. If the game is not aborted, $\mathcal{A}$ outputs its guess b'. $\mathcal{B}$ outputs 1 if $b' = b$ and 0 otherwise.

Analysis. If $\{a_i, v_i'+x_i\}_{i=0}^{k}$ are valid RLWE samples (i.e., $v_i' = a_i s$), $\mathcal{B}$ perfectly simulates the perspective of $\mathcal{A}$ in Game$_5$. Otherwise, the perspective of $\mathcal{A}$ is in Game$_6$. Therefore, $|\Pr[X_5] - \Pr[X_6]|$ is less than the advantage that $\mathcal{B}$ has after solving the $\mathsf{RLWE}_{n,k+2,q,\mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}}$ assumption. ◻

According to Lemma 5.3, if the $\mathsf{RLWE}_{n,k+2,q,\mathcal{D}^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}}$ assumption is hard, we have $|\Pr[X_5] - \Pr[X_6]| = \mathsf{negl}(n)$.

Game$_7$: This game continues to change the way how the challenged ciphertext is generated when $b = 0$ and the game is not aborted. In this game, the ciphertext is created as

$$\mathsf{C}^* = (c_{0,1} = v_{0,1}, c_{0,2} = v_{0,2}, \boldsymbol{c}_1 = [\boldsymbol{v}'|\boldsymbol{v}'\boldsymbol{R}_{\mathsf{id}^*}] + [\boldsymbol{x}_1|\boldsymbol{x}_2]) \in R_q \times R_q \times R^{2k}$$

Because $\phi(\boldsymbol{v}) = \phi(\boldsymbol{v}' + \boldsymbol{x}) = \phi(\boldsymbol{v}' + \phi(\boldsymbol{x}) \in \mathbb{Z}_q^{nk}$ in Game$_6$, for the output $\mathbf{c}$, we have

$$\mathbf{c} = \phi(\boldsymbol{v}') \cdot \mathsf{rot}([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{id}^*}]) + \boldsymbol{x}' = \phi([\boldsymbol{v}'|\boldsymbol{v}'\boldsymbol{R}_{\mathsf{id}^*}]) + \boldsymbol{x}',$$

where the distribution of $\boldsymbol{x}'$ is $\mathsf{negl}(n)$-close to $\mathcal{D}_{\mathbb{Z}^{2nk},\alpha'}$ according to Lemma 2.2. Therefore, we have $\Pr[X_6] - \Pr[X_7] = \mathsf{negl}(n)$.

Game$_8$: This game changes how the user's secret key and tracing key are generated. Instead of generating them by running SampleLeft or SampleRight, $\mathcal{B}$ directly returns the secret key and tracing key for an identity id by picking $\mathsf{usk}_{\mathsf{id}} = \boldsymbol{e} \hookleftarrow \mathcal{D}^{\mathsf{coeff}}_{\Lambda^{\top}_{\phi(u_1+u_2)}([\mathsf{rot}(\boldsymbol{a}^{\top})^{\top}|\mathsf{rot}(\mathsf{H}(\mathsf{id})^{\top})^{\top}]),\sigma}$ and $\mathsf{tsk}_{\mathsf{id}} = \boldsymbol{f} \hookleftarrow \mathcal{D}^{\mathsf{coeff}}_{\Lambda^{\top}_{\phi(u_2)}([\mathsf{rot}(\boldsymbol{a}^{\top})^{\top}|\mathsf{rot}(\mathsf{H}(\mathsf{id})^{\top})^{\top}]),\sigma}$, respectively, without using $\boldsymbol{R}_{\mathsf{id}}$. From the perspective of $\mathcal{A}$, similar to the change from Game$_3$ to Game$_4$, the distribution of the secret key and tracing key remains unchanged; therefore, we have $\Pr[X_7] - \Pr[X_8] = \mathsf{negl}(n)$.

Game$_9$: In this last game, $\mathcal{B}$ sets the challenged ciphertext to be

$$C^* = (c_{0,1} \hookleftarrow U(R_q), c_{0,2} \hookleftarrow U(R_q), \boldsymbol{c}_1 \hookleftarrow U(R_q^{2k})),$$

regardless of whether b is 1 or 0. Because $v_0, v_1 \hookleftarrow U(R_q)$, we can readily determine that the distribution of $(c_{0,1}, c_{0,2})$ between Game$_8$ and Game$_9$ is negligible. In the following paragraphs, we show that $\boldsymbol{c}_1$ in Game$_8$ is $\mathsf{negl}(n)$-close to the uniform distribution over R_q^{2k}. Specifically, because $[\boldsymbol{x}_1|\boldsymbol{x}_2] \in R^{2k}$, we only show that the distribution of $[\boldsymbol{v}'|\boldsymbol{v}'\boldsymbol{R}_{\mathsf{id}^*}]$ is statistically close to the uniform distribution over R_q^{2k}. Before furnishing such a proof, we demonstrate that the following distributions are $\mathsf{negl}(n)$-close; that is,

