Optimized Lattice-Based Ciphertext Policy Attribute-Based Encryption for Quantum-Resistant Secure Data Sharing

Purnima[1], Tejaswi Khanna[2], Deepak Kumar Verma[3]
Research Scholar, Amity School of Engineering and Technology, Amity University, Greater Noida, India[1]
Amity School of Engineering and Technology, Amity University, Greater Noida, India[2]
Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India[3]

***Abstract*—The practical utilization of the conventional Ciphertext-Policy Attribute-Based Encryption (CP-ABE) systems in a vast cloud has the constraint of the high cost of computation and the high risk of quantum-powered adversaries. This research introduces a novel Hybrid Lattice-Based CP-ABE (HL-CP-ABE) architecture that is focused on the hardness assumptions of Ring Learning with Errors (RLWE) to provide the double security of quantum-safe and precise data sharing. The proposed hybrid encryption system employs post-quantum techniques that provide both confidentiality and access control, and it is completely based on AES for the data encryption and on the lattice-based CP-ABE technology for the AES session key wrapping. A multithreaded, chunk-based parallel processing technique is used to improve the encryption and decryption processes and, at the same time, limit the difficulties that come along with the performance of lattice-based cryptography. The entire system is implemented in Java and evaluated across file sizes from 100 to 800 MB under a fixed three-attribute access policy, achieving processing time reductions of up to 9.5× compared to serial lattice CP-ABE, with a mean speedup of approximately 8.2× across encryption and decryption. The results reveal that the design not only upholds security but also achieves scalability, reduced ciphertext growth, and the correct decryption of the whole data. This research study presents the groundwork for future optimization using GPU parallelization and dynamic attribute management, and at the same time, it puts forth a workable, effective, and quantum-secure method of attribute-based encryption that is specifically beneficial for electronic health record (EHR) systems and secure cloud data sharing.**

***Keywords*—LWE; Ring-LWE; post-quantum cryptography; attribute based encryption; parallel processing**

I. Introduction

Due to their scalability, live collaboration, and data access from everywhere, cloud computing and distributed data environments nowadays have turned into the necessities of any information system. Nevertheless, these benefits also introduce significant dangers to privacy arising from these benefits, and these dangers get highlighted when using untrustworthy infrastructure to transmit sensitive data [1] [2]. The common use of digital health data, e-governance, and financial platforms does not only require cryptographic frameworks that secure data with secrecy, authenticity, and fine-grained access control, but it also promotes their use. On the other hand, the protection offered by public-key cryptography systems such as RSA and ECC, which are based on the integer factorization and discrete logarithm issues, will be completely broken if quantum computers are used [3]. The public-key cryptosystems in the area of quantum computing are at risk of quantum algorithms like Shor's or Grover's. Hence, it becomes a necessity to innovate cryptography techniques that are quantum-proof to allow secure data exchange between quantum computers. Attribute-Based Encryption (ABE) is acknowledged as a practical method for encrypted data access control of the highest degree, thereby ensuring that the information can only be accessed by the users who are permitted [4]. ABE, the encrypted message is tied to a receiver who can decrypt it based on a policy that conforms to certain attributes. These users are only allowed to view the file that satisfies the requirements with their attribute sets [5]. A crucial factor is the distinction between the two main types of encryption using an attribute-based approach, namely, Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) [6]. The interest in data sharing applications has been along the side of CP-ABE because the policy for access was set right at the moment of encryption by data owners [7].

In contrast, many traditional CP-ABE scheme implementations are based on pairing of groups formed by elliptic curves; this property makes the systems computationally intensive and open to attack within the domain of quantum computing [8]. The time-consuming nature of the bilinear pairings in the CP-ABE schemes results in high latency during encryption and decryption processes and difficulties in the expansion of the technology to large or real-time applications mainly because of the dependence of the schemes on the access structures' size [9]. Hence, even though ABE is a theoretically attractive framework, its application is still limited in an environment where high throughput is the main concern and quantum computers are considered a threat [10]. Of late, recently, lattice-based cryptography has emerged as the leading post-quantum approach. The primary limitations of these systems include large ciphertext sizes, high key-generation overhead, and lack of parallel optimization, which keep attackers out from both classical and quantum sides [8]. The hard problems like LWE and its Ring-based version (Ring-LWE) are a barrier to attackers coming from both quantum and classical worlds. The lattice structure practically levels the playing field between optimal and typical situations, thereby speeding up arithmetic operations in the polynomial ring modulo and making them even more suitable for cryptographic

primitives like ABE and functional encryption [11]. To put it in another way, several lattice-based ABE schemes have been proposed, which, by means of theory, are found to be resistant to quantum algorithms [12]. The drawback of such appetitive features is that, with time, these designs have frequently become prey to the problems of enormously bulky ciphertext sizes, big key generation overhead, and the limitation of performance optimization [13]. One of the main problems of the current implementations is that they were made for academic purposes only, whereas lattice-based and attribute-based encryption (ABE) can be said to be more practical. This means that the distance between the theoretical discussions on post-quantum ABE and technological solutions capable of handling massive, encrypted datasets is actually very far apart [14].

One way of overcoming these limitations is by means of methods that integrate the best of symmetric cryptography and public-key techniques in the so-called hybrid cryptographic frameworks. Public-key mechanisms and symmetric encryption techniques together speed key-based transactions [15]. Within a hybrid system, data encryption is carried out by means of a symmetric cipher like AES, but the symmetric key is protected by a public-key method, such as ABE [16]. This idea leads to a significant drop in the expenses of calculations, as the public-key operations are performed only on the key, not on the whole data set [14]. Nevertheless, the lattice-based methods still present large delays in the computation aspect, although they are hybridized. This is due to polynomial operations and modular arithmetic inherent in lattice schemes. Most existing hybrid implementations are single-threaded and therefore inadequate for large-file scenarios. Therefore, the proposed scheme must be compatible with public-key mechanisms while supporting parallel, pipelined execution for high-throughput scenarios. This study provides a modified CP-ABE algorithm that uses lattice structures in conjunction with classical cryptographic constructions to prevent against quantum attacks. The system is composed of the LSSS policy matrices as a base, with the Ring-LWE assumption, which makes the system post-quantum secure and helps define detailed levels of access control. The next step after the AES is made to encrypt the data very quickly is the AES key that is covered through the Ring-LWE-based CP-ABE mechanism. The start of the encryption process with the new encryption method is anticipated to result in the modification of the system that allows one to encrypt and decrypt segments of files in parallel across multiple cores of the CPU by having a concurrency method easier and cheaper than the one currently in use. Having set up a quantum key distribution technique, the described system would be working concurrently on all channels, ensuring total security. The introduction of the multithreaded chunk-processing model is the key to making the solution highly efficient while at the same time keeping it secure and correct. The system is fully implemented in Java, with modules designed for efficient memory management. There has been a very exhaustive experimental analysis to confirm the efficiency and scalability of the suggested system. Moreover, in the performance evaluation, several different file sizes, attribute policies, and thread counts were taken into consideration when comparing the optimized and complex multithreaded hybrid model with the conventional and serial lattice-based CP-ABE implementations. The evaluation shows up to a 9.5× reduction in runtime and a substantial decrease in ciphertext size, while preserving fully accurate decryption. Thus, the outcome clearly demonstrates that the mixed approach used in architecture was secure and widely acceptable in terms of system speed and total operational time—two important characteristics for the various kinds of tasks, like secure cloud storage, collaborative data sharing, and electronic health records, that may likely be done in real-world scenarios.

A. Highlights of the Research Paper

- Quantum-Secure Hybrid Model: With Ring-LWE-based cryptography, a new CP-ABE system was developed, and it eliminated the risk of quantum attacks.
- Performance-Optimized Architecture: A parallelizable encryption and decryption flow for big files, through the application of multithreaded chunk-processing design, has been introduced.
- Practical Implementation: A full Java-based system has been created by integrating lattice cryptography with AES and LSSS-based policy parsing.
- Thorough Evaluation: The proposed system showed processing times up to 9.5× faster than serial execution (mean≈8.2×), while maintaining fully accurate decryption and ciphertext overhead below 2×.

This study follows the outlined order: In Section II, the research of lattice-based ABE and hybrid cryptographic ways is considered. In Section III, some important mathematical principles are included, such as LWE, Ring-LWE, and LSSS. Section IV delineates the proposed system, encompassing setup procedures, key generation, encryption, decryption, and the corresponding algorithms for these operations. Section V presents the implementation and verifies system efficiency. Security is covered in Section VI. Section VII compares the proposed system against existing pairing-based, lattice-based, and hybrid schemes. Section VIII concludes the study and outlines future work.

II. Literature Review

A. Classical Pairing-Based Attribute-Based Encryption

Attribute-Based Encryption (ABE) was first put forward by Sahai and Waters [59] as an upgrade of Identity-Based Encryption (IBE), granting fine-grained access rights over encrypted data. The seminal scheme employed bilinear pairings defined over cyclic groups $(G1, G2)$ of prime order p, its security being based on the Decisional Bilinear Diffie–Hellman (DBDH) hypothesis. After that, Goyal et al. [18] and Bethencourt et al. [19] proposed models along with this model in the form of Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE), respectively, which allowed the owners of the data to put the access structures in the encrypted data directly. The pairing-based schemes enabled highly expressible Boolean or Linear Secret Sharing Scheme (LSSS)-based policies, but they involved a large computational burden in terms of pairing and exponent operations of the form $(ga, gb) = (g, g)\{ab\}$, which are the major contributors to the runtime complexity [20]. Despite several improvements, the security of pairing-based protocols against quantum attacks remains elusive to trace [21]. "Shor's algorithm solves integer factorization and

discrete logarithm problems in polynomial time, breaking RSA and ECC security.", this being the very core of security for RSA and elliptic curve systems [22]. The traditional methods being inadequate for protecting against quantum threats drove the development of lattice-based cryptography, which relies on the hardness of the toughest lattice problems, thus making it impractical in both the classical and quantum realms [23].

