Classical to Post-Quantum Secure ABE-IBE Proxy Re-Encryption Scheme

Muhammad Nauman Khan[1,2][a], Asha Rao[1][b], Seyit Camtepe[2][c] and Josef Pieprzyk[2,3][d]
[1]School of Science, RMIT University, Australia
[2]CSIRO DATA61, Australia
[3]Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland

Keywords: Attribute-Based Encryption, Identity-Based Encryption, Proxy Re-Encryption, Post-Quantum Cryptography, Data Confidentiality.

Abstract: Maintaining data confidentiality at the asymmetric-resource devices across emerging technologies needs varying cryptographic algorithms. Quantum computing makes preserving data confidentiality across asymmetric infrastructure more difficult. However, exploiting the architecture of classical cryptographic schemes to integrate the post-quantum constructs could be used to maintain post-quantum level confidentiality over the Internet. This paper presents a post-quantum secure classical ABE-IBE proxy re-encryption scheme ($\mathfrak{L}$_ABE-IBE PRE) that utilizes the classical ABE-IBE proxy re-encryption capabilities at the end nodes in a system and raises the data confidentiality to post-quantum secure level over the Internet. The proposed $\mathfrak{L}$_ABE-IBE PRE transforms a ciphertext of the classical ABE scheme to a post-quantum secure ciphertext and from a post-quantum secure ciphertext to a ciphertext of the classical IBE scheme. We compare our proposed $\mathfrak{L}$_ABE-IBE PRE scheme with classical ABE-IBE proxy re-encryption schemes, including Encryption Switching ABE-IBE (ES.ABE-IBE) scheme (He et al., 2019). We discuss the security and efficiency of our proposed scheme.

1 INTRODUCTION

Integrating asymmetric devices with emerging technologies (IoT, edge, fog, cloud and quantum) opens up new opportunities but poses new security challenges (Lohachab and Karambir, 2019). For example, data encrypted using lightweight cryptographic mechanisms for resource-limited devices become vulnerable over resourceful devices. Similarly, classical cryptographic primitives do not address the security needs of resource-constrained devices. Thus, existing classical cryptography does not address the security of the growing number of asymmetric devices over the Internet. Resource-limited devices can use resourceful parties (edge or fog platforms) for computation, but these parties work in less secure environments with a significant risk of attacks (such as man-in-the-middle, denial-of-service) (Roman et al., 2018). Despite this, outsourcing data to more resourceful parties (cloud, edge, and fog) continues to grow.

Identity-based encryption (IBE) and attribute-based encryption (ABE) schemes provide fine-grain access control over outsourced data. Proxy re-encryption schemes, such as ABE-IBE or IBE-ABE, have been developed for secure data outsourcing from one domain to another without compromising the sender's privacy. However, these schemes ignore the asymmetric nature of devices across the IT infrastructure. Furthermore, quantum computing tips the balance against asymmetric devices using classical cryptography. In this paper, we propose a proxy re-encryption scheme that transforms the existing classical ciphertext to a post-quantum one for secure data outsourcing via the insecure Internet.

This paper is organised as follows: Section 2 illustrates the related work. Section 3 discusses the problem statement and motivation. Section 4 gives basic mathematical preliminaries and notations. Section 5 describes our proposed scheme. Section 6 evaluates the security and Section 7 illustrates the efficiency of proposed scheme. Section 8 concludes this paper.

[a] https://orcid.org/0000-0002-3413-1039
[b] https://orcid.org/0000-0001-6222-282X
[c] https://orcid.org/0000-0001-6353-8359
[d] https://orcid.org/0000-0002-1917-6466

Khan, M., Rao, A., Camtepe, S. and Pieprzyk, J.
Classical to Post-Quantum Secure ABE-IBE Proxy Re-Encryption Scheme.
DOI: 10.5220/0012078200003555
In *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023)*, pages 85-98
ISBN: 978-989-758-666-8; ISSN: 2184-7711

2 RELATED WORK

The asymmetric nature of devices significantly affects data outsourcing/data sharing between parties via an insecure Internet. Several classical cryptographic primitives have been developed to address the security of individual or group devices. However, none of these primitives addresses the security of dispersed and asymmetric devices and secure data outsourcing requirements.

Shamir (1985) proposed the first IBE scheme that applies public identity information (such as email addresses) as public keys. IBE scheme based on bilinear pairings was proposed by (Boneh and Franklin, 2001). IBE has been extensively studied, see for example Hofheniz et al. (2018), as it simplifies public key management without public-key infrastructure (PKI) and certificates, and also improves efficiency and security of asymmetric devices (Xiong et al., 2019).

Sahai and Waters (2005) proposed the first attribute-based encryption (ABE) scheme that replaces the identity with attributes of an intended receiver and provides better access control over data. Many ABE variants have been proposed, see (Li et al., 2018, Chen et al., 2018, Li et al., 2019, Miao et al., 2021, Li et al., 2020). Extensible and expandable ABE methods (Susilo et al., 2017, Yang et al., 2018) provide secure data sharing between entities. However, these methods require the valid recipients to satisfy the access policies, which need to be continuously updated by adding or revoking entities.

The first proxy re-encryption (PRE) scheme was developed by Blaze et al. (1998) to transform a ciphertext encrypted for one receiver into a ciphertext that a different receiver could decrypt. Several ABE-IBE and IBE-ABE proxy re-encryption schemes have been developed (Cao et al., 2019, He et al., 2019, Deng et al., 2020). The security of these proxy re-encryption schemes depends on bilinear pairing, making them all insecure against a quantum adversary.

Post-quantum cryptography such as lattice-based cryptography (LBC) applies quantum intractable lattice problems for designing new cryptographic algorithms and protocols or re-designing existing classical cryptography schemes to withstand quantum adversaries (Banerjee et al., 2019, Nejatollahi et al., 2019, Fernández-Caramés, 2020, Tao et al., 2023). LBC also provides a rich source of cryptographic tools for secure data sharing through resource-rich Internet or cloud nodes.

The first LBC scheme was proposed by Ajtai (1996) and Regev (2009) giving a rigorous security proof of the scheme. Security of lattice-based cryptographic schemes depends upon intractable lattice problems (Peikert, 2016) such as learning with errors (LWE). Lattices are considered the best choice for the design of new post-quantum cryptographic algorithms and protocols in the research community.

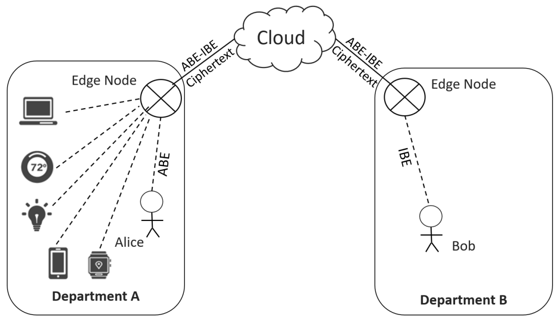

Figure 1: ABE-IBE Proxy Re-encryption between Alice and Bob through Untrusted Cloud Environment.

3 PROBLEM STATEMENT

Existing classical cryptographic schemes including ABE and IBE are vulnerable to quantum attacks (Shor, 1999). It is possible to address this problem by using quantum-resistant cryptographic primitives such as lattices (Asif, 2021). NIST has published the post-quantum security recommendations for commercial entities (Joseph et al., 2022). However, these primitives have not been thoroughly tested, making it highly likely that they will continue co-existing with classical cryptography.

In this paper, we propose the transformation of classical ciphertext to post-quantum secure ciphertext using a proxy re-encryption scheme and vice versa. Here, we solve the following problem.

> How do we securely share data between two local domains via the Internet under the following assumptions:
>
> - The local domains (consisting of classical asymmetric devices) predominantly use classical encryption, and are not accessible to quantum adversaries.
> - The Internet domain (consisting of cloud or quantum devices) supports post-quantum cryptography and is accessible to quantum adversaries.

This research aims to design a classical to post-quantum secure ABE-IBE proxy re-encryption ($\mathfrak{L}$_ABE-IBE PRE) scheme for secure data sharing between the two local domains. For this purpose, we adapt the ABE-IBE proxy model defined by He et al. (2019) and Deng et al. (2020) to incorporate post-quantum secure primitives (lattice-based encryption), transforming a classical ciphertext (ABE) to a post-quantum secure ciphertext for secure data sharing.

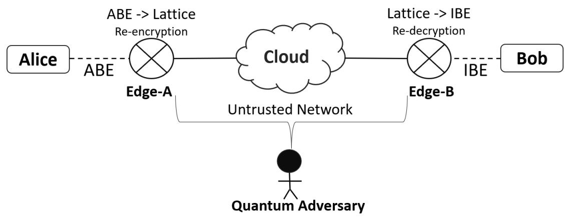

Figure 2: Proxy Re-encryption on Edge Nodes for secure communication between Alice and Bob via unsecure and untrusted network with the presence of quantum adversary.

The idea is illustrated in Fig. 1. Consider a company ABC with two isolated departments, A and B (local domains). Alice and Bob work in departments A and B, respectively. Department A deploys several asymmetric devices connected to a local Edge node to monitor the environment (such as an early storm warning system). The data inside Department A is encrypted using an access-control policy (ABE) based on the attributes of the devices and people working in Department A. Bob is interested in the encrypted data from department A. When he asks Alice for the data, she uses the ABE-IBE proxy (He et al., 2019) model to allow him to access data without changing department A's access-control policy. That is, ABE-IBE re-encryption facilitates one-way data sharing over the Internet. Once quantum adversaries are allowed over the Internet, the ABE-IBE cryptographic scheme (He et al., 2019) becomes vulnerable due to the Shor algorithm (Monz et al., 2016).

To solve this problem, we propose secure proxy re-encryption at the local Edge nodes, which "isolate" the local domains from the untrusted Internet – see Fig. 2. Alice sends ABE ciphertext (secure against a classical adversary) to the local Edge node (in her local domain), which re-encrypts the ABE ciphertext to post-quantum secure ciphertext (secure against the quantum adversary) and either stores it on cloud or sends it to Bob's local domain via the insecure Internet. When Bob requests the outsourced ciphertext, the local Edge node on his side receives it and applies re-decryption to transform the post-quantum secure ciphertext to IBE ciphertext. Finally, Bob decrypts the generated IBE ciphertext using his private key.

This scenario motivates our work, and our solution applies novel classical to post-quantum secure ABE-IBE proxy re-encryption ($\mathfrak{L}$_ABE-IBE) to secure data over the Internet from quantum adversaries.

