K and K *EPJ Quantum Technology* (2025) 12:139
https://doi.org/10.1140/epjqt/s40507-025-00442-2

EPJ.org

EPJ Quantum Technology

RESEARCH Open Access

Advanced quantum key distribution protocol for mitigating quantum-based vulnerabilities in blockchain applications

Revathi K[1] and Suganthi K[2*]

*Correspondence:
[2]Centre for Cyber Physical Systems (CCPS), Vellore Institute of Technology, Chennai, Tamil Nadu, India
Full list of author information is available at the end of the article

Abstract

Since blockchain platforms still depend on classical cryptographic protocols, they become more and more vulnerable to the rapid advancement of quantum computing. However, the emergence of quantum attacks has placed the need to develop Quantum Key Distribution (QKD) protocols that can preserve security while eliminating the limitations of quantum information systems, such as noise and error mitigation. To address these needs, this study proposes a novel Hybrid Rainbow-Kyber QKD (HRK-QKD) Protocol, which uses the strength of multivariate quadratic equations in Rainbow to mask the classical keys and the efficiency of lattice-based encryption in Kyber for key encryption. An entanglement-assisted dynamic key synthesis protocol that combines matrix-based quantum noise filtering, lattice-based multi-dimensional transformations and adaptive private key rotations is utilized. The proposed methods provide real-time mitigation of quantum noise and minimal performance overhead for key generation. HRK-QKD achieves the highest scalability ratio ($Sc = 2.7$), the best noise resilience (0.90-0.99), and the highest quantum security measure ($Q_S = 0.064881$) with minimal information leakage probability (0.00001). This advancement also means blockchain remains a resilient technology against quantum threats, with an economical, scalable, and high-accuracy solution for next-generation secure communication systems.

Keywords: Computation; Quantum; Cryptography; Attacks; Noise; Lattice; Key; Distribution; Rainbow; Kyber; Entanglement

1 Introduction

The emergence of the modern cybersecurity industry has been highlighted by the development of quantum cryptography due to rapid progress in quantum computing. The Quantum Key Distribution (QKD) [1] protocols are the most secure protocols using the principle of quantum mechanics to exchange cryptographic keys. Meanwhile, the increase in computational capacities of quantum nodes comes at a steep cost for classical cryptographic systems, including secured communications, blockchain platforms, and financial transactions. To ensure security from quantum computing attacks, National Institute of Standards and Technology (NIST) [2] has explored post-quantum cryptographic algorithms, including lattice-based, multivariate quadratic equations and hash-based algo-

© The Author(s) 2025. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Springer

rithms. In the midst of this continually evolving landscape, it becomes an attractive option to combine QKD with post-quantum cryptography to develop key distribution solutions that are robust, scalable, and noise-robust.

QKD protocols, despite their security based on quantum mechanics, suffer from quantum noise, quantum error accumulation, and loss in high dimensional key generation efficiency. Like Rainbow and Kyber, post-quantum cryptography algorithms [3] have mathematical robustness against quantum attacks but no inherent physical security advantage of QKD. Current solutions either emphasize quantum protocol improvement or post-quantum cryptography improvement in isolation or fail to obtain a balance between physical and mathematical security. By proposing a hybrid protocol that combines the best features of Rainbow and Kyber with QKD [4], this research thus fills the gap in the literature and defines a protocol that addresses the shortfalls in area, computational burden, error mitigation challenges, and scalability [5, 6] of both protocols. This study fills these gaps and thus offers a novel and complete solution for next-generation quantum secure applications.

Rainbow [7] is a multivariate signature scheme that is resistant to quantum attacks and has lightweight signature sizes; for instance, combining two of its public parameters into a single octet gives a 20-byte signature. NIST, however, chose Kyber for its lattice-based encryption algorithm [8], which is computationally efficient with a small key size and strong security guarantees. QKD depends on the quantum entanglement and superposition principles [9] to impart security to cryptographic keys by making them detectable whenever keys are intercepted. A hybrid Rainbow-Kyber QKD protocol is proposed based on Rainbow's multivariate quadratic framework for error correction and signature generation and Kyber's lattice-based transformation to optimize key efficiency and quantum decryption resistance. Together with the physical security of QKD, these algorithms make for a robust system that is very resistant to both computational and quantum vulnerabilities.