$$(\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'\boldsymbol{R}_0) \approx (\boldsymbol{a}, \boldsymbol{a}', \boldsymbol{v}', \boldsymbol{v}'') \approx (\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}''), \qquad (3)$$

where $\boldsymbol{a}, \boldsymbol{a}' \hookleftarrow U(R_q^k), \boldsymbol{R}_0 \hookleftarrow U([-\rho, \rho]_R^{k\times k})$ and $\boldsymbol{v}', \mathrm{v}'' \hookleftarrow U(R_q^k)$. Eq. (3) is satisfied according to Lemma 2.6. Specifically, we can demonstrate that the first and second distributions are $\mathsf{negl}(n)$-close by applying Lemma 2.6 for $[\boldsymbol{a}; \boldsymbol{v}'] \in R_q^{2\times k}$ and $\boldsymbol{R}_0$. Similarly, we can show that the second and third distributions are $\mathsf{negl}(n)$-close by applying the same lemma for $\boldsymbol{a}$ and $\boldsymbol{R}_0$. According to the preceding description, let $\widetilde{\boldsymbol{R}_{\mathsf{id}^*}} = \sum_{(j_1,\cdots,j_d)\in S(\mathsf{id}^*)} \mathsf{TrapEval}_d(\boldsymbol{R}_{1,j_1}, \cdots, \boldsymbol{R}_{d,j_d}, y_{1,j_1}, \cdots, y_{d,j_d})$; we thus have

$$\begin{aligned}(\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'\boldsymbol{R}_{\mathsf{id}^*}) &= \left(\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'\left(\boldsymbol{R}_0 + \widetilde{\boldsymbol{R}_{\mathsf{id}^*}}\right)\right)\\ &\approx \left(\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'' + \boldsymbol{v}'\left(\widetilde{\boldsymbol{R}_{\mathsf{id}^*}}\right)\right)\\ &\approx (\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}''),\end{aligned}$$

where $\boldsymbol{v}', \boldsymbol{v}'' \hookleftarrow U(R_q^k)$ and $\boldsymbol{R}_0 \hookleftarrow U([-\rho, \rho]_R^{k\times k})$ Therefore, we have $\Pr[X_8] - \Pr[X_9] = \mathsf{negl}(n)$.

Analysis. Combining the aforementioned games, we have

$$\begin{aligned}\left|\Pr[X_9] - \frac{1}{2}\right| &= \left|\Pr[X_1] - \frac{1}{2} + \sum_{i=1}^{8}(\Pr[X_{i+1}] - \Pr[X_i])\right|\\ &\geq \left|\Pr[X_1] - \frac{1}{2}\right| - \sum_{i=1}^{8} |\Pr[X_{i+1}] - \Pr[X_i]|\\ &\geq \frac{1}{(\kappa\xi^d n^d)^{\xi-1}d + 1}\left(\frac{\epsilon}{2} - \frac{dQ}{n^\xi}\right) - \mathsf{negl}(n)\\ &= \frac{1}{\mathsf{poly}(n)}\left(\frac{\epsilon}{2} - \frac{dQ}{n^\xi}\right) - \mathsf{negl}(n).\end{aligned}$$

Because the challenged ciphertext contains no information related to which b is used in Game$_9$, $\mathcal{A}$ can only return b' through a guessing process. That is, $\left|\Pr[X_9] - \frac{1}{2}\right| = 0$. This also implies that $\left(\frac{\epsilon}{2} - \frac{dQ}{n^\xi}\right)$ is negligible. However, according to Eq. (1), we have $\frac{\epsilon}{2} - \frac{dQ}{n^\xi} \geq \frac{1}{n^\xi}$ holding for infinitely many n. This, however, contradicts the underlying assumption. Therefore, by proof by contradiction, we conclude that there exists no such $\mathcal{A}$ that can win the IND-ANON-ID-CPA game with a nonnegligible advantage. □

6 CONCLUSION AND FUTURE WORK

In AIBET, a tracker can remove the anonymous security in anonymous IBE and identify the recipient; this thus increases the flexibility of anonymous IBE in some scenarios. In this paper, we first formalize the consistency property and then propose a novel concept for achieving AIBET from any lattice-based IBE scheme based on the anonymous IBE scheme presented by Agrawal *et al.*'s IBE [2]. Subsequently, we apply the concept to Katsumata and Yamada's anonymous IBE scheme [19] and construct the first quantum-resistant AIBET under the RLWE assumption.

