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 lattice-based IBE scheme to ensure 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, 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?
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 adopt 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., \( \mathbf{a} \)) and uppercase (e.g., \( \mathbf{A} \)) 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 \( \mathbf{A} \in \mathbb{R}^{m \times n} \), \( \|\mathbf{A}\|_\text{GS} \) 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 \([-\cdot]\) to denote the horizontal concatenation of vectors and matrices. For two random variables \( X \) and \( Y \) with support \( \mathcal{X} \), the statistical distance of \( X \) and \( Y \) is defined as \( \Delta(X, Y) := \frac{1}{2} \sum_{x \in \mathcal{X}} |\Pr[s = X] - \Pr[s = Y]| \).

For two integers \( a, b \in \mathbb{N} \), where \( a \leq b \), we use \([a, b]\) to denote the set \{\(a, a+1, \ldots, b-1, b\)\}. 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, \( \Omega, \tilde{\Omega}, \omega \) to classify the growth of functions. The notation \( \negl(n) \) denotes an arbitrary function \( f \) being negligible in \( n \), where \( f(n) = o(n^{-\epsilon}) \) for every fixed constant \( \epsilon \). The notation \( \poly(n) \) denotes an arbitrary function \( f(n) = O(n^{\epsilon}) \) for some constant \( \epsilon \). PPT is short for “probabilistic polynomial-time.” For a vector or matrix, a superscript \( \tau \) denotes its transpose. Finally, let \( D \) be a distribution over some finite set \( S \); accordingly, \( x \leftarrow D \) signifies that \( x \) is chosen from the distribution \( D \), and \( x \leftarrow U(S) \) 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 \( \Lambda \) is an additive discrete subgroup of \( \mathbb{R}^m \), which can be defined as follows:

\[
\Lambda(B) = \{ \sum_{i=1}^{n} b_i a_i \mid a_i \in \mathbb{Z} \},
\]

where \( b_1, \ldots, b_n \in \mathbb{R}^m \) are linearly independent vectors.

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

- \( \Lambda_q := \{ e \in \mathbb{Z}^m \mid \exists s \in \mathbb{Z}^n \text{ where } \mathbf{As} = e \mod q \} \)
- \( \Lambda^\perp_q := \{ e \in \mathbb{Z}^m \mid \mathbf{Ae} = 0 \mod q \} \)
- \( \Lambda^\perp_q := \{ e \in \mathbb{Z}^m \mid \mathbf{Ae} = u \mod q \} \)

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:

\[
\rho_{s,c}(x) = \exp(-\pi \|x-c\|^2/s^2).
\]

\[
\rho_{s,c}(\Lambda) = \sum_{x \in \Lambda} \rho_{s,c}(x).
\]

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

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

**Lemma 2.2 (Noise Randomization) (Lemma 1 of [19]).** Let \( q, f, m \) be positive integers, and let \( r \) be a positive real number satisfying \( r > \max\{\omega(\log m), \omega(\log r)\} \). Let \( b \in \mathbb{Z}^m_q \) be arbitrary, and let \( x \) be chosen from \( D_{\mathbb{Z}^m_q} \). Then for any \( \mathbf{V} \in \mathbb{Z}^{m \times m}_q \) and positive real number \( \sigma > s_1(\mathbf{V}) \), there exists a PPT algorithm \( \text{ReRand}(\mathbf{V}, b, x, r, \sigma) \) that outputs \( \mathbf{W} = \mathbf{bV} + x' \in \mathbb{Z}^m_q \) where \( x' \) is distributed statistically close to \( D_{\mathbb{Z}^m,\sigma r} \).

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

\[
\Pr \left[ \|x\| > s \sqrt{n} : x \leftarrow D_{\Lambda,\epsilon,\sigma}\right] \leq \frac{2}{1-\epsilon} \cdot 2^{-\epsilon \cdot n}.
\]

**Lemma 2.4 (Discrete Gaussian Error Bound) (Lemma 20 of [19]).** Let \( \mathbf{c} \) be some vector in \( \mathbb{Z}^n_q \) and let \( x \leftarrow D_{\mathbb{Z}^n_q,\alpha \sigma} \) for some \( \alpha \sigma \) \( > \omega(\log n) \). Then the quantity \( |\mathbf{c}^\top x| \) treated as an integer in \([0, \ldots, q-1]\) satisfies \( |\mathbf{c}^\top x| \leq \|\mathbf{c}\|_2 \alpha \sigma \omega(\log n) \) 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’sIBE scheme [19], we recapitulate some useful functions posited in [19]. Please refer to [19] for further information.

Let \( b \) be a power of 2. The ring can then be defined as \( R = \mathbb{Z}[X]/\Phi_{m}(X) \), where \( \Phi_{m}(X) = X^{m} + 1 \) is the mth cyclotomic polynomial where \( m = 2n \). Let \( R = \mathbb{Z}[X]/\Phi_{m}(X) \). Let \( q = 3 \) mod 8 be a prime such that there exists another prime \( p = 1 \) mod 1 satisfying \( p \leq q \leq 2p \), and let also \( aq \geq \frac{n^{2+1/4}k^{1/4}4\log(n)}{\sqrt{n}} \). Accordingly, there exists a probabilistic polynomial-time quantum reduction from an \( \tilde{O}(\sqrt{n}/\alpha) \)-approximate SIVP (or SVP) to RLWE\(_{n,k,q,X}\) with \( \chi = 2\gamma^{\text{coff}}_{aq} \).