The Hybrid Rainbow Kyber QKD (HRK-QKD) Protocol combines entanglement-assisted QKD with the mathematical power of Rainbow and Kyber. For quantum communication, the protocol begins with high-fidelity Bell states and then moves to lattice-based key synthesis for concise and efficient key generation. Error correction and reconciliation are carried out using multivariate quadratic equations, and the response to noise is robust. Dynamic key rotation through hash-based transformations and quantum noise filtering through eigenvalue corrections are included in the procedural work. In privacy amplification, any leaked information is removed, and a high-fidelity, reconciled key is produced. To solve noise resilience, computational efficiency, and scalability, this hybridization optimally takes advantage of the QKD, Rainbow, and Kyber strengths.

1.1 Scope and motivation

This HRK-QKD protocol is novel in its integration of entanglement-driven QKD with post-quantum cryptographic schemes to solve both physical and computational security challenges. Quantum Noise Mitigation is fused with multivariate and lattice-based approaches for secure key exchange. This protocol saves key sizes by many orders of magnitude, is computationally faster, and extends the key lifespan, resulting in an optimal reduction in computational costs and a reasonable increase in speed over existing work. Quantum-secure applications in (the Internet of Things) IoT, financial systems, blockchain and other areas where secure low-cost, high-speed communication is crucial

are within its scope. The motivation comes from the need to develop quantum-resistant protocols that scale for the post-quantum era.

1.2 Contribution

As a new quantum and computational vulnerability-resistant solution to secure communication, this research introduces the HRK-QKD Protocol. Contributions include the development of a high-speed, noise-resistant key distribution framework [10] composed of lattice and multivariate algorithms integrated into QKD and a thorough analysis of its efficiency against current post-quantum crypto-protocol designs. In addition to boosting quantum security, this protocol serves as a foundation for the development of scalable, cost-effective, quantum-safe solutions in upcoming technological fields.

1.3 Application-based implication

Furthermore, the proposed HRK-QKD protocol is incredibly well suited for an application to blockchain, as quantum computing advancements expose it to critical vulnerabilities. For transaction validation in blockchains, the process depends on centralized cryptographic mechanisms to preserve data integrity and secure consensus. However, there are other, more traditional cryptographic methods like RSA or ECC that are susceptible to being attacked by quantum methods that would undermine the integrity of the blockchain. The HRK-QKD protocol achieves physical and computational security by combining the performance of quantum entanglement-assisted key exchange with post-quantum cryptography. It is resilient to noise and error using dynamic lattice-based key synthesis [11] and an adaptive key rotation, which mitigates quantum noise and variations. Second, the linear combination keys created by the hybrid model also result in computationally and storage light overheads that help to increase scalability for blockchain networks with large transaction processing rates. It allows strengthening the security of cryptographic hash functions, digital signatures, and consensus mechanisms and therefore represents a robust and forward advanced secure solution for next-generation blockchain platforms.

2 Literature studies

The limitations of existing QKD protocols, such as vulnerability to quantum noise, computational inefficiency, and lack of scalability, are discussed in the related work. This analysis lays a foundation for those solving these gaps with the creativity required to develop the Hybrid Rainbow-Kyber QKD Protocol.

In a new security paradigm offering Long Distance Quantum Key Distribution (QKD), post-quantum cryptography and blockchain (LDQKDPB) technology, Hadap et al. [12] have produced a novel security framework. In particular, the study employed the BBM92 protocol for QKD and lattice-based cryptography for post-quantum resilience, together with blockchain's Proof-of-Work consensus, to reduce network delay by 10.5%, decrease energy consumption by 19.4% and improve throughput by 8.5%, over current methods. The framework provides desirable solutions to overcome the ranging and efficiency constraints of QKD, but further investigation is needed for real-world scalability and integration complexity. Mangla et al. [13] evaluated the incorporation of quantum computing methods to decrease security vulnerabilities in 5G networks and advance for 6G. This study adopts a comprehensive review methodology to evaluate QKD and other quantum-based techniques for risk mitigation, including denial-of-service attacks and