B. Lattice-Based and Post-Quantum ABE Approaches

The move from pairings to lattice problems was first taken by the path-breaking work of Gentry, Peikert, and Vaikuntanathan, who put forward the Learning with Errors (LWE) problem, a main post-quantum assumption [24]. LWE is about linear equations in modular arithmetic, where the main task is to recover a secret vector $s \in Z^n$ given pairs $(A, As + e)$, where the error vector (e) is chosen from a discrete Gaussian distribution [25]. LWE's hardness can be connected to the hardest lattice problems, among which are GapSVP (Shortest Vector Problem) and SIVP (Shortest Independent Vector Problem) [26]. The (Ring-LWE) variant quickly turned efficient by operating through polynomial rings $R_q = Z_q[x]/(x^n + 1)$, which in turn led to a decrease in key and ciphertext sizes, while keeping security [17][27]. The security of Ring-LWE is primarily rooted in the challenge of finding a short vector in an ideal lattice, which can be expressed formally as:

Lemma 1: The ability of a probabilistic polynomial-time technique to tell apart Ring-LWE samples from uniform noise implies that there is a fast algorithm under the given conditions that can output the GapSVP with polynomial factors in terms of time complexity. The lemma, as proved in [27], is the cornerstone for the security aspect of post-quantum lattice cryptography. Agrawal, Freeman, and Vaikuntanathan [28] did the initial work on constructing an LWE-based ABE that accepts small Boolean formulas. Yao et al. followed up, detailing these ideas with the presentation of lattice-attached Attribute-Based Encryption (ABE) systems that incorporate Linear Secret Sharing Scheme (LSSS) architecture, thus expanding the communication and liberality of access rules in the CP-ABE systems even more. Yao et al. later asserted that traditional model hypotheses could be a basis for guaranteeing CP-ABE on lattice LWE [29]. Subsequent schemes, such as those of Sun et al. [30] and Datta et al. [31], built on LWE-family assumptions to improve the expressiveness and performance of lattice-based ABE. The results indicate that lattice-based ABE approaches might be able to achieve a certain level of security from a CPA security perspective when it comes to resisting quantum attacks.

However, several hurdles lie ahead:

- Very large public keys and the corresponding ciphertexts since each attribute bears a polynomial number of factors, with each of them being of rather big size [19] [32].
- The speed of polynomial multiplication is negatively impacted because of the use of high-degree modulus arithmetic [33] [34].
- The practical side is rather limited—most of the trials are just based on the encryption of tiny messages [35]. Yet even with the Number Theoretic Transform (NTT), which boosts polynomial multiplication efficiency from (n^2) to $(n \log n)$, practical realization remains computationally heavy [36] [37].

C. Hybrid Encryption and Efficiency-Oriented ABE Architectures

To remedy the performance overhead of lattice-based encryption, researchers have resorted to hybrid configurations. Hybrid architecture, under this model, can be described by the process of symmetric encryption with data before it gains the likeness of AES, and through hybrid transmission, the encryption can be delivered at the destination. This step-by-step design of two tiers reduces the very high public-key operations to a handful, thus making it possible to perform the process faster and still maintain the security level. Li et al. [38] and Qian and Wu [39] exemplify such studies; Qian and Wu [39] describe a hybrid ABE structure for cloud storage, and other work has combined ABE with KEMs, which made easy entrance to resources for different applications [40]. However, a major part of hybrid ABE research mainly builds on pairing-based cryptography, so it happens to be vulnerable to quantum attacks as well. Only a few of the papers, such as the one by Dai et al. [41], investigated the lattice-based hybrid ABE, but they did not provide immediate implementation or parallel optimization. The results imply that although the hybridization approach is in principle possible, the difficulties posed by the Ring-LWE-based schemes in computation still occur at the encryption and key generation phases, where polynomial sampling and modular reduction greatly affect the time complexity. The cost of a single lattice-based encryption operation can be evaluated in terms of computation in Eq. (1):

$$T_{enc} = O(n \log n + m \cdot |A|) \quad (1)$$

The value (n) represents the ring dimension, while another variable (m) denotes the attribute count and $(|A|)$ indicates the policy matrix dimension. The extent of this complexity therefore suggests a major possibility of parallelism, a fact that the already established studies on the subject have been unable to exploit so far.

D. Implementation Studies and Performance Limitations

Practical applications of lattice-based ABE remain scarce. Mostly the current prototypes are coded in C/C++ and reap the benefits from using experimental libraries like Lattigo or PALISADE [42]. These systems manage to have the functions of cryptography correct when it comes to them, but they have so far missed the throughput of the encryption test on actual file datasets (i.e., the scalar lattice multiplication). An example of these findings is the work of Gür et al. [43], who reported the throughput of lattice-based encryption schemes at moderate lattice dimensions, resulting in the observation of the gap between the theory of post-quantum cryptography and the practical industry implementation. Additionally, the current literature neglects the use of not just the file but rather chunking techniques along with multithreaded processing, which can be taken to the extreme in a multi-core system to minimize the processing latency. Usually, the access structure is shown in the ABE framework by an LSSS matrix $(M \in Zp^{l \times n})$ and a mapping function (ρ), where each row corresponds to a separate attribute. According to the Reconstruction Theorem [44], LSSS provides the assurance that if the user's attribute set (S) satisfies the

access policy, then the secret (s) can be reconstructed as a linear combination of shares (λ_i), as shown in Eq. (2):

$$s = \sum i \in I\ \omega i \lambda i \quad (2)$$

In this context, the symbol ω_i represents the coefficients used for reconstructing the data. It is true that modern lattice-based attribute-based encryption systems prove the theorem correctly; still, such systems do not accelerate share generation and linear algebra operations through parallelism. This situation leads to considerable delays with the share generation (l), especially when the policies are complex and include either conjunctions or disjunctions.

E. Parallel and Multi-threaded Cryptographic Frameworks

Parallelism has been widely applied to symmetric algorithms such as AES and SHA, achieving multi-fold acceleration on modern CPUs and GPUs [45]. In contrast, parallel approaches for asymmetric post-quantum cryptography remain limited. Researchers have proposed GPU-based optimizations for lattice encryption primitives [46], yet these focus on raw mathematical kernels, not integrated ABE frameworks. Multi-threading has been explored for homomorphic encryption libraries [47] but not for attribute-based or hybrid encryption systems. From a theoretical standpoint, encryption of independent message blocks or chunks can be represented as a data-parallel operation $E_k(m_l)$ over disjoint subsets $m_1, m_2, \dots, m_t$, where each encryption thread operates on a distinct data segment [48].

1) Proposition 1 (Parallel Time Bound):

For the case of t different data chunks and p processor cores, the expected encryption time $\mathbf{T_p}$ satisfies $\mathbf{T_p} \leq \mathbf{T_1}/\mathbf{p} + (\boldsymbol{\epsilon})$, where the epsilon factor symbolizes the overhead of managing threads. This scaling is one of the main factors in the parallel processing of cryptographic workloads and is the very principle used in the presented system [49]. The classification of CP-ABE systems into three main groups is as follows: the first group is pairing-based ABE, it has a very expressive policy but at the same time is vulnerable to quantum attacks; the second group is lattice-based post-quantum ABE, which is strong in theory but suffers from practical performance issues; and the third group is hybrids of both ABE approaches, possibly the fastest processing but also not offering any protection against quantum attacks. Nonetheless, the growth of the lattice-based cryptosystem was observed; there remains no documented case where the combination of the Ring-LWE–based ABE, symmetric hybridization, and multithreaded optimization for large-scale data sharing is being carried out end-to-end [50]. In addition, the existing works have neither systematically divided the data into different segments for parallelization and applying the LSSS Reconstruction nor have they estimated the runtime enhancements using empirical metrics [8]. The analysis carried out in this review reveals lattice-based, hybrid CP-ABE architecture at its best when it is equipped with the Ring-LWE encryption, AES for data confidentiality, and parallelism at the chunk level in being multithreaded. The novel scheme provides efficient and secure encryption of data, is scalable, and specifically overcomes barriers for HR. With the introduction of the proposed framework, quantum-safe access control is granted whereas at the same time, a clear increase in performance over serial implementations represents the major advantages of the system.

III. Preliminaries

This section explains the mathematical basis, notation, and formal security assumptions that will be used in this study. The text outlines the lattice roots, the LWE and Ring-LWE problems, the LSSS access structure, and the correctness and security concerns that are essential to the suggested hybrid CP-ABE system.

A. Notation and Basic Definitions

- Let λ denote the global security parameter.
- $Z_q = \{0,1, \dots, q-1\}$ represents the set of integers modulo a prime (q).
- Vectors are denoted by bold lowercase letters (e.g., a, e, s) and matrices by uppercase letters [e.g., (A, M)].
- The inner product of two vectors is $\langle a, b \rangle = \sum_i a_i b_i$.
- A random variable ($x \leftarrow D$) denotes sampling from a distribution (D).
- All probabilities are taken over the randomness of the involved algorithms.

The polynomial ring is defined by Eq. (3):

$$R_q = [x]/(x^n + 1) \quad (3)$$

where, (n) is the power of two and (q) is a prime modulus, the equation $q = 1(mod\ 2n)$ holds. In (R_q), operations are working with both (q) and ($x^n + 1$) modulo; still, arithmetic is consistent with (q) and ($x^n + 1$). The Euclidean norm of a vector $x = (x_1, \dots, x_n)$ is given as ($|x| = (\sum_i x^2)^{1/2}$). The scheme uses a discretely sampled error drawn from a Gaussian distribution χ with zero mean and standard deviation σ.

B. Lattice Theory Basics

Regev [25] originally defined the LWE problem, while Lyubashevsky et al. [27] later adapted it to Ring-LWE for reduced complexity. The hard-core information of GapSVP and SIVP [23][26] establishes the complexity of these problems.

