An Efficient and Secure Post-Quantum Multi-Authority Ciphertext-Policy Attribute-Based Encryption Method Using Lattice

Prithwi Bagchi*, Basudeb Bera†, Raj Maheshwari‡, Ashok Kumar Das§, *Senior Member, IEEE*,
David K. Y. Yau¶, *Senior Member, IEEE*, and Biplab Sikdar‖, *Senior Member, IEEE*
*‡§ Center for Security, Theory and Algorithmic Research,
International Institute of Information Technology, Hyderabad 500 032, India
†¶ Information Systems Technology and Design, Singapore University of Technology and Design, Singapore, 487372
‖ Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583
E-mails: prithwi.bagchi@research.iiit.ac.in, basudeb_bera@sutd.edu.sg,
raj.maheshwari@students.iiit.ac.in, iitkgp.akdas@gmail.com,
david_yau@sutd.edu.sg, bsikdar@nus.edu.sg

***Abstract*—This article deals with designing an efficient post-quantum lattice based encryption scheme that relies on the multi-authority Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The security of the proposed scheme is based on the hardness of the ring learning with errors (RLWE) problem. The construction of the proposed scheme is done using the Shamir's threshold secret sharing along with the Lagrange interpolation during the key generation and decryption processes in order to achieve the segmentation and restoration of private keys. A comparative study with the existing state of art schemes has been performed to show the feasibility and efficiency of the proposed scheme. Furthermore, experiments on the proposed scheme have been conducted to illustrate the computational time required during the key generation, encryption and decryption processes.**

***Index Terms*—Post-quantum cryptography, lattice, attribute-based encryption, security.**

I. Introduction

Nowadays, the post-quantum lattice-based cryptography technology is rapidly growing in the security field in order to achieve the desired security level in the quantum world [1]. In the present quantum setting, the traditional classical cryptosystems, like RSA, ElGamal, "Diffie-Hellman", and "elliptic-curve cryptography" are all under a security threat [2]. These cryptosystems can be effectively attacked by quantum computers based the seminal Shor's algorithm [3], whereas "lattice-based cryptography (LBC)" has the potential to resist quantum attacks.

Ajtai [4] first proposed a LBC, which is quantum secure. LBC techniques, especially lattice-based signature schemes as well as lattice-based encryption and decryption schemes, are widely adopted in various real-time applications (for instance, smart home application [5], smart agriculture environment [6], Internet of Drone (IoD) applications [7], and Internet of Things (IoT) applications). Since the security of the LBC depends on certain hardness problems, such as, "learning with errors (LWE)", "short integer solution (SIS)" [8], and "shortest vector problem (SVP)" [9], the LBC schemes are hard to break by quantum computing within feasible time frame.

Consider IoT applications, where a huge volume of data is generated. As a result, data storage is the most pressing concern, which can be addressed by offloading data to the semi-trusted cloud servers [10]. Because a cloud server acts as a third party and it cannot be completely considered as trusted, maintaining security over it leads to use of other security protocols, like access control, authentication and key agreement [11], [12]. In this direction, one of the finest technology is the attribute-based cryptography [13].

The attribute-based cryptography can be categorized into two types based on access policy: 1) "key policy attribute-based encryption (KP-ABE)" [14] and 2) "cipher-text policy attribute-based encryption (CP-ABE)" [15]. In a CP-ABE scheme, the data owner sets the arbitrary access policy, where the access policy is actually a "boolean statement on attributes" and the "encrypted data can be decrypted by the user only if he or she has the attributes that satisfy the pre-defined access policy" [16]. Most existing CP-ABE schemes were constructed using the bilinear pairing [17], [18], which are not efficient and secure enough in the present day context. LBC is one of the prominent post-quantum cryptosystem, which gives a new direction for constructing the CP-ABE schemes [19], as they are efficient and safe against quantum attacks. The lattice-based CP-ABE schemes are also adopted in centralized and decentralized systems.

A. Motivation

If the lattice-based CP-ABE scheme [20] is adpoted in a decentralized and distributed system, several authorities can generate and use the data, and the attributes can be generated by multiple authorities. This makes it more flexible and scalable. Hence, we argue that it is necessary to build a quantum-resistant, decentralized and highly efficient lattice-base CP-ABE scheme that can provide desirable security attributes and ensure that the access policies cannot be revealed by any unauthorized party at the same time.

B. Research Contributions

The following contributions are highlighted below:

- We present a "post-quantum latticed based multi-authority CP-ABE scheme" based on the "ring learning with errors $(RLWE)$" hardness, which is efficient by considering the superiority of a ring variant of trapdoor over G-lattice [21]. This scheme is efficient, secure, and decentralized because it can support a distributed environment. In the designed scheme, the multi-authorities are treated as multiple servers (distributed servers), which are synchronized.
- We use the Shamir's threshold secret sharing together with the Lagrange interpolation in the key generation and decryption phases for achieving the segmentation and restoration of private keys. In addition, to achieve more efficiency we use the Gaussian pre-image sampling over G-lattice [21].
- We then provide a comparative study with the existing related schemes to show the feasibility and efficiency of the proposed scheme over the existing ones.
- Finally, the proposed scheme has been implemented and the experimental results show its efficiency for multiple authorities and multiple attributes.