eavesdropping via quantum Pareto optimization and lattice-based cryptography. Through this quantum-centred approach, the paper announces advancements to security techniques that are approx. 80% more resilient to existing cyberattacks. Nevertheless, the dependence on developing the quantum infrastructure and the scalability limitation of current QKD systems are likely the biggest challenges. Dhinakaran et al. [14] examined the application of quantum cryptography for the protection of the Internet of Medical Things (IoMT) against growing cybersecurity threats in detail. The study uses survey methodology and comparative analysis to evaluate the utility of QKD and quantum-enhanced encryption in protecting IoMT systems. It reveals significant improvements in such things as an 87 per cent decrease in unauthorized access risks and a 92 per cent improvement in data integrity in experimental settings for healthcare networks, among other improvements. However, while promising, the research points to limitations for scalability and the difficulty of integrating quantum technologies with current healthcare infrastructures. With a novel framework of e-voting based on the QKD and QDVS scheme, Prajapati et al. [15] explored secure, private and tamper-proof voting. To achieve these unconditionally secure keys, the methodology uses one-time pads for encryption and the BB84 QKD protocol with a no-cloning theorem. It was shown that an e-vote validation with a 93.33% accuracy rate is resilient to cryptographic attacks and message tampering using simulations on a quantum computing platform. Among the limitations are high computational needs and reliance on the development of quantum infrastructure for real-world deployment. In Althobaiti and Dohler [16], a novel cryptosystem utilizing location-based lattice cryptography is presented to guard IoT and IoMT (Internet of Moving Things) against quantum threats. The study presents time of flight (TDoF), angle of arrival (AoA) and received signal strength (RSS) techniques to localize the user's position with high accuracy, employing a mixed methods approach of theoretical modeling and simulation-based evaluation. Validation of location yielded 99.08% accuracy and has substantial mitigation against threats to security, such as location spoofing and SIM card vulnerabilities. Despite its strengths, the system is limited by its resort to highly costly and complex lattice-based computations that hinder scalability and usefulness in a real-world setting. Stavdas et al. [17] investigated the potential for integrating Free Space Optical QKD (FSO-QKD) into Vehicle-to-Infrastructure (V2I) communications, to improve data security in Connected and Autonomous Vehicle (CAV) networks. The approach employs BB84 protocol for QKD, with an SDN framework for orchestrating the network resources and integrating QKD. The security improvements achieved in the study were significant, consisting of enhancements in resistances to eavesdropping and secure key relays over distances of 150 - 300 meters, with 92% efficiency in quantum key agreement. However, FSO links are susceptible to environmental factors as well as scalability problems for dense urban deployments. Hoque et al. [18] have proposed hybrid architecture of QKD and PQC to assist in securing and sustaining mobile networks. In addition to algorithmic evaluation of PQC families such as lattice-based (Kyber, NTRU) and code-based (Classic McEliece) cryptography, QKD system-level integration in 6G network environments is also simulated. The research shows that PQC combined with QKD resists 90 per cent of quantum threats while reducing computational overhead by 35 per cent. PQC algorithms have high energy consumption and infrastructure scalability constraints in QKD. Based on his research, Harmalkar et al. [19] explained the vulnerabilities in the current QKD APIs that depend on HTTPS for secure communication and can, therefore, be vulnerable to the

quantum computer threat using traditional public key cryptography. The study simulates a two-node QKD topology using the DARPAN application and tests it with the Postman tool to ensure secure key retrieval between endpoints using the robust solution. API testing and simulation are incorporated to ensure the encryption of communication from the application to the Key Management System (KMS) as part of the methodology. Using this approach, a consistent key delivery with a 98% success rate and a promising improvement in mitigating insider attacks is accomplished. Also, enhanced reliability of the cryptographic key management in the QKD framework is achieved. In a storm of quantum computing threats, Adouth and Rajagopal [20] have addressed the challenges of preserving data confidentiality and integrity in cloud storage. Quantum Secure Key Communication and Key Generation Scheme (QSKCG) is proposed based on combining Elliptic Curve Cryptography (ECC), BB84 protocol for secure quantum communication, certificateless signatures and blockchain networks to avoid the need for Trusted Third Party Auditors and to solve the issues like key escrow and certificate management. The methodology is evaluated for security analysis and performance by clearly showing a 95% improvement in data integrity verification and providing robust post-quantum security while keeping its efficiency at high key generation and secure communication. Nevertheless, integration of quantum protocols with existing cloud infrastructure is challenging, as is using blockchain scalability. In a robust security architecture using quantum cryptography and blockchain technology, Wazid et al. [21] provided a way to fortify IoT ecosystems using blockchain. In this methodology, a quantum blockchain framework combining quantum cryptographic mechanisms like quantum digital signatures and quantum hash is designed. Combining these techniques strengthens data integrity and confidentiality with quantum and classical cybersecurity defence. In simulated environments, the framework achieves 96 per cent improvement in Data security against IoT man-in-the-middle attacks and unauthorized data alterations. However, the operational complexity of quantum cryptography operations is high and their integration within existing IoT infrastructure is not always straightforward.