2.5 Trapdoor for Rings

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

The following paragraphs provide 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 \( b \) be a power of 2 and \( q \) be a prime larger than \( 4n \) such that \( q \equiv 3 \) mod 8; moreover, consider some \( b, \rho \in \mathbb{Z}^{+} \) satisfying \( \rho < \frac{1}{2} \sqrt{q}/n \). In addition, let \( \log_b(\cdot) = \log_{g_{b}}(\cdot) \). According, we derive the following lemmas.

2.9 (TrapGen [23]). There exists a randomized polynomial-time algorithm TrapGen\(_{1,n,1,k,\rho} \) that outputs a vector \( a \in \mathbb{R}^{k} \) and a matrix \( T_{a} \in \mathbb{R}^{kxk} \) when \( k \geq 2 \log_{b} q \). Here, \( \text{rot}(a)^{T} \in \mathbb{R}^{kxk} \) is a full-rank matrix and \( \text{rot}(T_{a}) \in \mathbb{R}^{kxk} \) is a basis for \( \Lambda^{+}(\text{rot}(a)^{T}) \). Furthermore, \( a \) is \( \text{negl}(n) \)-close to uniform and \( \|\text{rot}(T_{a})\|_{\text{GS}} = 0 \left(b\rho+\sqrt{n\log_{b} q}\right) \).

2.10 (SampleLeft [9]). Consider \( a, b \in \mathbb{R}^{k} \) where \( \text{rot}(a)^{T} \in \mathbb{R}^{kxk} \) is full-rank matrices; an element \( u \in \mathbb{R}^{k} \), a matrix \( T_{a} \in \mathbb{R}^{kxk} \) such that \( \text{rot}(T_{a}) \in \mathbb{R}^{kxk} \) is a basis for \( \Lambda^{+}(\text{rot}(a)^{T}) \), and a Gaussian parameter \( \sigma > 0 \|\text{rot}(T_{a})\|_{\text{GS}} \cdot \omega(\sqrt{\log nk}) \). Accordingly, there exists a randomized polynomial-time algorithm SampleLeft\(_{a,b,u,T_{a},\sigma} \) that outputs a vector \( e \in \mathbb{R}^{k} \) sampled from a distribution that is \( \text{negl}(n) \)-close to \( \chi^{\text{coff}}_{\text{SampleLeft}(a,b,u,T_{a},\sigma)} \) with probability \( \omega(\text{rot}(a)^{T}\text{rot}(b^{T})\sigma) \).

2.11 (SampleRight [3]). Consider \( a, g_{b} \in \mathbb{R}^{k} \) where \( \text{rot}(a)^{T} \in \mathbb{R}^{kxk} \) are full-rank matrices; the elements \( u \in \mathbb{R}^{k} \) and \( v \in \mathbb{R}^{k} \); a matrix \( R \in \mathbb{R}^{kxk} \), a matrix \( T_{g_{b}} \in \mathbb{R}^{kxk} \) such that \( \text{rot}(T_{g_{b}}) \in \mathbb{R}^{kxk} \) is a basis for \( \Lambda^{+}(\text{rot}(g_{b})^{T}) \); and a Gaussian parameter \( \sigma > 0 \|\text{rot}(T_{g_{b}})\|_{\text{GS}} \cdot \omega(\sqrt{\log nk}) \). Accordingly, there exists a randomized polynomial-time algorithm SampleRight\(_{a,g_{b},R,u,v,T_{g_{b}},\sigma} \) that outputs a vector \( e \in \mathbb{R}^{k} \) sampled from a distribution that is \( \text{negl}(n) \)-close to \( \chi^{\text{coff}}_{\text{SampleRight}\(_{a,g_{b},R,u,v,T_{g_{b}},\sigma}} \) with probability \( \omega(\text{rot}(a)^{T}\text{rot}(b^{T})\sigma) \).

2.12 (Invertible Gadget Algorithm [23]). Let \( k \geq [\log_{b} q] \). There exists a publicly known matrix \( T_{g_{b}} \) such that
We apply the PubEval we cannot guarantee that no information is leaked with the use of wrong tracing keys. Hence, in this paper, we further formalize the model of AIBET provided by Blazy et al.

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 (Setup, USKG, TSKG, Enc, Dec, TVerify) along with an identity space \( I \), which are described as follows:

- **Setup** \( \lambda \): Given a security parameter \( \lambda \), the setup algorithm outputs a master public key mpk and master secret key msk.
- **USKG** (mpk, msk, id): Given a master public key mpk, a master secret key msk, and an identity id \( \in I \), the secret key generation algorithm outputs a secret key usk_id for an identity id.
- **TSKG** (mpk, msk, id): Given a master public key mpk, a master secret key msk, and an identity id \( \in I \), the tracing key generation algorithm outputs a tracing key tsk_id for identity id.
- **Enc** (mpk, id, M): Given a master public key, an identity id, and a message M, the encryption algorithm outputs a ciphertext C.
- **Dec** (usk_id, C): Given a user’s secret key usk_id and a ciphertext C, the decryption algorithm outputs a message M.
- **TVerify** (tsk_id, C): Given a user’s tracing key 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 \( \lambda \); all pairs (mpk, msk) generated by Setup(\( \lambda \)); all messages M; all identities id \( \in I \); all usk_id and tsk_id generated by USKG (mpk, msk, id) and TSKG (mpk, msk, id), respectively; and all ciphertexts C generated by Enc (mpk, id, M). Accordingly, we derive the following:

\[
\Pr[\text{Dec}(\text{usk}_\text{id}, C) = M \land \text{TVerify}(\text{tsk}_\text{id}, C) = 1] \geq 1 - \text{negl}(\lambda).
\]

**Definition 3.3 (Consistency).** Consider all security parameters \( \lambda \); all pairs (mpk, msk) generated by Setup(\( \lambda \)); all messages M, all identities id, id’ \( \in I \), where id \( \neq \) id’; all usk_id, usk_id’, tsk_id, and tsk_id’ generated by USKG (mpk, msk, id), USKG (mpk, msk, id’), TSKG (mpk, msk, id), and TSKG (mpk, msk, id’), respectively; and all ciphertexts C generated by Enc (mpk, id, M). Accordingly, we derive the following:

\[
\Pr[\text{TVerify}(\text{tsk}_\text{id}, C) = 0] \geq 1 - \text{negl}(\lambda).
\]

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 A and challenger B for AIBET scheme II.