II. Related Work

Fu *et al.* [19] proposed a "lattice based single authority CP-ABE scheme", which relies on the hardness of RLWE. Their scheme works in two phases: 1) offline and 2) online. The main drawback of their scheme is that they utilized a single authority for CP-ABE scheme based on lattice. Since it is centralized, a single server failure attack is not resisted.

Sun *et al.* [22] suggested a "lattice-based multi-authority CP-ABE scheme, which is a decentralized and more efficient than centralized single authority based schemes". The hardness of their scheme is based on the hardness of RLWE. Moreover, their scheme supports a "selective security under chosen plaintext attacks" and achieves moderate security level.

Zhao *et al.* [23] proposed a "revocable lattice-based CP-ABE scheme", which supports the cloud storage and the security of this scheme relies on the hardness of RLWE. In their scheme, a "fine-grained access control mechanism" is utilized for the users right for aggregating the shared data.

Yang *et al.* [20] designed a "revocable CP-ABE scheme", which consists of multi-authority, multi-valued attributes. The hardness of their scheme hinges on the hardness of RLWE. In this scheme, the multiple authorities are involved in key distribution process, and the attribute revocation is also achieved even if the users' access rights are changed.

Fun and Samsudin [24] utilized the RLWE hard problem for generating the secret keys and ciphertexts. This reduces the error coefficient during the decryption process and also escalates the "failure probability of decryption". However, in their scheme, the access policy is not adaptable enough.

III. Mathematical Background

In this section, we provides the relevant mathematical preliminaries that are needed for designing our proposed scheme.

Assume that $\mathbb{Z}$ is the set of all integers. Then, $\mathbb{Z}_q$ will be the set of all integers modulo a large prime q. We consider a ring of the form: $R = \mathbb{Z}[x]/ < x^f + 1 >$ consisting of all the polynomials of degree at most $f - 1$, where the co-efficients belong to $\mathbb{Z}$. R_q $=\mathbb{Z}_q[x]/ < x^f + 1 >$ is considered as a field consisting of all the polynomials of degree at most $f - 1$, where the co-efficients are integers and these are from the interval $(\lfloor \frac{-q}{2} \rfloor, \lfloor \frac{q}{2} \rfloor)$, and f is the power of 2. If $m \geq 1$, ${R_q}^m$ will represent a column vector that will have m polynomials from R_q, and ${R_q}^{1 \times m}$ will denote a row vector containing the m polynomials from R_q. We denote $u \leftarrow_R R_q$ as a sampling, which is a polynomial randomly chosen from R_q. Moreover, we denote N, S_{uid} and $S_{uid,\theta}$ as the "total number of authorities", the "attribute set of a user", and the subset of S_{uid} containing those attributes which are from the authority AA_θ, respectively, and W' will represent the access policy for the user.

A. Lattice-based Cryptography

Let $\mathbb{R}^n$ be an n-dimensional real space. Then, a lattice $\mathcal{L}$ of n-dimensional real space is a discrete subgroup of $\mathbb{R}^n$. Now, the lattice $\mathcal{L}$ is said to be a "full-rank lattice" if span($\mathcal{L}$) = $\mathbb{R}^n$. The integer lattice is the lattice $\mathcal{L}$, which is considered as a subset of Z^n. A basis is formed from a "set of independent vectors which generate any point in the lattice $\mathcal{L}$". Thus, the basis of $\mathcal{L}$ becomes a set $\mathcal{D} = \{\widehat{b_1}, \widehat{b_2}, \cdots, \widehat{b_n}\}$, such that $\mathcal{L}(\mathcal{D}) = \{\sum_{i=1}^{n} x_i.\widehat{b_i} \, |x_i \in Z\}$, where each $\widehat{b_i} \in \mathbb{R}^n$, $\forall i \in [n]$.

For $p \geq 1$, define a norm l_p on the lattice vector x as $||x||_p = \sqrt[p]{\sum_{i=1}^{n} |x_i|^p}$. Similarly, the sup-norm on the lattice vectors is defined as $||x||_\infty = \max\{|x_i|; i \in [n]\}$. The minimum distance of the lattice $\mathcal{L}(\mathcal{D})$, can be defined as ${\lambda_1}^p(\mathcal{L}(\mathcal{D})) = \min\{||x||_p; x \in \mathcal{L}(\mathcal{D}) - \{0\}\}$.

- *Learning with Errors* (LWE): Let $s \in_R \mathbb{Z}_q^f$ be a fixed vector and χ an "error distribution over $\mathbb{Z}$". We pick a vector $a \in \mathbb{Z}_q^f$ from a "uniform distribution over $\mathbb{Z}_q^f$" and a number $\bar{e} \in \mathbb{Z}$, called the error, and then compute $t = a.s + \bar{e} \pmod q$. Now, given ζ $(\geq f)$ samples $(a, a.s + \bar{e}$ $\pmod q)$, the task is to recover the unique random secret s. It is worth to note that when the "secret s is sampled from the same error distribution as $\bar{e}$", the hardness of the LWE still remains valid [8].
- *Ring-Learning with Errors (RLWE)*: It is another hard problem in the LBC. Recently, the security of most of the lattice-based schemes relies on the hardness of the RLWE problem [25].