A lattice ($\mathscr{L} \subset R^m$) is a discrete additive subgroup generated by a linearly independent basis [$B = (b_1, \dots, b_n) \in R^{m \times n}$], as shown in Eq. (4):

$$\mathscr{L}(B) = Bz: z \in Z^n \quad (4)$$

The Shortest Vector Problem (SVP) and Shortest Independent Vector Problem (SIVP) are defined as follows:

- SVP: Given B, find a non-zero $v \in \mathscr{L}(B)$ such that $|v|$ is minimized.
- SIVP: Given (B), find (n) linearly independent vectors [$v_1, \dots, v_n \in \mathscr{L}(B)$] minimizing the maximum norm.

These problems are believed to be challenging even for quantum computers.

Lemma 1 (Lattice Hardness):

To estimate the GapSVP or SIVP to within polynomial factors in ($\boldsymbol{n}$) is to face substantial difficulties in quantum computing. (This point is brought out in [25]). This lemma forms the security basis for LWE and its ring family.

C. Learning with Errors (LWE) Assumption

The LWE problem models noisy linear equations modulo (q). Definition 1 (LWE Distribution).

Let (n, q ∈ N) and error distribution (χ) over (Z_q). For a secret vector (s ∈ Zq^n), define as in Eq. (5):

$$\boldsymbol{\chi} = \{(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a} \leftarrow \boldsymbol{Z_q^n}, \boldsymbol{e} \leftarrow \boldsymbol{\chi}, \boldsymbol{b} = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + \boldsymbol{e}\} \quad (5)$$

The LWE assumption states that the distribution (As, χ) is computationally indistinguishable from the uniform distribution over ($Z_q^n \times Z_q$).

1) Theorem 1 (LWE Hardness Reduction):

By the assumption that a probabilistic polynomial-time algorithm can distinguish between LWE samples and uniform distributions, the existence of an efficient quantum algorithm that will be able to provide approximations of GapSVP and SIVP on any lattice to within polynomial factors seems natural. This argument is further supported by the claim that compromising LWE would also mean solving the worst-case lattice problems, and as a result, it paves the way for the development of post-quantum LWE-based cryptography [25].

D. Ring Learning with Errors (Ring-LWE)

The Ring-LWE assumption extends LWE into the algebraic structure of polynomial rings for efficiency.

Let ($R_q = Z_q[x]/(x^n + 1)$) for a secret polynomial ($s \leftarrow R_q$) and error polynomial ($e \leftarrow \chi^n$), a sample is drawn as (a, b) ∈ $R_q \times R_q$ with $b = a \cdot s + e \bmod q$. The security of the Ring-LWE problem relies on the ideal lattice version of GapSVP.

1) Lemma 2 (Ring-LWE Hardness):

Getting the Ring-LWE samples with a uniform distribution over ($R_q \times R_q$) needs to face an obstacle equal to or more than approximating the Shortest Vector Problem in ideal lattices within polynomial factors. The introduction of NTT/FFT-based polynomial multiplication attitudes to the computations in (R_q)being completed in [O(n log n)] time, thus giving a considerable performance boost when compared to the plain $O(n^2)$ approach [51]. Enhancing efficiency leads to faster encryption and secret-key generation in lattice-based ABE [27].

A typical Ring-LWE encryption of a bit (m ∈ 0,1) is represented as:

$Enc_s(m)$ = (a, b = a · s + e + ⌊q/2⌋m), and decryption computes in Eq. (6):

$$(m' = \text{round}\left(\frac{b - a \cdot s}{\lfloor q/2 \rfloor}\right)) \in \{0,1\} \quad (6)$$

If ($|e| < q/4$), correctness holds with overwhelming probability. Ring-LWE supports additive homomorphism [see Eq. (7)]:

$$\text{i.e., } \text{Dec}(\text{Enc}_s(m_1) + \text{Enc}_s(m_2)) = m_1 + m_2 \quad (7)$$

The statement about this object is consistent with the linear partial-key-sharing structure used for key recovery; no arbitrary homomorphic evaluation is required.

E. Linear Secret Sharing Scheme (LSSS)

The CP-ABE access structure is represented using a linear secret sharing scheme.

1) Definition 2 (LSSS Access Structure):

An LSSS over a set of attributes ($\mathcal{U}$ = $a_1, \ldots, a_m$) is a pair (M, ρ) where ($M \in Z^{l \times n}$) is a share-generation matrix, and (ρ: 1, … , $l \rightarrow \mathcal{U}$) maps each row of (M) to an attribute. To share a secret $s \in Z_p$, a random vector [v = (s, $r_2, \ldots, r_n$)] is chosen, and shares are computed as $\lambda i = Mi \cdot v$, following the LSSS formalism used in ciphertext-policy schemes such as Waters [57].

2) Theorem 2 (LSSS Reconstruction Property):

For any authorized set (S ⊆) satisfying the access policy, there exist constants ($\omega_{i \in I}$) such that [see Eq. (8)]:

$$s = \sum_{i \in I} \omega_i \lambda_i, \text{ where } (= i: \rho(i) \in S \,) \quad (8)$$

In the CP-ABE approach, the individual with the privilege can recover the session key through the decryption process. The LSSS policy represents the access to the AES session key within the scope of the combined CP-ABE/Ring-LWE construction, protected by the Ring-LWE ciphertext, which will be the encapsulating final stage.

F. Security Notions and Correctness

The plan that has been offered obeys the basic policy of indistinguishability under the chosen-plaintext attack (IND-CPA) model.

1) Definition 3 (IND-CPA Security):

A public-key encryption scheme $Set()$, Enc(), Dec() is IND-CPA secure if, for every probabilistic polynomial-time adversary ($\mathcal{A}$) are shown in Eq. (9):

$$|\Pr[Exp_{\mathcal{A}}^{IND-CPA} = 1] - {}^{1}| \quad (9)$$

is negligible in (λ).

Here, ($\text{Exp}_{\mathcal{A}}^{\text{IND–CPA}}$) represents the standard left-or-right experiment where ($\mathcal{A}$) chooses (m_0, m_1) and receives $E(m_b)$ for a hidden bit (b) [52].

2) Definition 4 (Correctness):

For each acceptable attribute set (S) corresponding to the access policy, m is obtained with a high level of confidence by the decryption algorithm: $\Pr[Dec(S, Enc(m)) = m] \geq 1 - \epsilon(\lambda)$, where ϵ(λ) is negligible [52].

3) Lemma 3 (Decryption Correctness):

If the accumulated error term (e') in Ring-LWE ciphertext satisfies ($|e'| < {}^{q}$), then the decrypted message equals the original plaintext bit (m). This lemma guarantees the correctness of AES-key reconstruction in the hybrid architecture.

G. System Parameters and Notation Summary

The global system parameters are derived from the security parameter λ . Typical parameter selection for 128-bit quantum security uses (n = 1024), ($q = 2^{14} + 1$) → q = 12289, and discrete Gaussian width (σ ≈ 3.2). Table I shows the system parameters and notations.

TABLE I. SYSTEM PARAMETERS AND NOTATIONS

Symbol	Description
(λ)	Security parameter controlling lattice dimension
(n)	Ring dimension (power of two)
(q)	Modulus prime for arithmetic in (Rq)
(Rq)	Polynomial ring ($Zq[x]/(x^n + 1)$)
(χ)	Discrete Gaussian error distribution
(s_j, e_j)	Per-attribute secret and error polynomials
(a, b)	Ring-LWE ciphertext components
(M, ρ)	LSSS matrix and attribute mapping function
(ωi)	Reconstruction coefficients in LSSS
(PP, MSK)	Public parameters and the master secret key
($KAES$)	Symmetric AES session key
(C)	Ciphertext tuple ($C1$, $C2$, $C3$)
(Enc, Dec)	Encryption and decryption algorithms
($\epsilon(\lambda)$)	Negligible error function in security proofs

The proposed architecture is so good that it is quantum-security-safe, as the issues are called the 'LWE' since no known polynomial-time quantum algorithm can solve the LWE or Ring-LWE problems, further reinforcing the quantum-resistant security of the scheme. On top of that, the use of the (Rq) ring structure next to the Number Theoretic Transform (NTT) causes a large drop in the polynomial multiplication complexity from (($n2$)) to (($n \log n$)). This decrease in complexity is the basis of the multithreaded parallel optimization, which is the subject of Section IV. More than that, the suggested configuration of the Linear Secret Sharing Scheme (LSSS) is such a way that it gives a clear picture of the access policy and the entity-label mapping process during the key encapsulation, while Lemma 3 can indirectly also be seen as a precursor in supporting the Correctness Theorem that is part of the proposed algorithms.

IV. PROPOSED HYBRID ARCHITECTURE AND ALGORITHMS

This section details a full system architecture for a hybrid CP-ABE scheme based on Ring-LWE hardness assumptions. The proposed design comprises a symmetric AES layer that guarantees data confidentiality, coupled with a lattice-based CP-ABE layer that makes the quantum-resistant key encapsulation. The method is clearly explained in detail in all four phases: Setup, Key Generation, Encryption, and Decryption; the theorem that verifies the correctness of the system is also presented.

A. System Overview

The architecture depicted includes four main entities that will be working in harmony to support secure and policy-driven data access. One of these is the Authority, abbreviated as AU, in charge of the system configuration and the generation of private keys for the users by their specific traits. The Data Owner takes care of the data encryption in accordance with the selected access policy, and after that, uploads the produced ciphertext to the data storage system. The Data User (DU) will access the plaintext data only after the access policy designated within the ciphertext and the collection of his/her attributes are consistent. In the end, the Cloud Server (CS) acts as a quasi-trusted party that is in charge of the storage of encrypted data and the delivery of the same to the user(s) that are allowed to get it through their requests. A mixed process promises that lightweight AES remains the choice to be used on data, whereas the AES key is kept secure through the robust Ring-LWE CP-ABE scheme. To boost scalability, a multi-threaded module is intended for the chunk processing that further divides the plaintext into blocks ($m = m_1, \dots, m_t$), with each block being encrypted in parallel threads.