The main contributions in this paper are:

- We design a proxy re-encryption scheme ($\mathfrak{L}$_ABE-IBE PRE) that securely transforms the attribute-based ciphertext to post-quantum secure ciphertext (at sender's local Edge-A) and post-quantum secure ciphertext to identity-based ciphertext (at receiver's Edge-B). Our scheme is post-quantum-safe because its security relies on the quantum intractability of NP-hard lattice problems.
- Our scheme provides an effective and secure communication channel between two local domains via an insecure cloud/Internet that could be controlled by a powerful quantum adversary. The re-encryption operations are performed by local Edge nodes – see Fig. 2.
- We evaluate the performance and security of our scheme. We also demonstrate that our scheme is selectively secure against indistinguishable chosen-ciphertext attacks (IND-sCCA).

4 PRELIMINARIES

This section illustrates the mathematical definitions, notations, and concepts related to bilinear pairing and lattice-based cryptography.

4.1 Bilinear Pairing

Definition 4.1 (**Bilinear Pairing** (Deng et al., 2014)). *Given cyclic groups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ of prime order p, where g_1 is a generator of $\mathbb{G}_1$ and g_2 is a generator of $\mathbb{G}_2$, a bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ with the following properties:*

i. Bilinearity: $\forall_{h_1,h_2}\forall_{a,b}\quad e(h_1^a, h_2^b) = e(h_1,h_2)^{ab}$, *where $h_1 \in \mathbb{G}_1, h_2 \in \mathbb{G}_2$ and $a,b \in \mathbb{Z}_p$.*

ii. Non-degeneracy: $e(g_1,g_2) \neq 1$.

iii. For $\mathbb{G}_1$ and $\mathbb{G}_2$, there exists an algorithm that can efficiently compute the bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. □

The bilinear map $e(,)$ is symmetric if $\mathbb{G}_1 = \mathbb{G}_2$.

Definition 4.2 (**Linear Secret Sharing Scheme (LSSS)** (Beimel, 1996, Susilo et al., 2017)). *Given a set of n parties $\mathcal{P} = \{P_1, P_2, ..., P_n\}$ as an access structure, a secret sharing scheme Π is a LSSS over $\mathbb{Z}_p$ if*

i. Each party's shares of the secret form a vector over $\mathbb{Z}_p$.

ii. There is an $(l \times n)$ matrix M (share generating) matrix. The i^{th} row of M, M_i is assigned to the party P_i according to a function $\rho(i)$, for all $i = 1,\dots,n$. Let vector $v = (s, r_2, ..., r_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared and $r_2,...,r_n \in \mathbb{Z}_p$ randomly chosen, then $M \cdot v$ represents l shares of s. The share of P_i is given by $\lambda_i = M_i \cdot v$. □

Recovery of a secret proceeds as follows. Given an authorized set $\widehat{\mathbb{U}} \in \mathbb{U}$ and $I \subseteq \{1,2,\cdots,l\}$ defined as $I = \{i : \rho(i) \in \widehat{\mathbb{U}}\}$, then there exist some constants $\{\omega_i \in \mathbb{Z}_p\}$ such that $\sum_i^l \omega_i\lambda_i = s$ for each valid share $\{\lambda_i\}$ of secret s.

Definition 4.3 (**Computational Bilinear Diffie-Hellman (CBDH) Problem** (Joux and Nguyen, 2003))**.** *Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a non-degenerate bilinear pairing. Then*

- *The bilinear Diffie-Hellman problem 1 (BDH-1) asks to find $z = e(R,S)^{ab}$ for given $R, aR, bR \in \mathbb{G}_1$, $S \in \mathbb{G}_2$ and random a, b.*
- *The bilinear Diffie-Hellman problem 2 (BDH-2) asks to find $z = e(R,S)^{ab}$ for given $R \in \mathbb{G}_1$, S, aS, $bS \in \mathbb{G}_2$ and random elements a, b.*

4.2 Lattices

Definition 4.4 (**Lattices** (Micciancio and Regev, 2009))**.** *Given a collection $B = \{b_1, ..., b_n\}$ consisting of n linearly independent vectors $b_1, \ldots, b_n \in \mathbb{R}^m$, an n-dimensional lattice Λ generated by B (further called a basis) is defined as:*

$$\Lambda = \mathcal{L}(b_1, \ldots, b_n) = \{\sum_{i=1}^{n} c_i \cdot b_i : c_i \in \mathbb{Z}^n, \forall 1 \leq i \leq n\}, \quad (1)$$

where n is the rank of lattice Λ. Λ is called full rank if and only if $n = m$. $\square$

Definition 4.5 (**q-ary Lattice** (Micciancio and Regev, 2009))**.** *Given a vector $\vec{u} \in \mathbb{Z}_q^n$ and a matrix $A \in \mathbb{Z}_q^{n\times m}$, whose entries are chosen uniformly at random, a q-ary lattice for prime q is defined as:*

$$\begin{aligned} \Lambda_q^{\vec{u}}(A) &:= \{\vec{e} \in \mathbb{Z}^m \, s.t. \, A\vec{e} = \vec{u}(mod\, q)\}, \\ \Lambda_q^{\perp}(A) &:= \{\vec{e} \in \mathbb{Z}^m \, s.t. \, A\vec{e} = 0(mod\, q)\}. \end{aligned} \quad (2)$$

The security of LBC schemes rests on the intractability assumptions of lattice problems, such as learning with error (Lindner and Peikert, 2011).

4.2.1 Learning with Error (LWE)

Let Ψ be a security parameter and $\mathcal{X} = \mathcal{X}(\Psi)$ be a Gaussian distribution over Z_q (Gentry et al., 2008). The $LWE_{n,m,q,\mathcal{X}}$ assumption requires that, if $A \in Z_q^{m\times n}$, $\vec{s} \in Z_q^n$, $\vec{e} \in \mathcal{X}^m$, $\vec{u} \in Z_q^m$, then $(A, A\vec{s} + \vec{e}) \approx_c (A, \vec{u})$, where $\approx_c$ is computational approximation.

The prime q must be sufficiently large such that $\sum_{i\in S} e_i \leq q/4$ holds.

Definition 4.6 (**TrapGen** (Micciancio and Peikert, 2012))**.** *Let $A \in \mathbb{Z}_q^{n\times m}$ and $G \in \mathbb{Z}_q^{n\times(k-1)z}$ be matrices with $m \geq z \geq n$ and $k \geq 2$. A trapdoor for A is a matrix $T_A \in \mathbb{Z}^{\overline{m}\times(k-1)z}$, where $\overline{m} = m + (k-1)z$, such that $A \begin{bmatrix} T_A \\ I \end{bmatrix} = HG$ for some invertible matrix $H \in \mathbb{Z}_q^{n\times n}$ and identity matrix $I \in \mathbb{Z}^{(k-1)z\times(k-1)z}$. H is the tag matrix and can be the identity matrix I.*

5 PROPOSED SCHEME

In this section, we detail the algorithms related to the basic building blocks (ABE, IBE and Lattice-based cryptographic) and then use these algorithms to construct our proposed scheme.

5.1 Building Blocks

We start with the mathematical details of ABE, IBE and Lattice-based schemes.

5.1.1 ABE

The Waters (2011) scheme consists four algorithms:

Setup$_{ABE}(\mathbb{U})$: Let $\mathbb{U}$ be a set of attributes, and $\mathbb{G}_1$ and $\mathbb{G}_2$ cyclic groups of prime order p with the bilinear pairing (Definition 4.1). First choose $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$ and random elements $h_1, ..., h_l \in \mathbb{G}_2$ associated with attributes from $\mathbb{U}$, where l is the number of attributes. In addition, choose two random exponents α_A, $a \in \mathbb{Z}_p$ (where the A in α_A represents ABE). The function Setup$_{ABE}$ outputs a master public key mpk_A and a master private key msk_A as follows:

$$\mathsf{mpk}_A = (g_1, e(g_1, g_2)^{\alpha_A}, g_2^a, h_1, ..., h_l), \ \mathsf{msk}_A = g_2^{\alpha_A}. \quad (3)$$

Encrypt$_{ABE}(\mathsf{mpk}_A, \mathcal{M}, (M, \rho))$: It takes mpk_A, a message $\mathcal{M}$ and access structure (M, ρ), where M is the share generating matrix and ρ is a function that links attributes in $\mathbb{U}$ to the rows of M (Definition 4.2). Choose a random secret s and variables $y_2, ..., y_n \in \mathbb{Z}_P$, and define a vector $v = (s, y_2, ..., y_n) \in \mathbb{Z}_p^n$. Then calculate $\lambda_i = M_i \cdot v$ from (Definition 4.2). The Encrypt$_{ABE}$ function chooses random $r_1, ..., r_l \in \mathbb{Z}_p$ and calculates ciphertext $C_A = (C, C', \{C_i, D_i\}_{i=1}^l)$ as follows:

$$\begin{aligned} C = \mathcal{M} \cdot e(g_1, g_2)^{\alpha_A s}, \quad C' = g_1^s, \\ \{C_i = g_2^{a\lambda_i} h_i^{-r_i}, \ D_i = g_1^{r_i}\}_{i\in I}. \end{aligned} \quad (4)$$

The Encrypt function outputs C_A.

KeyGen$_{ABE}(\mathsf{mpk}_A, \mathsf{msk}_A, \widehat{\mathbb{U}})$: Given the master public key mpk_A, the master secret key msk_A, an attributes set $\widehat{\mathbb{U}}$ and a random $t \in \mathbb{Z}_p$, generate a private key $\mathsf{sk}_S = (K, L, K_{\rho(i)})$ as follows:

$$K = g_2^{\alpha_A} g_2^{at}, L = g_1^t, \ \forall \rho(i) \in \widehat{\mathbb{U}}, i \in I : K_{\rho(i)} = h_i^t. \quad (5)$$

Decrypt$_{ABE}(C_A, \mathsf{sk}_S)$: Given mpk_A, sk_S, and $\mathbb{U}$, which qualifies access structure (M, ρ) and $I \subset \{1, 2, ..., l\}$ as $I = \{i : \rho(i) \in \widehat{\mathbb{U}}\}$, there exists a set of constants $\{\omega_i \in \mathbb{Z}_p\}_{i\in I}$ such that $\sum_{i\in I} \omega_i\lambda_i = s$ (Definition 4.2). The Decrypt$_{ABE}$ function decrypts as follows:

$$\begin{aligned} \mathcal{M} &= \frac{C \cdot \prod_{i\in I} \left(e(L, C_i) \cdot e(D_i, K_{\rho(i)})\right)^{\omega_i}}{e(C', K)}, \\ &= \frac{\mathcal{M} \cdot e(g_1, g_2)^{\alpha_A \, s} \cdot \prod_{i\in I} e(g_1, g_2)^{a\omega_i\lambda_i t}}{e(g_1, g_2)^{\alpha_A \, s} \cdot e(g_1, g_2)^{ast}}. \end{aligned} \quad (6)$$

5.1.2 IBE

The IBE scheme designed by Boneh and Boyen (2004) is a collection of four algorithms.