B. Discrete Gaussian

Let σ be an arbitrary parameter which is greater than 0. Then, an "n-dimensional Gaussian function" is defined over the lattice $\mathcal{L}(\mathcal{D}) \in \mathbb{Z}^n$ with center c and the parameter σ as follows: $\forall x \in \mathcal{L}(\mathcal{D})$, $\rho_{\sigma,c}(x) = exp(-\pi\frac{||x-c||^2}{\sigma^2})$ and $\rho_{\sigma,c}(\mathcal{L}(\mathcal{D})) = \sum_{x \in \mathcal{L}(\mathcal{D})} \rho_{\sigma,c}(x)$. The Gaussian distribution on

$\mathcal{L}(\mathcal{D})$ with center c and parameter σ can be then defined as [26]: $\forall y \in \mathcal{L}(\mathcal{D})$, $D_{\mathcal{L}(\mathcal{D}),\sigma,c}(y) = \frac{\rho_{\sigma,c}(y)}{\rho_{\sigma,c}(\mathcal{L}(\mathcal{D}))}$.

C. Trapdoor Generation

Consider a vector $J^T = [J_1, J_2, \cdots, J_k]$, where $J_i = 2^{i-1}$ for all $i \in [k]$. Assume that there is a prime $q = q(\lambda)$, $f = f(\lambda) \in \mathbb{Z}^+$ and a parameter $\sigma = \sigma(\lambda)$, $k = \lfloor \log_b q + 1 \rfloor$, where λ is called a security parameter and b is the base of J^T such that $b \geq 2$. The probabilistic polynomial time (PPT) "ring trapdoor generation algorithm" $RTrapGen(q, f, k, \sigma) \rightarrow (A, T'_A)$, where A is the output vector of size $m = k + 2$ and a trapdoor T'_A, such that $A = [1, a, J_1 \; -(ar_1' + e_1'), \cdots, J_k \; -(ar_k' + e_k')] \in R_q^{1 \times m}$, and $T'_A = (r', e')$, where $a \in_R R_q$. The hardness of A relies on the hardness of RLWE assumption, where T'_A is secret, and $(r', e') \in R_q^k \times R_q^k$ are generated from the Gaussian distribution $D_{R,\sigma}$ [27].

D. Gaussian Preimage Sampling

Given a vector $A \in R_q^{1 \times m}$ in conjunction with its trapdoor $T'_A = (r', e')$, $v \in R_q$, and the parameters σ, σ_s that are greater than 0. Then, there exists a PPT "ring Gaussian preimage sampling" algorithm $RSamplePre(A, T'_A, v, \sigma, \sigma_s)$, which generates a "disturbance vector $l' \in R_q^m$" and computes another vector $Y \in R_q^k$ such that $J^T.Y = v - A.l'$. The output becomes a vector $M = [l'_1 + e'.Y, l'_2 + r'.Y, l'_3 + Y_1, \cdots, l'_m + Y_k]^T \in R_q^m$ with $A.M = v$, and M is sampled from $D_{\Lambda_q(A),\sigma_s}$ [28].

E. Linear Secret Sharing Scheme (LSSS)

Consider a set of parties $[n]$ and $q \in \mathbb{N}$ is a prime. A "secret sharing scheme" Γ over the domain of secrets $\mathbb{Z}_q$ can de defined as follows. Suppose the access structure W on the parties $[n]$ is linear over $\mathbb{Z}_q$, a share-generating matrix is $F \in \mathbb{Z}_q^{h \times m}$, and a function $\tau : [h] \rightarrow [2n]$, where τ labels to the corresponding rows of F with the parity index from $[n]$ or from $[n+1, n+2, \cdots, 2n]$. A vector $\Sigma = (d, r_2, r_3, \cdots, r_m)^T \in \mathbb{Z}_q^m$, where $d \in \mathbb{Z}_q$ is the secret, generates h shares of the secret d corresponding to Γ as $Sh = F.\Sigma \in \mathbb{Z}_q^{h \times 1}$. (F, τ) is called the LSSS policy of W.

Let $\overline{S} = S \cup \{i \in [n+1, n+2, \cdots, 2n]; i - n \notin S\} \subset [2n]$. Now, $F_{\overline{S}}$ is a sub-matrix of F, which contains those rows of F belonging to $\overline{S}$ according to τ. S is authorized if the vector $(1, 0, \cdots, 0) \in \mathbb{Z}_q^m$ is in span of the rows of $F_{\overline{S}}$; otherwise, S is called unauthorized. Moreover, if S is unauthorized, we can obtain $d \in \mathbb{Z}_q^m$ with the first component of d as 1, and $F_{\overline{S}}.d^t = 0$, that is, zero vector [29].

IV. Security Model of Lattice-Based MA-CP-ABE

For the proposed lattice-based Multi-authority CP-ABE (MA-CP-ABE) scheme described in Section V, the security model is taken as "selectively secure against Chosen Ciphertext Attack (sCPA)". It consists of a sequence of games between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as decribed below [22], [30].

Initialization: The adversary $\mathcal{A}$ first announces a "challenge access structure W' together with a set of corrupted authorities $J_{Corrupt}$". After that, these are forwarded to the challenger $\mathcal{C}$.

Setup: $\mathcal{C}$ executes the $Setup$ and $AASetup$ algorithms in order to generate the public parameters, as well as the public and secret keys corresponding to each corrupted authority in the list $J_{Corrupt}$. Once these are generated, $\mathcal{C}$ forwards these parameters to the adversary $\mathcal{A}$.