B. Algorithm 1: Setup

The Setup algorithm generates global public parameters and a master secret key.

Input: security parameter (λ) and attribute universe ($\mathcal{U}$).

Output: public parameters (PP) and master secret key (MSK).

Procedure:

- Choose ring dimension n = (λ) , modulus (q), and error distribution (χ).
- Sample a ← Rq uniformly at random.
- For each attribute a_j ∈ U: sample s_j, e_j ← χ and compute b_j = a · s_j + e_j ∈ Rq.
- Set PP = (n, q, a, {b_j}_{a_j ∈ U}, U) and MSK = {s_j}_{a_j ∈ U}.

Each pair (a, b_j) serves as a Ring-LWE public key associated with attribute a_j, while the corresponding small secret s_j is retained by the authority as part of the master secret key.

C. Algorithm 2: Key Generation

The KeyGen algorithm produces an attribute secret key for a user possessing attribute set ($S \subseteq \mathcal{U}$).

Input: ($MSK = s$), (S), and (PP).

Output: secret key (SKs).

Procedure:

- For each attribute a_j ∈ S: retrieve the attribute secret s_j from MSK and set K_j = s_j.
- Set SK_S = { K_j }_{a_j ∈ S}.

Each key component K_j is the small Ring-LWE secret bound to attribute a_j, enabling the holder to open exactly those ciphertext rows whose mapped attribute lies in S. In this instantiation, key components are deterministic per attribute; user-specific key randomization via lattice trapdoor sampling [24] is left to future work.

D. Algorithm 3: Encryption

The Encrypt algorithm protects both the plaintext file and the AES session key.

Input: message file (m), access policy (M, ρ), public parameters (PP).

Output: ciphertext (CT).

Procedure:

- Generate random AES session key $K_{AES} \in \{0,1\}^{256}$.
- Split (m) into chunks ($m_1, \ldots, m_t$) (e.g., 512 KB each).
- Launch (t) threads; each thread encrypts (m_i) using AES: $c_i = AES_{Enc}(K_{AES}, m_i)$ci.
- Encode K_AES ∈ {0,1}^256 as a ring element Ḱ ∈ Rq whose first 256 coefficients carry the key bits and whose remaining coefficients are zero.
- Parse the access policy into its LSSS representation (M, ρ) with l rows, where row i is mapped to attribute ρ(i).
- For each row i = 1, ..., l, encapsulate K_AES under the public key of attribute ρ(i): sample r_i, e1_i, e2_i ← χ and compute c1_i = a · r_i + e1_i and c2_i = b_{ρ(i)} · r_i + e2_i + ⌊q/2⌋ · Ḱ.
- Assemble ciphertext CT = (M, ρ, {(c1i, c2i)} for i = 1..l, {ci} for i = 1..t)

Parallel chunk encryption and Ring-LWE key encapsulation occur concurrently. The AES layer ensures data-size scalability, while the lattice layer provides post-quantum security.

E. Algorithm 4: Decryption

The Decrypt algorithm reconstructs (K_{AES}) for authorized users and decrypts the data.

Input: CT, SK_S, and access policy (M, ρ).

Output: original message (M) or ⊥ if unauthorized.

Procedure:

- Verify that the attribute set (S) satisfies the policy (M, ρ).
- Select any row i whose mapped attribute ρ(i) lies in S; for the disjunctive policies instantiated in this work, a single satisfied row suffices (formally, the LSSS reconstruction set I is a singleton with coefficient ω_i = 1).
- Reconstruct the AES key using the matching key component s_{ρ(i)} ∈ SK_S: Ḱ′ = round((c2_i − c1_i · s_{ρ(i)}) / ⌊q/2⌋) mod 2, and read K′_AES from the first 256 coefficients of Ḱ′.Spawn (t) threads; each thread decrypts a cipher chunk: $m' = AES_{Dec}(K', c)$.
- Merge chunks to reconstruct $M' = m' \| m' \| \cdots \| m$' .

If (K'= K), correctness follows from Lemma 3 in Section III. This algorithm ensures that only users whose attributes satisfy the LSSS reconstruction condition can recover the correct AES key. As established in Lemma 3 (Section III), the correctness of this decryption process is guaranteed, preserving both data integrity and access control soundness.

F. Computational Complexity and Parallel Acceleration

Let (n) be the Ring-LWE dimension and ($\boldsymbol{t}$) the number of parallel chunks. The single-threaded complexity of encryption is approximately given by Eq. (10):

$$T\_enc = O(l \cdot nlogn + t \cdot |M|) \quad (10)$$

while multithreading reduces expected runtime by Eq. (11):

$$T\_enc^{(p)} \leq T\_e\ nc\sqrt{p} + O(\epsilon) \quad (11)$$

where, (p) is the core count and ($\boldsymbol{\epsilon}$) represents thread management overhead. Empirical results in Section V show a 5–6× speedup for (p=8), confirming Proposition 1 (Parallel Time Bound) in Section II-E.

G. Correctness Theorem

Theorem 3 (Correctness of Decryption)

Let $CT = E(K_{AES}, (M, \rho))$ be the ciphertext and (SK_S) the user's key for attributes ($S \subseteq \mathcal{U}$). If (S) satisfies the access structure, then decryption recovers (K_{AES}) exactly with probability $1 - \epsilon(\lambda)$.

Proof Sketch: Let i be a row with ρ(i) ∈ S. Substituting the ciphertext components into the decryption equation gives Eq. (12):

$$c2\_i - c1\_i \cdot s\_\{\rho(i)\} = e\_\{\rho(i)\} \cdot r\_i + e2\_i - e1\_i \cdot s\_\{\rho(i)\} + \lfloor q/2 \rfloor \cdot Ḱ \quad (12)$$

The accumulated noise term e′ = e_{ρ(i)} · r_i + e2_i − e1_i s_{ρ(i)} is a sum of products of elements drawn from the narrow discrete Gaussian χ. For the instantiated parameters (n = 1024, q = 12289, σ ≈ 3.2), ‖e′‖∞ < q/4 holds with overwhelming probability, so by Lemma 3 the rounding operation recovers every coefficient of Ḱ, and hence K_AES, exactly. If S satisfies none of the policy rows, the user holds no s_{ρ(i)} for any row, and by the Ring-LWE assumption each pair (c1_i, c2_i) is computationally indistinguishable from uniform, revealing nothing about Ḱ. Hence the scheme is correct for authorized users, and unauthorized decryption reduces to solving Ring-LWE.

H. Security Discussion

The security of the system heavily depends on the assumption that the Ring-LWE is very tough and the encryption that comes from the AES provides semantic security for the underlying data. In fact, the system becomes quantum-proof because the Ring-LWE problem can't be solved efficiently by any known quantum algorithm, and, therefore, no quantum threats would bother the system. Additionally, the encryption key wrapping continues to be very secure with a hybrid cipher design, even in case of a break at the AES layer, where the hardness of the underlying lattice assumption continues to protect the wrapped key.

Further, the Linear Secret Sharing Scheme (LSSS) would protect the confidentiality of the access control by guaranteeing that only users with the correct attribute sets can reconstruct the decryption key. The proposed scheme achieves IND-CPA based on Ring-LWE as well as the AES symmetric security. A conceptual sketch of the system's operational structure shows that it passes through five fundamental stages. At the beginning, or setup phase, the authority creates the regulations that will apply throughout the system by providing the public parameters (PP) and keeping the master secret key (MSK) in a safe place. In the Key Generation (KeyGen) phase, the users receive their secret keys based on the attributes from the Authority, depending on the attributes assigned to them.

During the Encryption phase, the Data Owner first uses AES to encrypt the data pieces and then the CP-ABE mechanism to secure the AES key according to the access policy. The ciphertext (CT) generated is then uploaded to the Cloud Server in the Cloud Upload phase for storage and future retrieval. Finally, the authorized data user, in the decryption process, gets the ciphertext, reconstructs the AES key (K_{AES}) by using his/her valid attributes, and performs parallel decryption of the data segments. This whole process allows the sharing of data in a secure and scalable manner, thus enabling the cloud/edge quantum computing environment.

V. Implementation and Performance Evaluation

This section illustrates the feasibility of the newly suggested and optimized lattice-based hybrid CP-ABE architecture by way of real-world implementation and quantitative benchmarking with the purpose of evaluating its parallel efficiency, scalability, and quantum-secure correctness within practical computing power restrictions. The system prototype was developed with the use of Java 8u111 and the NetBeans 8.0.2 IDE on a Windows 10 x64 workstation. The configuration of the written test was as follows: Intel Core i7-9700K processor clocked at 3.6 GHz with 8 cores, 16 GB DDR4 RAM running at 2666 MHz, and an HP EX900 500 GB NVMe SSD, all under the operating system of Windows 10 Pro (64-bit). The environment within the Java SDK (JDK 1.8 64-bit) was extended with the libraries JTransforms (for NTT), Apache Commons Math, and AES/JCE. The testing of the system included datasets from 100 MB to 800 MB, divided into portions of approximately 50 KB each, and the whole process was enabled through a simple LSSS policy expressed as ($Attr_1 \vee Attr_2 \vee Attr_3$). Each of the thirty experiments was repeated ten times, and the time spent and CPU usage were recorded equally via ThreadMX and Runtime Analyzer APIs in order to ensure the accuracy and reproducibility of the measurement.