Setup$_{IBE}$: Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be cyclic groups of prime order p (Definition 4.1). First, choose elements $g_5, h_{ID} \in \mathbb{G}_1$, $g_3, g_4 \in \mathbb{G}_2$, and $\alpha_I \in \mathbb{Z}_p$ (where the I in α_I represents IBE) to calculate $g_4 = g_3{}^{\alpha_I}$. Then, Setup$_{IBE}$ outputs a master public key mpk_I and a master secret key msk_I as follows:

$$\mathsf{mpk}_I = (g_3, g_4, g_5, h_{ID}),\ \mathsf{msk}_I = \alpha_I. \tag{7}$$

Encrypt$_{IBE}(\mathsf{mpk}_I, \mathcal{M}, ID)$: Taking an identity ID, mpk_I and $\mathcal{M} \in \mathbb{G}_T$ as input and choosing random $w' \in \mathbb{Z}_p$ to output a ciphertext C_I as follows:

$$C_I = (C_I^1, C_I^2, C_I^3) = (g_3^{w'}, (g_5^{ID} h_{ID})^{w'}, \mathcal{M}.e(g_5, g_4)^{w'}). \tag{8}$$

KeyGen$_{IBE}(\mathsf{mpk}_I, \mathsf{msk}_I, ID)$: Given mpk_I, msk_I and ID as input, this function picks a random $u \in \mathbb{Z}_p$ and generates a private key sk_{ID} for ID as follows:

$$\mathsf{sk}_{ID} = (SK_{ID}^1, SK_{ID}^2) = (g_5^{\alpha_I}(g_5^{ID} h_{ID})^u, g_3^u). \tag{9}$$

Decrypt$_{IBE}(C_I, \mathsf{sk}_{ID})$: Given CT_{ID} and sk_{ID} as input, this function computes $\mathcal{M}$ as follows:

$$\mathcal{M} = \frac{C_I^3 \cdot e(C_I^2, SK_{ID}^2)}{e(SK_{ID}^1, C_I^1)}. \tag{10}$$

5.1.3 Learning with Error - Lattice-Based Cryptography (LWE-LBC)

LWE-LBC (Lindner and Peikert, 2011) scheme is a collection of the following four algorithms.

Setup$_{LBC}$ takes a system security parameter Ψ and defines $\mathcal{X} = \mathcal{X}(\Psi)$ to be a Gaussian distribution $\mathcal{D}_{\mathbb{Z}_q}$. It chooses positive integers m, n, q, where q is prime, and generates a lattice (Definition 4.4) of n linearly independent vectors of length m with an $m \times n$ matrix $A = \{a_1, ..., a_n\} \in \mathbb{Z}_q^n$ using uniform distribution and a trapdoor T_A using $TrapGen(n)$ (Definition 4.6), where the master public key $\mathsf{mpk}_L = A$ and the master secret key $\mathsf{msk}_L = T_A$.

KeyGen$_{LBC}(A, m, n, q, \mathcal{X})$ takes positive integers m, n, q, and $\mathcal{X}$ as input and chooses random error vector $\{e_1, ..., e_m\} \in \mathcal{X}$. Then it chooses uniform short vector $\gamma \in \mathbb{Z}_q^n$ from a Gaussian distribution for basis of T_A as a secret key and generates the public key as follows:

$$\mathsf{pk}_L = \{\beta_i\}_{i=1}^n \ where\ \beta_i = < A, \gamma > + e_i \ mod\, q. \tag{11}$$

Encrypt$_{LBC}(\mathsf{mpk}_L, \mathsf{pk}_L, \mathcal{M})$ takes mpk_L, pk_L and $m \in \mathcal{M}$ as input. Then, it chooses random $s' \in \mathbb{Z}_q^m$ to generate the ciphertext $C_L = (u, v)$ as follows:

$$u := (A^T s' + e_1) \quad v := \beta^T s' + e_2 + \lceil q/2 \rfloor .m. \tag{12}$$

Decrypt$_{LBC}(C_L, \gamma)$: This function takes a secret key γ and C_L and outputs a message $m \in \mathcal{M}$ as follows:

$$m := (v - \gamma^T u). \tag{13}$$

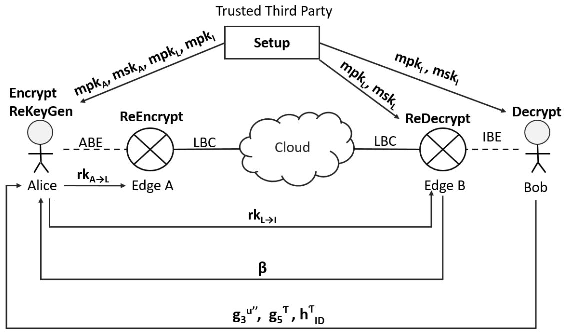

Figure 3: Construction of $\mathfrak{L}$_ABE-IBE Proxy Re-encryption Scheme between Alice and Bob.

5.2 Construction of $\mathfrak{L}$_ABE-IBE PRE

We construct a classical to post-quantum secure ABE-IBE proxy re-encryption ($\mathfrak{L}$_ABE-IBE PRE) scheme using the basic building blocks. Our scheme consists of seven algorithms, and four of them are as follows:

- **Setup** $= \langle$Setup$_{ABE}$, Setup$_{IBE}$, Setup$_{LBC}\rangle$.
- **KeyGen** $= \langle$KeyGen$_{ABE}$, KeyGen$_{IBE}$, KeyGen$_{LBC}\rangle$.
  - Alice chooses a random $t \in \mathbb{Z}_p$ and executes KeyGen$_{ABE}$ to generate her private key sk_S for a set of attributes $\mathbb{U}$.
  - Bob chooses a random $u \in \mathbb{Z}_p$ and executes KeyGen$_{IBE}$ for his ID to generate his private key sk_{ID}.
  - Edge-B chooses a random uniform secret vector $\gamma \in \mathbb{Z}_q^n$ and generates β for a uniform random matrix A using KeyGen$_{LBC}$ algorithm.
- **Encrypt** $= \langle$Encrypt$_{ABE}(\mathsf{mpk}_A, \mathcal{M}, (M, \rho)\rangle$: Alice executes the Encrypt$_{ABE}$ algorithm defined in Eq. (4).
- **Decrypt**(C_I, sk_{ID}): This function is derived from Eq. (10). Bob receives an IBE ciphertext C_I from Eq. (18) and uses his private key sk_{ID} to execute the following Decrypt algorithm to get a message $\mathcal{M}$.

$$\mathcal{M} = \frac{C_I}{e(\mathsf{sk}_{ID}^1 \cdot (g_5^{ID} h_{ID})^{u'}, g_3^{\tau})}. \tag{14}$$

The other three algorithms are: ReKeyGen, ReEncrypt and ReDecrypt.

More precisely, Alice executes ReKeyGen algorithm, and Edge-A and Edge-B execute ReEncrypt and ReDecrypt algorithms, respectively, and finally Bob executes Decrypt algorithm (Eq. (14)). The working of our proposed scheme using these algorithms is illustrated in Fig. 3.

$(\mathsf{rk}_{A \to L}, \mathsf{rk}_{L \to I}) \leftarrow$**ReKeyGen**$(\mathsf{mpk}_A, \mathsf{mpk}_I, \mathsf{mpk}_L, \widehat{\mathbb{U}}, ID, \mathsf{sk}_S, \mathsf{sk}_{ID}^2{}', g_5^{\tau}, h_{ID}^{\tau})$: Given the parameters mpk_A (Eq. (3)), mpk_I (Eq. (7)), mpk_L (Eq. (11)), Alice's private key sk_S, Bob's identity ID, three components $\mathsf{sk}^{2}_{ID}{}'$, g_5^{τ} and h^{τ}_{ID} from Bob, and pk_L from Edge-B. Alice and Bob execute the following steps to generate re-encryption and re-decryption keys:

- Bob chooses two random variables $u', \tau \in \mathbb{Z}_p$, and computes $\mathsf{sk}^{2}_{ID}{}' = \mathsf{sk}^{2}_{ID} . g_3^{u'} = g_3^{u''}$ and g_5^{τ}, where $u + u' = u''$. Bob shares sk^{2}_{ID}, g_5^{τ}, and h^{τ}_{ID} with Alice.
- Edge-B chooses β and generates a secret γ from a Gaussian distribution for a uniform random matrix A. Edge-B share β with Alice.

Alice generates the re-encryption key $\mathsf{rk}_{A\to L}$ for Edge-A and re-decryption key $\mathsf{rk}_{L\to I}$ for Edge-B as follows:

$$\begin{aligned} R_a =& K \cdot g_2^{a \cdot ID} \cdot \mathsf{sk}^{2}_{ID}{}' = g_2^{\alpha_A} g_2^{at} g_2^{a \cdot ID} g_3^{u''}, \\ R_b =& \{\hat{L}, \hat{K_{\rho(i)}}\} = \{L \cdot g_1^{ID}, K_{\rho(i)} \cdot h_i^{ID}\}_{\rho(i) \in \widehat{\mathbb{U}}}, \\ R_c =& g_5^{\tau \cdot ID} \cdot h^{\tau}_{ID},\ R_d = \langle A, \beta \rangle,\ R_e = e(g_5^{\tau}, g_4). \end{aligned} \tag{15}$$

Edge-A receives $\mathsf{rk}_{A\to L} = (R_a,\ R_b,\ R_c,\ R_d)$ to re-encrypt ABE ciphertext to post-quantum ciphertext and Edge-B receives $\mathsf{rk}_{L\to I} = (R_e)$ to transform post-quantum ciphertext to IBE ciphertext.