Phase 1: In this phase, the adversary $\mathcal{A}$ now generates (uid, S_{uid}) and forwards it to $\mathcal{C}$, and inquires the private key generation query frequently. Note that S_{uid} denotes the attribute set of a user uid. Let T be the attribute set associated to the corrupted authorities. Since $|S_{uid} \cap T|$ is not sufficient to satisfy the challenge access structure W', the key generation algorithm, $KeyGen$ is executed by the challenger $\mathcal{C}$, and $\mathcal{C}$ forwards the private key to $\mathcal{A}$.

Challenge: $\mathcal{A}$ then picks the messages ϕ_0 and ϕ_1 randomly and forwards these to $\mathcal{C}$. $\mathcal{C}$ selects $\alpha \in \{0, 1\}$, and encrypts the message ϕ_α based on the access structure W' to generate the ciphertext ct. Next, the produced ct is forwarded to $\mathcal{A}$.

Phase 2: In this phase, $\mathcal{A}$ asks frequently the "secret key query" similar to **Phase 1**.

Guess: $\mathcal{A}$ mow makes a guess $\alpha' \in \{0, 1\}$ for α. If $\alpha' = \alpha$ holds, it means that the adversary $\mathcal{A}$ will win the game. The wining probability, also called the advantage of $\mathcal{A}$, corresponding to the game is defined by $Adv(\mathcal{A}) = |Pr[\alpha' = \alpha] - \frac{1}{2}|$.

Definition 1. *Our proposed lattice-based MA-CP-ABE scheme is said to be 'indistinguishability under selective chosen plaintext attack ($IND - sCPA$) secure if $Adv(\mathcal{A})$ of wining the game is negligible."*

V. Proposed Lattice-based Multi-authority CP-ABE Scheme

In this section, we design an efficient post-quantum lattice-based CP-ABE scheme. Initially, a trusted key generation center KGC performs the setup phase (Sections V-A and V-B) for generating the public parameters and distinct identities corresponding to the legal users as well as authorities. An access policy is considered as arbitrary that can be formed based on the universal attribute set by the data owner. Next, the encrypted messages, known as ciphertexts, generated from the encrypt phase (Section V-D) are uploaded to the cloud server. The encrypted messages can be downloaded from the cloud server by the data user. For this purpose, the data user needs to send a request to each authority for issuing his/her private key. The data user can only decrypt the ciphertext only if his/her private key satisfies the access policy (Section V-E). The detailed description of each phase is described below. We use the notations and their meanings mentioned in Table I.

A. Setup

The trusted key generation center KGC executes the following steps:

- The KGC takes the input λ as a security parameter, and selects $u \in_R R_q$, and then outputs the public parameters as $pp = (q,\ f,\ k,\ \sigma,\ \sigma_s,\ u)$, where q is a large prime number, and $\sigma \geq 0$ and $\sigma_s \geq 0$ represent the Gaussian parameters.
- Assume that the total number of authorities is N, and the set of authorities is $\{AA_1,\ AA_2,\ \cdots,\ AA_N\}$. During

TABLE I
NOTATIONS AND THEIR MEANINGS

Symbol	Description
KGC	A trusted key generation center
q	A large prime
h	Total number of attributes in the system
$\|W'\|$	Total number of attributes in access policy
n_k	Number of attributes that can satisfy the access policy, $(n_k < h)$
N	Total number of authorities AA_θ
f	Power of 2, degree of irreducible polynomial
S	Total number of attributes set by KGC in [23]
J	The set of attributes contained in the ciphertext in [23]
η	A positive integer such that $m = \eta\|S\|$ holds in [23]
R_q	A finite field of the type: $\mathbb{Z}_q[x]/ < x^f + 1 >$, where $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$, f is the highest degree of the polynomial, and $q \equiv 1 \pmod{2f}$
n_a	The number of attributes in access structure in [20]
n_v	The number of virtual attributes in [20]
m	A positive integer of the form: $\lfloor \log_b q + 1 \rfloor + 2$
n_u	The number of attributes held by a user in [20]
n_r	The number of revoked attributes in [20]

the registration of each authority AA_θ, the KGC selects a polynomial $E(x)$ of degree $N-1$ uniformly at random, where $E(x) = u + \sum_{I=1}^{N-1} G_I x^I$, and G_I are picked uniformly at random from the R_q, for all $I \in \{1, 2, \cdots, N-1\}$. Finally, the polynomial value $E(\theta) \in R_q$ for each authority AA_θ is computed and provided it to the AA_θ.

B. AASetup

This phase is executed by each authority AA_θ with the help of the following steps:

• AA_θ first runs the ring trap generation algorithm, known as $RTrapGen$, and produces the output as a pair (A_θ, T_{A_θ}), where $A_\theta \in R_q^{1\times m}$, $T_{A_\theta} = (r_\theta, e_\theta)$, r_θ, and $e_\theta \in R_q^k$. If we denote $\chi'_\theta = \{x_1, x_2, \cdots, x_{h_\theta}\}$ be the attribute set corresponding to the authority AA_θ, then for every attribute $x_i \in \chi'_\theta$, AA_θ will select a pair $(b^+_{\theta,i}, b^-_{\theta,i})$ uniformly at random from $R_q^{1\times m} \times R_q^{1\times m}$.

