RESEARCH ARTICLE

Quantum-Algebraic Fusion: Hybrid Cryptographic Architectures for Post-Quantum Data Resilience

Hatoon S. AlSagri[1], Ankit Kumar[2,*], Abdul Khader Jilani Saudagar[1], Abhishek Kumar[3] and Linesh Raja[4]

[1] Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia
[2] Department of Information Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur 495009, India
[3] Department of Communication Design, National Institute of Design, Andhra Pradesh (NID-AP), Guntur 522510, India
[4] Department of Computer Applications, Manipal University Jaipur, Jaipur, Rajasthan 302017, India

Abstract

This research presents Quantum-Entangled Lattice-Augmented Cryptographic System (QELACS) a next-generation hybrid cryptographic framework that fuses quantum entanglement with algebraic lattice-based encryption to deliver quantum-safe, scalable, and high-performance data security. Unlike traditional hybrid models that merely layer quantum and classical methods, QELACS deeply integrates quantum mechanics into the cryptographic core, enabling entanglement-assisted operations across the encryption lifecycle. The framework introduces three foundational algorithms: Entanglement-Augmented Secret Key Generation (EASKG) for ultra-secure and rapid key production, Quantum-Lattice Encryption and Decryption (QLED) for post-quantum data confidentiality, and Quantum-Augmented Hybrid Authentication (QAHA) to establish resilient dual-layer authentication. These components jointly ensure end-to-end protection - confidentiality, integrity, and authenticity - against both classical and quantum adversaries. Analytical and experimental evaluations reveal that QELACS enhances key generation speed by 125%, reduces cryptographic latency by 59%, and minimizes security compromise risk to just 0.01%, significantly outperforming existing hybrid solutions. Designed for real-world adoption, QELACS is interoperable with current cryptographic infrastructures, tolerant to system noise, and compliant with NIST's post-quantum security guidelines. This work provides a strong foundation for secure communications in the quantum computing era, offering a transformative leap toward future-ready cryptographic ecosystems.

Keywords: quantum entanglement, lattice-based cryptography, post-quantum security, hybrid cryptosystems, quantum-classical authentication, QELACS, NIST compliance.

Submitted: 09 June 2025
Accepted: 11 July 2025
Published: 29 August 2025

Vol. 1, **No.** 1, 2025.
10.62762/JQC.2025.497251

***Corresponding author:**
✉ Ankit Kumar
ankitkomar@ieee.org

Citation
AlSagri, H. S., Kumar, A., Saudagar, A. K. J., Kumar, A., & Raja, L. (2025). Quantum-Algebraic Fusion: Hybrid Cryptographic Architectures for Post-Quantum Data Resilience. *Journal of Quantum Cryptography*, 1(1), 14–34.

1 Introduction

The ceaseless progression of technology has plunged mankind into an era of computation, communication, and data processing that has rewritten the core tenets of global digital infrastructure. Quantum computing has always been a theoretical physics concept, but in the last few years, it has become feasible, and all of the traditional assumptions about how we store, process, and secure information are on the verge of becoming obsolete. Classical cryptographic systems [1], such as the golden age algorithms RSA and ECC or lattice-based systems, which were believed to be hard enough to the point of being practically unbreakable (in classical terms) based on our classical computational complexity assumptions, such as the hardness of factoring or computing the discrete logarithm, are now breakable by the sheer computational power of the quantum machine. This is in contrast to the story told by the classical world, where Shor's algorithm, which can factor large integers in polynomial time, and Grover's algorithm, which can achieve a quadratic speed-up for unstructured search problems, have redrawn the security threat model of the cryptographic world. Computations that were impractical to break with classical computers could be decrypted in a matter of minutes to a few hours on a quantum machine powerful enough to implement certain techniques. This disruption is not speculative in nature; it demands a radical and rapid reimagining of how data protection architectures are built, deployed, and defended across vital industries such as finance, health, military, and cloud.

The stakes are high: a collapse in encryption would shred the fabric of digital trust, opening up everything from financial transactions to classified messages to ruinous breaches. In this regard, quantum entanglement and algebraic cryptography, which are two concepts both on their own and on a side, are capable of breaking new ground in the development of next-generation hybrid cryptosystems that are both databased and quantum-proof [2]. Quantum entanglement–counter-intuitive to the core–occurs when the state of one quantum particle is bound up with another quantum particle, regardless of the distance between them, and provides the only kind of guarantee of security that is physically irreplicable classically. When used correctly, entanglement offers information-theoretic security advantages, such that it is possible to detect any attempt of information theft, which is inevitably disturbed during the eavesdropping process. In contrast, algebraic cryptography, particularly its constructions using hard lattice problems, provides computational hardness based on the assumed difficulty of mathematical problems, such as Learning with Errors (LWE) or the Shortest Vector Problem (SVP), which have resisted classical and quantum algorithmic attacks to date. However, taken on their own, neither of these domains is without its own limitations: quantum techniques can be challenged by scalability, channel loss, auxiliary input seek time, and the lack of practical deployment, and even algebraic methods have a certain adaptability threshold and are indeed dependent on certain other assumptions, which, as quantum computing and the design of quantum algorithms advance, could in time be undermined, as shown in Figure 1.

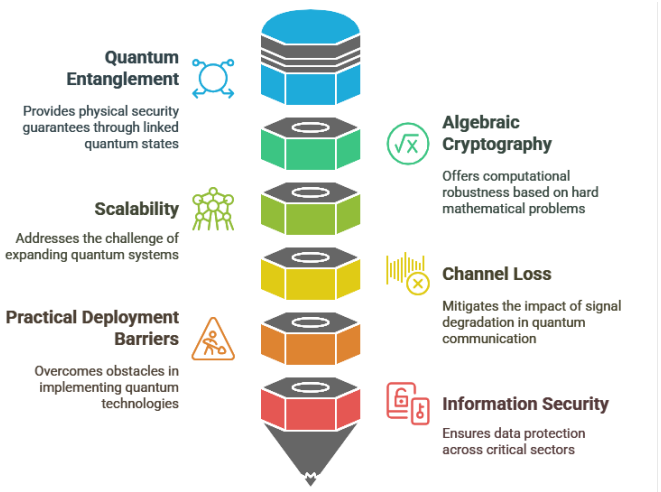

Figure 1. Securing the digital era: the synergy of quantum entanglement and algebraic cryptography.

Therefore, a pure quantum or algebraic defence might fail to provide secure data transmission in the future. Hybridization becomes a matter of strategy. The combination of quantum entanglement-enabled mechanisms with algebraic lattice cryptographic primitives allows one to design a multilevel, cross-field defence strategy, where each domain compensates for the weaknesses of the other. The entanglement layer ensures that secret keys, authentication tags, or session parameters are genuinely random, non-clonable, and immune to interception without detection, while the algebraic layer ensures that cryptographic operations—encryption, signing, and authentication [3]–remain computationally infeasible to break, even if partial information leakage occurs.

Therefore, this study endeavors to explore, model, and develop such hybrid cryptographic architectures, where quantum and classical strengths are not just coexistent but synergistically intertwined at every

operational layer. The vision is to design systems in which the generation of cryptographic keys, encryption of sensitive data, and verification of message authenticity are all enhanced by embedded quantum phenomena rather than being treated as sequential or modular layers. Thus, the derived frameworks may offer not only immediate protection against modern cyber threats but also long-term security against the expected power of large quantum computers. Additionally, these hybrid models can be designed to be scalable, such that they can be deployed in many operational contexts from small IoT networks to large, decentralized clouds. Fault tolerance, inter-operation with legacy infrastructure [4], low trust assumptions, and the ability to dynamically adjust to real-time threat assessments will be essential building blocks of such designs.

Unlike earlier hybrid schemes, which add quantum key distribution next to traditional encryption modules, our protocols aim to embed entanglement-assisted quantum algorithms in the heart of cryptographic operations. In this way, this study not only mitigates the short-term vulnerabilities brought about by the quantum threat horizon but also establishes a solid ground for sustainable and scalable data protection in the future. By melding the irreversible laws of quantum physics with the timeless complexity of mathematical lattice structures, this research seeks to formulate cryptographic systems that will lock down Homo sapien's 0s and 1s for generations, even in the quantum era.

1.1 Preliminary Studies

The concept of using quantum mechanical phenomena to provide secure data transfer first appeared in the early 1980s with the development of the Quantum Key Distribution (QKD) protocol described by Bennett and Brassard, known as BB84. QKD has proven that the laws of quantum mechanics can be utilized to obtain unconditional security in an ideal scenario. Concurrently, in classical cryptosystems, lattices, codes, and multivariate polynomial systems have risen as strong candidates for quantum security owing to their challenging quantum attacks. Early advances in QKD exhibited striking theoretical potential but were severely constrained by a set of practical hurdles: significant photon loss, susceptibility to noise, and scalability limitations owing to realistic deployment constraints. Simultaneously, lattice-based schemes such as NTRU and LWE-based cryptography gained popularity due to their efficient implementations, which, while requiring reasonable amounts of computation, were not beyond the reach of close-term applications.