**Game – IND-ANON-ID-CPA:**

- **Setup.** The challenger B runs Setup(\( \lambda \)) to generate (mpk, msk) and give mpk to A.
- **Phase 1.** A is allowed to adaptively query the secret key generation and tracing key generation oracles as follows:
  - \( \text{O}^{\text{USKG}} \): After receiving an identity id \( \in I \) submitted by A, B returns usk_id \( \leftarrow \text{USKG}(\text{mpk}, \text{msk}, \text{id}) \).
  - \( \text{O}^{\text{TSKG}} \): After receiving an identity id \( \in I \) submitted by A, B returns tsk_id \( \leftarrow \text{TSKG}(\text{mpk}, \text{msk}, \text{id}) \).
- **Challenge.** After Phase 1, A outputs a challenge message M and an identity id’ \( \in I \) to B, where id has not been queried to oracles. B picks a random coin b \( \leftarrow U(\{0, 1\}) \) and a random ciphertext C from the ciphertext space. If b = 0, then B outputs a ciphertext Enc(mpk, id’, M) \( \rightarrow C^* \); otherwise, B sets C’ = C. Subsequently, B returns C’ as a challenge to A.
- **Phase 2.** A can continue to query the oracles as executed in Phase 1. The only restriction is that A cannot query these oracles on the challenge identity id’.
- **Guess.** Finally, A outputs a guess b’. If b’ = b, A wins the game. The advantage of A winning the game can be defined as follows:

\[
\text{Adv}_{\text{AIBET}}^\lambda = \Pr[b’ = b] - \frac{1}{2}.
\]

**Definition 3.4 (IND-ANON-ID-CPA for AIBET).** For all PPT adversaries A, we suggest that AIBET scheme II is IND-ANON-ID-CPA secure if Adv_{\text{AIBET}}^\lambda is negligible.

4 OUR CONCEPT AND CONSTRUCTION

This section presents our concept and the AIBET scheme that is secure under the RLWE assumption.
Quantum-resistant Anonymous IBE with Traceable Identities

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 $A_1, A_2, B,$ and $u$ be public parameters; let a user’s identity id be associated with the matrix $[A_1, A_2, H(id)]$; let the user’s secret USK$_{id}$ be generate from the SampleLeft function; and let $F_{id}$ be USK$_{id}$ = $u$, where $F_{id} = [A_1, A_2, H(id)] \cdot B$. The ciphertext has two parts $C = \left\{ c_0 = au + x + \left\lfloor \frac{y}{2} \right\rfloor, c_1 = F_{id}s + \left\lceil \frac{y}{2} \right\rceil \right\}$, where $c_0$ is related to the message $b$ and $c_1$ is related to the identity. If the parameters are set correctly, the message $b$ can be recovered by computing $w = c_0 - USK_{id} \cdot c_1$ and $b = 1$ if $w$ is close to $\lfloor q/2 \rfloor$, and $b = 0$ otherwise.

To incorporate traceability into lattice-based IBE, an intuitive approach is to generate another formal part of the ciphertext; that is, $c'_0 = u's + x'$ according to the original scheme. Here, let $u'$ be an added public parameter with the same distribution as $u$. The tracing key TSK$_{id}$ is generated in a manner similar to that of the user’s secret key, except that $F_{id} \cdot$ TSK$_{id} = u'$. If the result $w' = c'_0 - TSK_{id} \cdot c_1$ is "not" close to $\lfloor q/2 \rfloor$, then the recipient can be considered to be identity id. However, in this approach, if the encryptor is malicious and wishes to hide the recipient’s identity, he/she may randomly generate $c'_0$ such that $w'$ cannot be computed correctly, then tracker cannot trace the recipient of the ciphertext even if the tracker has the tracing key.

To solve the aforementioned problem, two conditions have to be satisfied: (1) $c_0$ must connect to $c_0'$, (2) identity $id$ can be traced even if $c_0'$ does not be correctly generated. Hence, we carefully make the following adjustments:

- each user’s secret key USK$_{id}$ is sampled to satisfy $F_{id} \cdot USK_{id} = (u + u')$;
- there are two tracing keys (TSK$_{id,1}$, TSK$_{id,2}$) for an identity id such that $F_{id} \cdot TSK_{id,1} = u'$ and $F_{id} \cdot TSK_{id,2} = u'$;
- for decryptor, he/she must first compute $c_0 = c_0 + c_0'$ for decryption, instead of only using $c_0$;
- for tracker, for $i \in \{1, 2\}$, he/she first obtains $w_i = c'_0 - TSK_{id, i} \cdot c_1$. Then, he/she compares $w_i$ with $\lfloor q/2 \rfloor$ and sets $b_i = 1$ if $w_i$ close to $\lfloor q/2 \rfloor$, and $b_i = 0$, otherwise. We say that the ciphertext is traced if $b_1 = b_2$.