• After that, AA_θ selects $P_\theta \in R_q^m$, where $P_\theta = (P_{\theta,1}, P_{\theta,2}, \cdots, P_{\theta,m})^T$. For each $\Pi \in [m]$, $P_{\theta,\Pi}$=$\sum_{U=0}^{f-1} P_{\theta,\Pi,U}(z_{1,i}, z_{2,i}, \cdots, z_{V,i})x^U$, where $(z_{1,i}, z_{2,i}, \cdots, z_{V,i}) \in (Z_q)^V$. Note that, for all $\theta \in [N]$, $\Pi \in [m]$, $U \in \{0, \cdots, f-1\}$, and $P_{\theta,\Pi,U}$ are linear in $(z_{1,i}, z_{2,i}, \cdots, z_{V,i})$.

• Finally, the public key and secret key for AA_θ are considered as $\{APK'_\theta$ and $ASK'_\theta\}$, respectively, where $APK'_\theta = \{A_\theta, (b^+_{\theta,i}, b^-_{\theta,i})_{i\in[h_\theta]}\}$, and $ASK'_\theta = \{T_{A_\theta}, P_\theta\}$.

C. KeyGen

Each authority AA_θ executes this phase. Assume $\theta \in [N]$, uid is the user identity, and the attribute set of the user is denoted by $S_{uid} = \cup_{\theta\in[N]} S_{uid,\theta}$. This phase contains the following steps:

• For each $x_i \in \chi'_\theta$, with $i \in [h_\theta]$, AA_θ picks $(z_{1,i}, z_{2,i}, \cdots, z_{V,i})$ uniformly at random from the $(Z_q)^V$, and then calculates $y_{\theta,i} = (P_\theta)_{(z_{1,i}, z_{2,i}, \cdots, z_{V,i})}$. For $y_{\theta,i} \in R_q^m$, $\forall\theta \in [N]$, $i \in [h_\theta]$, and for each $x_i \in \chi'_\theta$, AA_θ sets

$$n_{\theta,i} = \begin{cases} (b^+_{\theta,i}).y_{\theta,i}, & \text{if}\, x_i \in S_{uid,\theta} \\ (b^-_{\theta,i}).y_{\theta,i}, & \text{if}\, x_i \in \chi'_\theta \setminus S_{uid,\theta} \end{cases}$$

• Next, AA_θ calculates $\Delta_\theta = E(\theta) - \sum_{i=1}^{h_\theta} n_{\theta,i}$, and runs the Gaussian preimage sampling algorithm $RSamplePre(A_\theta$, T_{A_θ}, Δ_θ, σ, $\sigma_s)$ to obtain the output as y_{θ,A_θ}.

• Finally, the secret key of the user is taken as $SK_{uid} = \{y_{uid,\theta}; \theta \in [N]\}$, where $y_{uid,\theta} = \{y_{\theta,A_\theta}, y_{\theta,1}, \cdots, y_{\theta,h_\theta}\}$.

D. Encryption

This phase is executed by a user, say uid, for generating the corresponding ciphertext given a plaintext message, using the following steps:

- With inputs $\{APK'_\theta\}_{\theta\in[N]}$, an access structure $W' = \cup_{\theta\in[N]} W'_\theta = \cup_{\theta\in[N]}({W_\theta}^+ \cup {W_\theta}^-)$, where W'_θ is the access structure formed by the attributes assigned for AA_θ, and a plain text message $\phi = (\phi_i)_{i\in\{0,\cdots,f-1\}} \in \{0,1\}^f$, where $\phi(x) \in R_q$, the user selects $F \in R_q^{h_\theta\times m}$ and a vector $\Sigma = (d, r_2, \cdots, r_m)$, where $d \in R_q$ is the secret to be shared, for all $i \in \{2, 3, \cdots, m\}$, and r_i's are picked uniformly at random from the R_q.
- Now, pick uniformly random $\tilde{e}$ from R for the following:
  – Compute $c_0 = 2.u.d+ \tilde{e}+ \phi\lfloor q/2 \rfloor$.
  – Sample $e_{\theta,A_\theta} \in R_q^{1\times m}$, $c_{\theta,A_\theta} = A_\theta.d + e_{\theta,A_\theta}$.
  – If $x_i \in {W_\theta}^+$, sample $e_{\theta,i,1} \in R_q^{1\times m}$, and $e_{\theta,i,2} \in R_q$, calculate $c_{\theta,i,1} = (b^+_{\theta,i}).d + e_{\theta,i,1}$, and $c_{\theta,i,2} = (F_{i,1}).u.d+ \sum_{j=2}^m F_{i,j}.r_j + e_{\theta,i,2}$.
  – If $x_i \in {W_\theta}^-$, sample $e_{\theta,i,1} \in R_q^{1\times m}$, $e_{\theta,i,2} \in R_q$, and calculate $c_{\theta,i,1} = (b^-_{\theta,i}).d+ e_{\theta,i,1}$ and $c_{\theta,i,2} = (F_{i,1}).u.d+ \sum_{j=2}^m F_{i,j}.r_j+ e_{\theta,i,2}$.
  – If $x_i \in \chi'_\theta \setminus W'_\theta$, select $e^+_{\theta,i,1}$, $e^-_{\theta,i,1} R_q^{1\times m}$, and $e_{\theta,i,2} \in R_q$. In addition, compute $c^+_{\theta,i,1} = (b^+_{\theta,i}).d + e^+_{\theta,i,1}$, $c^-_{\theta,i,1} = (b^-_{\theta,i}).d + e^-_{\theta,i,1}$, $c_{\theta,i,2} = (F_{i,1}).u.d + \sum_{j=2}^m F_{i,j}.r_j + e_{\theta,i,2}$.
- Finally, the ciphertext as output is taken as $ct = \{c_0, \{c_{\theta,i,1}, c_{\theta,i,2}\}_{x_i\in W'_\theta}, \{c^+_{\theta,i,1}, c^-_{\theta,i,1}, c_{\theta,i,2}\}_{x_i\in\chi'_\theta\setminus W'_\theta}, \{c_{\theta,A_\theta}\}_{\theta\in[N]}, W'\}$.