$C_L \leftarrow$ **ReEncrypt**$(\mathsf{rk}_{A\to L}, C_A)$: For $\mathsf{rk}_{A\to L}$ and ABE ciphertext $C_A = (C, C', \{C_i, D_i\}_{i=1}^{l})$ (Eq. (4)), Edge-A performs ReEncrypt to output a post-quantum ciphertext $C_L = (C_L^1, C_L^2)$. Let $\{\omega_i \in \mathbb{Z}_p\}_{i\in I}$ be a set of constants such that if λ_i are valid shares of any secret s, then $\sum_{i\in I} \omega_i \lambda_i = s$ (Definition 4.2). Then compute C_2 using C_i and D_i for all $i = 1, \cdots, l$, where

$$\begin{aligned} C_1^{'} =& \frac{C \cdot e(C^{'} R_c, g_3^{u''})}{e(C^{'}, R_a)}, \\ C_2^{'} =& \prod_{i=1}^{l} (e(\hat{L}, C_i) \cdot e(D_i, \hat{K_{\rho(i)}}))^{\omega_i}. \end{aligned} \tag{16}$$

$C_1^{'}$ and $C_2^{'}$ lie on the bilinear vector space $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Using the bilinear vector space, given bilinear results $C_1^{'} = \{x_1, y_1\}$ and $C_2^{'} = \{x_2, y_2\}$, we use the *Encode* function as $\vec{a}1 = Encode(x_1, y_1)$ where $\{a1_1, \cdots, a1_{n/2}\} \leftarrow x_1$ and $\{a1_{n/2+1}, \cdots, a1_n\} \leftarrow y_1$. Similarly, we use the *Encode* function for $C_2^{'}$ to get $\vec{a}2$. Transformed vectors are symmetric, non-degenerate and bilinear under vector space of map e. These transformed vectors $\vec{a}1$ and $\vec{a}2$ are used as an input to a black box lattice-based encryption function (Ioannou and Mosca, 2011) to output the post-quantum secure ciphertext as follows:

$$\begin{aligned} C_L^1 = (u_1, v_1) = (A^T s' + e_1, \beta^T s' + e_2 + \lceil q/2 \rfloor \cdot a1), \\ C_L^2 = (u_2, v_2) = (A^T s' + e_1, \beta^T s' + e_2 + \lceil q/2 \rfloor \cdot a2), \end{aligned} \tag{17}$$

where the output is $C_L = (C_L^1, C_L^2)$.

$C_I \leftarrow$ **ReDecrypt**$(\mathsf{rk}_{L\to I}, C_L, \gamma)$ takes C_L, $\mathsf{rk}_{L\to I}$ and a secret vector γ. Edge-B performs ReDecrypt algorithm and decodes the results to bilinear vectors (Bartocci et al., 2009) using the *Decode* function as follows:

$$\begin{aligned} r1 :=& (v_1 - \gamma^T u_1),\ r2 := (v_2 - \gamma^T u_2), \\ D_L^1(x,y) =& Decode(r1), \\ D_L^2(x,y) =& Decode(r2), \\ C_I =& \mathsf{rk}_{L\to I} \cdot D_L^1 \cdot D_L^2. \end{aligned} \tag{18}$$

The ciphertext C_L is post-quantum secure and stored on the cloud, while Bob works in the classical IBE domain. Therefore, the ReDecrypt algorithm on the Edge-B transforms this post-quantum secure ciphertext into classical IBE ciphertext, making it suitable for Bob to decrypt using his secret key. Moreover, Edge-B also performs multiplication operations on decoded ciphertexts to reduce the number of operations on Bob's side without leaking any information about the encrypted message (i.e., IBE ciphertext) to Edge-B. Bob uses the output ciphertext C_I to perform decryption as defined in Eq. (14).

5.3 CBDH Assumption

Given cyclic groups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ of prime order p, generators g_x of $\mathbb{G}_1$ and g_y of $\mathbb{G}_2$, and bilinear mapping $e : (\mathbb{G}_1 \times \mathbb{G}_2) \to \mathbb{G}_T$ (Definition 4.3), let $a, b \in \mathbb{Z}_p$ be randomly chosen. Consider a polynomial time adversary $\mathcal{A}$ in the CBDH problem who takes the tuple $(\mathbb{G}_1, \mathbb{G}_2, p, g_x, g_y, g_x^a, g_x^b, g_y^a, g_y^b)$ as an input, and outputs $e(g_x, g_y)^{ab}$ with advantage

$$Adv_{\mathcal{A}} = \Pr\left[\mathcal{A}(\mathbb{G}_1, \mathbb{G}_2, p, g_x, g_y, g_x^a, g_x^b, g_y^a, g_y^b) = e(g_x, g_y)^{ab}\right] \tag{19}$$

Definition 5.1. *The CBDH assumption holds if there exists no PPT adversary with non-negligible advantage (defined above) in solving the CBDH problem.*

5.4 Hard Assumptions of $\mathfrak{L}$_ABE-IBE

The key actors involved are Alice as a sender, Bob as a receiver, and a trusted third party (TTP). In the proposed scheme, the collusion of all the communicating parties, except Alice, will not allow an adversary to retrieve Alice's secret key. Trusted third parties (TTP) may be compromised, and corruption of master secret keys can affect re-encryption and re-decryption algorithms. However, TTP will not leak any information about Alice and Bob's encrypted message or secret keys to adversary at edge nodes.

Moreover, the local edge nodes perform re-encryption and re-decryption of ciphertexts. However, the generation of correct or incorrect ciphertexts from these algorithms entirely depends on parameters, such as master keys, private keys, random and independent variables. Based on hardness assumptions i.e., CBDH and LWE, in our proposed $\mathfrak{L}$_ABE-IBE PRE scheme, if all the parties involved in communication are corrupted, the ReEncrypt and ReDecrypt algorithms will still generate random indistinguishable ciphertexts. In the following subsection, the security of the proposed scheme is modeled as a game.

5.5 Security Game of Proposed Scheme

The indistinguishability security of our proposed $\mathfrak{L}$_ABE-IBE scheme is modeled by a game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. $\mathcal{C}$ generates $\mathfrak{L}$_ABE-IBE, while $\mathcal{A}$ tries to break it. To start, $\mathcal{C}$ generates the master key pairs $(\mathsf{mpk}_A, \mathsf{msk}_A)$ and $(\mathsf{mpk}_I, \mathsf{msk}_I)$. $\mathcal{A}$ has access to master public keys mpk_I and mpk_A, while master secret keys msk_A and msk_I are not known to $\mathcal{A}$. $\mathcal{A}$ then outputs two message m_0 and m_1 from the message space, an access structure $(M,\rho)^*$ for a set of attributes $\widehat{\mathbb{U}}^*$ and identity ID^* to be challenged. The challenger $\mathcal{C}$ generates two classical challenge ciphertexts C_A^* and C_I^* for the given $(M,\rho)^*$ and ID^*, and one post-quantum secure challenge ciphertext C_L^* for the given A^* and β^*. Note a classical adversary $\mathcal{A}$ tries to break C_A^* and C_I^* while a quantum adversary $\mathcal{A}_L$ tries to break C_L^*.

During the game, $\mathcal{A}$ can make private key queries on any access structure and identity other than the challenge access structure and challenge identity. In particular, $\mathcal{A}$ can make re-encryption and decryption queries on $((M,\rho),ID,C_A,C_I)$ satisfying either $(M,\rho) \neq (M,\rho)^*$ or $ID \neq ID^*$ or $C_A \neq C_A^*$ or $C_I \neq C_I^*$. Similarly $\mathcal{A}_L$ make post-quantum encryption queries on $(A,\gamma,T_A C_L)$, where $A \neq A^*$ or $\gamma \neq \gamma^*$ or $T_A \neq T_A^*$. $\mathcal{A}$ guesses the chosen message in the challenge ciphertexts C_A^* and C_I^*, and $\mathcal{A}_L$ guesses the encrypted ciphertext C_A in the post-quantum challenge ciphertext C_L^*. Here we only give the classical security game. The details of post-quantum security of challenge ciphertext C_L^* against $\mathcal{A}_L$ are given under Theorem 3.

The selective indistinguishability game against chosen-ciphertext attacks (IND-sCCA) is as follows:

1. **Setup:** Challenger $\mathcal{C}$ runs this algorithm to generate master key pairs $(\mathsf{mpk}_A, \mathsf{msk}_A)$ and $(\mathsf{mpk}_I, \mathsf{msk}_I)$ and sends mpk_A and mpk_I to $\mathcal{A}$, but keeps master keys msk_A and msk_I secret for queries from $\mathcal{A}$.
2. **Phase 1**: $\mathcal{A}$ can make the following queries.
   - **Key Queries:** $\mathcal{A}$ chooses a set of attributes $\mathbb{U}$ and an identity ID. Then $\mathcal{A}$ makes key queries and $\mathcal{C}$ runs key generation algorithms KeyGen_{ABE} and KeyGen_{IBE} to return the sk_S and sk_{ID} respectively to the $\mathcal{A}$.
   - **Decryption Queries:** For chosen C_A and C_I, the $\mathcal{A}$ makes decryption queries. $\mathcal{C}$ runs $\mathsf{Decrypt}_{ABE}$ and $\mathsf{Decrypt}_{IBE}$ and returns result to the $\mathcal{A}$.
   - **ReKey Queries:** $\mathcal{A}$ makes re-encryption key queries on $(\mathbb{U},(M,\rho),\mathsf{sk}_S,ID)$, $\mathcal{C}$ runs ReKeyGen and returns $\mathsf{rk}_{A\to L}$ and $\mathsf{rk}_{L\to I}$ to the $\mathcal{A}$.
3. **Challenge:** $\mathcal{A}$ adaptively chooses two messages m_0 and m_1 from a message space, an access structure $(M,\rho)^*$ and an identity ID^* to be challenged. We restrict the access structure $(M,\rho)^*$ and the identity ID^* to that not previously queried in **Phase 1**. $\mathcal{C}$ randomly chooses $c \in \{0,1\}$ and computes the two classical challenge ciphertexts; one before re-encryption $C_A^* = E[\mathsf{mpk},(M,\rho)^*,m_c]$ and other after re-decryption $C_I{}^* = ReDec[\mathsf{rk}^*_{L\to I}, ReEnc[mpk, \mathsf{rk}^*_{A\to L}, C_A{}^*]]$, and one post-quantum ciphertext C_L^* where $\mathsf{rk}^*_{A\to L} \neq \mathsf{rk}_{A\to L}$ and $\mathsf{rk}^*_{L\to I} \neq \mathsf{rk}_{L\to I}$.
4. **Phase 2:** $\mathcal{C}$ responds to all private-key queries, re-key queries and decryption queries from $\mathcal{A}$ in the same way as in **Phase 1** with restriction that the $\mathcal{A}$ can not make private key queries on $(M,\rho)^*$ and ID^*, and no decryption queries on either $((M,\rho)^*,C_A^*)$ or (ID^*,C_I^*).
5. **Guess:** The adversary $\mathcal{A}$ outputs a guess c' of c and wins the game if $c' = c$. The advantage ε of the $\mathcal{A}$ in winning this game is defined as

$$\varepsilon = 2(\Pr[c' = c] - 1/2). \tag{20}$$

Definition 5.2. *The scheme is said to be IND-sCCA secure, if there exists no probabilistic polynomial time (PPT) adversary having non-negligible advantage in the above mentioned game.*

5.6 Correctness of $\mathfrak{L}$_ABE-IBE PRE

We prove the correctness of $\mathfrak{L}$_ABE-IBE PRE using the following Theorem.