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].

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 $ID \subseteq \{0, 1\}^k$ for some $k \in \mathbb{N}$, and let the message space be $\{0, 1\}^m \subset R$. In addition, we use an efficiently computable injetive map to map the identity id $\in \{0, 1\}^k$ to a subset $S(id)$ of $\{1, t\}^d$, where $t = \lceil x^{1/2} \rceil$ and $d \in \mathbb{N}$. The parameters of the scheme are $n = n(\lambda), b = b(n), m = 2n, q = q(n), k = k(n), \ell = \ell(n), \alpha = \alpha(n), \alpha' = \alpha'(n)$ and $\sigma = \sigma(n)$. This choice of parameters is justified in Section 4.4.

- Setup $(1^\lambda) \rightarrow (mpk, msk)$:
  (1) Compute $a \in R_q^n$ associated with its trapdoor $T_a \in R^{n \times k}$, where $(a, T) \leftarrow \text{TrapGen}(1^n, 1^k, q, \rho)$.
  (2) Sample two uniformly random polynomials $u_1, u_2 \leftarrow U(R_q)$, and a polynomial $b_0 \leftarrow U(R_q^n)$.
  (3) For $(i, j) \in [d] \times [\ell]$, sample random polynomial vectors $b_{i,j} \leftarrow U(R_q^n)$.
  (4) Define a deterministic function $H : ID \rightarrow R_q^d$:
    

\[
H(id) = b_0 + \sum_{(j_1, \ldots, j_d) \in S(id)} \text{PubEval}(b_{1,j_1}, b_{2,j_2}, \ldots, b_{d,j_d}) \in R_q^d.
\]

- Output $mpk := (a, u_1, u_2, b_0, \{b_{i,j}(i,j)\}_{(i,j) \in \{d\} \times \{\ell\}}, H)$, msk := $T_a$.

- Output $uskd := e \in R^{n\times q}$.

- TSK$_{id}(mpk) := (a, u_1, u_2, b_0, \{b_{i,j}(i,j)\}_{(i,j) \in \{d\} \times \{\ell\}}, H)$, msk := $T_{a, id} \in ID \rightarrow uskd$:
  (1) Compute $e \leftarrow \text{SampleLeft}(a, H(id), u_1 + u_2, T_{a, \sigma})$.
  (2) Output $uskd := e \in R^{n\times q}$.

- Enc$(mpk) := (a, u_1, u_2, b_0, \{b_{i,j}(i,j)\}_{(i,j) \in \{d\} \times \{\ell\}}, H)$, id, M $\in \{0, 1\}^m \subset R$ $\rightarrow$ C:
  (1) Sample $s \leftarrow U(R_q), x_{01}, x_{02} \leftarrow \mathcal{D}^{\text{coeff}}_{2^n, sqq}$
  (2) Sample $x_1, x_2 \leftarrow \mathcal{D}^{\text{coeff}}_{2^n, \alpha q'}$
  (3) Compute $c_{0,1} = su_1 + x_{01} + \lfloor q/2 \rfloor M, c_{0,2} = su_2 + x_{02},$ and $c_1 = s[a(H(id))] + [x_{1} x_{2}]$.
  (4) Output $C := \{c_{0,1}, c_{0,2}, c_1\} \rightarrow M$:
    - Dec$(uskd = a, C := \{c_{0,1}, c_{0,2}, c_1\}) \rightarrow M$:
      (1) Compute $c_0 = c_{0,1} + c_{0,2} \in R_q$.
      (2) Compute $w = \left(\left\lceil \frac{(2/q) + \phi(c_0 - c_1 e^	au)}{2} \right\rceil \bmod 2\right)$, where the rounding function $\lceil \cdot \rceil$ is applied component-wise.
    - Output $M.$ $\rightarrow w.$

- $T\text{Verify}(uskd = (f_1, f_2), C = \{c_{0,1}, c_{0,2}, c_1\}) \rightarrow 1/0$:
  (1) For $i \in \{1, 2\}$, compute $b_i = \left(\left\lceil \frac{(2/q) + \phi(c_0 - c_1 f_i)}{2} \right\rceil \bmod 2\right)$, where the rounding function $\lceil \cdot \rceil$ is applied component-wise.
  (2) If $w_1 = w_2$, output $1$; otherwise, output $0$.

\footnote{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 the identity, our concept is not applicable to these schemes, which is consistent with the description in [6].}
4.3 Correctness and Consistency

Lemma 4.1 (Correctness). Given a pair comprising a master public key and master secret key (mpk = (a, u1, u2, b1, {hj})i,j∈[d]×[f]×[H], msk = Tm ← Setup(1λ)) generates a ciphertext C = (c1, c2, c1) ← Enc(mpk, id, M), given a secret key usk = e, and a tracing key tsk = (f1, f2) 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 Dec(usk, C) and TVerify(tsk, C) return the message M and 1, respectively.

We first consider the correctness of the decryption algorithm. In the Dec algorithm, we have
\[ \phi(c0 - c1e^T) = \left| \frac{1}{2} \left( \phi(M) + \phi(x_{01}) + \phi(x_{02}) - \phi(x_{12}) \right) \right|, \]
where \( c0 = c0_1 + c0_2 \).