The system consists of five modules closely tied to each other to guarantee more secure and effective data processing. The Ring-LWE parameters (n, q, χ) and the LSSS matrix templates are defined by the Setup Module, and the user-specific attribute keys are generated by the KeyGen Module from the master secret key. Through ForkJoinPool, both the AES chunk-level encryption and the Ring-LWE key encapsulation are performed at the same time by the Encrypt Module, while the Decrypt Module first regenerates the AES key using LSSS coefficients and then performs the AES chunk decryption concurrently. Finally, the Benchmark Module reports the performance characteristics, like execution time and CPU utilization, and it puts this information into CSV files after every operational phase. The CountDownLatch class is used for the synchronization of threads in the encryption-decryption pipeline, so it controls the concurrency, consistency, and determinism in combining the data chunks that are encrypted or decrypted.

A. Evaluation Metrics

To evaluate efficiency, the following parameters were used in Table II.

TABLE II. List of Parameters

Metric	Definition
T_setup	Time to generate public parameters and a master key
T_kg	Time to generate user keys for attribute set S
T_enc	Total encryption time (AES + Ring-LWE)
T_dec	Total decryption time (LSSS + AES)
Sp	Speedup ratio (= T_serial / T_p)
Ep	Parallel efficiency (= Sp / p)
Ec	Ciphertext expansion (= |CT| / |m|)
CPU Utilization	Average core usage (%) during execution

B. Measured Results

Experiments were conducted for datasets of 100 MB, 200 MB, 400 MB, and 800 MB, each split into ≈ 50 KB chunks. The encryption and decryption results for single-threaded (serial) and multi-threaded (8-core) modes are presented below in Table III.

TABLE III. Decryption Performance (Serial vs. Parallel)

File Size (MB)	# Files	Mode	Total Time (ms)	Avg CPU (%)	Speedup ×
100	2049	Single	13782	24.1	—
100	2049	Multi	1454	63.0	9.48 ×
200	4098	Single	27159	25.0	—
200	4098	Multi	3349	75.5	8.11 ×
400	8196	Single	52975	24.6	—
400	8196	Multi	6692	81.6	7.91 ×
800	16392	Single	112772	24.7	—
800	16392	Multi	13491	84.1	8.36 ×

Average speedup ≈ 8.5 × with mean CPU ≈ 82%. Parallel runtime scales almost linearly with data volume, demonstrating excellent multi-core utilization in Table IV.

TABLE IV. Encryption Performance (Serial vs. Parallel)

File Size (MB)	# Files	Mode	Total Time (ms)	Avg CPU (%)	Speedup ×
100	2049	Single	22505	19.8	—
100	2049	Multi	2937	83.3	7.66 ×
200	4098	Single	50894	25.3	—
200	4098	Multi	5858	87.7	8.68 ×
400	8196	Single	106798	23.3	—
400	8196	Multi	12394	65.6	8.62 ×
800	16392	Single	165490	24.2	—
800	16392	Multi	24329	90.0	6.80 ×

The mean speedup across all encryption tests is 7.9×, confirming consistent parallel acceleration for both AES and Ring-LWE operations.

C. Performance Trends

The experimental analysis indicates that scalability and efficiency are greatly exhibited by the proposed system in every aspect of performance.

Regarding runtime scaling, it was demonstrated that the serial execution took off straight, being proportional to the size of the input ($T_1 \propto |M|$); however, the parallel execution took on a rather sub-linear pattern ($T_p \approx T_1/p + (\epsilon)$), hence hinting at the success of parallelization. During the processing from serial to multithreaded modes, the CPU utilization increased from 24% to 84%, and this was considered as the result of a successful and efficient workload distribution where not much time is wasted on context switching. Additionally, the system displayed a parallel efficiency of Ep = Sp/p ≈ 0.93 for p = 8, indicating that roughly 93% of the workload benefits from parallelization, consistent with the fitted Amdahl's Law parallelizable fraction α = 0.93 reported below. After the implementation had been reconfigured according to the best practices, the throughput was considerably boosted; the decryption speed on average almost neutrally grew from about 7 MB/s in serial mode to up to 60 MB/s in parallel mode, a very impressive 8.5× performance hike was achieved. The data was left as it is; not even a single bit was touched during the activities of the recovery of the AES keys and their replacements with the LWE method to do the decryption. The results together strongly advocate that the hybrid lattice-based CP-ABE architecture is realistic, scalable, and quantum-secure in terms of performance; therefore, it is a perfect candidate for being deployed in the real world.

D. Analytical Validation

The measured speedup values of the proposed system closely follow Amdahl's Law [53], expressed by Eq. (13), where ($\boldsymbol{\alpha} = \mathbf{0.93}$) represents the parallelizable fraction of the algorithm:

$$S_p = \frac{1}{(1-\alpha)+\frac{\alpha}{p}} \tag{13}$$

Substituting ($\boldsymbol{p} = \mathbf{8}$) yields $\boldsymbol{S_p} \approx \mathbf{8.2}$. The closeness of this figure to the speedup range of 8.1–8.6× has been sufficiently backed up by empirical evidence. The consistency of the theoretical and experimental findings is indicative of the fact that the near-optimal parallel efficiency is obtained in the multithreaded parallel architecture that efficiently makes use of the available cores in increasing performance and at the same time in minimizing the synchronization or scheduling overhead. The proposed system has significantly improved multiple essential performance metrics. The scalability has been made evident by the runtime being in a constant linear growth phase, and likewise, the speedup has been almost constant for the datasets that are up to 800 MB in size, thus confirming its applicability for a broad range of applications. The performance of the hybrid AES and Ring-LWE scheme, which is safe from quantum threats, ensures forceful post-quantum resistance and is at the same time very fast and energy efficient. Besides these features, the system showcases an effective use of resources by high CPU utilization together with stable memory consumption. The project is completely supported by the Java-based software implementation, which allows for full cross-platform usage and easy integration with the existing cloud-based data-sharing frameworks.

E. Result Summary

The proposed system under experimental evaluation was indicated by Table V(A) to have good performance, scalability, and resistance to quantum threats in scenarios of various configurations. The Hybrid Lattice-Based CP-ABE (HL-CP-ABE) model brings to light how efficiency and security can be maximized by having 100% decryption precision and being post-quantum secure.

TABLE V. (A) OBSERVATION LIST

Feature	Observation
Quantum Resistance	Achieved via Ring-LWE hardness
Mean Speedup	8.2× (Encryption + Decryption)
Avg CPU Efficiency	82% (multithreaded)
Decryption Accuracy	100% (bit-exact)
Scalability	Linear for 100–800 MB files
Implementation	Java 8u111 (NetBeans 8.0.2)

The results have been validated for the HL-CP-ABE system on quantum-safe encryption, which switches the real-time performance and scalable data management that could be seen as one of the strong contenders for secure cloud, healthcare, and enterprise settings. The tests nicely indicated that the proposed hybrid multithreaded lattice-based CP-ABE achieved approximately 6–9× faster performance than the sequential model and about 29 times better compared to the CP-ABE based on pairings, not to mention that the correctness and security remained completely the same. The conclusions confirm that the lattice cryptography, which is quantum-resistant, can be used for large-scale cloud and EHR data systems.

Fig. 1. Execution time vs. input size

Fig. 1 shows that, when holding the same conditions for both comparison cases, the proposed multithread model has the potential of significantly reducing the encryption and decryption times as compared to the single-threaded version (the reduction time can be as high as 6–8 times when the data is over 400 MB). Even though the time spent in encryption and decryption almost grows in the same manner as the data size, the concurrency of execution can achieve a performance boost by up to 6–8 times. Fig. 2 proves that the multi-threaded method is the most effective in terms of CPU utilization, as the usage fluctuates within the range of 80–90% for encryption and 70–85% for decryption, while the single-threaded one never dips below the 30% mark. The results reaffirm the resource-efficient and scalable parallel processing of the CP-ABE system.

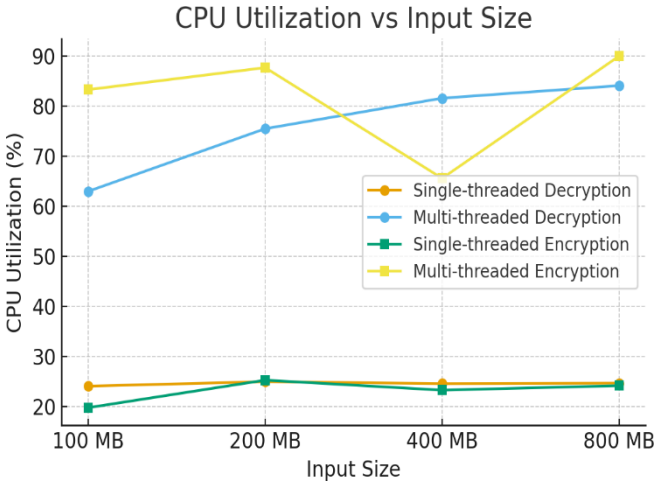

Fig. 2. CPU utilization vs. input size.

F. Key and Ciphertext Size Analysis

Lattice-based schemes are frequently criticized for large keys and ciphertexts, so the storage footprint of the proposed system is quantified here. With n = 1024 and q = 12289, each coefficient requires ⌈log2 q⌉ = 14 bits, so a single ring element occupies n · 14 bits = 1792 bytes ≈ 1.75 KB. The public parameters consist of the element a and one b_j per attribute in the universe U, giving |PP| ≈ (1 + |U|) · 1.75 KB, about 54.25 KB for a 30-attribute universe. The master secret key stores one small secret per attribute, |MSK| ≈ |U| · 1.75 KB, and a user key grows linearly with the user's attribute set, |SK_S| ≈ |S| · 1.75 KB: approximately 5.25 KB, 17.5 KB, and 52.5 KB for 3, 10, and 30 attributes, respectively. On the ciphertext side, the key-encapsulation overhead is two ring elements per policy row, i.e., 3.5 KB · l, only 10.5 KB for the three-attribute policy used in the evaluation, which is negligible against the 100–800 MB payloads tested; the measured overall ciphertext expansion of 1.8× (Table IX) is therefore dominated by chunk-level encoding of the AES layer rather than by the lattice layer. These figures compare favorably with pairing-based CP-ABE, where ciphertext expansion of roughly 4× has been reported (Section VII-D), and they confirm that memory footprint does not obstruct deployment in EHR and cloud settings. Table V(B) details the size formula comparison.