E. Decryption

This phase is used to decrypt a ciphertext to recover the orginal plaintext messsage with the following involved steps:

- Given the inputs as the encrypted ciphertext ct, the share generating matrix F of the LSSS scheme , and the set of secret keys SK_{uid} corresponding to the attribute set χ'_θ of each authority AA_θ. If $(1, 0, \cdots, 0) \notin Span < F_i; i \in [h_\theta] >$, the decryption will not be successful. Otherwise, take $\{g_i \in \{0, 1\}; i \in [h_\theta]\}$ which consists of a set of scalars, such that $\sum_{i=1}^{h_\theta} g_i.F_i = (1, 0, \cdots, 0)$, where F_i denotes the i^{th} row of F.
- For each authority $AA_\theta(\theta \in [N])$, compute $\Lambda_{\theta,0} = (c_{\theta,A_\theta})y_{\theta,A_\theta}$. Next, for each $x_i \in \chi'_\theta$, compute $\Lambda_{\theta,i,1}$, $\Lambda_{\theta,i,2} \in R_q$ as follows:

1) For each $x_i \in W'_\theta$, compute $\Lambda_{\theta,i,1} = (c_{\theta,i,1}).y_{\theta,i}$ and $\Lambda_{\theta,i,2} = g_i.(c_{\theta,i,2})$. For other $x_i \in S_{uid,\theta}$, compute $\Lambda_{\theta,i,1} = ({c_{\theta,i,1}}^{+}).y_{\theta,i}$ and $\Lambda_{\theta,i,2} = g_i.(c_{\theta,i,2})$.
2) Now, for $x_i \in \chi'_\theta \setminus W'_\theta \cup S_{uid,\theta}$, compute $\Lambda_{\theta,i,1} = ({c_{\theta,i,1}}^{-}).y_{\theta,i}$, $\Lambda_{\theta,i,2} = g_i.(c_{\theta,i,2})$, $\Lambda_\theta = \Lambda_{\theta,0} + \sum_{i=1}^{h_\theta} [\Lambda_{\theta,i,1} + \Lambda_{\theta,i,2}] \in R_q$.

- Next, compute $\phi' = (\phi'_0, \phi'_1, \cdots, \phi'_{f-1}) = c_0 - \sum_{\theta \in [N]} \mathcal{L}_\theta \ \Lambda_\theta$, where $\mathcal{L}_\theta$ is the Lagrangian polynomial.
- Finally, for every $i \in \{0, \cdots, f-1\}$, the output is considered as $\phi_i = 0$ if $|\phi'_i| < \frac{q}{4}$; else, the output becomes $\phi_i = 1$.

Based on the above, the original message can be now recovered by utilizing the values of $\phi' = (\phi'_0, \phi'_1, \cdots, \phi'_{f-1})$, where each ϕ'_i may be 0 or 1 based on the conditions: $\phi' \in \{0,1\}^f$. Note that the message is considered as $\phi = (\phi_i)_{i \in \{0,\cdots,f-1\}} \in \{0,1\}^f$, where $\phi(x) \in R_q$. Thus, the original message can be constructed by comparing the coefficients of ϕ' with ϕ, that is, whether $\phi = \phi'$.

TABLE II
COMPARISON OF THE PROPOSED SCHEME WITH EXISTING LATTICE-BASED CP-ABE SCHEMES

Scheme	Public Key	Private Key	Ciphertext	Plaintext
[19]	$(2mh + 1 + m)f\lceil \log q \rceil$	$h.mf\lceil \log q \rceil$	$(2h - \|W'\| + 1)mf\lceil \log q \rceil$	f
[23]	$mf\lceil \log q \rceil \|S\| + \eta f\lceil \log q \rceil$	$2n_k mf\lceil \log q \rceil$	$2\|J\|mf\lceil \log q \rceil$	ηf
[22]	$(2mh+mN+1)f\lceil \log q \rceil$	$n_k mf\lceil \log q \rceil$	$(2h - \|W'\| + N)mf\lceil \log q \rceil$	f
[20]	$(2mh+mN+1)f\lceil \log q \rceil$	$2(2n_u+2n_v-n_r)mf\lceil \log q \rceil$	$\{2(n_a + n_v - n_k + 1)m + m + 1\}f\lceil \log q \rceil$	f
Proposed	$(2mh+mN+1)f\lceil \log q \rceil$	$n_k mfd$	$(2h - \|W'\| + N)(m + 1)f\lceil \log q \rceil$	f

VI. Security Analysis

We highlight through Lemma 1 that our designed scheme is "selectively secure against Chosen Ciphertext Attack (sCPA)" based on the hardness of the decisional RLWE problem.