Next we analyze the norm of the error term by following the analogue of the Proof of Lemma 10 in [19]. Because x0_1 and x0_2 are chosen from \( \mathcal{D}_{2nq}^{\text{coeff}} \), the vectors \( \phi(x_{01}) \) and \( \phi(x_{02}) \) are subgaussian with the parameter q. Thus, let each jth entry of \( \phi(x_{01}), \phi(x_{02}), \phi(x_{12}) \) be less than \( aq\phi(\sqrt{\log n}) \) with overwhelming probability. Similarly, because \( x_1 \) and \( x_2 \) are chosen from \( \mathcal{D}_{2nq}^{\text{coeff}} \), we have \( \phi(x_{12}) \leq \mathcal{D}_{2nq}^{\text{coeff}} \).

In addition, according to the definition of the rotation function, the norm of each column of \( \rho(e^T) \) is \( \|\phi(e)\|_2 \), where \( \phi(e) \rightarrow \mathcal{D}_{2nq}^{\text{coeff}} \).

Hence, we can conclude that each jth entry of the error term is bounded as \( \|\phi(x_{01}) + \phi(x_{02}) - \phi(x_{12})\rho(e^T)\| \leq 2aq\phi(\sqrt{\log n} + \sqrt{n}k\alpha\sigma_\omega(\sqrt{\log n}) \leq \frac{q}{5} \), 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, for \( i = 1, 2 \), we have
\[ \phi(c0_2 - c1f_1^T) = \phi(x_{02}) - \phi(x_{12})\rho(f_1^T). \]

Using the preceding steps of the proof, we can also deduce that each jth entry of the error term is bounded as \( \|\phi(x_{02}) - \phi(x_{12})\rho(f_1^T)\| \leq aq\phi(\sqrt{\log n} + \sqrt{n}k\alpha\sigma_\omega(\sqrt{\log n}) \leq \frac{q}{5} \), 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 (mpk = (a, u1, u2, b1, {hj})i,j∈[d]×[f]×[H], msk = Tm ← Setup(1λ)) generates a ciphertext C = (c1, c2, c1) ← Enc(mpk, id, M); a secret key usk = e, and a tracing key tsk = (f1, f2) for user id, 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 TVerify(tsk, C) returns 0.

Consider the process of the trace verification algorithm. In the TVerify algorithm, for \( i = 1, 2 \), we have
\[ \phi(c0_2 - c1f_1^T) = \phi(c1_2 - \phi(s\{a|H(id)\})\rho(f_1^T) \phi(x_{02}) - \phi(x_{12})\rho(f_1^T). \]

According to the aforementioned assumption, the error term is bounded only by q/5. Because \( s\{a\} \in \{1\} \), \( H(id) \in \{0, 1\} \), the term \( \phi(s\{a\})\rho(H(id))\rho(f_1^T) \) 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 the 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 \( aq\phi(\sqrt{\log n}) + \sqrt{n}k\alpha\sigma_\omega(\sqrt{\log n}) \) and \( 2aq\phi(\sqrt{\log n}) + \sqrt{n}k\alpha\sigma_\omega(\sqrt{\log n}) \) are less than q/5 with overwhelming probability (required by Lemma 4.1 and 4.2);
- \( p < \frac{1}{2}\sqrt{q}/n \) and \( k \geq 2\log q \) to ensure that TrapGen can function correctly (required by Theorem 2.9);
- \( k \geq \log q \) such that the gadget matrix \( g \) can be defined (required by Theorem 2.12);
- \( \sigma > O(\log q) \cdot \omega(\sqrt{\log n}) \) and \( \sigma > s_1(R)\sqrt{\log n} + \omega(\sqrt{\log n}) \) such that the algorithms SampleLeft and SampleRight function correctly (required by Theorem 2.10 and 2.11). Here, \( s_1(R) \leq C'' \cdot \|V\| \cdot \sqrt{\omega(\sqrt{\log n})} \cdot (cn)^{d-1} + bnk(\sqrt{\log n}) \) for some absolute constant \( C'' \);
- \( k = \left( \frac{a^2}{(\log^2 p + 1)} \right)^n \) such that regularity lemma can be applied in the security proof (required by Lemma 2.6); and
- \( aq \geq n/2 + \frac{1}{4}\omega(\sqrt{\log n}) \) such that a worst-case-to-average-case reduction is achieved (required by Theorem 2.8);
- \( a' > 2aq + 1 \) and \( a' > 2\log q \) 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.
Quantum-resistant Anonymous IBE with Traceable Identities

5 SECURITY PROOF

This section demonstrates that our above proposed scheme is adaptively IND-Anonymous-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-Anonymous-ID-CPA secure assuming that RLWE_{n,k+2,q,F_{\text{poly}}} is hard, where the ciphertext space is $C = R_q \times R_q \times R_k^q$.

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 $n = O(\lambda^5)$, where $\lambda$ is a constant, we have $4Q + 1 \leq n^6$ 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 $2\epsilon \geq n^{-V}$ for infinitely many elements $n$, where $\psi \in \mathbb{N}$. Therefore, for infinitely many $n \in \mathbb{N}$, we have

$$4Q \leq n^6$$

for all $n \in \mathbb{N}$ and $\frac{\epsilon}{2Q + 1} \geq \frac{1}{n^6}$,

(1)

where $\xi = \varphi + \psi$. Because $\xi$ 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-Anonymous-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 Gamei.

Game1: This game is identical to the real IND-Anonymous-ID-CPA game. Suppose $\mathcal{A}$ outputs a guess $b$ at the end of the game, by the definition of the advantage of $\mathcal{A}$, we have

$$\Pr[X_1] - \frac{1}{2} = \Pr[b = b] - \frac{1}{2} = \epsilon.$$

Game2: 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 $y = \{y_0, \{y_{i,j}\}_{(i,j) \in S(id)}\}$, where $y_0 \xleftarrow{} U([\xi, \xi + 1], R_{\xi - 1} + 1)$ and $y_{i,j} \xleftarrow{} U([1, n], R_{\xi - 1} + 1)$. Here, for two integers $m, n \in \mathbb{Z}$, $\{m, n\} = \{m + k, n + k\} \in R_k$.