In our future work, we will explore methods of obtaining more flexible and revocable trace keys. Additionally, we will consider whether the traceability system can be incorporated into other lattice-based IBE schemes, such as revocable IBE [10, 18, 31], identity-based proxy re-encryption [14, 15, 17], and IBE schemes with equality test [13, 25].

ACKNOWLEDGMENTS

This research was supported by the Ministry of Science and Technology, Taiwan (ROC), under Project Numbers MOST 108-2218-E-004-001-, 108-2218-E-004-002-MY2, MOST 109-2218-E-011-007-.

REFERENCES

[1] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. 2005. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In *Annual International Cryptology Conference*, V. Shoup (Ed.). Springer, Berlin, Heidelberg, 205–222. https://doi.org/10.1007/11535218_13
[2] Shweta Agrawal, Dan Boneh, and Xavier Boyen. 2010. Efficient lattice (H) IBE in the standard model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, H. Gilbert (Ed.). Springer, Berlin, Heidelberg, 553–572. https://doi.org/10.1007/978-3-642-13190-5_28
[3] Shweta Agrawal, Dan Boneh, and Xavier Boyen. 2010. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In *Annual Cryptology Conference*, T. Rabin (Ed.). Springer, Berlin, Heidelberg, 98–115. https://doi.org/10.1007/978-3-642-14623-7_6
[4] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. 2019. Quantum supremacy using a programmable superconducting processor. *Nature* 574, 7779 (2019), 505–510. https://doi.org/10.1038/s41586-019-1666-5
[5] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. 2001. Key-privacy in public-key encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, C. Boyd (Ed.). Springer, Berlin, Heidelberg, 566–582. https://doi.org/10.1007/3-540-45682-1_33
[6] Olivier Blazy, Laura Brouilhet, and Duong Hieu Phan. 2019. Anonymous identity based encryption with traceable identities. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/3339252.3339271
[7] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. 2014. (Hierarchical) identity-based encryption from affine message authentication. In *Annual Cryptology Conference*, J.A. Garay (Ed.). Springer, Berlin, Heidelberg, 408–425. https://doi.org/10.1007/978-3-662-44371-2_23
[8] Dan Boneh and Matt Franklin. 2001. Identity-based encryption from the Weil pairing. In *Annual International Cryptology Conference*, J. Kilian (Ed.). Springer, Berlin, Heidelberg, 213–229. https://doi.org/10.1007/3-540-44647-8_13
[9] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. 2010. Bonsai trees, or how to delegate a lattice basis. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, H. Gibert (Ed.). Springer, Berlin, Heidelberg, 523–552. https://doi.org/10.1007/978-3-642-13190-5_27
[10] Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Khoa Nguyen. 2012. Revocable identity-based encryption from lattices. In *Australasian Conference on Information Security and Privacy*, W. Susilo, Y. Mu, and J Seberry (Eds.). Springer, Berlin, Heidelberg, 390–403. https://doi.org/10.1007/978-3-642-31448-3_29
[11] Clifford Cocks. 2001. An identity based encryption scheme based on quadratic residues. In *IMA International Conference on Cryptography and Coding*, B. Honary (Ed.). Springer, Berlin, Heidelberg, 360–363. https://doi.org/10.1007/3-540-45325-3_32

[12] Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. 2014. Efficient identity-based encryption over NTRU lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, P. Sarkar and T. Iwata (Eds.). Springer, Berlin, Heidelberg, 22–41. https://doi.org/10.1007/978-3-662-45608-8_2

[13] Dung Hoang Duong, Huy Quoc Le, Partha Sarathi Roy, and Willy Susilo. 2019. Lattice-based IBE with equality test in standard model. In *International Conference on Provable Security*, R. Steinfeld and T. Yuen (Eds.). Springer, Cham, 19–40. https://doi.org/10.1007/978-3-030-31919-9_2

[14] Priyanka Dutta, Willy Susilo, Dung Hoang Duong, Joonsang Baek, and Partha Sarathi Roy. 2020. Identity-Based unidirectional proxy re-encryption in standard model: A lattice-based construction. In *International Conference on Information Security Applications*, I. You (Ed.). Springer, Cham, 245–257. https://doi.org/10.1007/978-3-030-65299-9_19

[15] Priyanka Dutta, Willy Susilo, Dung Hoang Duong, and Partha Sarathi Roy. 2020. Collusion-resistant identity-based proxy re-encryption: Lattice-based constructions in standard model. *arXiv preprint arXiv:2011.08456* (2020).