Lemma 1. *The proposed multi-authority lattice-based CP-ABE scheme is IND-sCPA secure based on the hardness of decisional RLWE assumption. In particular, if a "probabilistic polynomial time adversary (PPT) adversary", say $\mathcal{A}$ is able to win the IND-sCPA game with the wining probability $\epsilon > 0$, where ϵ is a non-negligible number, then there exists another adversary $\mathcal{B}$ that can solve the RLWE problem with an advantage $\frac{\epsilon}{2}$.*

VII. Experimental Results and Discussion

We have simulated our proposed scheme using the Python 3.8.10 on Ubuntu 20.04.5 platform. Our simulation operates in five phases: a) Setup, b) AASetup, c) Key generation, d) Encryption and e) Decryption. All the lattice operations have been implemented using the numpy and random libraries available with the python. The different classes of KGC, users and AA (authorities) contain the necessary functions for executing these phases. In our scheme, there are multiple authorities, where we have considered three authorities for the experiments. Since the authorities are considered independent of each other, we have assumed that all the processing takes place in parallel as well.

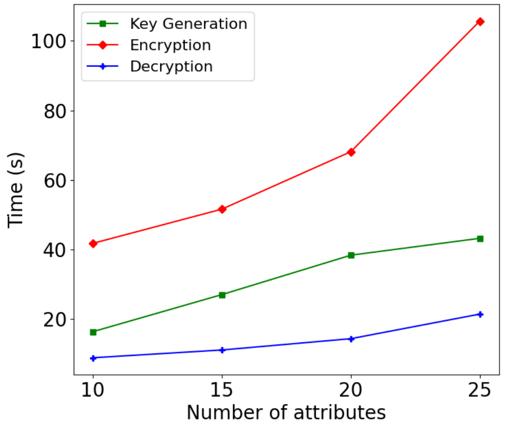

Fig. 1. Experimental results for varying number of attributes

Using the simulation, we have obtained the time required for key generation, encryption and decryption phases by varying the number of attributes, h_θ. The corresponding computational time are plotted in Fig. 1. It can be observed that the time required for decryption of a message is quite low as compared to encryption process. The key generation phase does not require too much time. Moreover, it needs to be called only during the initial phase. The encryption of the message takes more time when there is an increase in the number of used attributes.

VIII. Performance Analysis

Here, we present a comparison study among the designed scheme and other existing CP-ABE schemes, such as the schemes of Fu *et al.* [19], Zhao *et al.* [23], Sun *et al.* [22], and Yang *et al.* [20].

For the comparative study, we utilize the notations mentioned in Table I. Table II reports that the private key size of our scheme is less than that for other schemes. Moreover, the plaintext size of our scheme is also less than that for Zhao *et al.*'s scheme [23].

TABLE III
PERFORMANCE COMPARISON WITH LATTICE-BASED CP-ABE SCHEMES

Scheme	Authority	Architecture	Security	Efficiency	Privacy Protection
[19]	Single	Centralized	Moderate	Low	Low
[23]	Multi	Decentralized	High	Moderate	High
[22]	Multi	Decentralized	Moderate	High	Moderate
[20]	Multi	Decentralized	Moderate	Moderate	Moderate
Proposed	Multi	Decentralized	High	High	High

The performance analysis comparison shown in Table III tells that the scheme by Fu *et al.* [19] uses a central (single) authority, and its efficiency level is then low. Thus, the scheme [19] achieves low privacy protection. Although the remaining schemes, like the schemes of Zhao *et al.* [23], Sun *et al.* [22], Yang *et al.* [20], and the proposed scheme utilize the multi-authority access policies, the schemes [22], [20] only achieve a moderate security level and privacy protection whereas the proposed scheme attains a high security and privacy protection.

IX. Conclusion

We designed an efficient "multi-authority ciphertext policy attribute-based encryption scheme" that relies on the hardness of the RLWE problem. In this work, since the multi-authorities are treated as multi-servers (decentralized distributed servers), it signifies that the proposed scheme supports distributed computing environment. This scheme also consists multiple authorities with access policy and it then achieves strong security because only the authorized parties have the legitimate access policies for accessing the services. The performance analysis shows that the designed scheme is efficient as compared to other existing lattice-based ABE schemes after using G-lattice together with the Gaussian preimage sampling algorithm.

Acknowledgments

This work was supported in part by the Quantum Engineering Program, Singapore under grant NRF2021-QEP2-01-P04. This work was also supported in part by the project: "Design of Blockchain-Assisted Post-Quantum Lattice-Based Secure Systems for Internet of Things (IoT) Applications" under Ripple Centre of Excellence Scheme, CoE in Blockchain, IIIT Hyderabad, India.

References

[1] D. Micciancio and O. Regev, "Lattice-based Cryptography," in *Post-Quantum Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191.

[2] E. Kasper, "Fast Elliptic Curve Cryptography in OpenSSL," in *Financial Cryptography and Data Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 27–39.

[3] A. G. Fowler and L. C. L. Hollenberg, "Scalability of Shor's algorithm with a limited set of rotation gates," *Phys. Rev. A*, vol. 70, Sep 2004.