2. Let $id^*$ be the challenged identity and $id_1, \ldots, id_Q$ be the identities queried on the secret key generation and tracing key generation oracles, $\mathcal{B}$ then checks whether the following condition is satisfied:

$$F_y(id^*) = 0 \land F_y(id_1) \land \cdots \land F_y(id_Q) \in R_q^Q,$$

where $F_y : J \mathcal{D} \rightarrow R_q$ is defined as:

$$F_y(id) = y_0 + \sum_{(i,j) \in S(id)} y_{i,j} \cdots y_{d,i,j}.$$

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

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

$$\Pr[X_1] - \frac{1}{2} \geq \frac{1}{2Q + 1} \left( \frac{\xi}{dQ + 1} \right).$$

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.

Game2: This game differs only slightly from the previous game, with the difference being the manner of choosing $b_0, b_{i,j}$. Specifically, in place of choosing $b_i, b_{i,j} \leftarrow U(R_q^2)$, $b_i, b_{i,j}$ are chosen as follows:

$$b_i = aR_0 + y_0 b_i, b_{i,j} = aR_{i,j} + y_{i,j} b_i,$$

for $(i, j) \in [d] \times [f]$. According to regularity lemma (Lemma 2.6), the distributions of $(a, b_0, b_{i,j})$ in Game1 and Game2 are negl-close. Therefore, we have $|Pr[X_1] - Pr[X_2]| = \text{negl}(n)$.

Game3: In the previous games, when the condition

$$F_y(id^*) = 0 \land F_y(id_1) \land \cdots \land F_y(id_Q) \in R_q^Q,$$

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 Game2 and Game3, we have $Pr[X_1] = Pr[X_3]$.

Before moving to the next game, we define and provide the following results. First, we can define $R_d$ for an identity as follows:

$$R_d = R_0 + \sum_{(j_1, \ldots, j_d) \in S(id)} \text{TrapEval}_d(b_{1,j_1}, \ldots, b_{d,j_d}).$$

Additionally, according to the definition of $R_d$, $H(id), \text{PubEval},$ and Lemma 2.13, we have

$$H(id) = b_0 + \sum_{(j_1, \ldots, j_d) \in S(id)} \text{PubEval}_d(b_{1,j_1}, \ldots, b_{d,j_d})$$

$$= aR_d + F_y(id) g_b.$$

Furthermore, we consider the bound of $s_1(R_d)$. First, because $y_{i,j}$ is chosen from $[1, n], R_{\xi - 1}$, we have $\|y_{i,j}\| \leq 2n$. Then, according to Lemma 2.5, we have $s_1(R_0), s_1(R_{i,j}) \leq B$ with all but negligible probability because $R_0$ and $R_{i,j}$ are chosen from $[-\rho, \rho R]^k$, where $B = C' \cdot \rho \sqrt{n} (\sqrt{\xi} + \text{log}(n))$. Therefore, we have

$$s_1(R_d) \leq s_1(R_0) + \sum_{(j_1, \ldots, j_d) \in S(id)} s_1 \left( \text{TrapEval}_d(R_{1,j_1}, \ldots, R_{d,j_d}, y_{1,j_1}, \ldots, y_{d,j_d}) \right)$$

$$\leq B \left( 1 + k(\xi n)^d + k n^d \frac{(\xi n)^d - 1}{\xi n - 1} \right),$$

(2)

for any $id \in J \mathcal{D}$ with all but negligible probability.
Game1: In this game, instead of generating $a$ using the TrapGen algorithm, $B$ picks $a \leftarrow U(R_k^k)$. According to Lemma 2.9, $a$ is 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 = $e \leftarrow \text{SampleLeft}(a, H(id), u_1 + u_2, T_a, \sigma)$ and tracing key tsk = $(f_1, f_2) \leftarrow \text{SampleLeft}(a, H(id), u_2, T_a, \sigma)$ for the identity id $\in I \mathcal{D}$ and $F_y(id) \in R_y^n$, $B$ answers them as follows: For any identity id $\in I \mathcal{D}$, if $F_y(id) \notin R_y^n$, $B$ aborts it. Otherwise, $B$ first computes $R_{a\sigma}$ and then returns the secret key by computing usk = $e \leftarrow \text{SampleRight}(a, g, R_y, F_y(id), u_1 + u_2, T_{a\sigma}, \sigma)$ and returns the tracing key by computing tsk = $(f_1, f_2) \leftarrow \text{SampleRight}(a, g, R_y, F_y(id), u_2, T_{a\sigma}, \sigma)$, depending on which oracle was queried by $\mathcal{A}$. Therefore, according to the proper choice of $e$ and according to Eq. (2), Theorem 2.10, and Theorem 2.11, the output distribution of SampleRight is negl($n$)-close to the distribution of SampleLeft. Hence, from the perspective of $\mathcal{A}$, the change is negligible. We have $|Pr[X_5] - Pr[X_4]| = \text{negl}(n)$.