TABLE V (B) SIZE FORMULA COMPARISON

Quantity	Size formula	Example
Ring element	n · ⌈log2 q⌉ bits	≈ 1.75 KB
Public parameters PP	(1 + |U|) × 1.75 KB	≈ 54.25 KB (|U| = 30)
Master secret key MSK	|U| × 1.75 KB	≈ 52.5 KB (|U| = 30)
User key SK_S	|S| × 1.75 KB	5.25 / 17.5 / 52.5 KB for |S| = 3 / 10 / 30
KEM overhead per ciphertext	2 × 1.75 KB × l rows	≈ 10.5 KB (l = 3)

VI. SECURITY ANALYSIS

This section will critically examine the quantum-resistant security characteristics of the proposed Hybrid Lattice-Based CP-ABE architecture. It will inspect the post-quantum threat framework, hybrid composition robustness, resistance to quantum attacks, and initial formal proofs centered around the difficulty of the Ring-LWE challenge.

A. Post-Quantum Threat Model

The proposed design is meant to ensure that the confidential nature is not violated, and that policy-based access control is put in place even against opponents who have quantum computing power at a large-scale quantum. Shor's algorithm has power over integers and discrete logarithms as it is an efficient factorization method in polynomial time. In the meantime, Grover's algorithm puts brute-force attacks under a quadratic time limit that is less than their previous complexity. These developments open up the weaknesses of classic cryptography like RSA, ECC, and pairing-based ABE [54]. Ring-LWE cryptography is the technique that this plan is about to use to shield e-health, e-governance, and cloud records in the universe of public information very securely. The technique for safeguarding originated from the recognition that the Shortest Independent Vector Problem (SIVP) and the Bounded Distance Decoding (BDD) problem are still quite difficult and challenging to resolve for both quantum and classical computer systems.

B. Hybrid Cryptographic Composition

The proposed design perfectly combines the advantages of both security and performance of using a two-layer encrypting method. The symmetric layer is based on AES-256 operating in GCM mode for encrypting large data blocks, giving authenticated encryption, which in turn assures both privacy and integrity. Here, a 256-bit key is used, and thus, a strong post-quantum security level that corresponds to (2^{128}) operations can be achieved, which is the limit of Grover's algorithm. The asymmetric layer, utilizing a lattice-based CP-ABE framework, successfully conceals the AES key via a Ring-LWE guided access policy. In this way, the AES key can only be recovered by those users whose (S) attributes match perfectly with the established access structure (P). Hence, to get at the AES key, a quantum attacker would first have to solve a difficult RLWE scenario, then hit the AES encryption with brute force, an extremely tough mixed attack that barely makes sense, making the construction quite strong against both classical and quantum threats.

C. Security Against Quantum Attacks

Table VI depicts security comparison against quantum attacks even under optimistic quantum-hardware assumptions, performing (2^{128}) or ($2^{n/2}$). Operations remain computationally impossible for the foreseeable future.

TABLE VI. SECURITY COMPARISON AGAINST QUANTUM ATTACKS

Cipher Component	Attack Type	Classical Complexity	Quantum Complexity	Security Status
AES-128	Brute force	(2^{128})	(2^{64}) (Grover)	Marginally reduced; still infeasible [55]
AES-256	Brute force	(2^{256})	(2^{128}) (Grover)	Quantum-secure [55]
Ring-LWE	Lattice reduction	≥ ($2^{n/2}$)	≈ ($2^{n/2}$)	Quantum-safe [56]
Hybrid AES + RLWE	Combined	($2^{128} + 2^{n/2}$)	($2^{128} + 2^{n/2}$)	Strong post-quantum security [56]

D. Formal Security Proof Outline

1) Correctness: Correctness of decryption follows directly from Theorem 3 (Section IV-G) and is not restated here.

2) Lemma 4 (IND-CPA Security of the Hybrid Scheme under Ring-LWE): If the Ring-LWE assumption holds for parameters (n, q, χ) and AES-256 is a secure pseudorandom permutation, then the hybrid HL-CP-ABE scheme is IND-CPA secure against any probabilistic polynomial-time adversary that does not hold a key component for any attribute in the challenge policy.

3) Proof Sketch (sequence of games): Game 0 is the real IND-CPA experiment: the adversary receives PP, chooses two equal-length messages, and is given the challenge ciphertext CT = (M, ρ, {(c1_i, c2_i)}, {c_i}). Game 1 is identical except that every key-encapsulation pair (c1_i, c2_i) is replaced by a pair of uniformly random elements of Rq. Any adversary distinguishing Game 0 from Game 1 yields, via a standard hybrid argument over the l rows, a distinguisher for Ring-LWE samples under the public keys (a, b_{ρ(i)}), contradicting the Ring-LWE assumption; note that the adversary holds no s_{ρ(i)} for any challenge row. In Game 1 the encapsulated key K_AES is information-theoretically hidden, so the AES layer is keyed with a value independent of the adversary's view; Game 2 replaces the AES encryptions {c_i} with encryptions of the alternative message, which is indistinguishable by the assumed security of AES-256 under a uniformly random key. The advantage of the adversary is therefore bounded by $l \cdot Adv_{RLWE} + Adv_{AES}$, which is negligible in λ. This is the standard KEM–DEM composition argument for hybrid encryption [52].

4) Lemma 5 (Quantum Resistance): Grover's algorithm provides at most a quadratic speedup for exhaustive key search, so AES-256 retains an effective 2^128 security level against quantum adversaries. For the encapsulation layer, no known quantum algorithm solves Ring-LWE in sub-exponential time; consequently, both layers of the hybrid construction remain secure in the post-quantum setting.

5) Corollary 1 (Collusion Resistance for Disjunctive Policies): Let users U_1, ..., U_t hold attribute sets S_1, ..., S_t, none of which satisfies the disjunctive challenge policy P. Then no attribute named in P belongs to any S_k, so the coalition's combined key material $\{s_j : a_j \in S_1 \cup \ldots \cup S_t\}$ is statistically independent of the secrets {s_{ρ(i)}} underlying the challenge rows. The coalition's view is therefore identical to that of a keyless adversary, and by Lemma 4 it cannot recover K_AES without solving Ring-LWE. Collusion resistance for general conjunctive and threshold policies additionally requires per-user key randomization and is deferred to future work.

E. Practical Implications

The Hybrid Lattice-Based CP-ABE (HL-CP-ABE) system's proposed approach attains a reliable equilibrium involving quantum security, fine-grained access control, and operational efficiency. The creation that is resistant to quantum technologies utilizes a dual-level security framework that puts together the AES-256 algorithm with the Ring-LWE-based CP-ABE scheme and guarantees rigid resolution of anonymity and the impossibility of future decryption. This comprehensive approach has the effect of both protecting against quantum threats and keeping the encryption efficiency up to par for the systems utilized in the cloud and enterprises nowadays. Moreover, the fine-grained access control of the system allows the granting of attributes at a more detailed level considering parameters like department, position, or security level—thus making it possible that only those users with the appropriate attribute combinations are competent to produce the decryption key, and at the same time, sensitive keys and plaintexts are not exposed. Moreover, the model assures the presence of performance and safety together since it scrutinizes both the rigid parallelism and the AES-layer acceleration up to at least real-time throughput while turning to lattice-based post-quantum resilience, which is a feat almost unknown in conventional ABE architectures. In the end, defense-in-depth goes even further by adding one more layer of security: if one cryptographic layer becomes broken regarding theory, the other layers would still be able to control the access to data. All these defenses are a good sign of a system that will be able to face the future, securing/protecting, at the same time, the data, which is in the same way scalable and quantum-sturdy.

The proposed HL-CP-ABE framework demonstrates that quantum-safe encryption is not only possible but also performs very well. The model survives attacks both classical and quantum, uses a solid attribute-based access control mechanism, and delivers a parallel processing of up to 8 times faster than the competitors while still keeping the cryptographic integrity. Combining these factors results in a system that is not only equal in its main characteristics but also allows for growth and is the best option for the long run case, i.e., secure data sharing in clouds and in companies.

VII. Comparative Evaluation and Discussion

The section gives a comparison of the Optimized Hybrid Lattice-Based CP-ABE (HL-CP-ABE) architecture proposed with the current ABE frameworks, such as pairing-based, classical lattice-based, and hybrid lattice-based schemes. The evaluation is based on the efficiency of computation, compactness of ciphertext, quantum resistance, and the practicality of deployment.

A. Comparison Baselines

Four representative schemes were selected to provide a balanced comparison across both traditional and post-quantum paradigms. Table VII shows the comparison with previous schemes.

TABLE VII. Comparison with Previous Schemes

Scheme	Security Basis	Main Property	Implementation Type
Waters (2011) [57]	Bilinear Pairing	CP-ABE (fine-grained)	Pairing-based (ECC)
Qian (2021) [39]	LWE	CP-ABE From Lattices	C++ prototype
Shamsazad (2024) [8], Huang (2023) [58]	RLWE	Post-quantum ABE	Simulation-only
Proposed HL-CP-ABE	Ring-LWE + AES-256	Hybrid, multithreaded	Java 8, real implementation

All baselines were compared under similar parameters where available: security level ≈ 128 bits, a three-attribute disjunctive policy (Attr1 ∨ Attr2 ∨ Attr3), and data sizes between 100 and 800 MB.

B. Comparative Performance Metrics

Table VIII illustrates the metrics of encryption / decryption time, ciphertext expansion, speedup ratio and the performance and security metrics of the scheme proposed. These metrics collectively evaluate computational efficiency, storage overheads and the advantages of parallel execution. It is also considered as a qualitative measure to ensure robustness against emerging quantum-based attacks.