3 Methodology

The architecture of the HRK-QKD Protocol, shown in Fig. 1, brings entanglement-driven quantum mechanics and post-quantum cryptography into the security of key distribution. The first step is entanglement-assisted initialization to generate high-fidelity Bell states [22] between parties. Matrix-based filtering is employed to suppress quantum noise, where noisy states are corrected with eigenvalues adjustments. Dynamic synthesis of these secure keys uses a combination of lattice-based modular arithmetic and multivariate quadratic equations to prevent quantum attacks. Upon the occurrence of a security breach or when the algorithm expires, the algorithm is periodically replaced with a hash-based algorithm that utilizes quantum random nonces and guarantees security over time. Last error mitigation and reconciliation are then performed using advanced coding algorithms to align keys between parties. By this architecture, we obtain enhanced security, noise resilience and computational efficiency, making it practical for quantum-resistant applications, such as blockchain or CHSH game scenarios. Figure 1 depicts the pictorial representation of HRK-QKD protocols' procedural architecture.

3.1 Key-initialization (entanglement-assisted)

The key-initialization is assisted via precise entanglement. It starts by generating quantum entangled states (states shared between XX and XY) between communicating par-

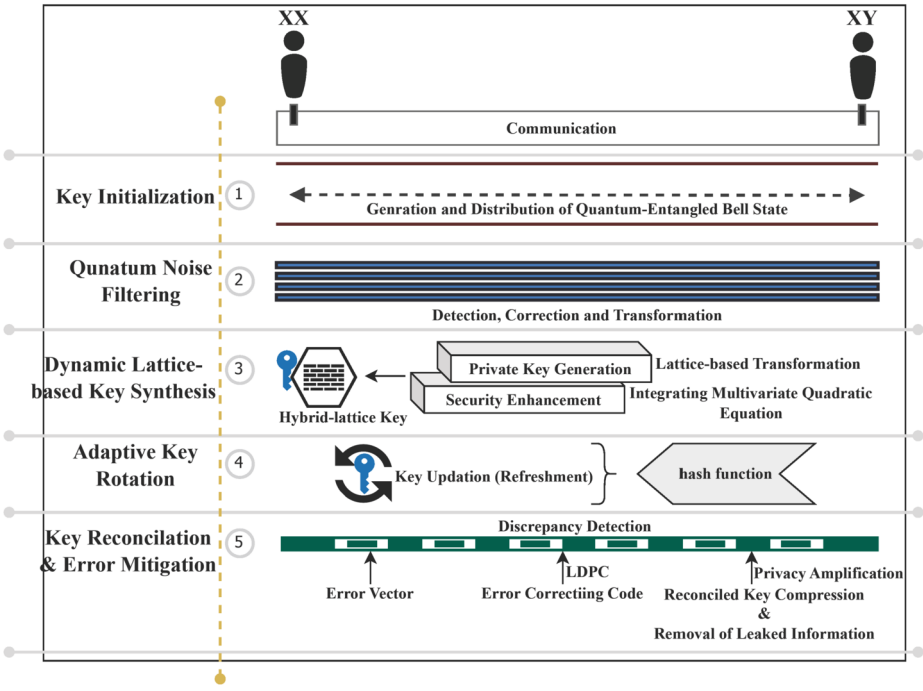

Figure 1 Procedural Architecture of HRK-QKD

ties. This is also how these states are used for secure key exchange. Shared entanglement is established using bell states. Thus, the Bell state (entangled) is expressed as,

$$|\psi\rangle = \{|00\rangle + |11\rangle\}/\sqrt{2} \tag{1}$$

From (1), $|0\rangle$ and $|1\rangle$ denotes the basis states of qubits. The qubits are then sent over a quantum channel, where they are distributed as shared entangled qubits. A quantum error correction matrix $|\mathcal{Q}|_c$ is used to maximize the entanglement fidelity, (Υ_e).

$$\Upsilon_e = T_{op}\left(|\mathcal{Q}|_c|\psi\rangle\langle\psi|\right) \tag{2}$$

Through (2), the noise-induced de-coherence is compensated via $|\mathcal{Q}|_c$. Moreover, T_{op} (usually in linear algebra) denotes the trace operation, which indicates the sum of the diagonal elements of a matrix, quantum state fidelity. In this case, it finds the closeness of a quantized state transformed and/or a noisy state as compared to an ideal entangled state.