Game2: In the preceding game, when $b = 0$, $B$ generates the challenged ciphertext following the real scheme. In the current game, if the game does not abort and $b = 0$, $B$ creates the challenged ciphertext as follows. First, $B$ picks $s \leftarrow U(R_q)$ and picks $x \leftarrow \{\mathcal{D}_{\text{coff}}^{z^nq,k} \}^k$ before computing $v = sa + x \in R_k$. Additionally, according to Lemma 2.2, $B$ computes $e \leftarrow \text{ReRand}([\{I_k[R_{a\sigma}]\}]_1, \{v\}_2, a, \frac{q}{q^{z^nq,k}}) \in Z_q^{2nk}$, where $I_k \in R_k^{k \times k}$ is the identity matrix of size $k \times k$. $B$ then picks $x_{01}, x_{02} \leftarrow \mathcal{D}_{\text{coff}}^{z^nq,k}$ and sets the challenged ciphertext to be

$$C^* = (c_{01} = v_{01} + \lfloor q/2 \rfloor, M, c_{02} = v_{02}, c_1 = \phi^{-1}(e)) \in R_q \times R_k^k,$$

where $v_{01} = su_1 + x_{02}, v_{02} = su_2 + x_{02}$ 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 $\phi(v) = \phi(sa + x) = \phi(s)\phi(a) + \phi(x)$, where $\phi(x)$ has the distribution $\phi(x) \leftarrow \mathcal{D}_{\text{coff}}^{z^nq,k}$ with the proper choices of $a$ and $\phi$ and according to the property of ReRand, we have

$$c = \left(\phi(s)\text{rot}(a) \cdot \text{rot}([I_k[R_{a\sigma}]]) + x'\right.$$

$$= \phi(s) \cdot \text{rot}([aH(id')]) + x'$$

$$= \phi(s)(aH(id')) + x'$$

$$= \phi(s)(aR_{a\sigma}) + x'.$$

Thus, according to Lemma 2.2, the distribution of $x'$ is negl($n$)-close to $\mathcal{D}_{\text{coff}}^{z^nq,k}$. From the perspective of $\mathcal{A}$, the distribution of $c_1$ between Game3 and Game3 is statistically close. Therefore, $|Pr[X_4] - Pr[X_5]| = \text{negl}(n)$.

Game3: This game continues to change how the challenged ciphertext is generated when $b = 0$ and when the game is not aborted. In this game, $B$ picks $s_{01}, s_{02} \leftarrow U(R_q), v' \leftarrow U(R_k^k)$, and $x \leftarrow \mathcal{D}_{\text{coff}}^{z^nq,k}$. Then, $B$ computes $e \leftarrow \text{ReRand}([\{I_k[R_{a\sigma}]\}], \phi(v'), a, \frac{q}{q^{z^nq,k}}) \in Z_q^{2nk}$, where $v = v' + x$.

Finally, the challenged ciphertext is set to be

$$C^* = (c_{01} = v_{01}, c_{02} = v_{02}, c_1 = \phi^{-1}(e)) \in R_q \times R_x \times R_k^k,$$

where $s \leftarrow U(R_q)$ and $x_{02} \leftarrow \mathcal{D}_{\text{coff}}^{z^nq,k}$.

Lemma 5.3. For any adversary $\mathcal{A}$, we have $|Pr[X_5] - Pr[X_4]| = \text{negl}(n)$ under the RLWE$_{n,k+2,q}$, $\mathcal{D}_{\text{coff}}^{z^nq,k}$ assumption.

Proof. Suppose that there exists an adversary $\mathcal{A}$ that can distinguish between Game3 and Game3 with a nonnegligible advantage. Accordingly, there exists another algorithm $B$ that can solve RLWE$_{n,k+2,q}$, $\mathcal{D}_{\text{coff}}^{z^nq,k}$, assumption with a nonnegligible advantage.

Instance. Before the Setup phase, $B$ is given an RLWE instance: $(\{a_i, v_i[k]\}_{i \in [1]} \in (R_q \times R_q)^{k+2}$. Without loss of generality, we assume that $v_i = v_i' + x_i$ for $x_i \leftarrow \mathcal{D}_{\text{coff}}^{z^nq,k}$. The target of $B$ is to distinguish whether $v_i' = a_i s$ for some $s \in R_q$ or $v_i' \leftarrow U(R_q)$.

Setup. $B$ first picks $u_1 \leftarrow U(R_q)$, and sets $u_2 = a_0 - u_1$, $a = \{a_2, \ldots, a_{k+2}\}$, $u_0 \leftarrow u_1, v := \{v_2, \ldots, v_{k+4}\}$. In addition, $B$ picks $y$ as in Game1; picks $R_0, R_1, \ldots$, as in Game2, sets $b_0$ and $b_1$, as in Game2, and defines a function $H$ as in Game2. Finally, $B$ outputs mpk = $(e, u_1, u_2, b_0, \{b_{i,j}\}_{(i,j) \in \delta[t], H}) \rightarrow \mathcal{A}$.

Phase 1 and Phase 2. The secret key generation and tracing key generation oracles are answered in Game4. That is, the keys are generated by $R_0$ and $R_1$.

Challenge. In this phase, $\mathcal{A}$ submits a challenge identity id$^*$ and message $M$ to $B$. If $F_y(id^*)$ ≠ 0, $B$ aborts and sets $b' \leftarrow U(\{0, 1\})$. Otherwise, $B$ first randomly picks $b \leftarrow U(\{0, 1\})$. Then, if $b = 0$, $B$ computes $R_{a\sigma}$ and $c$ as in Game3. Subsequently, $B$ sets the challenged ciphertext $C^*$ as in Game3. If $b = 1$, $B$ picks $c_{01}, c_{02} \leftarrow U(R_q), c_1 \leftarrow U(R_k^k)$, and sets $C^* = (c_{01}, c_{02}, c_1)$. Finally, $B$ returns $C^* \rightarrow \mathcal{A}$.