THEOREM 1 (Correctness). *Given a $\mathfrak{L}$_ABE-IBE PRE scheme. If the reverse substitution of parameters from the* Decrypt *function to* Encrypt *function (from Section 5) yields the message $\mathcal{M}$, then the scheme is correct.*

Proof: We start with the IBE decryption algorithm (Eq. (14)) and apply reverse substitution of security parameters or equations up to the encryption algorithm given in Eq. (4). We start with Eq. (14) and substitute Bob's private secret key as follows:

$$\mathcal{M} = \frac{C_I}{e(\mathsf{sk}_{ID}^1 \cdot (g_5^{ID} h_{ID})^{u'}, g_3^{\tau})},$$
$$= \frac{C_I}{e(g_5^{\alpha_I} \cdot (g_5^{ID} h_{ID})^{u} \cdot (g_5^{ID} h_{ID})^{u'}, g_3^{\tau})},$$

where $u + u' = u''$. Substituting C_I from Eq. (18):

$$\mathcal{M} = \frac{R_{L\to I} \cdot D_L^1 \cdot D_L^2}{e(g_5^{\alpha_I} \cdot (g_5^{ID} h_{ID})^{u''}, g_3^{\tau})}.$$

We apply decode function on $D1$ and $D2$ (Eq. (18)), and re-decryption function for a secret vector γ and $\mathsf{rk}_{L\to I}$ (Eq. (15)) to reduce the above as:

$$\mathcal{M} = \frac{e(g_5^{\tau}, g_4) \cdot (v_1 - \gamma^T u_1) \cdot (v_2 - \gamma^T u_2)}{e((g_5^{\alpha_I} \cdot g_5^{ID} h_{ID})^{u''}, g_3^{\tau})}.$$

Applying $g_4 = g_3^{\alpha_I}$ from Eq. (7), substituting functions from Eq. (17) and *Encode* to transform resulting $\{x_1, y_1\}$ and $\{x_2, y_2\}$ to C_1' and C_2' respectively, gives:

$$\mathcal{M} = \frac{e(g_5^{\tau}, g_3^{\alpha_I}) \cdot \{x_1, y_1\} \cdot \{x_2, y_2\}}{e(g_5^{\alpha_I} \cdot (g_5^{ID} h_{ID})^{u''}, g_3^{\tau})},$$
$$= \frac{C_1' \cdot C_2'}{e((g_5^{ID} h_{ID})^{u''}, g_3^{\tau})}.$$

Substituting C_1' and C_2' from Eq. (16):

$$\mathcal{M} = \frac{C \cdot e(C' R_c, g_3^{u''}) \cdot \prod_{i=1}^{l} (e(\hat{L}, C_i) \cdot e(D_i, \hat{K_{\rho(i)}}))^{\omega_i}}{e(C', R_a).e((g_5^{ID} h_{ID})^{u''}, g_3^{\tau})}.$$

Substituting C, C', C_i and D_i from Eq. (4):

$$\mathcal{M} = \frac{\mathcal{M} \cdot e(g_1, g_2)^{\alpha_A s} \cdot e(g_1^s R_c, g_3^{u''}) \cdot e(g_1^t g_1^{ID}, g_2^{as})}{e(g_1^s, R_a).e((g_5^{ID} h_{ID})^{u''}, g_3^{\tau})},$$

where $\sum_{i=1}^{l} \omega_i \lambda_i = s$. Applying re-encryption key $\mathsf{rk}_{A\to L}$ (Eq. (15)) and bilinear pairing properties as follows.

$$\mathcal{M} = \frac{\mathcal{M} \cdot e(g_1, g_2)^{\alpha_A s} \cdot e(g_1^s g_5^{\tau \cdot ID} h_{ID}^{\tau}, g_3^{u''}) \cdot e(g_1^t g_1^{ID}, g_2^{as})}{e(g_1^s, g_2^{\alpha_A} g_2^{at} g_2^{a \cdot ID} g_3^{u''}).e((g_5^{ID} h_{ID})^{u''}, g_3^{\tau})},$$
$$= \mathcal{M}. \qquad \square$$

Based on this, we give the following corollary.

Corollary 1.1. *If reverse substitution method yields a message $\mathcal{M}$, then our proposed $\mathfrak{L}$_ABE-IBE proxy re-encryption scheme is correct.*

6 SECURITY ANALYSIS

We consider the following theorem to analyze that our proposed $\mathfrak{L}$_ABE-IBE PRE scheme is selectively IND-sCCA secure (Section 5.5):

THEOREM 2. *Given a $\mathfrak{L}$_ABE-IBE PRE scheme. Assuming the CBDH problem is intractable, then the scheme is IND-sCCA secure.*

Sketch of Proof. We illustrate the security of the proposed scheme as a game played between adversary $\mathcal{A}$ and challenger $\mathcal{C}$. In **Setup** phase, $\mathcal{C}$ computes the master public keys and shares them with $\mathcal{A}$. In **Phase 1**, $\mathcal{A}$ can make an unlimited number of private key, re-key, and decryption queries for the challenge ciphertexts. Once **Phase 1** is over, we restrict $\mathcal{A}$ from making any key or decryption queries to $\mathcal{C}$. Then $\mathcal{A}$ selects two messages from the message space, any attribute set, and identity for a challenge with restrictions that $\mathcal{A}$ has not queried these attributes and identity in **Phase 1**. $\mathcal{C}$ randomly selects one of the messages and computes the challenge ciphertexts using encryption and re-encryption algorithms. $\mathcal{C}$ presents challenge ciphertexts to $\mathcal{A}$ to break. The target of $\mathcal{A}$ is to correctly guess the ciphertext generated from one of the two known messages. Here the CBDH assumptions come into play when $\mathcal{C}$ generates the challenge ciphertexts for $\mathcal{A}$. Moreover, the simulator $\mathcal{B}$ simulates the scheme as closely related to the proposed scheme as possible such that $\mathcal{A}$ cannot distinguish between the simulated and real schemes. Below in detailed proof, we use $\mathcal{B}$ instead of the challenger $\mathcal{C}$ to respond to the adversary's queries (Guo et al., 2018).

Detailed Proof. Let there exist a PPT adversary $\mathcal{A}$ who can $(t, q_k, q_d, \varepsilon)$-break the $\mathfrak{L}$_ABE-IBE PRE scheme, where t is time cost, q_k is number of key queries, q_d is number of decryption queries, and ε is the advantage of $\mathcal{A}$. We construct a simulator $\mathcal{B}$ to solve the CBDH problem. Given the instance of the problem $(g_x, g_x^a, g_x^b, g_x^c, g_y, g_y^a, g_y^b, g_y^c)$ over the pairing group $\mathbb{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, g_x, g_y, e)$ as an input, $\mathcal{B}$ runs $\mathcal{A}$ and works as follow:

Init: $\mathcal{A}$ outputs an access structure $(M, \rho)^*$ and an identity ID^*.

Setup: $\mathcal{B}$ randomly selects $x_1, x_2, x_3, y_1, y_2 \in \mathbb{Z}_p$ and computes master public keys:

$$e(g_1, g_2)^{\alpha_A} = e(g_x, g_y)^{x_1 + ab} = e(g_x, g_y)^{x_1} e(g_x, g_y)^{ab},$$
$$g_1 = g_x,\ g_2 = g_y^{x_2 + a},\ g_3 = g_y,$$
$$g_4 = g_3^{\alpha_I} = g_y^{y_1 + ac} = g_y^{y_1} g_y^{ac},\ g_5 = g_x^b,$$

where $\alpha_A = x_1 + ab$, $\alpha_I = y_1 + ac$, and a, b, c are from problem instance. The master public keys are

$$\mathsf{mpk}_A = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_x, g_y^{x_2 + a}, e(g_x, g_y)^{x_2} e(g_x, g_y)^{ab}, h_{i=1}^{l}\},$$
$$\mathsf{mpk}_I = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_y, g_y^{y_1} g_y^{ac}, g_x^b, h_{ID}\}.$$

$\mathbf{h}_i$ Queries: For the set of attributes $\widehat{\mathbb{U}}$, $\mathcal{B}$ chooses h_i for $1 \le i \le l$ uniformly from $\mathbb{G}_2$ and sends to $\mathcal{A}$.

$\mathbf{h}_{ID}$ Queries: For the identity ID, $\mathcal{B}$ chooses a random value h_{ID} from $\mathbb{G}_1$ and sends to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ makes private-key, re-key, and decryption queries in this phase. For the private-keys and re-key queries, $\mathcal{A}$ chooses $(M,\rho) \neq (M,\rho)^*$ and $ID \neq ID^*$. $\mathcal{B}$ chooses $t', t'' \in \mathbb{Z}_p$ and computes

$$\begin{aligned} K =& g_y^{x_1+ab} g_y^{(x_2+a)t'}, L = g_x^{t'}, K_i = h_i^{t'}, \\ SK_{ID}^1 =& g_x^{b(y_1+ac)} (g_x^{bID} h_{ID})^{t''}, SK_{ID}^2 = g_y^{t''}, \end{aligned}$$

and constructs: $\mathsf{sk}_S = (K, L, K_i)$, $\mathsf{sk}_{ID} = (SK_{ID}^1, SK_{ID}^2)$.

For re-key queries, $\mathcal{B}$ chooses random τ, $t_1{}'' \in \mathbb{Z}_p$ where $t'' + t_1'' = t_2''$ and computes:

$$\begin{aligned} R_a =& K.g_y^{(x_2+a)ID} \mathsf{sk}_{ID}^2{}' = g_y^{x_1+ab} g_y^{(x_2+a)t'} g_y^{(x_2+a)ID} g_y^{t_2''}, \\ R_b =& (L \cdot g_x^{ID}, K_i \cdot h_i^{ID}) = (g_x^{t'} g_x^{ID}, h_i^{t'} h_i^{ID}), \\ R_c =& g_x^{b\tau ID} \cdot h_{ID}^{\tau}, \text{ and } R_e = e(g_x^{b\tau}, g_x^{y_1+ac}), \end{aligned}$$

where $\mathsf{rk}_{A \to L} = (R_a, R_b, R_c)$ and $\mathsf{rk}_{L \to I} = R_e$.

For a decryption queries on $((M,\rho), ID, C_A, C_I)$, suppose $C_A = (C, C', C_i, D_i)$ and C_I derives from D_L^1 and D_L^2. If $(M,\rho) \neq (M,\rho)^*$ and $ID \neq ID^*$, $\mathcal{B}$ generates the corresponding private keys and re-keys to perform decryption of C_A and C_I. For $(M,\rho) = (M,\rho)^*$, $\mathcal{B}$ continuous the simulation if it satisfies $\sum_{i \in I} \omega_i \lambda_i = s$ for a set of constants ω_i. If $\sum_{i \in I} \omega_i \lambda_i \neq s$, it aborts the simulation. Then $\mathcal{B}$ uses (M,ρ) to compute

$$\begin{aligned} d =& \prod_{i \in I} \left(e(L, C_i) \cdot e(D_i, K_i)\right)^{\omega_i}, \\ =& \prod_{i \in I} \left(e(g_x^{t'}, g_y^{(x_2+a)\lambda_i} h_i^{-r_i}) \cdot e(g_x^{r_i}, h_i^{t'}) \right)^{\omega_i}, \\ =& \prod_{i \in I} e(g_x, g_y)^{(x_2+a)\omega_i \lambda_i t'}, \\ =& \prod_{i \in I} \left(e(g_x, g_y)^{x_2 \omega_i \lambda_i t'} \cdot e(g_x, g_y)^{a \omega_i \lambda_i t'} \right). \end{aligned}$$

Therefore for valid (M,ρ) satisfying $\sum_{i \in I} \omega_i \lambda_i = s$, the simulator $\mathcal{B}$ uses d to decrypt C_A.