[16] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. 2008. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*. Association for Computing Machinery, New York, NY, USA, 197–206. https://doi.org/10.1145/1374376.1374407

[17] Jinqiu Hou, Mingming Jiang, Yuyan Guo, and Wangan Song. 2019. Efficient identity-based multi-bit proxy re-encryption over lattice in the standard model. *Journal of Information Security and Applications* 47 (2019), 329–334. https://doi.org/10.1016/j.jisa.2019.05.015

[18] Shuichi Katsumata, Takahiro Matsuda, and Atsushi Takayasu. 2020. Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. *Theoretical Computer Science* 809 (2020), 103–136. https://doi.org/10.1016/j.tcs.2019.12.003

[19] Shuichi Katsumata and Shota Yamada. 2016. Partitioning via non-linear polynomial functions: more compact IBEs from ideal lattices and bilinear maps. In *International Conference on the Theory and Application of Cryptology and Information Security*, J. Cheon and T. Takagi (Eds.). Springer, Berlin, Heidelberg, 682–712. https://doi.org/10.1007/978-3-662-53890-6_23

[20] Alex Lombardi, Vinod Vaikuntanathan, and Thuy Duong Vuong. 2019. Lattice trapdoors and IBE from middle-product LWE. In *Theory of Cryptography Conference*, D. Hofheinz and A. Rosen (Eds.). Springer, Cham, 24–54. https://doi.org/10.1007/978-3-030-36030-6_2

[21] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. 2010. On ideal lattices and learning with errors over rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, H. Gilbert (Ed.). Springer, Berlin, Heidelberg, 1–23. https://doi.org/10.1007/978-3-642-13190-5_1

[22] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. 2013. On ideal lattices and learning with errors over rings. *Journal of the ACM (JACM)* 60, 6 (2013), 1–35. https://doi.org/10.1145/2535925

[23] Daniele Micciancio and Chris Peikert. 2012. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, D. Pointcheval and T. Johansson (Eds.). Springer, Berlin, Heidelberg, 700–718. https://doi.org/10.1007/978-3-642-29011-4_41

[24] Daniele Micciancio and Oded Regev. 2007. Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.* 37, 1 (2007), 267–302. https://doi.org/10.1137/S0097539705447360

[25] Giang Linh Duc Nguyen, Willy Susilo, Dung Hoang Duong, HuyQuoc Le, and Fuchun Guo. 2020. Lattice-based IBE with equality test supporting flexible authorization in the standard model. In *International Conference on Cryptology in India*, K. Bhargavan, E. Oswald, and M. Prabhakaran (Eds.). Springer, Cham, 624–643. https://doi.org/10.1007/978-3-030-65277-7_28

[26] Claudia P Rentería-Mejía and Jaime Velasco-Medina. 2020. Lattice-based cryptoprocessor for CCA-secure identity-based encryption. *IEEE Transactions on Circuits and Systems I: Regular Papers* 67, 7 (2020), 2331–2344. https://doi.org/10.1109/TCSI.2020.2981089

[27] Adi Shamir. 1984. Identity-based cryptosystems and signature schemes. In *Workshop on the Theory and Application of Cryptographic Techniques*, G.R. Blakley and D. Chaum (Eds.). Springer, Berlin, Heidelberg, 47–53. https://doi.org/10.1007/3-540-39568-7_5

[28] Peter W Shor. 1994. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Institute of Electrical and Electronics Engineers, New York, NY, USA, 124–134. https://doi.org/10.1109/SFCS.1994.365700

[29] Peter W Shor. 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* 41, 2 (1999), 303–332. https://doi.org/10.1137/S0097539795293172

[30] Kunwar Singh, C Pandurangan, and AK Banerjee. 2012. Adaptively secure efficient lattice (H) IBE in standard model with short public parameters. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*, A. Bogdanov and S. Sanadhya (Eds.). Springer, Berlin, Heidelberg, 153–172. https://doi.org/10.1007/978-3-642-34416-9_11

[31] Atsushi Takayasu and Yohei Watanabe. 2017. Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance. In *Australasian Conference on Information Security and Privacy*, J. Pieprzyk and S. Suriadi (Eds.). Springer, Cham, 184–204. https://doi.org/10.1007/978-3-319-60055-0_10

[32] Shota Yamada. 2016. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, M. Fischlin and JS. Coron (Eds.). Springer, Berlin, Heidelberg, 32–62. https://doi.org/10.1007/978-3-662-49896-5_2

[33] Shota Yamada. 2017. Asymptotically compact adaptively secure lattice IBEs and verifiable random functions via generalized partitioning techniques. In *Annual International Cryptology Conference*, J. Katz and H. Shacham (Eds.). Springer, Cham, 161–193. https://doi.org/10.1007/978-3-319-63697-9_6

[34] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. 2020. Quantum computational advantage using photons. *Science* 370, 6523 (2020), 1460–1463. https://doi.org/10.1126/science.abe8770