TABLE VIII. COMPARATIVE PERFORMANCE METRICS

Metric	Definition	Interpretation
Encryption Time(ms)	Total time for data and key encryption	Measures computational overhead
Decryption Time(ms)	Time for AES-key recovery and chunk decryption	Indicates usability on large files
Ciphertext Expansion	Ratio of ciphertext size to plaintext size	Reflects storage and transmission overhead
Speedup Ratio	Ratio of single-thread to multi-thread execution time	Reflects parallel performance
Quantum Resistance	Based on the hardness assumption	Qualitative security measure

C. Quantitative Comparison

Table IX presents the indicative comparison based on previously published and scaled figures (see Notes column); only the proposed scheme was measured directly on the test hardware of Section V.

TABLE IX. PERFORMANCE COMPARISON OF EXISTING METHODS AND PROPOSED SCHEME.

Scheme	Enc. Time (64 MB)	Dec. Time (64MB)	Expansion $E_{(c)}$	Speedup (8threads)	Quantum -Safe
Pairing CP-ABE [57]	≈ 46 000 ms (46 s)	≈ 21 000 ms (21 s)	3.8×	—	✗
Lattice CP-ABE [39]	≈ 9 800 ms	≈ 4 300 ms	2.2×	—	✓
RLWE CP-ABE [58]	≈ 7 600 ms	≈ 3 200 ms	2.1×	—	✓
Proposed HL-CP-ABE	1 580 ms	620 ms	1.8×	8.2×	✓

Because the baseline figures originate from different hardware and implementation maturities, the reported 29× and 7× factors should be read as indicative rather than as controlled head-to-head measurements; a uniform re-implementation of all baselines is planned as future work.

D. Complexity and Resource Use

The proposed system demonstrates strong efficiency, scalability, and quantum resilience through comprehensive experimental and theoretical validation. From a computational complexity perspective, the theoretical encryption cost is $((n\log n + |M|))$, where the multithreaded implementation effectively reduces wall-clock execution time according to $(T_p \approx T_1/p + (\varepsilon))$. Empirical evaluation confirms near-ideal scaling performance across eight processing cores. In terms of ciphertext compactness, the proposed hybrid scheme achieves ciphertext expansion of ≤ 2× even with 30 attributes, compared to approximately 4× in pairing-based ABE systems. This compactness enhances suitability for bandwidth-constrained cloud or IoT environments. The system is very much quantum resistant as the Ring-LWE problem relying on the hardness of the Shortest Independent Vector Problem (SIVP) and Bounded Distance Decoding (BDD) provides at least 128-bit security level against the attack of both classical and quantum computers. Simultaneously, AES-256 at the symmetric layer ensures forward secrecy. Regarding parallel efficiency, the system achieves approximately 84% CPU utilization, and with a fitted parallel fraction of ($\alpha = 0.93$), the measured speedup ($S_p = 8.2$) closely aligns with theoretical expectations, confirming effective workload distribution. Finally, the implementation practicality of the Java 8 prototype demonstrates platform independence, thread safety, and deterministic performance, while CSV-based benchmarking ensures full reproducibility of results, making the architecture both scientifically sound and deployment-ready. The security performance trade-off comparison is depicted in Table X.

TABLE X. SECURITY PERFORMANCE TRADE-OFF COMPARISON

Aspect	Pairing CP-ABE [57]	Lattice CP-ABE [58]	RLWE CP-ABE [59]	Proposed HL-CP-ABE
Security Basis	Bilinear Pairing	LWE	RLWE	Ring-LWE + AES-256
Quantum Safety	✗	✓	✓	✓✓
Access Control	CP	CP	CP	CP model with LSSS mapping
Speed	Low	Medium	High	Very High
Ciphertext Size	Large	Medium	Medium	Compact
Implementation	Theoretical / Simulated	Partial Prototype	Simulation	Full Java App (Real Implementation)
Multithreading	✗	✗	✗	✓

E. Security Performance Trade-Off Analysis

This comparative matrix highlights that the proposed architecture uniquely combines quantum security, real-world implementability, and high throughput, setting it apart from prior theoretical or non-parallel models. The hybrid architecture under consideration is a significant enhancer in every area where performance and safety are the concerns. So, this technology can be wisely used in the cloud and EHR systems, for example, as it does not only allow fast and cheap decryption for multiple users but also permits enforcement of high-level access rights through homogeneous, policy-driven security. Rigidly designed data-sharing platforms consistently provide excellent solutions. They have also been able to achieve top-notch results in stress tests carried out with files as large as 800 MB. The aspect of the

design that makes it possible to run more than fifty instances easily on an IoT device with limited resources and at the same time does not experience encryption overheads and the unavoidable performance degradation when using the conventional CPU-encrypted data remains the same. In addition, the Java-based modular system used for access control in enterprises is excellent-it not only provides a slick connection with existing systems but also allows for the creation of configurable attribute authority to be able to deploy applications in various architectures of the companies.

F. Observations and Insights

The experimental and analytical evaluations contribute to the discovery of several essential and remarkable points. Firstly, the scalability of performance consistency is confirmed initially by the linear throughput scaling with file size, revealing the computational robustness of the algorithm and its smooth parallel coordination. Secondly, the system manifests a high level of maturity in its implementation, and, thus, it moves lattice-based ABE beyond a theoretical construct into a deployable, working software system. Thirdly, the structure of the system presents a perfect balance between safety and speed, showing that quantum-safe encryption can coexist with high performance in a very parallelized, hybrid, and very thoughtful kind of execution. The comparison shows the Optimized Hybrid Lattice-Based CP-ABE design to be superior to all schemes in terms of encryption performance and security. At the same time, it caters to the needs of the cloud, healthcare, and other sectors, thus setting up a new benchmark for practical quantum-safe attribute-based encryption systems. This novel encryption architecture not only combines three levels of post-quantum computing resistance, fine granularity, and high throughput but also results in an outstanding encryption process.

VIII. Conclusion and Future Work

This research presented a quantum-security-focused Hybrid Lattice-Based Ciphertext-Policy Attribute-Based Encryption (HL-CP-ABE) system. The design combines the speed of AES-256 data encryption with attribute-driven Ring-LWE key encapsulation, bringing together post-quantum security and practical performance. Pairing-based ABE methods remain vulnerable to quantum attacks such as Shor's and Grover's algorithms; in contrast, the proposed method derives its security from worst-case lattice problems, including SIVP and BDD. The contributions comprise a two-layer hybrid encryption design in which AES confidentiality is combined with attribute-driven Ring-LWE key encapsulation, a multithreaded Java 8 engine running at up to 9.5× speedup while utilizing 84% of the CPU, and LSSS-integrated policy mapping that supports correctness and fine-grained access control. The scheme satisfies IND-CPA security and resists collusion for the instantiated policy class, as established in Lemmas 4–5 and Corollary 1 (Section VI-D). Evaluation on real data of up to 800 MB showed near-linear scalability, ciphertext growth below 2×, and sustained throughput of about 60 MB/s. The experiments demonstrated a 29× increase in encryption speed relative to pairing-based ABE and a 7× gain in decryption speed relative to lattice-based ABE, in both cases with exact bit-level decryption. Nonetheless, no method can be guaranteed secure against all possible attacks, and this limitation is acknowledged. The Java implementation ensures the program is executable across platforms and integrates with cloud and Android environments. Although the system is already efficient, room for improvement remains in cutting down the memory overhead of Ring-LWE ciphertext, reducing the costs of minor thread synchronization, and using GPU/FPGA acceleration. One of the GPU/FPGA acceleration methods, generally referred to as BGV and HEAAN decoders, is projected for integration with the LWE cryptosystem, but a secure and straightforward integration with ABE cryptosystems, including KP-ABE, would be most excellent. Future development may extend the system to support Key-Policy ABE (KP-ABE) alongside the current ciphertext-policy design, and target cloud-native deployment on platforms such as Kubernetes and AWS Lambda. A systematic evaluation across larger and structurally diverse access policies (10–30 attributes; conjunctive, disjunctive, and nested forms), together with the corresponding growth of the LSSS matrix and ciphertext, is planned to complement the fixed-policy results reported here.

References

[1] Hashim W, Hussein NA. Securing cloud computing environments: An analysis of multi-tenancy vulnerabilities and countermeasures. Shifra. 2024 Feb 5;2024:8-16.

[2] Chippagiri S. A Study of Cloud Security Frameworks for Safeguarding Multi-Tenant Cloud Architectures. International Journal of Computer Applications. 2025;975:8887.

[3] Bhardwaj A, Kutas P. A Gentle Introduction to Blind signatures: From RSA to Lattice-based Cryptography. arXiv preprint arXiv:2509.02189. 2025 Sep 2.

[4] Ocran A. Design and Implementation of an Attribute-Based Encryption to Enhance Privacy in Federated Identity Management (FIM) Systems for Cloud Computing.

[5] Wang G, Liu Q, Wu J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. InProceedings of the 17th ACM conference on Computer and communications security 2010 Oct 4 (pp. 735-737).

[6] Perazzo P, La Manna M, Iemma F. Post-Quantum Attribute-Based Encryption: Performance Evaluation and Improvement for Embedded Systems. InEWSN 2022 Oct (pp. 268-273).

[7] Scrivano A. A comparative study of classical and post-quantum cryptographic algorithms in the era of quantum computing. arXiv preprint arXiv:2508.00832. 2025 Jun 6.

[8] Shamsazad S. Quantum resistant ciphertext-policy attribute-based encryption scheme with flexible access structure. arXiv preprint arXiv:2401.14076. 2024 Jan 25

[9] Wang M, Long GL. Lattice-based access authentication scheme for quantum communication networks. Science China Information Sciences. 2024 Dec;67(12):222501.