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

Analysis. If $(a_i, v_i'[k])_{i \in [1]}$ are valid RLWE samples (i.e., $v_i' = a_i s$), $B$ perfectly simulates the perspective of $\mathcal{A}$ in Game2. Otherwise, the perspective of $\mathcal{A}$ is in Game3. Therefore, $|Pr[X_5] - Pr[X_4]|$ is less than the advantage that $B$ has after solving the RLWE$_{n,k+2,q}, \mathcal{D}_{\text{coff}}^{z^nq,k}$ assumption.

According to Lemma 5.3, if the RLWE$_{n,k+2,q}$, $\mathcal{D}_{\text{coff}}^{z^nq,k}$ assumption is hard, we have $|Pr[X_5] - Pr[X_4]| = \text{negl}(n)$.

Game4: 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

$$C^* = (c_{01} = v_{01}, c_{02} = v_{02}, c_1 = \{v'v'R_{a\sigma} \} + [x_1[x_2]] \in R_q \times R_q \times R_k^k,$$

Because $\phi(v) = \phi(v' + x) = \phi(v') + \phi(x) \in Z_q^{2nk}$ in Game4, for the output $e$, we have
\[ c = \phi(v') \cdot \text{rot}([I_k]\{R_{d}]) + x' = \phi([v'|R_{ad}]) + x', \]

where the distribution of \(x'\) is \(\text{negl}(n)\)-close to \(\mathcal{D}_{2^{2nk},d'}\) according to Lemma 2.2. Therefore, we have \(\text{Pr}[X_s] - \text{Pr}[X_t] = \text{negl}(n)\).

Games: 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 \(u_{skd} = e \leftarrow \mathcal{D}^{\text{coeff}}_{\Lambda_{\phi(x,y)}}([\text{rot}(a^+)^{\top} \text{rot}(H(id)^{\top})]),\sigma\) and \(t_{skd} = (f_1, f_2) \leftarrow \mathcal{D}^{\text{coeff}}_{\Lambda_{\phi(x,y)}}([\text{rot}(a^+)^{\top} \text{rot}(H(id)^{\top})]),\sigma\), respectively, without using \(R_d\). From the perspective of \(\mathcal{A}\), similar to the change from Game3 to Game4, the distribution of the secret key and tracing key remains unchanged; therefore, we have \(\text{Pr}[X_t] - \text{Pr}[X_s] = \text{negl}(n)\).

Games: In this last game, \(\mathcal{B}\) sets the challenged ciphertext to be

\[ C^* = (c_{0,1} \leftarrow U(R_q), c_{0,2} \leftarrow U(R_q), c_1 \leftarrow U(R_q)), \]

regardless of whether \(b\) is 1 or 0. Because \(c_{0,0} = U(R_q)\), we can readily determine that the distribution of \((c_{0,1}, c_{0,2})\) between Games4 and Game5 is negligible. In the following paragraphs, we show that \(c_1\) in Game5 is \(\text{negl}(n)\)-close to the uniform distribution over \(R_{d^t2}\).

Specifically, because \([x_1|x_2] \in R_{d^t2}\), we only show that the distribution of \([v'|R_{d^t2}]\) is statistically close to the uniform distribution over \(R_{d^t2}\). Before furnishing such a proof, we demonstrate that the following distributions are \(\text{negl}(n)\)-close; that is,

\[ (a, aR_0, v', vR_0) \approx (a, a', v', v') \approx (a, aR_0, v', v'), \tag{3} \]

where \(a, a' \leftarrow U(R_q), R_0 \leftarrow U([-\rho, \rho])_{R}^{\text{sk}}, v', v'' \leftarrow U(R_{d^t2}).\) Eq. (3) is satisfied according to Lemma 2.6. Specifically, we can demonstrate that the first and second distributions are \(\text{negl}(n)\)-close by applying Lemma 2.6 for \([a, v'] \in R_{d^t2}\) and \(R_0\). Similarly, we can show that the second and third distributions are \(\text{negl}(n)\)-close by applying the same lemma for \(a\) and \(R_0\). According to the preceding description, let \(R_{d^t2} = \sum_{(j_1, \ldots, j_d) \in S(d')} \text{TrapEval}_{(R_{d^t2})}([R_{d^t2}, \ldots, R_{d^t2}]),\)

we thus have

\[ (a, aR_0, v', v'R_0) \approx (a, aR_0, v' \leftarrow U(R_{d^t2}) + R_{d^t2}), \]

\[ \approx (a, a, aR_0, v', v' + v' \leftarrow U(R_{d^t2})), \]

where \(v', v'' \leftarrow U(R_{d^t2})\) and \(R_0 \leftarrow U([-\rho, \rho])_{R}^{\text{sk}}.\) Therefore, we have \(\text{Pr}[X_s] - \text{Pr}[X_t] = \text{negl}(n)\).

**Analysis.** Combining the aforementioned games, we have

\[ \text{Pr}[X_s] = \frac{1}{2} \approx \text{Pr}[X_t] = \frac{1}{2} + \frac{8}{n} \left(\text{Pr}[X_{i+1}] - \text{Pr}[X_i]\right) \approx \frac{1}{2}, \]

\[ \approx \frac{1}{2} - \frac{\epsilon}{n^2} > 0. \]

Because the challenged ciphertext contains no information related to \(b\) which is used in Gameq, \(\mathcal{A}\) can only return \(b^*\) through a guessing process. That is, \(\text{Pr}[X_s] = \frac{1}{2} = 0.\) This also implies that \(\frac{\epsilon}{n^2} > \frac{1}{2}\) 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. \(\square\)

### 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