Similarly for $ID = ID^*$, $\mathcal{B}$ continues the decryption ($\mathsf{Decrypt}_{IBE}$) of C_I. $\mathcal{B}$ searches h_{ID} from the list of $\mathbf{h}_{ID}$ and chooses random τ, $t_2'' \in \mathbb{Z}_p$ where $t'' + t_1'' = t_2''$ satisfying ID. $\mathcal{B}$ computes d' as

$$\begin{aligned} d' =& e\left(\mathsf{sk}_{ID}^1 \cdot (g_x^{bID} h_{ID})^{u'}, g_y^{\tau} \right), \\ =& e\left(g_x^{b(y_1+ac)} (g_x^{bID} h_{ID})^{t''} \cdot (g_x^{bID} h_{ID})^{t_1''}, g_y^{\tau} \right), \\ =& e(g_x, g_y)^{by_1\tau} \cdot e(g_x, g_y)^{abc\tau} \cdot e(g_x, g_y)^{bIDt_2''\tau} \cdot e(h_{ID}, g_y)^{t_2''\tau}. \end{aligned}$$

Let $IDt_2'' = -b(y_1 + ac)$, then we have $d' = e(h_{ID}, g_y)^{t_2''\tau}$. Therefore, $\mathcal{B}$ uses d' for valid t_2'' and randomly chosen τ to decrypt ciphertext C_I. Here we distinguish two cases as follow:

- Case I: For the queries satisfying the conditions and hash mentioned above, $\mathcal{B}$ returns the correct challenge ciphertext to $\mathcal{A}$.
- Case II: For the queries not satisfying the conditions mentioned in the above equations, the simulator returns incorrect challenge ciphertext to $\mathcal{A}$.

Challenge: $\mathcal{A}$ adaptively chooses two distinct messages m_0 and m_1, a challenge access structure $(M,\rho)^*$, and a challenge identity ID^*. $\mathcal{B}$ randomly flips the coin $c \in \{0,1\}$ and sets the challenge ciphertext $C_A^* = (C^*, C'^*, C_i^*, D_i^*)$ as

$$C_A^* = (m_c \cdot e(g_x, g_y)^{(x_1+ab)s}, g_x^s, g_y^{(x_2+a)\lambda_i^*} h_i^{-r_i}, g_x^{r_i}).$$

$\mathcal{B}$ returns challenge C_A^* to $\mathcal{A}$. At this stage, there exists the two more cases for computing C_I^* from C_A^* as follows.

- Case I: $\mathcal{B}$ utilizes the challenge C_A^* generated in the above step to compute challenge C_I^*.
- Case II: $\mathcal{A}$ randomly chooses C_A^* and $\mathcal{B}$ uses that C_A^* to compute the challenge C_I^*.

$\mathcal{B}$ computes the challenge C_I^* for the identity ID^* as

$$\begin{aligned} C_I^* =& \mathsf{rk}_{L \to I}^* \cdot m_c \cdot e\left((g_x^{bID^*} h_{ID^*})^{\tau}, g_y^{t_2''} \right), \\ =& e(g_x^{b\tau}, g_y^{y_1+ac}) \cdot m_c \cdot e\left((g_x^{bID^*} h_{ID^*})^{\tau}, g_y^{t_2''} \right), \\ =& e(g_x, g_y)^{b\tau(y_1+ac)} \cdot m_c \cdot e(g_y^{t_2''}, g_x^{b\tau ID^*}).e(h_{ID^*}, g_y^{t_2''})^{\tau}, \\ =& e(g_x, g_y)^{b\tau(y_1+ac)} \cdot m_c \cdot e(g_x, g_y)^{b\tau ID^* t_2''}.e(h_{ID^*}, g_y)^{t_2''\tau}. \end{aligned}$$

Therefore, C_A^* and C_I^* for the message m_c are correct from the point of view of $\mathcal{A}$.

Phase 2: Here, $\mathcal{A}$ is allowed to make queries similar as in the **Phase 1** with following restrictions:

- No private key queries are allowed on any access structure $(M,\rho)^*$ or identity matching ID^* in the key query phase.
- No decryption queries are allowed on $((M,\rho)^*, C_A^*)$, (ID^*, C_I^*), or $((M,\rho)^*, ID^*, C_A^*, C_I^*)$.

The challenge C_I^* can be computed from C_A^* or randomly chosen ABE ciphertext using $\mathsf{rk}_{A \to L}^*$ and $\mathsf{rk}_{L \to I}^*$.

Guess: $\mathcal{A}$ outputs a guess c' of c and wins the game if $c' = c$. Otherwise, it outputs $\perp$.

According to the simulation, $\mathcal{B}$ can compute private keys and re-encryption keys for (M,ρ) and ID. Then, $\mathcal{B}$ performs the decryption simulation correctly. For the hash queries to $\mathbf{h}_i$ and $\mathbf{h}_{ID}$, $\mathcal{B}$ randomly selects a hash value from the hash list as the challenge hash. $\mathcal{B}$ can use the hash query to solve the CBDH problem.

According to the simulation, given the decryption query for the challenge $C_A = (C, C', C_i, D_i)$, the simulator $\mathcal{B}$ can perform correct decryption simulation if $(M,\rho) \neq (M,\rho)^*$ and $ID \neq ID^*$. If $(M,\rho) = (M,\rho)^*$ and $ID = ID^*$, we have following cases:

- For the access structure (M,ρ), if $\sum_{i \in I} \omega_i \lambda_i = s$, $\mathcal{B}$ can compute d and perform decryption.

- If $\sum_{i \in I} \omega_i \lambda_i \neq s$, $\mathcal{B}$ return the invalid d.

If $\mathcal{A}$ has no advantage in computing d and d', $\mathcal{B}$ will perform decryption simulation successfully with negligible probability. The random and independent numbers used in the generation of master keys, private keys, re-encryption keys, and challenge ciphertexts are:

master keys: $x_1 + ab, x_2 + a, y_1 + ac,\ \{h_i\}_{i=1}^{l}, h_{ID}$,
private keys: t', t'', t_1'', τ,

$$s : \omega_i \text{ satisfying } \sum_{i \in I} \omega_i \lambda_i = s.$$

This illustrates that the randomness property holds and $x_1, x_2, x_3, t', t'', t_1'', \tau$ are randomly chosen by the simulator. Therefore, the simulation is indistinguishable from the real attack.

The simulation is successful if no abort occurs in the query or challenge phase. If the challenge access structure $(M, \rho)^*$ and the identity ID^* are the i-th access structure and j-th identity queried to the $\mathbf{h}_i$ and $\mathbf{h}_{ID}$ respectively, the adversary cannot query private keys and re-encryption keys, so that simulation will be successful in the query phase and the challenge phase. The success probability is $1(q_{k_1} q_{k_2})$, where q_{k_1} are the queries for an access structure and q_{k_2} are the queries for an identity.

Moreover, if the adversary $\mathcal{A}$ makes decryption queries for randomly selected C_A with success probability $1/p$ of breaking C_A, second time it is $1/(1-p)$, and $q_{d_1}/(p - q_{d_1})$ for q_{d_1} queries of C_A. Similarly, the success probability for the adaptive choice of C_I is $q_{d_2}/(p - q_{d_2})$ for q_{d_2} queries. Therefore, $\mathcal{A}$ has success probability at most $(1/2) + (q_{d_1}/p - q_{d_1})$ of guessing the encrypted message in C_A and $\frac{1}{4} + \frac{q_{d_2}}{p - q_{d_2}}$ in C_I.

In simulation, if $e(g_x, g_y)^{(x_2+a)\omega_i \lambda_i^* t'}$ from d and $e(g_x, g_y)^{abc\tau} \cdot e(g_x, g_y)^{bID^* t_2'' \tau} \cdot e(h_{ID^*}, g_y)^{t_2'' \tau}$ from d' has not been queried, the adversary has no advantage in correctly guessing the c except the probability $1/2$ for the challenge ciphertext C_A and probability of $1/4$ for the challenge ciphertext C_I. $\mathcal{A}$ makes q_d queries to $e(g_x, g_y)^{(x_2+a)\omega_i \lambda_i t'}$ and $q_{d'}$ queries to $e(g_x, g_y)^{abc\tau} \cdot e(g_x, g_y)^{bIDt_2'' \tau} \cdot e(h_{ID}, g_y)^{t_2'' \tau}$ with probability ε. Therefore, the probability of correctly finding the solution is $\frac{\varepsilon}{q_d q_{d'}}$.

Let T_s denote the time cost of the simulation. We have $T_s = O(q_k + q_d)$, which is mainly dominated by the key generation and the decryption. Therefore, $\mathcal{B}$ can solve the CBDH problem with $\left(t + T_s, \frac{\varepsilon}{q_{d_1} q_{d_2} q_d q_{d'}}\right)$.

Thus, PPT $\mathcal{A}$ has no advantage except given above in solving the underlying CBDH hard problem and $\mathcal{A}$ cannot break the challenge ciphertexts. Therefore, our proposed $\mathfrak{L}$_ABE-IBE PRE scheme is provably IND-sCCA secure as per (Guo et al., 2018). □

Note 1: Collusion resistance restricts $\mathcal{A}$ from obtaining more knowledge about C_A^* and C_I^* even when $\mathcal{A}$ queries the decryption keys associated with different attribute sets and identities. Moreover, the challenge C_A^* and C_I^* are generated by $\mathcal{B}$ using random and independent numbers and $\mathcal{A}$ has no knowledge of $(M, \rho)^*$ and ID^* or any random number used in generating the challenge ciphertexts.