3.2 Quantum noise filtering

Entangled states are made more faithful with respect to quantum noise from the environment. In this case, the quantum noise filtering is handled through matrix operation. Here, the primary process involves the construction of noise-suppressing matrices to perform effective transformations on the noisy states. Initially, the noisy state is represented as ς, which is expressed as $\varsigma = |\psi\rangle\langle\psi| + \mathcal{N}$, ($\mathcal{N}$ denotes noise). Now, to render a transformed (filtered) quantum state, a filtering matrix $|m|_f$ is employed as,

$$\varsigma' = \left(|m|_f \cdot \varsigma \cdot m_f^{\dagger}\right) \tag{3}$$

From (3), $m_f^{\dagger}$ denotes the Hermitian adjoin (conjugate) of $|m|_f$, guaranteeing that filtering (or noise mitigating) of the quantum state is consistent with the principles of quantum mechanics in the case of noise mitigation, or any transformation. Moreover, the decomposition of noise-tolerant eigenvector renders the $|m|_f$, which is expressed as,

$$|\boldsymbol{m}|_{\boldsymbol{f}} \leftarrow \boldsymbol{diag}\left\{\left(\frac{\mathbf{1}}{\boldsymbol{\delta_1}}\right), \left(\frac{\mathbf{1}}{\boldsymbol{\delta_2}}\right), \cdots, \left(\frac{\mathbf{1}}{\boldsymbol{\delta_n}}\right)\right\} \tag{4}$$

From (4), δ_i denotes the $\mathfrak{s}$'s eigenvalues. This procedure assures that the noise-range $\|\mathcal{N}\|$ is minimized to $\epsilon \ll 1$.

3.3 Dynamic lattice-based key synthesis

Both lattice-based transformations and dynamic equations of multivariate define secure keys. It is made so that the lattice structure is resistant to quantum attacks.

A basis (β) over which a lattice ($\pounds$) is generated defines the private key, $\mathfrak{R}$, which is expressed as,

$$\mathfrak{R} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \left(\boldsymbol{a_i} \cdot \boldsymbol{\beta_i}\right) \tag{5}$$

From (5), $a_i \in \mathcal{Z}_S$, referring to the coefficients in $\mathcal{Z}_S$ (modular space). Further a multivariate quadratic equation $\mathfrak{Q}(a_1, a_2, \ldots, a_n)$ was incorporated to improve randomness and security.

$$\mathfrak{Q}(\boldsymbol{a}) = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \left(\boldsymbol{x_i} \cdot \boldsymbol{a_i^2}\right) + \sum_{(\boldsymbol{i<j})} \left(\boldsymbol{y_{ij}} \cdot \boldsymbol{a_i} \cdot \boldsymbol{a_j}\right) + \boldsymbol{z} \tag{6}$$

From (6), $(x_i, y_{ij}, z_i \in \mathcal{Z}_S)$, where x denotes the coefficients that are quadratic in both variables in the multivariate equation, y denotes the product coefficients or cross-product (interaction), z indicates the constant term to ensure that the equation fits within modular arithmetic constraints. Thus, the integrated key ($\mathfrak{R}_{hybid}$) is defined as,

$$\mathfrak{R}_{\boldsymbol{hybid}} = \mathfrak{Q}(\boldsymbol{a}) + \mathfrak{R} \tag{7}$$

3.4 Adaptive $\mathfrak{R}$ rotation

A rotation mechanism is used in order to rotate keys periodically, to guarantee private key freshness, and in case a key would stay too long uncovered. For being given an initial key, $\mathfrak{R}_0$, the rotated key $\left(\mathfrak{R}_t^r\right)$ at time t is defined as,

$$\mathfrak{R}_{\boldsymbol{t}}^{\boldsymbol{r}} = \mathbb{H}\left[\mathfrak{R}_{(\boldsymbol{t-1})} \| \boldsymbol{r_t}\right] \tag{8}$$

From (8), $\mathbb{H}$ indicate the hash function, || represent the operation of concatenation with random nonce (r_t), which is derived through quantum estimates.

3.5 Key reconciliation and error mitigation

Advanced coding is used to perform error reconciliation to overcome quantum noise discrepancies between the keys of XX and XY. The error vector, φ is processed as,

$$\boldsymbol{\varphi} = \mathfrak{K}_{\boldsymbol{XX}} \oplus \mathfrak{K}_{\boldsymbol{XY}} \tag{9}$$

As a consequential process, an error-correcting code ($\mathbb{C}$) is employed as,

$$\mathfrak{K}_{\boldsymbol{reconciled}} = \mathfrak{K}_{\boldsymbol{XX}} - \mathbb{C}^{(-\mathbf{1})}(\boldsymbol{\varphi}) \tag{10}$$