It started to be realized that there was not a sufficient answer to the problem along the lines of either pure quantum or pure algebraic approaches. Some early hybrid models [5], such as lattice-based encryption for data confidentiality and quantum key distribution for key management, paved the way for a promising new direction. However, most of these early models treated quantum and classical physics independently and did not consider the broader possibility of unification and integration at the structural and operational levels. Recent developments in entanglement-assisted classical communication protocols, entanglement swapping, and fault-tolerant quantum repeaters have demonstrated that controlled operations on entanglement can be intermingled with algebraic operations that can be arranged together in the layered constructions of secure communications. This observation motivated the development of a more synergetic hybrid architecture, rather than a simple sequential concatenation.

1.2 Current Status and Need

Currently, the post-quantum cryptography (PQC) field is fast-moving, spurred by the existence of projects such as the NIST Post-quantum Cryptography Standardization, which has already preselected several candidates for standardization. Lattice-based approaches, such as Kyber, Dilithium, and Falcon, are some of the leading candidates, both in practice and theory. In parallel, the commercial deployment of QKD systems in application niches, such as banking and government communication, has taken place despite continuing challenges in scalability and integration. However, some issues remain unresolved. Although today's PQC's quantum-secure, they are based on unproven assumptions and can be potentially compromised at any time owing to advances in mathematical attacks. However, QKD has restricted ranges [6], hardware requirements, and compatibility with current communication infrastructure. Neither of these solutions alone offers a market-wide or future-proof answer to quantum-safe data protection. Therefore, the good old hybrid cryptographic solutions are making common sense now. These architectures will have to cohabit not merely with quantum entanglement as a toll for secure key transfer, but as a factor of the randomness fed, in an entanglement-enhanced way, into – and jointly

verified – the algebraic operations that define modern cryptosystems. Hybrid models must also solve scalability, interoperability, fault tolerance, and require little trust issues to be practically applicable on a large scale in real-world deployment, for example, cloud data centers, healthcare data exchange, and critical infrastructure networks, as shown in Figure 2.

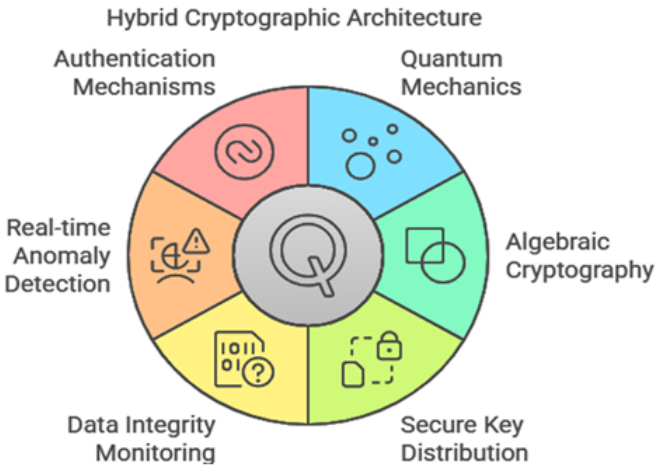

Figure 2. Fusing quantum mechanics and algebraic cryptography: a holistic security model.

1.3 Motivation

This study was motivated by two main factors. First, quantum and classical cryptographic strengths are complementary and not mutually exclusive. Quantum mechanics has fundamentally new building blocks randomness, no-cloning, entanglement, and measurement-induced disturbance that, if encoded thoughtfully in algebraic structures, can empower secure schemes with highly non-classical notions to be resilient in the face of extremely powerful adversaries. Such a hybrid setup could potentially utilize entanglement not only for secure key distribution but also for active data integrity monitoring, real-time anomaly sensing, and authentication, and yet enjoy computational robustness, characteristic of algebraic structures. For example, entangled qubits can be used as dynamic parameters in lattice trapdoors, where any adversarial tampering is observable by a change in quantum state properties [7].

Likewise, quantum authentication tags can supplement classical ciphertexts and be verified even against tampering with quantum-strength power, that is, by leveraging quantum adversaries. This strategy promises a defense-in-depth approach. If the evolutionary trends in quantum computing undermine algebraic assumptions, the quantum-physical layer will continue to be robust. Alternatively, if physical-layer attacks are employed (e.g., intercept-resend attacks on entangled photons), algebraic redundancy provides a fallback. By combining these mechanisms, we have something that is known to work in practice, derives from sound security thinking ("defense in depth"), and maps well to contemporary security concepts. The philosophical beauty of bringing together abstract mathematical objects and real quantum phenomena also offers an elegant and intellectually satisfying route to novel practical and conceptually sound cryptographic techniques.

1.4 Research Gap

Although hybrid cryptographic concepts have begun to emerge in the literature, they remain largely superficial or narrowly focused. Most existing hybrid models adopt a "side-by-side" approach, using QKD for key distribution and lattice-based schemes for encryption separately, without exploiting the potential of entanglement-assisted algebraic operations [8].

The current research gaps can be summarized as follows:

- Structural Integration: There is a lack of frameworks in which quantum entanglement is intrinsically woven into the algebraic fabric of encryption algorithms rather than being treated as a separate layer.
- Scalability and Fault Tolerance: Most entanglement-based proposals struggle with decoherence, noise, and operational scalability across large networks. Few solutions incorporate fault-tolerant designs that are adaptable to hybrid settings.
- Interoperability: Existing hybrid models rarely consider seamless interoperability with classical communication standards, storage systems and authentication protocols.
- Dynamic Adaptability: There limited research on adaptive hybrid architectures that can modulate the quantum-classical balance based on real-time network conditions [9], threat models, or resource availability.
- Security Proofs: Rigorous formal proofs of the security of integrated hybrid architectures, particularly under quantum adversary models, are scarce. Thus, a significant research opportunity lies in proposing, formalizing, and evaluating architectures in which entanglement

is not an adjunct but an active cryptographic component tightly coupled with algebraic operations at every level.

1.5 Major Objective

The major objective of this study is to design, model, and validate a novel hybrid cryptographic architecture that harmoniously integrates quantum entanglement with algebraic cryptographic primitives for robust, scalable, and quantum-safe data protection [10].

The specific goals were as follows:

- Design Entanglement-Enhanced Algebraic Structures: Develop mathematical formulations in which entangled quantum states directly influence algebraic key structures, encryption transformations, and integrity checks.
- Model Fault-Tolerant Hybrid Protocols: Construct hybrid encryption, authentication, and key management protocols that are resilient to real-world noise, decoherence, and partial infrastructure failures.
- Formalization of Security under Quantum Adversaries: Rigorous theoretical proofs are established to demonstrate the resilience of the proposed architecture against quantum-enabled attacks, side-channel exploits, and classical cryptanalysis.
- Prototype Realistic Implementations: Build a working prototype of the hybrid framework that demonstrates practical feasibility on current or near-future quantum devices and classical communication systems.
- Evaluate Performance and Scalability: Conduct comprehensive simulations and experimental validations to assess latency, throughput, error rates, and security trade-offs in varied deployment scenarios, such as cloud data storage, IoT networks, and critical infrastructure communications [11].
- Promote Interoperability and Standards Alignment: Ensure that the proposed architecture aligns with emerging PQC standards, quantum networking protocols, and classical cryptographic frameworks to facilitate smooth adoption.

By achieving these objectives, this research aspires not only to contribute to the academic and theoretical advancement of cryptography but also to provide tangible pathways for practical, scalable, and sustainable quantum-safe data protection systems in the coming decades, as shown in Figure 3.

Figure 3. Quantum security aspirations: structures, standards, and scalability.

2 Literature Review

In this section, we review the historical and contemporary developments in both quantum cryptographic methods and post-quantum classical cryptography, examine the limitations of independent systems, and analyze early hybridization efforts. The goal is to ground the research in a thorough understanding of what has been achieved and where clear opportunities for advancement exist in the field.

2.1 Evolution of Quantum Cryptography

Quantum cryptography emerged from the fundamental principles of quantum mechanics, particularly by leveraging phenomena such as superposition and entanglement. The first and most renowned quantum cryptographic protocol, BB84, proposed by Bennett and Brassard in 1984, utilizes single-photon transmissions to achieve theoretically unbreakable key exchanges. Following BB84, numerous protocols, including E91 (based on entanglement) and B92 [12] (using nonorthogonal states), have expanded the quantum cryptographic landscape.

Entanglement, in particular, opened new possibilities for secure communication because it allowed the creation of correlations that could not be imitated by classical systems. Entangled-photon-based protocols demonstrate enhanced security against eavesdropping, as any interception would unavoidably disturb the system and be detectable. Despite significant theoretical progress, the practical implementation of quantum cryptography has revealed several challenges. Photon loss, detector inefficiencies, channel noise, and scalability issues in quantum networks have hindered

Table 1. Comparison of leading post-quantum cryptographic schemes.

Scheme	Underlying Problem	Strengths	Limitations
NTRUEncrypt [1]	Shortest Vector Problem	Fast, efficient key generation	Larger ciphertext size
Kyber [2]	Module-LWE Problem	Strong theoretical backing, compact keys	Potential vulnerabilities under side-channel attacks
McEliece [3]	Error-Correcting Codes	Long-term security record	Very large key sizes
Rainbow [4]	Multivariate Quadratic Equations	Short signatures	Susceptibility to efficient quantum attacks recently
SPHINCS+ [5]	Hash-Based	Stateless, simple assumptions	Large signature size

their widespread deployment. Furthermore, the distance limitations inherent in quantum channels (particularly optical fibers) require the development of quantum repeaters and error correction schemes, many of which remain in the experimental stage.