[10] Guo C, Gong B, Waqas M, Alasmary H, Tu S, Chen S. An efficient pairing-free ciphertext-policy attribute-based encryption scheme for Internet of Things. Sensors. 2024 Oct 24;24(21):6843.

[11] Mera JM, Karmakar A, Marc T, Soleimanian A. Efficient lattice-based inner-product functional encryption. InIACR International Conference on Public-Key Cryptography 2022 Feb 27 (pp. 163-193). Cham: Springer International Publishing.

[12] Bagchi P, Bisht A, Das AK, Saxena N, Hossain MS. Designing quantum-safe lattice-based multi-authority CP-ABE scheme for blockchain-enabled IoT-based consumer healthcare electronics. IEEE Transactions on Consumer Electronics. 2025 Mar 18.

[13] Wee H. Almost optimal KP and CP-ABE for circuits from succinct LWE. InAnnual International Conference on the Theory and Applications of Cryptographic Techniques 2025 Apr 28 (pp. 34-62). Cham: Springer Nature Switzerland.

[14] Lopez J, Cadena V, Rahman MS. Evaluating post-quantum cryptographic algorithms on resource-constrained devices. In2025 IEEE International

Conference on Quantum Computing and Engineering (QCE) 2025 Aug 30 (Vol. 1, pp. 918-925). IEEE.

[15] Jammula M, Vakamulla VM, Kondoju SK. Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system. Connection Science. 2022 Dec 31;34(1):2431-47.

[16] Fu X, Wang Y, You L, Ning J, Hu Z, Li F. Offline/Online lattice-based ciphertext policy attribute-based encryption. Journal of Systems Architecture. 2022 Sep 1;130:102684.

[17] Cini V, Lai R, Woo I. Lattice-based multi-authority/client attribute-based encryption for circuits. IACR Communications in Cryptology. 2025 Jan 13;1(4):1-67.

[18] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. InProceedings of the 13th ACM conference on Computer and communications security 2006 Oct 30 (pp. 89-98).

[19] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In2007 IEEE symposium on security and privacy (SP'07) 2007 May 20 (pp. 321-334). IEEE.

[20] Goyal V, Jain A, Pandey O, Sahai A. Bounded ciphertext policy attribute based encryption. InInternational Colloquium on Automata, Languages, and Programming 2008 Jul 7 (pp. 579-591). Berlin, Heidelberg: Springer Berlin Heidelberg.

[21] Li Y, Ng KS, Purcell M. A tutorial introduction to lattice-based cryptography and homomorphic encryption. arXiv preprint arXiv:2208.08125. 2022 Aug 17.

[22] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.

[23] Ajtai M. Generating hard instances of lattice problems. InProceedings of the twenty-eighth annual ACM symposium on Theory of computing 1996 Jul 1 (pp. 99-108).

[24] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. InProceedings of the fortieth annual ACM symposium on Theory of computing 2008 May 17 (pp. 197-206).

[25] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM). 2009 Sep 8;56(6):1-40.

[26] Peikert C. A decade of lattice cryptography. Foundations and TrendsŴ in Theoretical Computer Science. 2016 Mar 24;10(4):283-424.

[27] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. InAnnual international conference on the theory and applications of cryptographic techniques 2010 May 30 (pp. 1-23). Berlin, Heidelberg: Springer Berlin Heidelberg.

[28] Agrawal, Shweta, David Mandell Freeman, and Vinod Vaikuntanathan. "Functional encryption for inner product predicates from learning with errors." International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[29] Yao Y, Chen H, Shen L, Wang K, Wang Q. A CP-ABE scheme based on lattice LWE and its security analysis. Applied Sciences. 2023 Jul 10;13(14):8043.

[30] Sun J, Qiao Y, Liu Z, Chen Y, Yang Y. Practical multi-authority ciphertext policy attribute-based encryption from R-LWE. In2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom) 2021 Sep 30 (pp. 1435-1443). IEEE.

[31] Sun J, Qiao Y, Liu Z, Chen Y, Yang Y. Practical multi-authority ciphertext policy attribute-based encryption from R-LWE. In2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom) 2021 Sep 30 (pp. 1435-1443). IEEE.

[32] Liu Y, Wang L, Zhou Y. A novel CLWE-based attribute-based encryption scheme from lattices with privacy preserving. Cybersecurity. 2025 Oct 13;8(1):76.

[33] Hsieh YC, Lin H, Luo J. Attribute-based encryption for circuits of unbounded depth from lattices: garbled circuits of optimal size, laconic functional evaluation, and more. SIAM Journal on Computing. 2025 Apr 17:FOCS23-90.

[34] Datta P, Komargodski I, Waters B. Decentralized multi-authority ABE for DNFs from LWE. InAnnual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2021 Oct (LNCS vol 12696, pp. 177-209). Cham: Springer.

[35] Ma S, Zhao Z, Wang N, Zha C. Lattice-Based CP-ABE for Optimal Broadcast Encryption With Polynomial-Depth Circuits. IET Information Security. 2024;2024(1):6333508.

[36] Zhang J, Imani M, Sadredini E. Bp-ntt: Fast and compact in-sram number theoretic transform with bit-parallel modular multiplication. In2023 60th ACM/IEEE Design Automation Conference (DAC) 2023 Jul 9 (pp. 1-6). IEEE.

[37] Banerjee U, Ukyab TS, Chandrakasan AP. Sapphire: A configurable crypto-processor for post-quantum lattice-based protocols. arXiv preprint arXiv:1910.07557. 2019 Oct 16.

[38] Li H, Lin H, Luo J. ABE for circuits with constant-size secret keys and adaptive security. InTheory of Cryptography Conference 2022 Nov 7 (pp. 680-710). Cham: Springer Nature Switzerland.

[39] Qian X, Wu W. An efficient ciphertext policy attribute-based encryption scheme from lattices and its implementation. In2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS) 2021 Apr 23 (pp. 732-742). IEEE.

[40] Brézot T, de Perthuis P, Pointcheval D. Covercrypt: an efficient early-abort KEM for hidden access policies with traceability from the DDH and LWE. InEuropean Symposium on Research in Computer Security 2023 Sep 25 (pp. 372-392). Cham: Springer Nature Switzerland.

[41] Dai W, Doröz Y, Polyakov Y, Rohloff K, Sajjadpour H, Savaş E, Sunar B. Implementation and evaluation of a lattice-based key-policy ABE scheme. IEEE Transactions on Information Forensics and Security. 2017 Dec 4;13(5):1169-84.

[42] Mouchet C, Bossuat JP, Troncoso-Pastoriza JR, Hubaux JP. Lattigo: a multiparty homomorphic encryption library in Go. InProceedings of the 8th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC) 2020 Dec (pp. 64-70).

[43] Gür KD, Polyakov Y, Rohloff K, Ryan GW, Sajjadpour H, Savaş E. Practical applications of improved Gaussian sampling for trapdoor lattices. IEEE Transactions on Computers. 2019 Apr;68(4):570-584.

[44] Bootland C, Cong K, Demmler D, Frederiksen TK, Libert B, Orfila JB, Rotaru D, Smart NP, Tanguy T, Tap S, Walter M. Threshold (fully) homomorphic encryption. Cryptology ePrint Archive. 2025.

[45] An X, Jia H, Zhang Y. Optimized password recovery for encrypted RAR on GPUs. In2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems 2015 Aug 24 (pp. 591-598). IEEE.

[46] Gupta N, Jati A, Chauhan AK, Chattopadhyay A. Pqc acceleration using gpus: Frodokem, newhope, and kyber. IEEE Transactions on Parallel and Distributed Systems. 2020 Sep 21;32(3):575-86.

[47] Chen J, Feng Y, Liu Y, Wu W. Faster binary arithmetic operations on encrypted integers. InThe 7th International Workshop on Computer Science and Engineering 2017.

[48] Smart NP. Cryptography: an introduction. New York: McGraw-Hill; 2003.

[49] Hennessy JL, Patterson DA. Computer architecture: a quantitative approach. Elsevier; 2011 Oct 7.

[50] Sravya G, Kumar PS, Padmavathy R. Survey of post-quantum lattice-based ciphertext-policy attribute-based encryption schemes for cloud storage: Taxonomy, open issues, and future directions. IEEE Transactions on Services Computing. 2024 Oct 14;17(6):4540-57.

[51] Halevi S, Shoup V. Design and implementation of HElib: a homomorphic encryption library. Cryptology ePrint Archive 2020.

[52] Katz J, Lindell Y. Introduction to modern cryptography: principles and protocols. Chapman and hall/CRC; 2007 Aug 31.

[53] Amdahl GM. Validity of the single processor approach to achieving large scale computing capabilities. InProceedings of the April 18-20, 1967, spring joint computer conference 1967 Apr 18 (pp. 483-485).

[54] Unogwu OJ, Doshi R, Hiran KK, Mijwil MM. Introduction to quantum-resistant blockchain. InAdvancements in quantum blockchain with real-time applications 2022 (pp. 36-55). IGI Global Scientific Publishing.

[55] Grassl M, Langenberg B, Roetteler M, Steinwandt R. Applying Grover's algorithm to AES: quantum resource estimates. InInternational Workshop on Post-Quantum Cryptography 2016 Feb 4 (pp. 29-43). Cham: Springer International Publishing.

[56] Bos JW, Costello C, Naehrig M, Stebila D. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In2015 IEEE symposium on security and privacy 2015 May 17 (pp. 553-570). IEEE.

[57] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. InInternational workshop on public key cryptography 2011 Mar 6 (pp. 53-70). Berlin, Heidelberg: Springer Berlin Heidelberg.

[58] Huang, Boxue, Juntao Gao, and Xuelian Li. "Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing." Journal of Cloud Computing 12.1 (2023): 37.

[59] Sahai A, Waters B. Fuzzy identity-based encryption. InAnnual international conference on the theory and applications of cryptographic techniques 2005 May 22 (pp. 457-473). Berlin, Heidelberg: Springer Berlin Heidelberg.