Using the following theorem and its brief proof, we analyze $\mathfrak{L}$_ABE-IBE PRE scheme is quantum selectively IND-qsCCA secure:

THEOREM 3. *Given a $\mathfrak{L}$_ABE-IBE PRE scheme. Assuming the LWE problem is intractable, then the scheme is IND-qsCCA secure.*

Brief Proof. The quantum security of the proposed scheme is shown as a game played between the quantum adversary $\mathcal{A}_L$ and challenger $\mathcal{C}$. Assume there exists an quantum adversary $\mathcal{A}_L$ that can break the $\mathfrak{L}$_ABE-IBE PRE with non-negligible probability. We construct a quantum simulator $\mathcal{B}_q$ that can solve a LWE problem with non-negligible probability. Given a LWE problem instance, $\mathcal{B}_q$ runs $\mathcal{A}_L$ as follows:
Init: $\mathcal{A}_L$ outputs a noise set $\mathcal{X}^*$, a uniform matrix A_0^*, a basis T_A^* and a short vector γ^*.
Setup: $\mathcal{B}_q$ randomly selects a uniform random matrix A_0 and a basis T_A to generate $A = [A_0| - A_0 T_A + G]$. The master public key $\mathsf{mpk}_L = A$ and master secret key is $\mathsf{msk}_L = T_A$.
Phase 1: In this phase, $\mathcal{A}_L$ make private key and decryption queries. For the private key queries, $\mathcal{A}_L$ selects $A_0 \neq A_0^*$ and $T_A \neq T_A^*$. For the decryption queries, $\mathcal{A}_L$ selects $\gamma \neq \gamma^*$.
Challenge: $\mathcal{A}_L$ adaptively chooses two distant ABE ciphertexts c_A^1 and c_A^2. $\mathcal{B}_q$ randomly selects one of the ciphertext c_A^c, random secret s^*, and random errors $\{e_1^*, e_2^*\} \in \mathcal{X}^*$ as input and generates a challenge post-quantum ciphertext C_L^* as

$$C_L^* = (A^{*T} s^* + e_1^*,\ \beta^{*T} s^* + e_2^* + \lceil q/2 \rceil \cdot c_A^c).$$

$\mathcal{B}_q$ returns C_L^* to $\mathcal{A}_L$.
Phase 2: In this phase, $\mathcal{A}_L$ makes queries similar to **Phase 1** with restriction that $\mathcal{A}_L$ can not make private key queries for A_0^* and T_A^*. Similarly, $\mathcal{A}_L$ can not make decryption queries for γ^*.
Guess: $\mathcal{A}_L$ guess the encrypted ABE ciphertext c' of c_A^c and wins if $c' = c_A^c$. Otherwise, it returns $\perp$.

Here we analyze the probability of a successful simulation. Consider $\mathcal{A}_L$ makes q_{H_1} and q_{H_2} queries in **Phase 1** and **Challenge** phase respectively. The success probability of the simulation is $1 - 1/(q_{H_1} q_{H_2})$. Therefore, $\mathcal{A}_L$ has advantage ε, and

Table 1: Comparative Analysis of our $\mathfrak{L}$_ABE-IBE with naive ABE-Decrypt & IBE-ReEncrypt and Encryption Switching (ES) ABE-IBE schemes.

Schemes	Theoretical Analysis		
	Computation	Communication	Storage
Naive ABE-Dec & IBE-ReEnc	ABE.Dec + IBE.Enc: $(3+2l)E_p+(6+4l)E_e$ IBE.Dec: $2E_p$	ABE.CT.Size+IBE.CT.Size: $2\lvert\mathbb{G}_T\rvert+(3+2l)\lvert\mathbb{G}_1\rvert$	ABE.CT+IBE.CT: $2\lvert\mathbb{G}_T\rvert+(3+2l)\lvert\mathbb{G}_1\rvert$
ES.ABE-IBE He et al. (2019)	ES.ReKey: $E_p+(5+3l)E_e$ ABE.Enc: $E_p+(2+3l)E_e$ ES.ReEnc: $(2l+1)E_p+(3+l)E_e$ IBE.Dec: $2E_p+3E_e$	ES.ReKey.Size: $\lvert\mathbb{G}_T\rvert+(4+l)\lvert\mathbb{G}_1\rvert$	ES.Enc.CT: $\lvert\mathbb{G}_T\rvert+(1+2l)\lvert G_1\rvert$ ES.ReEnc.CT: $\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}_1\rvert$
$\mathfrak{L}$_ABE-IBE	$\mathfrak{L}$_ReKey: $E_p+4E_e+E_v$ $\mathfrak{L}$_ABE.Enc: $E_p+(2+l)E_e$ $\mathfrak{L}$_ReEnc: $2E_p+lE_e$ $\mathfrak{L}$_ReDec: E_p, $\mathfrak{L}$_IBE.Dec: E_p+2E_e	$\mathfrak{L}$_ReKey.Size: $\lvert\mathbb{G}_T\rvert+3\lvert\mathbb{G}_1\rvert+V_n$	$\mathfrak{L}$_Enc.CT: $\lvert\mathbb{G}_T\rvert+(1+l)\lvert\mathbb{G}_1\rvert$ $\mathfrak{L}$_ReEnc.CT: $\lvert\mathbb{G}_T\rvert+\lvert\mathbb{G}_1\rvert+\lvert C_l\rvert$ $\mathfrak{L}$_ReDec.CT: $\lvert\mathbb{G}_T\rvert$

Enc: Encryption, *Dec*: Decryption, *ReKey*: Re-encryption Key, *ReEnc*: Re-Encryption, *ReDec*: Re-Decryption, *CT*: Ciphertext, E_p: Number of bilinear pairing operation, E_e: Number of exponentiation operations, E_v: Vector multiplication operations, l: Number of attributes, V_n: Size of n-dimensional vector, C_l: post-quantum ciphertext

probability $|\Pr[c' = c_A^c]| \geq \frac{1}{2} + \varepsilon$. Thus, $\mathcal{B}_q$ has advantage $\frac{1}{2}(1 - 1/(q_{H_1} q_{H_2})) \cdot \varepsilon$ in solving hard LWE assumption.

Conclude that the quantum adversary $\mathcal{A}_L$ has no advantage in solving underlying LWE hard problem, and $\mathcal{A}_L$ can not break challenge ciphertext. This implies that the proposed scheme is quantum secure in the IND-qsCCA model since the quantum attacker trying to break the proposed scheme must solve the lattice problem, which is known to be hard. $\square$

7 DISCUSSION

In this section, we discuss a theoretical and experimental analysis of our scheme in comparison with the existing classical ABE-IBE scheme (He et al., 2019).

7.1 Theoretical Analysis

We consider communication, computation, and storage complexities to perform the theoretical analysis of our proposed scheme. For this purpose, we take the expensive set of operations for analysis as given at the bottom of Table 1.

The comparative analysis of our $\mathfrak{L}$_ABE-IBE scheme with a naive decrypt-and-reencrypt scheme and the ES.ABE-IBE (He et al., 2019) scheme is shown in Table 1. In the naive solution, the client downloads the ABE ciphertext from the Cloud, decrypts it and then encrypts it to IBE ciphertext before sharing. ES.ABE-IBE improves efficiency by automatically transforming ABE to IBE ciphertext without downloading and decrypting it. The computational complexity (Column 2, Table 1) shows that the naive solution requires linear cost of $(3+2l)E_p + (6+4l)E_e$ and ES.ABE-IBE requires $E_p+(2+3l)E_e$. $\mathfrak{L}$_ABE-IBE significantly reduces to $E_p + (2+l)E_e$ reduce. Similarly, computational complexity for re-encryption in ES.ABE-IBE is $(2l+1)E_p + (3+l)E_e$, while $\mathfrak{L}$_ABE-IBE reduces it to $2E_p + lE_e$. Moreover, computational complexity for IBE.Dec in ES.ABE-IBE is $2E_p+3E_e$, while in $\mathfrak{L}$_ABE-IBE it is E_p+2E_e.

The communication complexity (Column 3, Table 1) illustrates the size of communication packets between the communicating parties. The communication cost of the naive solution is $2|\mathbb{G}_T| + (3+2l)|\mathbb{G}_1|$ and ES.ABE-IBE scheme is $|\mathbb{G}_T| + (4+l)|\mathbb{G}_1|$. However, $\mathfrak{L}$_ABE-IBE reduces it to $|\mathbb{G}_T| + 3|\mathbb{G}_1| + V_n$.

Similarly, ES.ABE-IBE reduces storage complexity (Column 4, Table 1) by splitting the storage requirements between sender and Cloud, while $\mathfrak{L}$_ABE-IBE scheme takes advantage of local edge nodes (as shown in Fig. 3) to make it more storage efficient. $\mathfrak{L}$_ABE-IBE reduces the storage complexity sufficiently for end nodes (sender and receiver) by moving the complex re-encryption operations to edge nodes. Thus, the $\mathfrak{L}$_ABE-IBE proxy re-encryption scheme designed in this paper can surpass existing solutions in terms of security as well as complexity.

7.2 Experimental Analysis

Our implementation of the $\mathfrak{L}$_ABE-IBE scheme is written in C-language using the PBC library (pairing-based cryptography) (Lynn, 2007). The simulations were tested on a Linux virtual machine with 1 GB RAM over the host system with Intel(R) Core(TM) i5-7200U processor with CPU of 2.50 GHz - 2.71 GHz. We implemented ES.ABE-IBE (He et al., 2019) for comparative analysis along with our proposed scheme. For this purpose, we used the bilinear pairings (Definition 4.1) and LWE. We simulated the worst-case scenario by generating access policies

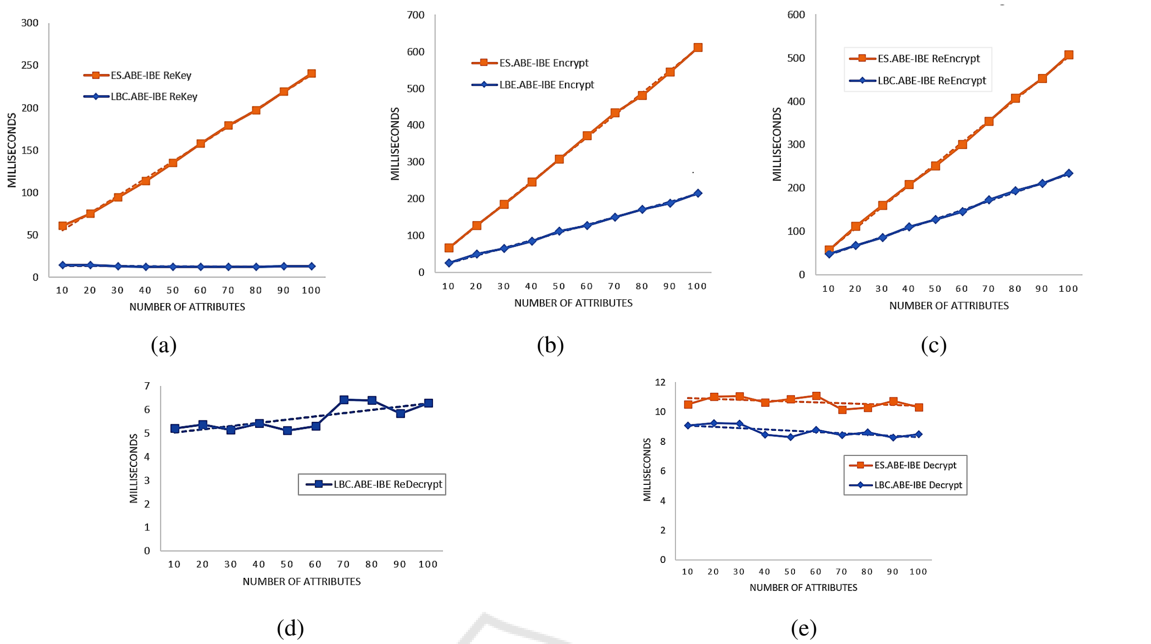

Figure 4: Experimental Analysis of $\mathfrak{L}$_ABE-IBE scheme with ES.ABE-IBE scheme where (a) illustrates the Re-Encryption Key Generation Time, (b) ABE Encryption Time, (c) Re-encryption Time of ABE-quantum and ES.ABE-IBE, (d) Re-decryption Time of quantum-IBE, and (e) IBE Decryption Time.