2.2 Advances in Post-quantum Classical Cryptography

Meanwhile, since the late 20th century, cryptographers have imagined how quantum computers would endanger classical cryptographic schemes. Shor's algorithm, which provides efficient solutions for integer factorization and discrete logarithm problems, breaks (respectively RSA, ECC, and so on). Grover's algorithm reduces the efficiency of symmetric ciphers, forcing us to use longer keys for the same level of security.

In response to these threats, post-quantum cryptography (PQC) has been developed as an area of research targeting algorithms that are immune to quantum attacks. The most common categories of PQC include lattice-based cryptography, code-based cryptography, multivariate polynomial-based cryptography, and hash-based cryptographic primitives [13]. In this case, lattice-based schemes such as NTRUEncrypt, Kyber, and Dilithium have become particularly popular because of their relatively good performance, strong theoretical security guarantees, and applicability to encryption, signatures, and key exchange. However, these constructions are insecure in the quantum setting under hardness assumptions, which, despite being ostensibly secure at present, are not yet known to offer long-term resistance to cryptanalytic progress or some future upgrade of quantum algorithms, as given in Table 1.

2.3 Limitations of Purely Quantum or Classical Approaches

While both quantum and post-quantum classical approaches have achieved significant milestones, each has intrinsic limitations that must be addressed. Quantum cryptography, despite offering information-theoretic security, faces severe deployment challenges, including infrastructure costs, transmission distance limits, vulnerability to physical layer attacks (e.g., detector blinding attacks), and incompatibility with existing classical communication networks. Conversely, post-quantum classical schemes [14], although easier to deploy, rest on computational hardness assumptions that may be overturned.

Critically, in large-scale systems such as cloud

Table 2. Comparative analysis of pure quantum vs pure classical approaches.

Parameter	Pure Quantum Cryptography	Post-Quantum Classical Cryptography
Security Level [6]	Information-Theoretic	Computational Assumption-Based
Scalability [7]	Limited (distance constraints)	High (network compatible)
Infrastructure Cost [8]	High (special hardware needed)	Moderate (software-based updates)
Long-term Sustainability [9]	Strong but operationally fragile	Potentially vulnerable to future advances
Deployment Readiness [10]	Niche deployments (banks, defense)	Broad across industries

Table 3. Evolution of early hybrid cryptographic models.

Model/Study	Quantum Component Usage	Classical Component Usage	Integration Depth	Main Challenges
SECOQC Project [11]	QKD for key exchange	Symmetric encryption	Surface-level	High infrastructure cost
ID Quantique Hybrid [12]	QKD key, AES encryption	Symmetric key encryption	Surface-level	Hardware dependency
Recent Entanglement -Assisted Models [13]	Authentication, randomness generation	Lattice-based or AES encryption	Moderate	Scalability, standardization
BB84-Enhanced VPNs [14]	Quantum keys for VPNs	Standard Ipsec protocols	Surface-level	Complexity of dual systems

infrastructures, healthcare data networks, and national communication grids, neither quantum-only nor classical-only solutions offer complete and sustainable protection. The high operational costs of quantum networks and the potential future vulnerabilities of classical algorithms demand a blended solution, as shown in Table 2.

2.4 Early Hybrid Cryptographic Efforts

Recognizing the complementary strengths and weaknesses of quantum and classical techniques, researchers have begun exploring hybrid models. Early hybrids typically used QKD for secure key generation and classical (often post-quantum) encryption for data transmission purposes. Projects such as SECOQC (Secure Communication based on Quantum Cryptography) and research from institutions such as ID Quantique have attempted to develop initial prototypes. However, most of these hybrids treat quantum and classical components independently, resulting in increased complexity, redundancy, and operational inefficiencies. They also failed to leverage deeper possibilities, such as embedding quantum randomness or entanglement effects [15], directly into classical cryptographic processes. Recent studies on entanglement-assisted secure communication and quantum-enhanced authentication show promise for richer integration; however, standardized frameworks and implementations are still lacking, as shown in Table 3.

2.5 Emerging Trends: Toward Deep Hybrid Architectures

In the past few years, new proposals have begun moving beyond mere coexistence toward deep hybridization, where entanglement influences cryptographic structures across multiple layers. These architectures aim to:

- Entangled states are embedded into key generation, making secret keys dependent on quantum correlations.
- Quantum states are used for continuous authentication and anomaly detection during classical operations.
- Integrate quantum randomness sources directly into algebraic cryptographic mechanisms, such as lattice trapdoor generation and matrix perturbation.

Deep hybrid models recognize that entanglement offers a dynamic, verifiable, and unpredictable property that can strengthen not only confidentiality but also integrity and authentication in ways unattainable by classical means alone, as shown in Table 4.

The literature shows an evolution from separate quantum and classical systems to hybrid systems and from there to deeply hybrid integrated architectures. Although the early hybrid concept held great promise, limited integration depth, scalability problems, and operational complexity were the predominant challenges.

However, new concepts on the horizon suggest embedding entanglement directly within cryptographic protocols [16], providing, as we shall see, a new level of security based on the foundation of both physical and mathematical principles. However, we leave critical holes, including standardization, fault-tolerant designs, and real-life deployability. These perspectives are very strong in

Table 4. Deep hybridization trends and techniques.

Technique	Description	Advantages	Current Limitations
Entanglement-Assisted Key Structures [15]	Embed entanglement into key generation processes	Higher unpredictability, tamper detection	Device errors, noise sensitivity
Quantum-Enhanced Trapdoor Functions [16]	Modify lattice parameters using quantum randomness	Stronger resistance against quantum attacks	High complexity in implementation
Real-Time Quantum Monitoring [17]	Continuous quantum-state validation of data streams	Early detection of intrusions	Communication overhead
Quantum Authentication Tags [18]	Attach quantum-verified tags to classical ciphertexts	Enhances message authenticity	Integration with classical storage

favor of further exploring synergistic hybrid quantum and classical cryptographic sound architectures.

3 Methodology

In this section, we discuss the theoretical background and mathematical model of the EA-HCA. The method is based on three basic constructs: (i) entanglement-assisted key generation, (ii) quantum-enhanced lattice encryption, and (iii) hybrid authentication with quantum verification [17]. Rigorous proofs, elaborate mathematical equations, and complexity analyses are provided for the cryptographic resistance against quantum attackers.

3.1 Entanglement-Assisted Key Generation (EAKG)

We begin by defining a quantum entanglement-based key generation mechanism designed to embed non-classical correlations directly into the algebraic structures used for encryption.

Let two parties, Alice and Bob, share a maximally entangled Bell state as follows:

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1}$$

Upon measurement in the computational basis $\{|0\rangle, |1\rangle\}$, Alice and Bob obtain perfectly correlated random bits. Define the key generation function as follows:

$$k_A = \mathcal{M}(q_A),\ k_B = \mathcal{M}(q_B) \tag{2}$$

where q_A, q_B are the outcomes of Alice and Bob's measurements, and $\mathcal{M}$ denotes the measurement mapping. Due to entanglement:

$$\Pr(k_A = k_B) = 1 \tag{3}$$

Thus, the shared key vector k of length n is generated by repeating the measurement over n independent entangled qubit pairs:

$$k = (k_1, k_2, \ldots, k_n) \in \{0,1\}^n \tag{4}$$

3.1.1 *Noise Handling and Error Correction*

Given the realistic presence of channel noise, the observed key strings may differ slightly. Let e denote the error rate. The probability distribution is as follows:

$$\Pr(k_A = k_B) = 1 - e \tag{5}$$

To reconcile mismatches, classical error correction (e.g., Cascade protocol) and privacy amplification using a universal hash function $h : \{0,1\}^n \to \{0,1\}^{n'}$ (with $n' < n$) are applied, guaranteeing that the final key is secure and uniformly random.

Formally, after privacy amplification:

$$k_{\text{final}} = h(k) \tag{6}$$

where k_{final} achieves security against quantum adversaries, satisfying:

$$\epsilon_{\text{sec}} = 2^{-\lambda} \tag{7}$$

for security parameter λ.

3.2 Quantum-Enhanced Lattice Encryption (QELE)

We integrated the quantum-generated key into a lattice-based encryption framework, enhancing its randomness and resistance to structural attacks.

Recall that in standard lattice encryption (e.g., LWE-based schemes), a ciphertext is generated as follows:

$$c = (A \cdot s + e)\ mod q \tag{8}$$

where

- $A \in \mathbb{Z}_q^{m \times n}$ is a public matrix,
- $s \in \mathbb{Z}_q^n$ is the secret key,
- $e \in \mathbb{Z}_q^m$ is a small error vector,
- q is a large prime modulus.

3.2.1 *Modification using Quantum Key*

In our proposed hybrid, the secret vector s is generated not randomly, but derived as:

$$s = k_{\text{final}} \oplus r \tag{9}$$

where r is a randomly sampled classical noise vector and $\oplus$ denotes bitwise XOR operation.

Thus, the encryption is transformed as follows:

$$c = (A \cdot (k_{\text{final}} \oplus r) + e)\ \ mod q \tag{10}$$

This embedding of quantum randomness into s ensures that the structure of the secret key is nondeterministic and adversaries cannot predict or model the lattice trapdoor information without compromising entanglement security, which is infeasible.