[4] M. Ajtai, "Generating Hard Instances of Lattice Problems (Extended Abstract)," in *Twenty-Eighth Annual ACM Symposium on Theory of Computing*, Philadelphia, Pennsylvania, USA, 1996, p. 99–108.

[5] A. C. Jose and R. Malekian, "Improving Smart Home Security: Integrating Logical Sensing Into Smart Home," *IEEE Sensors Journal*, vol. 17, no. 13, pp. 4269–4286, 2017.

[6] K. A. Patil and N. R. Kale, "A model for smart agriculture using IoT," in *International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC)*, Jalgaon, India, 2016, pp. 543–545.

[7] B. Vergouw, H. Nagel, G. Bondt, and B. Custers, *Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments*. The Hague: T.M.C. Asser Press, 2016, pp. 21–45.

[8] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with Small Parameters," in *Advances in Cryptology – CRYPTO 2013*, Santa Barbara, CA, USA, 2013, pp. 21–39.

[9] O. Bernard and A. Roux-Langlois, "Twisted-PHS: Using the Product Formula to Solve Approx-SVP in Ideal Lattices," in *Advances in Cryptology – ASIACRYPT 2020*, Daejeon, South Korea, 2020, pp. 349–380.

[10] D. Dharminder, U. Kumar, A. K. Das, B. Bera, D. Giri, S. S. Jamal, and J. J. P. C. Rodrigues, "Secure cloud-based data storage scheme using postquantum integer lattices-based signcryption for IoT applications," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 9, p. e4540, 2022.

[11] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744–5761, 2021.

[12] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-Based Access Control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *IEEE Symposium on Security and Privacy (S&P '07)*, Berkeley, CA, USA, 2007, pp. 321–334.

[14] F. Han, J. Qin, H. Zhao, and J. Hu, "A general transformation from KP-ABE to searchable encryption," *Future Generation Computer Systems*, vol. 30, pp. 107–115, 2014.

[15] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE With Constant-Size Keys for Lightweight Devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 763–771, 2014.

[16] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded Ciphertext Policy Attribute Based Encryption," in *Automata, Languages and Programming*, Reykjavik, Iceland, 2008, pp. 579–591.

[17] F. Zhang, R. Safavi-Naini, and W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications," in *Public Key Cryptography – PKC 2004*, Singapore, 2004, pp. 277–290.

[18] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with Partially Hidden Access Structures," in *7th ACM Symposium on Information, Computer and Communications Security*, New York, NY, USA, 2012, p. 18–19.

[19] X. Fu, Y. Wang, L. You, J. Ning, Z. Hu, and F. Li, "Offline/Online lattice-based ciphertext policy attribute-based encryption," *Journal of Systems Architecture*, vol. 130, p. 102684, 2022.

[20] Y. Yang, J. Sun, Z. Liu, and Y. Qiao, "Practical revocable and multi-authority CP-ABE scheme from RLWE for Cloud Computing," *Journal of Information Security and Applications*, vol. 65, pp. 103–108, 2022.

[21] G. Birkhoff, "Applications of lattice algebra," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 30, p. 115–122, 1934.

[22] J. Sun, Y. Qiao, Z. Liu, Y. Chen, and Y. Yang, "Practical Multi-Authority Ciphertext Policy Attribute-Based Encryption from R-LWE," in *IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking*, New York City, NY, USA, 2021, pp. 1435–1443.

[23] S. Zhao, R. Jiang, and B. Bhargava, "RL-ABE: A Revocable Lattice Attribute Based Encryption Scheme Based on R-LWE Problem in Cloud Storage," *IEEE Transactions on Services Computing*, vol. 15, no. 2, pp. 1026–1035, 2022.

[24] T. Soo Fun and A. Samsudin, "Lattice Ciphertext-Policy Attribute-Based encryption from ring-LWE," in *International Symposium on Technology Management and Emerging Technologies (ISTMET)*, Langkawi, Malaysia, 2015, pp. 258–262.

[25] M. Rosca, D. Stehle, and A. Wallet, "On the Ring-LWE and Polynomial-LWE Problems," in *Advances in Cryptology – EUROCRYPT 2018*, 2018, pp. 146–173.

[26] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni, and M. O'Neill, "On Practical Discrete Gaussian Samplers for Lattice-Based Cryptography," *IEEE Transactions on Computers*, no. 3, pp. 322–334, 2018.

[27] R. El Bansarkhani and J. Buchmann, "Improvement and Efficient Implementation of a Lattice-Based Signature Scheme," in *Selected Areas in Cryptography – SAC 2013*, Burnaby, BC, Canada, 2014, pp. 48–67.

[28] P. Bert, G. Eberhart, L. Prabel, A. Roux-Langlois, and M. Sabt, "Implementation of Lattice Trapdoors on Modules and Applications," in *Post-Quantum Cryptography*, 2021, pp. 195–214.

[29] P. Datta, I. Komargodski, and B. Waters, "Decentralized Multi-authority ABE for DNFs from LWE," in *Advances in Cryptology - EUROCRYPT 2021*, Zagreb, Croatia, 2021, pp. 177–209.

[30] Y. Liu, L. Wang, L. Li, and X. Yan, "Secure and Efficient Multi-Authority Attribute-Based Encryption Scheme From Lattices," *IEEE Access*, vol. 7, pp. 3665–3674, 2019.