$(U_1, \cdots, U_l)$ from 10 to 100 and tested corresponding algorithms (ES.ABE-IBE and $\mathfrak{L}$_ABE-IBE) 20 times for each set of attributes to take the best results.

Fig. 4 (including Figures 4a, 4b, 4c, 4d and 4e) illustrates the experimental analysis of our proposed $\mathfrak{L}$_ABE-IBE proxy re-encryption scheme compared to the classical ES.ABE-IBE (He et al., 2019) scheme.

Fig. 4a shows that $\mathfrak{L}$_ABE-IBE takes almost constant re-encryption key generation time (approximately 13 ms) with the increase in the number of attributes as compared to ES.ABE-IBE. Fig. 4b shows both ES.ABE-IBE and $\mathfrak{L}$_ABE-IBE perform identically for a small number of attributes, but $\mathfrak{L}$_ABE-IBE encryption scheme performs more efficiently as the number of attributes grows. Fig. 4c shows that both schemes take almost equivalent re-encryption time for a smaller set of attributes, but with the increase in the number of attributes, $\mathfrak{L}$_ABE-IBE outperforms ES.ABE-IBE. Note, re-encryption in ES.ABE-IBE is performed in the Cloud, while in $\mathfrak{L}$_ABE-IBE, the re-encryption is performed at the local edge nodes. Fig. 4d shows that the re-decryption time of $\mathfrak{L}$_ABE-IBE is constant (approx 6 ms) when decoding post-quantum secure ciphertext to IBE ciphertext. Finally, Fig. 4e gives the decryption time of IBE ciphertext for both ES.ABE-IBE and $\mathfrak{L}$_ABE-IBE schemes. The decryption function in both schemes takes almost constant time but $\mathfrak{L}$_ABE-IBE decryption consumes 2 ms less than ES.ABE-IBE.

In general, the results of the experimental and security analysis both show that our $\mathfrak{L}$_ABE-IBE is efficient and secure against quantum adversaries.

8 CONCLUSIONS

In this paper, we proposed a classical to post-quantum-safe ABE-IBE proxy re-encryption scheme, which allows the conversion of ABE to IBE via post-quantum secure lattice-based encryption. The proposed $\mathfrak{L}$_ABE-IBE PRE allows secure conversion of ABE ciphertext to post-quantum secure ciphertext at the sender-side local Edge node and then post-quantum secure ciphertext to IBE ciphertext at receiver-side local Edge node to deal with the asymmetric resources of devices. We used the game-based framework to illustrate the selectively IND-sCCA and selectively quantum IND-qsCCA security of the proposed $\mathfrak{L}$_ABE-IBE PRE scheme. The theoretical analysis and experimental results highlighted that the proposed scheme improved efficiency as well as security in comparison to both the naive solution and classical ES.ABE-IBE proxy re-encryption scheme.

ACKNOWLEDGEMENTS

M. N. Khan is supported by a PhD stipend scholarship from CSIRO Data61 (50050661) and an International Tuition Fee scholarship from the School of Science, RMIT, Australia. Josef Pieprzyk is supported by the Polish National Science Center (NCN) grant 2018/31/B/ST6/03003.

REFERENCES

Ajtai, M. (1996). Generating hard instances of lattice problems. In *28th ACM Symp.*, STOC '96, pages 99–108.

Asif, R. (2021). Post-quantum cryptosystems for IoT: A survey on lattice-based algorithms. *IoT*, 2(1):71–91.

Banerjee, U., Pathak, A., and Chandrakasan, A. P. (2019). An energy-efficient configurable lattice cryptography processor for the quantum-secure Internet of Things. In *2019 IEEE ISSCC*, pages 46–48.

Bartocci, C., Bruzzo, U., and Ruipérez, D. H. (2009). *Lattices*, volume 276 of *PM*, pages 339–345. Birkhäuser.

Beimel, A. (1996). *Secure Schemes for Secret Sharing and Key Distribution*. Phd thesis, Technion-Israel Inst. of Technol., Fac. of Comput. Sci. Haifa.

Blaze, M., Bleumer, G., and Strauss, M. (1998). Divertible protocols and atomic proxy cryptography. In *EUROCRYPT 98*, volume 1403, pages 127–144. Springer.

Boneh, D. and Boyen, X. (2004). Secure identity based encryption without random oracles. In *Advances in Cryptology —CRYPTO 2004*, pages 443–459. Springer.

Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Advances in Cryptology—CRYPTO 2001*, pages 213–229. Springer.

Cao, Z., Wang, H., and Zhao, Y. (2019). AP-PRE: Autonomous path proxy re-encryption and its applications. *IEEE Trans. on Depend. & Sec. Comput.*, 16:833–842.

Chen, J., Gong, J., Kowalczyk, L., and Wee, H. (2018). Unbounded ABE via bilinear entropy expansion, revisited. In *EUROCRYPT 2018*, pages 503–534, Cham. Springer.

Deng, H., Qin, Z., Wu, Q., Guan, Z., and Zhou, Y. (2020). Flexible attribute-based proxy re-encryption for efficient data sharing. *Inf. Sciences*, 511:94 – 113.

Deng, H., Wu, Q., Qin, B., Domingo-Ferrer, J., Zhang, L., Liu, J., and Shi, W. (2014). Ciphertext-policy hierarchical ABE with short ciphertexts. *Inf. Sci.*, 275:370–384.

Fernández-Caramés, T. M. (2020). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things J.*, 7(7):6457–6480.

Gentry, C., Peikert, C., and Vaikuntanathan, V. (2008). Trapdoors for hard lattices and new cryptographic constructions. In *40th Annu. ACM Symp.*, pages 197–206.

Guo, F., Susilo, W., and Mu, Y. (2018). *Foundations of Security Reduction*, pages 29–146. Springer, Cham.

He, K., Mao, Y., Ning, J., Liang, K., Huang, X., Panaousis, E., and Loukas, G. (2019). A new encrypted data switching protocol: Bridging IBE and ABE without loss of data confidentiality. *IEEE Access*, 7:50658–50668.

Hofheinz, D., Jia, D., and Pan, J. (2018). Identity-based encryption tightly secure under chosen-ciphertext attacks. In *ASIACRYPT 2018*, volume 11273, pages 190–220.

Ioannou, L. M. and Mosca, M. (2011). A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. In *PQC 2011*, pages 255–274.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., and Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909):237–243.

Joux, A. and Nguyen, K. (2003). Separating decision diffie–hellman from computational diffie–hellman in cryptographic groups. *J. Cryptol.*, 16(4):239–247.

Li, J., Wang, Y., Zhang, Y., and Han, J. (2020). Full Verifiability for Outsourced Decryption in Attribute-Based Encryption. *IEEE Trans. on Serv. Comput.*, 13:478–487.

Li, J., Yao, W., Han, J., Zhang, Y., and Shen, J. (2018). User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage. *IEEE Syst. J.*, 12:1767–1777.

Li, J., Yu, Q., and Zhang, Y. (2019). Hierarchical ABE with continuous leakage-resilience. *Inf. Sci.*, 484:113–134.

Lindner, R. and Peikert, C. (2011). Better key sizes (and attacks) for LWE-based encryption. In *CT-RSA 2011*, volume 6558 of *LNCS*, pages 319–339. Springer.

Lohachab, A. and Karambir (2019). ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. *J. of Inf. Secur. and Appl.*, 46:1–12.

Lynn, B. (2007). *On the implementation of pairing-based cryptosystems*. PhD thesis, Stanford University Stanford.

Miao, Y., Liu, X., Choo, K.-K. R., Deng, R. H., Li, J., Li, H., and Ma, J. (2021). Privacy-preserving attribute-based keyword search in shared multi-owner setting. *IEEE Trans. on Depend. & Secure Comput.*, 18(3):1080–1094.

Micciancio, D. and Peikert, C. (2012). Trapdoors for lattices: Simpler, tighter, faster, smaller. In *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718. Springer.

Micciancio, D. and Regev, O. (2009). *Lattice-based Cryptography*, pages 147–191. Springer.

Monz, T., Nigg, D., Martinez, E. A., Brandl, M. F., Schindler, P., Rines, R., Wang, S. X., Chuang, I. L., and Blatt, R. (2016). Realization of a scalable Shor algorithm. *Sci.*, 351(6277):1068–1070.

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., and Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. *ACM Comput. Surv.*, 51(6):41.

Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends® in Theoretical Comput. Sci.*, 10(4):283–424.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *J. of the ACM*, 56(6).

Roman, R., Lopez, J., and Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.*, 78:680 – 698.

Sahai, A. and Waters, B. (2005). Fuzzy identity-based encryption. In *EUROCRYPT 2005*, pages 457–473.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In *CRYPTO 84*, volume 196, pages 47–53.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332.

Susilo, W., Jiang, P., Guo, F., Yang, G., Yu, Y., and Mu, Y. (2017). Eacsip: Extendable access control system with integrity protection for enhancing collaboration in the cloud. *IEEE Trans. Inf. Forens. Sec.*, 12:3110–3122.

Tao, X., Qiang, Y., Wang, P., and Wang, Y. (2023). Lmibe: Lattice-based matchmaking IBE for internet of things. *IEEE Access*, 11:9851–9858.

Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *PKC 2011*, volume 6571, pages 53–70.

Xiong, J., Ren, J., Chen, L., Yao, Z., Lin, M., Wu, D., and Niu, B. (2019). Enhancing privacy and availability for data clustering in intelligent electrical service of IoT. *IEEE Internet of Things J.*, 6(2):1530–1540.

Yang, Y., Chen, X., Chen, H., and Du, X. (2018). Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing. *IEEE Access*, 6:18009–18021.