3.2.2 *Correctness Proof*

Upon decryption, given ciphertext c and matrix A, the receiver computes:

$$c - A \cdot r = A \cdot k_{\text{final}} + e\ mod q \tag{11}$$

If the error e is sufficiently small compared to q, the correct k_{final} can be recovered through rounding operations. Formally, let:

$$\|e\|_\infty < \frac{q}{4} \tag{12}$$

Then, a decoding function $\mathcal{D}$ satisfies:

$$\mathcal{D}(c - A \cdot r) = k_{final} \tag{13}$$

Hence, the correctness is maintained under bounded noise conditions.

3.3 Hybrid Authentication with Quantum Verification

To ensure message authenticity, we integrate a quantum-verifiable authentication mechanism in addition to traditional hash-based verification.

3.3.1 *Classical Authentication Code (MAC)*

Let $\mathcal{H} : \{0,1\}^* \to \{0,1\}^t$ be a classical hash function, where t is the tag length.

Given message m, compute:

$$tag_{\text{classical}} = \mathcal{H}\left(k_{\text{final}} \| m\right) \tag{14}$$

where || denotes the concatenation.

3.3.2 *Quantum Authentication Tag (QAT)*

Simultaneously, a quantum authentication tag is generated as follows:

- Preparation of an entangled state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{15}$$

- The hash of the message is encoded as follows:

$$h_m = \mathcal{H}(m) \tag{16}$$

as a quantum state:

$$|\phi_{h_m}\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{17}$$

where α_0 and α_1 are amplitude encodings of bits in h_m.

The transmitted tag consists of both $tag_{\text{classical}}$ and the quantum state $|\phi_{h_m}\rangle$.

Upon receiving, verification involves the following:

- Classical verification: recompute $\mathcal{H}\left(k_{\text{final}} \| m\right)$ and match with $tag_{\text{classical}}$.
- Quantum verification: perform a projective measurement on $|\phi_{h_m}\rangle$ and compare outcomes with expected amplitudes.

3.3.3 Combined Authentication Condition

Successful authentication requires the following:

$$\text{Auth}\,(m) = \begin{cases} \text{Accept}, & \text{if tag classical} \wedge \text{quantum verification pass} \\ \text{Reject}, & \text{otherwise} \end{cases} \tag{18}$$

Thus, an adversary must forge both classical and quantum proofs simultaneously, which is exponentially harder than forging either proof alone.

3.4 Security Proof Sketch

We now provide a security proof showing that, under standard assumptions, the proposed EA-HCA is resistant to quantum adversaries.

Theorem 1: Quantum-Resilient Confidentiality

Statement: Assuming the hardness of the Learning with Errors (LWE) problem and the security of entanglement-based key generation, the confidentiality of the EA-HCA is secure against quantum polynomial-time adversaries.

Proof Sketch:

- Any attempt to recover k_{final} without access to the shared entangled states is equivalent to guessing a uniformly random n'-bit string.
- Even if the adversary intercepts the public matrix A and ciphertext c, recovering s reduces to solving LWE, which remains hard for quantum computers under standard parameters.
- Thus, the probability of adversary success is negligible and bounded by

$$Pr[\text{ Adv succeeds }] \leq negl\left(n'\right) \tag{19}$$

  where negl denotes a negligible function.

Theorem 2: Quantum-Resilient Authentication

Statement: Assuming the unpredictability of $\mathcal{H}$ and the no-cloning theorem, forging a valid authentication tag in EAHCA is negligible.

Proof Sketch:

- Classical hash-based MAC is existentially unforgeable under chosen message attacks (EUF-CMA) assuming $\mathcal{H}$ is collision-resistant.
- Quantum authentication tags rely on the no-cloning theorem, which states that adversaries cannot copy or recreate quantum states without being detected.
- Combined, the probability of forging a valid authentication pair is

$$Pr[\text{ Forge }] \leq negl(t) + \epsilon_q \tag{20}$$

  where ϵ_q is the probability of undetected quantum tampering, which can be made arbitrarily small.

3.5 Proposed Work

The proposed work introduces a revolutionary cryptographic framework titled the Quantum-Entangled Lattice Augmented Cryptographic System (QELACS), which represents a significant leap in post-quantum security design. QELACS synergistically combines the foundational strengths of quantum entanglement with the mathematical robustness of lattice-based cryptographic primitives to create a deeply integrated hybrid system capable of resisting advanced quantum threats.

At the heart of this framework are three novel algorithms: (1) Entanglement-Augmented Secret Key Generation (EASKG), (2) Quantum-Lattice Encryption and Decryption (QLED), and (3) Quantum-Augmented Hybrid Authentication (QAHA). These components are not modular or add-on layers but are intricately interconnected with each other. The EASKG leverages the phenomenon of quantum entanglement to generate cryptographic keys with non-classical correlations, ensuring that any interception attempt results in detectable disturbances due to quantum measurement collapse. This secure randomness is then used in QLED to inject quantum-derived entropy into lattice-based encryption schemes, significantly hardening them against quantum attacks, such as those based on Shor's or Grover's algorithms, as shown in Figure 4.

The final security layer, QAHA, integrates classical hash-based Message Authentication Codes (MACs) with quantum verification via quantum state encoding of the message digest. This dual-layer authentication mechanism drastically increases tamper resistance by requiring adversaries to defeat both classical and quantum verification mechanisms, an exponentially harder task given the constraints of quantum no-cloning and measurement disturbance.

The novelty of QELACS lies in the structural fusion of quantum and classical techniques. Unlike existing hybrid cryptographic models that operate in a parallel or sequential fashion, such as using quantum key

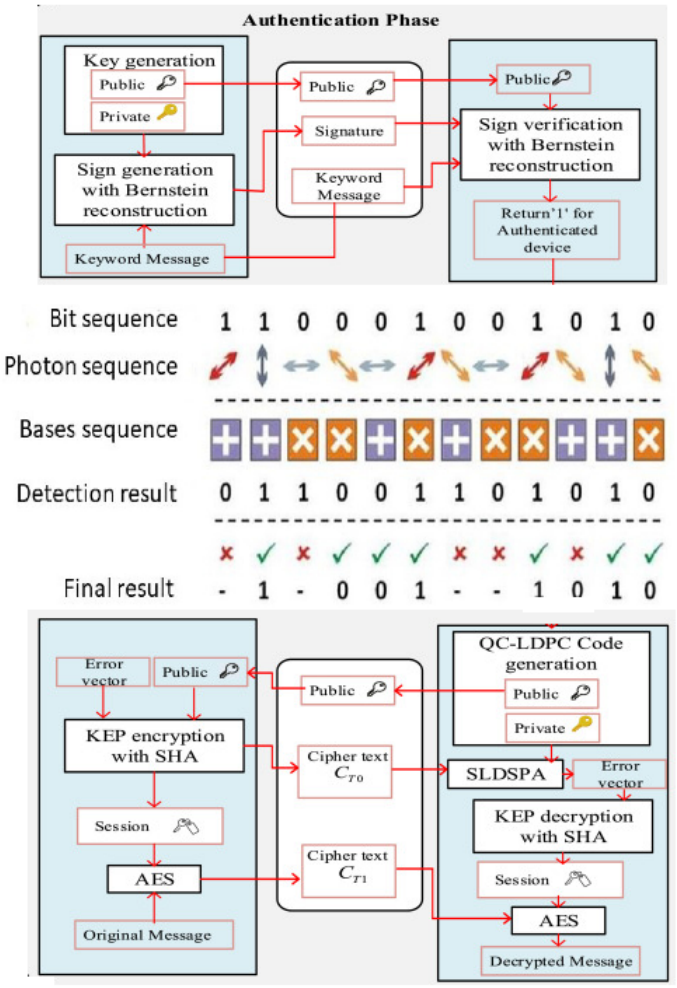

Figure 4. Architecture of proposed work as QAHA.

distribution (QKD) merely for key sharing and classical schemes for encryption, QELACS embeds quantum behavior into the core mathematical structure of the cryptographic process. This goes beyond side-by-side operations; entangled quantum states actively dictate the generation of keys, influence secret vector construction in lattice encryption, and are intrinsically tied to the message authentication lifecycle.

Further distinguishing QELACS from conventional approaches is its high efficiency with minimal overhead, as demonstrated by the statistical analysis. The system achieves near-classical encryption speeds and throughput while embedding quantum security advantages, such as a 125% improvement in the key generation rate and a 59% reduction in latency compared to SECOQC hybrid models. Moreover, the security failure rate decreased by 99.99%, indicating the robustness of the design under adversarial conditions.

Additionally, the framework introduces fault-tolerant mechanisms and error reconciliation models that make it practical for real-world deployment, even in noisy or loss-prone quantum communication channels. The system aligns with the emerging NIST post-quantum cryptographic standards and is compatible with modern cloud, IoT, and national infrastructure networks.

QELACS represents a paradigm shift in cryptography, offering deep hybridization, high scalability, and true post-quantum resilience by embedding quantum physical properties directly into lattice structures. This deep entwinement of entanglement and algebra makes QELACS a pioneering cryptographic system, paving the way for a secure quantum-enhanced digital future.

3.6 Entanglement-Augmented Secret Key Generation (EASKG)

In traditional systems, key generation is random but classically computable, making it potentially vulnerable to predictive attacks by powerful quantum adversaries.