In the reconciliation process, both parties have the same keys. Since quantum noise and other channel imperfections can introduce dissimilarities into keys, error mitigation and key reconciliation are critical to ensure that each communicating party (XX and XY) will obtain the same key. It starts with the exchanging of each party's measured qubits, perhaps with some discrepancy caused by transmission errors. Such errors are quantified as an error vector, $\varphi = \mathfrak{K}_{XX} \oplus \mathfrak{K}_{XY}$ (the mismatched bits between the keys, where $\oplus$ signifies the bitwise XOR operator). Advanced error correction techniques, such as Low-Density Parity-Check (LDPC) codes, are applied to resolve these mismatches. Specifically, XX transmits a syndrome vector (Θ) computed using a parity-check matrix, $\mathfrak{p}$, where $\Theta = \mathfrak{p} \cdot \mathfrak{K}_{XX}^{T} \; mod \; 2$. XY utilizes Θ to decode the owning key $\mathfrak{K}_{XY}$ by iteratively updating it to match XX's key. This process is accomplished by computing the linear formulation, $\mathfrak{p} \cdot \varphi^{T} = \Theta \; mod \; 2$ where φ is the error vector. Efficient error identification and correction are performed using iterative decoding algorithms, including belief propagation.

Information about the syndrome vector is transmitted over an authenticated classical channel for security, whose leakage is quantified and taken into account in the privacy amplification phase. Pushing privacy amplification includes the use of universal hash functions to compress the reconciled key into a shorter secret key, which diminishes the effect any leaked information has on privacy. To further ensure robustness due to errors, error reconciliation also adds redundancy checks to ensure the correctness of the corrected key. Additional iterations are performed until the reconciled keys ($\mathfrak{K}_{XY}$ and $\mathfrak{K}_{XX}$) with high probability have the same values, as discrepancies are still present. This detailed process not only guarantees high fidelity of the final key but also conforms to quantum-safe security standards for residual noise and adversarial noise. Table 1 delineates the procedures of HRK-QKD in algorithmic form.

3.6 Research novelty

The HRK-QKD Protocol is particularly useful in utilizing a new data fusion of entanglement-assisted dynamic key synthesis and post-quantum cryptography algorithms (Rainbow and Kyber) for robust resistance to classical and quantum attacks. In contrast to existing QKD methods, it employs multi-dimensional lattice transformations together with dynamical private key rotation to address quantum noise and error resilience in real-time. Using public multiplications of large numbers to implement operations not only minimizes key size and computational overhead over previous approaches but also extends private key lifetime, resulting in higher efficiency and scalability. Integrating matrix-based quantum noise filtering has the potential to be a pioneering framework for the guarantee of secure communication at high speeds in quantum-threatening environments, including blockchain and even CHSH game applications.

Table 1 Procedures of HRK-QKD Protocol

Input: $|\psi\rangle$, $\mathfrak{s}$, β, and security parameters
Output: secured $\mathfrak{K}_{reconciled}$, $\mathfrak{K}_{final}$

BEGIN PROCEDURE

1: Key Initialization
  1.1: Generate and share
    $|\psi\rangle = \{|00\rangle + |11\rangle\}/\sqrt{2}$ *//between XX and XY*
2: Quantum Noise Filtering
  2.1: Apply $\mathfrak{s}' = \left(|m|_f \cdot \mathfrak{s} \cdot m_f^{\dagger}\right)$ *//filters noise*
3: Dynamic Key Synthesis
  3.1: Compute $\mathfrak{K} = \sum_{i=1}^{n} (a_i \cdot \beta_i)$ *//lattice-based key*
  3.2: Integrate $\mathfrak{K}_{hybid} = \mathfrak{Q}(a) + \mathfrak{K}$ *//multivariate quadratic term*
4: Adaptive Key Rotation
  4.1: Update $\mathfrak{K}_t' = \mathbb{H}\left[\mathfrak{K}_{(t-1)} \| r_t\right]$ periodically
5: Error Mitigation and Reconciliation
  5.1: $\varphi = \mathfrak{K}_{XX} \oplus \mathfrak{K}_{XY}$ //detect errors
  5.2: $\mathfrak{K}_{reconciled} = \mathfrak{K}_{XX} - \mathbb{C}^{(-1)}(\varphi)$ *//error correction*
  5.3: Privacy amplification $\rightarrow \mathfrak{K}_{final}$