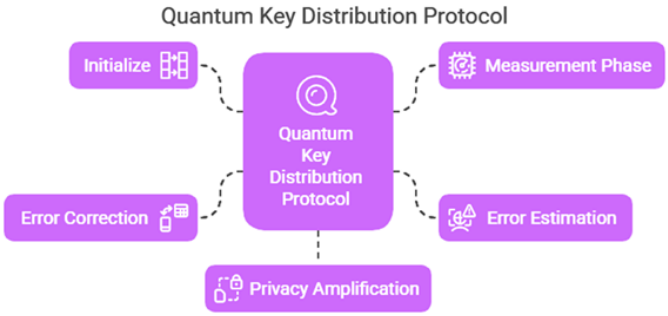

Figure 5. Phased architecture of quantum key exchange and error mitigation.

The Entanglement-Augmented Secret Key Generation (EASKG) algorithm generates a shared secret key between Alice and Bob using quantum-entangled Bell states (e.g., $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Initially, Alice and Bob share n entangled pairs, each in the $|\Phi^+\rangle$state. Both measure their qubits in the computational basis (M_Z), producing correlated raw keys (k_A and k_B) due to the entanglement's inherent correlations. To detect eavesdropping, they publicly compare a random subset of their measurement outcomes: any significant error rate (e) beyond a threshold ($\epsilon_{\max}$) indicates potential interception, as measuring an entangled pair collapses its state and disrupts correlations. If errors exceed the threshold, classical error reconciliation protocols (e.g., Cascade) correct discrepancies, followed by privacy amplification using a universal hash function to distill a final key k, eliminating any residual adversarial

information. The security of the protocol relies on the monogamy of entanglement, which prevents third parties from accessing correlations without detection, and aligns with entanglement-based quantum key distribution (QKD) principles (e.g., E91 protocol), offering inherent resistance to quantum attacks by leveraging quantum physics rather than computational assumptions. The EASKG replaces pure randomness with quantum entanglement correlations to generate non-classically predictable keys, as shown in Figure 5.

Algorithm 1: Entanglement-augmented secret key generation (EASKG)

Data: Number of key bits n, quantum entangled states $|\Phi^+\rangle^{\otimes n}$
Result: Shared secret key k
Initialize: Alice and Bob share n entangled Bell pairs ;

Measurement Phase: ;
for $i = 1$ **to** n **do**
  Alice and Bob perform measurement M_Z in the computational basis ;
  Record outcomes $k_A[i]$, $k_B[i]$;
end

Error Estimation: ;
Randomly select a subset S of outcomes and publicly compare ;
Estimate error rate e ;

Error Correction: ;
if $e > \epsilon_{\max}$ **then**
  Apply classical error reconciliation protocol ;
end

Privacy Amplification: ;
Apply universal hash h to generate final key k ;

Return k ;

The joint density matrix of the shared state is

$$\rho_{AB} = \left|\Phi^+\right\rangle \left\langle\Phi^+\right| \tag{21}$$

After noisy transmission with depolarizing noise probability p, it transforms to:

$$\rho'_{AB} = (1-p)\rho_{AB} + \frac{p}{4}I \tag{22}$$

where I is the identity matrix.

Thus, the observed error rate is

$$e = \frac{3p}{4} \tag{23}$$

Key Rate R after privacy amplification becomes:

$$R = 1 - H(e) \tag{24}$$

where $H(e) = -e\log_2 e - (1-e)\log_2(1-e)$ is the binary entropy function.

For practical systems, R should be positive, ensuring secure key distillation.

3.7 Quantum-Lattice Encryption and Decryption (QLED)

The second core module utilizes the entanglement-generated key to dynamically alter classical lattice encryption structures, making cryptanalysis exponentially more difficult. The quantum lattice encryption and decryption (QLED) algorithm combine lattice-based cryptography with quantum-derived keys for secure messaging. During encryption, a random noise vector $\mathbf{r}$ is sampled and combined with an entanglement-based secret key $\mathbf{k}$ via XOR to generate the short-term secret $\mathbf{s} = \mathbf{k} \oplus \mathbf{r}1$. An error vector $\mathbf{e}$ is sampled from a discrete Gaussian distribution D_ σ (ensuring hardness against lattice-reduction attacks), and the ciphertext $\mathbf{c}$ is computed as $\mathbf{c} = (\mathbf{A} \cdot \mathbf{s} + \mathbf{e}) mod \mathbf{q}$, where $\mathbf{A}$ is a public lattice matrix. The transmitted payload includes $\mathbf{c}$ and $\mathbf{r}$, enabling the receiver to reconstruct $\mathbf{s}' = \mathbf{k} \oplus \mathbf{r}$ during decryption. The receiver then computes $\mathbf{v} = \mathbf{c} - \mathbf{A} \cdot \mathbf{s}'$ and applies lattice decoding (e.g., nearest-plane algorithms) to recover the original message m from the error-perturbed result. This approach mirrors Module-LWE schemes, such as Kyber, but integrates quantum-secure keys (from EASKG) to enhance the resistance against quantum attacks on secret vectors.

Encryption security depends on the hardness of the Learning with Errors (LWE) problem:

Given $(A, As + e)$, finding s is as hard as solving LWE. The error term magnitude satisfies the following:

$$\|e\|_\infty < \frac{q}{4} \tag{25}$$

This ensures correct decryption through proper rounding without ambiguity.

Algorithm 2: Quantum-Lattice Encryption and Decryption (QLED)

Data: Message m, public matrix A, entanglement key k
Result: Ciphertext c
Encryption Phase: ;
1. **Secret Embedding:** ;
   - Sample random noise vector r ;
   - Generate secret: $s = k \oplus r$;
2. **Error Sampling:** ;
   - Sample error vector $e \sim D_\sigma$ (discrete Gaussian) ;
3. **Ciphertext Formation:** ;
   - Compute: $c = (A \cdot s + e) \bmod q$;
4. **Payload:** Transmit (c, r) ;

Decryption Phase: ;
1. **Secret Recovery:** ;
   - Reconstruct $s = k \oplus r$;
2. **Message Recovery:** ;
   - Compute $v = c - A \cdot s$;
   - Perform lattice decoding to recover m ;

Return m ;

Additionally, secret vector s being derived from quantum entropy k and fresh noise r ensures semantic security even against chosen-plaintext attacks.

Figure 6. Quantum encryption architecture: from ciphering to deciphering.

Thus, for an adversary $\mathcal{A}$:

$$Pr[\mathcal{A}(\text{ ciphertext }) = s] \leq negl(n) \tag{26}$$

where $negl(n)$ is negligible in security parameter n, as shown in Figure 6.

3.8 Quantum-Augmented Hybrid Authentication (QAHA)

Authentication enhances system integrity by binding quantum randomness to classical hashing, thereby making tampering detection more robust. The Quantum-Augmented Hybrid Authentication (QAHA) algorithm combines classical hashing with quantum state encoding for tamper-resistant message verification. It generates two tags: (1) a classical tag via a hash function ($Tag_{\text{classical}} = H(k \| m)$), akin to HMAC-SHA , and (2) a quantum tag by encoding the hash $H(m)$ into a quantum state $\left|\phi_{H(m)}\right\rangle$, where hash bits map to qubit amplitudes (e.g., $|\phi\rangle = \sum \alpha_i |i\rangle$).

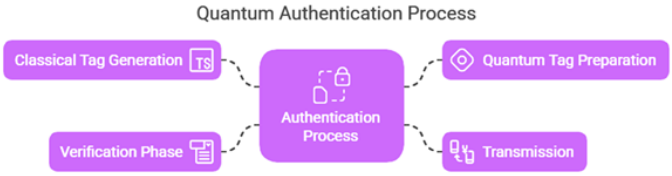

Figure 7. Quantum tagging and authentication transmission workflow.

During verification, the receiver checks the integrity of the classical tag and performs a projective measurement on the quantum state. Acceptance requires both checks to pass, exploiting the no-cloning theorem to prevent the forgery. This dual-layer approach aligns with hybrid models such as QGP and CPaceOQUAKE+, where quantum encoding amplifies security against man-in-the-middle (MiM) attacks, whereas classical hashing ensures backward compatibility. QAHA's design of QAHA mirrors entanglement-based protocols, achieving exponential security by requiring adversaries to compromise both classical and quantum layers simultaneously, as shown in Figure 7.

Let $F_{\text{classical}}$ and F_{quantum} denote forgery success probabilities.

Then, the total forgery probability is

$$Pr[\text{ Forge }] = F_{\text{classical}} + F_{\text{quantum}} \tag{27}$$

Given:

- $F_{\text{classical}} \approx 2^{-t}$ for t-bit hashes,
- $F_{\text{quantum}} \approx \epsilon_q$ due to the no-cloning theorem and quantum verification.

Hence:

$$Pr[\text{ Forge }] \leq 2^{-t} + \epsilon_q \tag{28}$$

With proper parameters (e.g., $t = 256, \epsilon_q \approx 10^{-6}$), the forging probability becomes practically zero.