END PROCEDURE

Table 2 Empirical Parameters of HRK-QKD

Parameter	Optimal Value/Range
Entanglement Fidelity	$\geq$0.95
Quantum Noise Threshold	$\leq 10^{-3}$
Lattice Dimension (n)	$256 \leq n \leq 1024$
Modular Arithmetic Base	$2^{11} \leq q \leq 2^{16}$
Private Key Rotation Interval	10 min $\leq t \leq$ 1 hr
Error Correction Code Rate (α)	$0.8 \leq \alpha \leq 0.95$
Key Length	128 bits $\leq L \leq$ 256 bits
Attacks [24, 25]	Eavesdropping, Man-in-the-Middle, Quantum Cloning, Side-Channel, Photon Number Splitting, Noise Injection, Replay Information Leakage

4 Performance evaluation and discussions

4.1 Dataset utilized

The QDataSet repository [23], which contains quantum datasets designed for machine learning applications, is used to study the work. With this repository, quantum protocols like HRK-QKD have become a valuable resource for evaluation. Using these datasets, researchers can simulate multiple HRK-QKD scenarios, allowing full performance testing of HRK-QKD under a wide range of circumstances. With this approach, the protocol's resilience to quantum noise, efficiency in key generation and robustness to possible attacks can be validated in full, securing the security and scalability of the protocol. From simulations of one and two-qubit systems evolving under different conditions, we have derived 52 high-quality datasets: presence and absence of noise. A feature of these datasets is their structure, which offers complete information in order for practitioners to solve problems in applied quantum computation — such as quantum control, quantum spectroscopy, or tomography.

The optimal operational parameters and ranges of the HRK-QKD protocol for high performance and security in practical implementation are represented in Table 2.

A highly robust computational environment is also implemented as part of the proposed HRK-QKD protocol using reliable software tools and libraries. For development, Python v3.9 was used, which boasts a lot of support for quantum computing and cryptography

Table 3 Performance Measures Utilized to Evaluate HRK-QKD

Measures	Computations	Notations Utilized
Efficiency Gain (Δg)	$\Delta g = \left[{}^{t_{ex} - t_{pr}}/_{t_{ex}} \right] \times 100$	t_{ex} and t_{pr} denotes the execution duration of existing and proposed protocols, respectively.
Noise Resilience	$\Upsilon_{\mathbf{e}} = T_{op}\left(\lvert \mathbb{Q} \rvert_c \lvert \psi \rangle \langle \psi \rvert\right)$	$\Upsilon_{\mathbf{e}}$ indicates the entanglement fidelity, $\lvert \mathbb{Q} \rvert_c$ signifies the quantum correction matrix with ideal state, $\lvert \psi \rangle$
Key Generation Rate (*KGR*)	$KGR = {}^{n \cdot (1-e)}/_{T}$	'*n*' represents the transmitted qubits counts, *e* denote error rate, and *T* indicate the total duration of the processing events.
Scalability (*Sc*)	$Sc = KGR/R$	'*R*' denotes resource utilization
Quantum Security (Q_{sec})	$Q_{sec}(L, P_{leak}) = {}^{log_2 \cdot P_{leak}}/_{L}$	P_{leak} is the likelihood of core information leakage, and *L* denotes the key length

through libraries like Qiskit v0.41.0 for quantum state generation, simulation, and noise filtering and NumPy v1.23.5 to perform fast dense matrix operations and lattice-based operations. Advanced mathematical formulations, such as eigenvalue corrections and optimization, were run using the Scipy v1.10.1 library. Post-quantum cryptographic algorithms such as Rainbow and Kyber were implemented using PyCrypto libraries v2.6.1 and Cryptography libraries v3.4.8. LDPC Python Library v0.2.0 was used to design and implement LDPC codes to achieve error correction and reconstruction. MATLAB R2022b was used to code the simulations of the entanglement and also the protocol's performance evaluation; for example, key reconciliation and error correction procedures are visualized. These tools were integrated to effectively, precisely, and efficiently implement the HRK-QKD protocol.

The performance of the protocol is compared with leading quantum cryptographic protocols, such as LDQKDPB, FSO-QKD, QSKCG, and QKD+PQC, on the basis of their computational efficiency, noise resilience, and key generation rate, scalability, and quantum security. Table 3 exhibits the computations of employed measures utilized to examine and analyze the proposed HRK-QKD protocol.