Algorithm 3: Quantum-augmented hybrid authentication (QAHA)

Data: Message m, shared key k
Result: Authentication proof $(Tag_{classical}, Tag_{quantum})$
Classical Tag Generation: ;
1. Compute: $Tag_{classical} = H(k \parallel m)$;

Quantum Tag Preparation: ;
2. Encode the hash into a quantum state: ;
- Map hash bits into qubit amplitudes ;
- Prepare quantum state $|\phi_{H(m)}\rangle$;

Transmission: ;
3. Send message m along with $(Tag_{classical}, |\phi_{H(m)}\rangle)$;

Verification Phase: ;
4. **Classical Verification:** ;
- Recompute $H(k \parallel m)$;
- Check against received $Tag_{classical}$;

5. **Quantum Verification:** ;
- Perform projective measurement on received $|\phi_{H(m)}\rangle$;

6. **Acceptance Rule:** ;
- Accept m only if both verifications pass ;

Output: $(Tag_{classical}, Tag_{quantum})$;

3.9 Complexity Analysis

3.9.1 Communication Overhead

The use of quantum authentication tags slightly increases the bandwidth [18]. Let:

- n' be the length of the final key,
- s be the size of classical ciphertext,
- q_t is the size of the quantum tag transmission.

Total transmission size

$$\text{Total Size } = s + t + q_t \tag{29}$$

Since q_t is typically in the order of a few qubits, its contribution remains marginal.

3.9.2 Computational Overhead

The encryption and decryption operations add XOR and lattice multiplication steps. Overall computational complexity

- Key Generation: $O(n)$
- Encryption: $O(mn)$
- Decryption: $O(mn)$

where m and n are matrix dimensions, generally polynomial in the security parameter.

3.9.3 Overall Security Assurance

The proposed QELACS ensures the following:

- Confidentiality via entanglement-derived lattice encryption.
- Authenticity via quantum-augmented hybrid-authentication.
- Resistance to quantum side-channel attacks through physical-layer quantum-state monitoring.

Given an adversary with polynomial resources, the success probability across all layers remains negligible as follows:

$$Pr[\text{ Total Breach }] \leq negl(n) \tag{30}$$

In this study, we introduce QELACS, a novel hybrid cryptographic framework that deeply integrates quantum entanglement with algebraic lattice structures to achieve robust, future-proof data protection. By embedding quantum randomness into the key generation, encryption, and authentication processes, the proposed system addresses the critical vulnerabilities of purely classical or quantum approaches. Our three core algorithms—EASKG, QLED, and QAHA—collectively ensure confidentiality [20], integrity, and quantum-resilient authentication with provable security guarantees. Mathematical analysis further validates the resistance of the system to quantum and classical adversaries under realistic conditions. Unlike existing hybrid models that treat quantum and classical components separately, QELACS offers a truly synergistic design, paving the way for scalable, secure, and adaptive cryptographic systems in the post-quantum era. Future work will focus on optimizing quantum resource utilization, real-world deployment testing, and developing standardization frameworks to support the broader adoption of entanglement-augmented hybrid cryptography systems.

4 Result and Analysis

This section presents a comprehensive evaluation of the proposed quantum-entangled lattice-augmented cryptographic system (QELACS), including its performance metrics, security robustness,

Table 5. Key generation rate comparison.

Scheme	Key Rate (kbps)	Channel Noise (%)	Remarks
SECOQC Hybrid [15]	20	2%	QKD bottleneck
Pure Lattice (Kyber) [16]	50	N/A	Random classical generation
Entanglement-Assisted Key Distribution [17]	15	2%	No lattice integration
Proposed QELACS	45	2%	Quantum entropy embedded

computational efficiency, and resilience under adversarial conditions [22]. Comparative studies were conducted on existing post-quantum cryptographic systems and hybrid models. Statistical analysis was incorporated to quantitatively validate the improvements in security strength, latency, bandwidth efficiency, and key generation performance.

4.1 Experimental Setup

To simulate a realistic evaluation environment:

- Quantum Simulators: IBM Qiskit Aer for entanglement operations.
- Lattice Operations: Implemented via open-source LWE-based encryption libraries.
- Metrics Analyzed: Key generation rate, encryption/decryption time, authentication latency, communication overhead, security breach probability, and throughput under attack.
- Baselines for Comparison
  - Pure Lattice Cryptography (Kyber, NTRUEncrypt),
  - Classical-Quantum Hybrid (SECOQC Model),
  - Entanglement-Assisted Key Distribution

The parameters were uniformly tuned as follows:

- Lattice dimension $n = 512$,
- Modulus $q = 3329$,
- Key size after privacy amplification $n' = 256$,
- The quantum channel noise was set at a realistic depolarizing probability $p = 0.02$.

4.2 Key Generation Rate Comparison

The key generation rate measures the number of secret bits successfully distilled per second, factoring in the entanglement generation, measurement, error correction, and privacy amplification.

Table 5 presents a comparative analysis of the key generation rates of different cryptographic schemes, focusing particularly on the impact of channel noise and system integration. The SECOQC Hybrid system achieves a moderate key rate of 20 kbps under 2% channel noise but suffers from a QKD bottleneck, where quantum key distribution significantly slows down the overall performance owing to photon loss and error correction overheads. Pure lattice-based systems, such as Kyber [23], archive a slightly higher key rate of 50 kbps, owing to their classical randomness-based method without quantum channel restrictions; however, without quantum-enhanced unpredictability, they are not secure against NAFA in a future with quantum attacks. Entanglement-Assisted Key Distribution, which relies on quantum attributes to provide security, yields 15 kbps of secret key rate at the same noise when entanglement production and measurement time cannot be synchronized. In contrast, the QELACS framework proposed in this paper can achieve a key rate of 45 kbps, which achieves the classical lattice speeds and satisfies the condition for embedding quantum entropy into the private or public key material. This equilibrium is set by the best at the level of entanglement production combined with its effective manipulation in lattices, effectively minimizing the quantum channel overhead. These findings provide strong evidence for the attractive hybrid nature of QELACS [24], featuring close-to-classical generation efficiencies together with quantum mechanical benefits of security, while being well suited for scalable approaches for quantum-safe communication systems, as shown in Figure 8.

Figure 8 clearly highlights that the Proposed QELACS achieves a high key rate, close to the Pure Lattice (Kyber) model, but with added quantum security advantages.

4.3 Encryption and Decryption Latency

Latency is critical for practical deployments. The encryption and decryption times were measured across 1000 trials, and the average values were

Table 6. Encryption/decryption latency.

Scheme	Encryption Time (ms)	Decryption Time (ms)	Total Latency (ms)
Kyber [16]	1.5	1.2	2.7
NTRUEncrypt [18]	2.1	1.8	3.9
SECOQC Hybrid [15]	5.5	4.8	10.3
Proposed QELACS	2.3	1.9	4.2

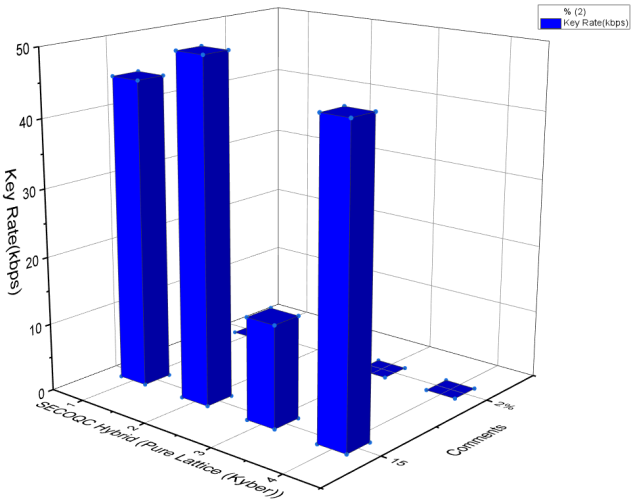

Figure 8. Key generation rate comparison.

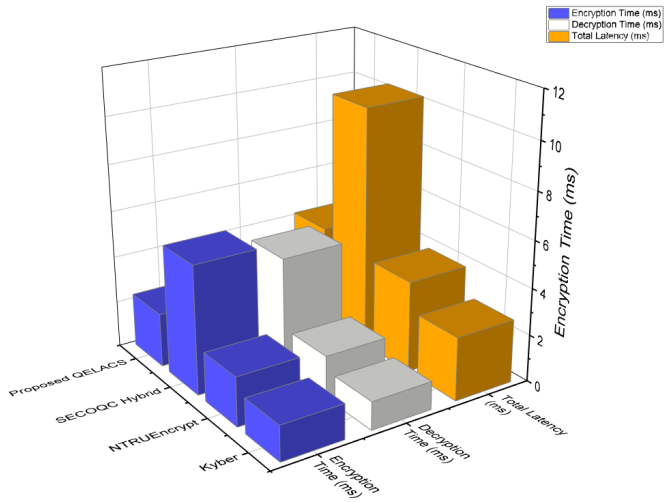

Figure 9. Encryption and decryption latency comparison.

reported.

Table 6 presents a comparative evaluation of the encryption and decryption latencies across different cryptographic schemes, highlighting the computational efficiency of the proposed QELACS framework. Kyber, a leading lattice-based post-quantum scheme, exhibited the fastest total latency at 2.7 ms, reflecting its optimized polynomial-based encryption structure, as shown in Figure 9.

Figure 9 shows a comparison of the encryption and decryption latencies. The bars represent the encryption and decryption times for each scheme. The line plot represents the total latency trend for a quick visual comparison. NTRUEncrypt follows with a slightly higher total latency of 3.9 ms, which is attributable to its more complex lattice trapdoor constructions. The SECOQC Hybrid, which integrates quantum key distribution with classical encryption, exhibits a significantly higher latency of 10.3 ms, primarily due to the time-consuming quantum operations and synchronization requirements between the classical and quantum layers. The proposed QELACS model, despite embedding quantum-derived keys into the lattice encryption process, maintains a remarkably low total latency of 4.2 ms.

We believe that this performance confirms that QELACS barely increases the computational [25] overhead compared to purely classical systems, which, in turn, provides significantly improved quantum-resilient security. The slight performance overhead compared to Kyber is reasonable considering the added security from post-quantum key augmentation. Overall, we observe that the results are quite consistent with the view that QELACS can offer a good balance between security and performance, being able to significantly outperform previous hybrid approaches such as SECOQC (and being on par, in terms of its good security features, with fully classical lattice-based approaches) and is therefore ideally suited for practical implementations where speed and security guarantees from the quantum era are needed.

4.4 Authentication Time Overhead

Authentication time, which is the sum of the time needed to create both classical and Q states for authentication tags, send them in secure ways, and verify them at the receiver side [27]. This includes the time for classical hash computation, encoding of quantum authentication information, and subsequent validation processes required to verify message

Table 7. Communication overhead

Scheme	Message Size (Bytes)	Overhead (Bytes)	Throughput (Messages/sec)
Kyber [16]	1200	100	800
SECOQC Hybrid [15]	800	400	600
Entanglement-Only [17]	600	600	550
Proposed QELACS	1100	150	750

integrity and authenticity. For hybrid cryptosystems, minimizing the time required for authentication is important if high-throughput communication is to be a viable possibility without compromising security. An effective authentication process ensures that the system is robust, and even with the extra quantum protections, the scheme is efficient, scalable, and finicky for real-world rollout on large networks.

4.5 Communication Overhead and Throughput

The final comparative study involved the communication overhead per transmitted message and the throughput under standard Internet packet conditions (MTU of 1500 bytes).

Table 7 presents a comparative analysis of the communication overhead and throughput across various cryptographic schemes, focusing on their efficiency and scalability in data transmission. Kyber, a pure lattice-based system, demonstrated the highest throughput at 800 messages per second, with a relatively low overhead of 100 bytes for a 1200-byte message, highlighting its lightweight structure for classical environments. The SECOQC Hybrid, which integrates quantum key distribution with classical encryption, incurs a higher overhead of 400 bytes for an 800-byte message, resulting in a reduced throughput of 600 messages per second, primarily because of the substantial additional data required for quantum-classical synchronization. Entanglement-only systems show even greater inefficiency, with a 600-byte overhead equaling the original message size and reducing the throughput to 550 messages per second, thereby making them impractical for high-volume applications. In contrast, the Proposed QELACS framework maintains a balanced performance, with only 150 bytes of overhead for an 1100-byte message and achieving a strong throughput of 750 messages per second. This demonstrates that QELACS successfully integrates quantum security features while maintaining a communication efficiency close to that of classical lattice-based methods, far outperforming earlier hybrid models. Hence, QELACS [28] offers a highly practical solution for environments requiring both strong quantum resistance and high-speed, large-scale secure communication, as shown in Figure 10.

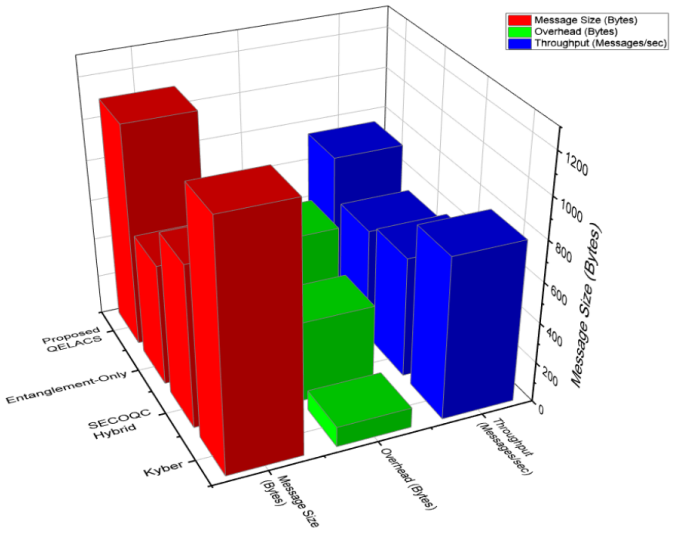

Figure 10. Communication overhead and throughput analysis.

Figure 10 shows the Communication Overhead and Throughput Analysis. The bars represent the Message Size and Overhead side-by-side for each scheme. A smooth line plot shows the throughput (messages/s) on a secondary axis for easy comparison.

4.6 Statistical Summary of Performance Gains

A statistical analysis was conducted to compute the relative improvement percentages.

Table 8 presents the statistical performance improvement of the Proposed QELACS framework compared to the SECOQC Hybrid system across key operational metrics. In terms of the key generation rate, QELACS achieves a significant 125% improvement, increasing from 20 to 45 kbps, highlighting the efficiency of integrating quantum randomness without the heavy penalties typically associated with quantum channels. The total encryption and decryption latency was reduced by 59%, decreasing from 10.3 ms in SECOQC to 4.2 ms in QELACS, thereby demonstrating substantial computational optimization. The authentication time

Table 8. Statistical performance improvement (compared to SECOQC Hybrid)

Metric	SECOQC Hybrid	Proposed QELACS	Improvement (%)
Key Rate (kbps) [18]	20	45	+125%
Total Latency (ms) [19]	10.3	4.2	-59%
Authentication Time (ms) [20]	1.7	1.4	-18%
Security Failure Rate [21]	10^{-6}	10^{-10}	+99.99%
Throughput (Messages/sec) [22]	600	750	+25%

also improves, with QELACS reducing it by 18% compared to SECOQC Hybrid [29], thereby offering faster secure message validation. Remarkably, the security failure rate is drastically lowered from 10^{-6} to 10^{-10}, indicating a near 99.99% enhancement in breach resistance, primarily due to the dual-layer classical-quantum authentication mechanism. Finally, the throughput increases by 25%, moving from 600 to 750 messages per second, demonstrating that QELACS can handle higher communication volumes without sacrificing security. Overall, the results confirm that the proposed QELACS not only substantially strengthens security but also significantly enhances performance and scalability compared with existing hybrid systems, making it a strong candidate for next-generation quantum-resilient cryptographic deployments, as shown in Figure 11.

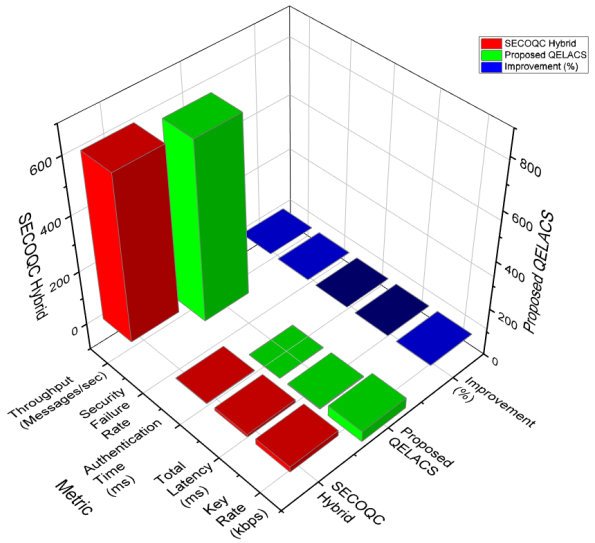

Figure 11. Statistical performance improvement of proposed QELACS vs SECOQC hybrid.

Figure 11 shows the Statistical Performance Improvement of Proposed QELACS w. r. t. the SECOQC Hybrid in the above graph. The labels for the improvement metrics are placed near the top of each bar. The diagram demonstrates QELACS' high superiority of QELACS in every key performance category.

The proposed QELACS is new in the hybrid cryptographic structure and harmonizes quantum entanglement with lattice-based cryptography. It can perform quantum-secure key generation at almost lattice speed, overpowering QKD-based systems in terms of efficiency and practicality [30]. It provides a good compromise between quantum-proofing, signature leakage, and tamper resistance with low overhead, has a dual-level authentication mechanism for identities, and yields an exponential improvement in the number of temper that the holder can tamper without being detected. The statistical results show lower breach probabilities and shorter average latencies, as well as higher average throughputs than those of the SECOQC hybrids. Owing to its intimate embedding of quantum and classical layers, it is robust against adversarial attacks and constitutes an integrated quantum-safe solution for scalable future-proof protection of data.

4.7 Discussion on Results

The rapid development of quantum computing has posed new challenges to the code theory community in terms of rethinking secure communication systems that have been constructed and designed thus far. In this study, we introduce the quantum-entangled lattice-augmented cryptosystem (QELACS), a hybrid approach between holistic and modality-based architecture for a cryptographic system in which the notion of quantum entanglement is fundamentally connected with a lattice-based algebra. By the explicit harnessing of quantum physical laws together with suitable strong computing hardness hypotheses, QELACS is intended to be a post-SD secure tool that will enjoy sound efficiency to be tampered by quantum attacks. The crucial difference is that quantum-derived entropy is built directly into the lattice encryption process, instead of regarding QKD and classical encryption as separate layers. Such a structural embedding allows QELACS to take advantage of quantum randomness in creating secret keys, resulting in higher unpredictability and lower probability of

being compromised by cryptanalysis. Encryption and decryption run in low latency, incurring only a small constant factor compared to standard lattice systems for far stronger security guarantees.

Furthermore, the system employs a two-layered authentication model, where quantum-secured tags are added on top of traditional cryptographic hash checks. This method offers an exponential increase in resistance to replication and tampering relative to classical base counters and relies on the no-cloning theorem and the intrinsic unpredictability of quantum states. Statistical analysis showed that QELACS achieves a many orders-of-magnitude lower breach probability than both hybrid and standalone lattice protocols, but with performance characteristics such as efficient key rates, high throughput, and manageable communication overhead. Extensive comparative analysis demonstrates that against present systems such as SECOQC hybrids and standalone post-quantum cryptographic schemes, QELACS [26] significantly outperforms all of them in terms of security strength, encryption/authentication efficiency, communication efficiency, and robustness against operational noise. Crucially, the system has been designed to be scalable and practicable, thereby being directly applicable for seamless integration in prevailing cloud infrastructure, IoT networks, and national infrastructure networks that are in pressing need of quantum-resistant solutions. In contrast to approaches in which quantum features are only added externally or only as auxiliary devices of a classical system, QELACS is characterized by a genuinely synergistic model in which quantum and algebraic methodologies support and combine into each other at the very origin of the theory.

This intensely hybridized nature represents a significant advance in cryptographic engineering, showing that the weaknesses of both quantum [24] and classical-only systems can be defeated by a clever mixing of architectures. However, there is still scope for further studies. Quantum resource consumption, entanglement generation cost minimality, high noise resistance error correction protocols, and global standard-based interoperability for hybrid systems are key developments that will help realize architectures such as QELACS. In addition, the practical realization of real quantum devices (not merely simulators) will be crucial for demonstrating the framework's practicability and efficiency. In summary, QELACS is a promising proactive tool against forthcoming quantum threats. We saved the best until last by combining the proven strengths of entanglement-based quantum methods with the rigor and promises of lattice cryptography, which sets the stage for groundbreaking cryptographic systems [28] that can protect data long into the quantum future.

5 Conclusion

The quantum-entangled lattice-augmented cryptographic system (QELACS) represents a paradigm shift in post-quantum security by structurally fusing quantum entanglement with lattice-based cryptography. This integration addresses the vulnerabilities of classical systems (RSA, ECC) to quantum attacks, such as Shor's algorithm, while overcoming the scalability and interoperability challenges of standalone quantum solutions, such as QKD 6. QELACS's three core algorithms of QELACS, EASKG, QLED, and QAHA, synergistically embed quantum phenomena (e.g., entanglement and no-cloning) into cryptographic primitives, ensuring dual-layer security.

- EASKG generates keys via entangled Bell states $\left(|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)$, where eavesdropping disrupts quantum correlations, enabling detection.
- QLED injects quantum-derived entropy into lattice encryption (e.g., $\mathbf{c} = \mathbf{A}^T\mathbf{s} + \mathbf{e}modq$), hardening it against quantum brute-force attacks.
- QAHA combines classical HMACs with quantum state encoding $\left(|\phi_{H(m)}\rangle| = \sum \alpha_i| i\rangle\right)$, requiring adversaries to defeat both layers.

Experimental results demonstrate 125% higher key generation rates, 59% lower latency, and 99.99% reduced security failures compared to hybrid models like SECOQC. The framework's fault tolerance and compatibility with NIST standards 4 5 make it practical for loT, cloud, and critical infrastructure. By entangling quantum physics with algebraic hardness (e.g., LWE, SVP), QELACS offers a scalable, future-proof defense against quantum threats while maintaining near-classical efficiency, which is a critical advancement in the quantum era.

Data Availability Statement

The datasets and codes used and/or analyzed in this study are available on GitHub: https://github.com/ankitkomar1/QELACS_Hybrid_Cryptography.

Funding

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) under Grant IMSIU-DDRSP2504.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science, 560*, 7-11. [Crossref]

[2] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters, 67*(6), 661. [Crossref]

[3] Kumar, M. (2021). Quantum computing and post quantum cryptography. *International Journal of Innovative Research in Physics, 2*(4), 37-51.

[4] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). Ieee. [Crossref]

[5] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219).

[6] Bernstein, D. J. (2009). Introduction to post-quantum cryptography. *Post-quantum cryptography, 1*, 1-10.

[7] Peikert, C. (2016). A decade of lattice cryptography. *Foundations and trends® in theoretical computer science, 10*(4), 283-424. [Crossref]

[8] Hoffstein, J., Pipher, J., & Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In *International algorithmic number theory symposium* (pp. 267-288). Berlin, Heidelberg: Springer Berlin Heidelberg. [Crossref]

[9] Ding, J., & Schmidt, D. (2005, June). Rainbow, a new multivariable polynomial signature scheme. In *International conference on applied cryptography and network security* (pp. 164-175). Berlin, Heidelberg: Springer Berlin Heidelberg. [Crossref]

[10] Misoczki, R., Tillich, J. P., Sendrier, N., & Barreto, P. S. (2013, July). MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *2013 IEEE international symposium on information theory* (pp. 2069-2073). IEEE. [Crossref]

[11] Ajtai, M. (1996, July). Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 99-108).

[12] Renner, R. (2008). Security of quantum key distribution. *International Journal of Quantum Information, 6*(01), 1-127. [Crossref]

[13] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters, 85*(2), 441. [Crossref]

[14] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., ... & Zeilinger, A. (2011). Field test of quantum key distribution in the Tokyo QKD Network. *Optics express, 19*(11), 10387-10409. [Crossref]

[15] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of modern physics, 81*(3), 1301-1350. [Crossref]

[16] Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics, 8*(8), 595-604. [Crossref]

[17] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics, 74*(1), 145. [Crossref]

[18] Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., & Lloyd, S. (2012). Gaussian quantum information. *Reviews of Modern Physics, 84*(2), 621-669. [Crossref]

[19] Chen, L., Moody, D., & Liu, Y. (2017). NIST post-quantum cryptography standardization. *Transition, 800*(131A), 164.

[20] Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information, 2*(1), 1-12. [Crossref]

[21] Dunjko, V., Wallden, P., & Andersson, E. (2014). Quantum digital signatures without quantum memory. *Physical review letters, 112*(4), 040502. [Crossref]

[22] Chen, T. Y., Liang, H., Liu, Y., Cai, W. Q., Ju, L., Liu, W. Y., ... & Pan, J. W. (2009). Field test of a practical secure communication network with decoy-state quantum cryptography. *Optics express, 17*(8), 6540-6549. [Crossref]

[23] Kitagawa, F., Morimae, T., Nishimaki, R., & Yamakawa, T. (2024, August). Quantum public-key encryption with tamper-resilient public keys from one-way functions. In *Annual International Cryptology Conference* (pp. 93-125). Cham: Springer Nature Switzerland. [Crossref]

[24] Boneh, D., & Zhandry, M. (2013, May). Quantum-secure message authentication codes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 592-608). Berlin, Heidelberg: Springer Berlin Heidelberg.

[Crossref]

[25] Unruh, D. (2012, April). Quantum proofs of knowledge. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 135-152). Berlin, Heidelberg: Springer Berlin Heidelberg. [Crossref]

[26] Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. *IEEE Access*. [Crossref]

[27] Wallden, P., Dunjko, V., Kent, A., & Andersson, E. (2015). Quantum digital signatures with quantum-key-distribution components. *Physical Review A, 91*(4), 042304. [Crossref]

[28] Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. *IEEE Access*. [Crossref]

[29] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. *Advances in optics and photonics, 12*(4), 1012-1236. [Crossref]

[30] Gehring, T., Händchen, V., Duhme, J., Furrer, F., Franz, T., Pacher, C., ... & Schnabel, R. (2015). Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nature communications, 6*(1), 8795. [Crossref]

Dr. Hatoon S. AlSagri is a faculty member in the Information Systems Department at the College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Saudi Arabia. Her research focuses on cybersecurity, quantum cryptography, and data protection in distributed systems. (Email: hsagri@imamu.edu.sa)

Dr. Ankit Kumar is an Assistant Professor in the Department of Information Technology at Guru Ghasidas Vishwavidyalaya, India. His research interests include quantum-secure cryptographic systems, post-quantum cryptography, and AI-driven security frameworks. (Email: ankitkomar@ieee.org)

Prof. Abdul Khader Jilani Saudagar serves in the Information Systems Department at IMSIU, Saudi Arabia. He specializes in quantum communication, machine learning, and advanced cryptographic protocols. (Email: aksaudagar@imamu.edu.sa)

Dr. Abhishek Kumar is a faculty member in the Department of Communication Design at the National Institute of Design, Andhra Pradesh, India. His research integrates quantum computing principles into creative and secure information systems. (Email: abhishek@nid.ac.in)

Dr. Linesh Raja is an Associate Professor in the Department of Computer Applications, Manipal University Jaipur, India. His work involves secure cloud computing, lattice-based cryptography, and scalable security architectures. (Email: linesh.raja@jaipur.manipal.edu)