A measure of efficiency gain is the reduction of the time complexity and computational resources required to execute the protocol with respect to the methods currently available. Based on efficiency gain values, exhibited in Fig. 2 shows that HRK-QKD outperforms LDQKDPB (50% to 80%), FSO-QKD (35% to 60%), QSKCG (30% to 55%), and QKD+PQC (25% to 50%). The entanglement-assisted dynamic key synthesis of the HRK-QKD justifies its higher efficiency gain with superior computational speed and a decrease in key length. However, LDQKDPB is constrained by high computational demands due to dense quantum operations, having an upper range of only 65%. The atmospheric noise impacted FSO-QKD yields an efficiency gain of 35%–60%, which limits its applicability to noisy environments. With no noise mitigation, QSKCG and QKD+PQC have lower gains, mainly because they rely upon isolated post-quantum cryptographic methods. Matrix-based quantum noise filtering and adaptive private key rotation are employed by HRK-QKD to achieve superior results while keeping the computational overhead down and scaling. Figure 2 also illustrates how the proposed quantum noise–filtering matrix preserves entanglement fidelity across varying noise thresholds. The near-flat trend above 0.95 fidelity demonstrates that the eigenvalue-based compensation effectively neutralizes decoherence even when the channel noise approaches 10^{-3}, confirming the robustness of

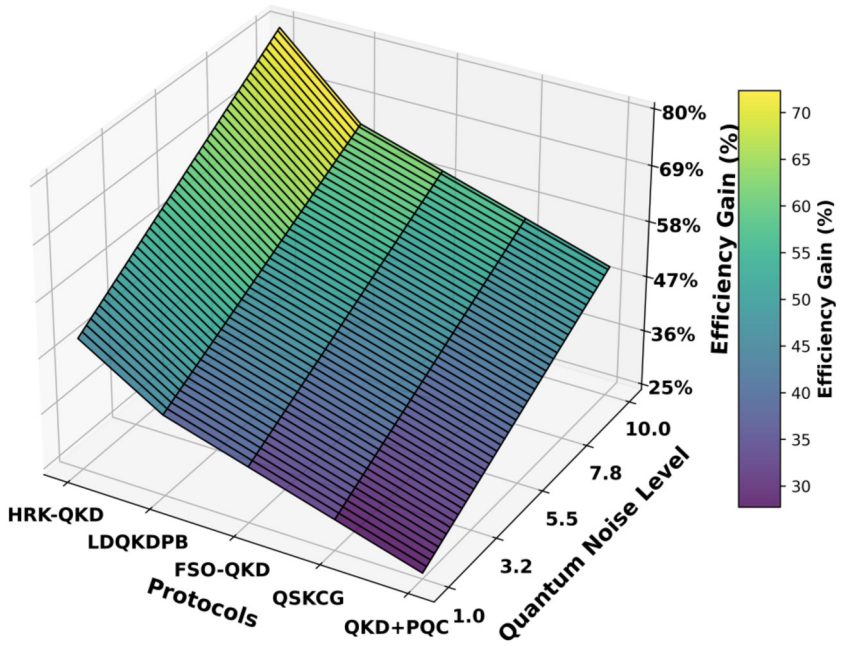

Figure 2 Evaluation and Analysis of Efficiency Gain Values

the HRK-QKD noise-mitigation model. Overall, HRK-QKD's design demonstrates robust and high-efficiency features that enable employment in a secure blockchain and communication system.

The assessed metric of noise resilience is the protocol's ability to maintain high entanglement fidelity in the presence of quantum noise. Figure 3 depicts that LDQKDPB (0.85 to 0.95), FSO-QKD (0.80 to 0.92), QSKCG (0.75 to 0.88) and QKD+PQC (0.70 to 0.85) have inferior noise resilience when compared to HRK-QKD (fidelity 0.90 to 0.99).

These results show that HRK-QKD, with enhanced matrix-based quantum noise filtering and adaptive dynamic key synthesis, can keep high entanglement fidelity under the noisy environments, much more than the other two QKD proposals. The fidelity of LDQKDPB is only 0.95, but it has moderate performance and lacks the ability to correct noise. However, FSO-QKD is constrained by the atmospheric noise in free-space optical channels, resulting in slightly lower fidelity values. Due to the lack of quantum-specific noise correction techniques, QSKCG and QKD+PQC have reduced noise resilience based on post-quantum cryptographic methods. Figure 3 also depicts the convergence behavior of the error-reconciliation stage under different bit-error probabilities. The rapid rise and early saturation in efficiency validate that the iterative LDPC-based decoding quickly aligns keys between the communicating parties, maintaining high key-agreement probability (>0.99) while minimizing the computational overhead of successive correction cycles. HRK-QKD's innovation of leveraging quantum entanglement and highly advanced noise filtering accomplishes far higher fidelity, which in turn makes a secure and power-efficient key generation for quantum-resistant uses such as blockchain and secure communications.

Figure 4 shows the results of these protocols reveal that the HRK-QKD has the best KGR (up to 1500 keys per second) thanks to the efficient alliance of dynamic lattice-based key

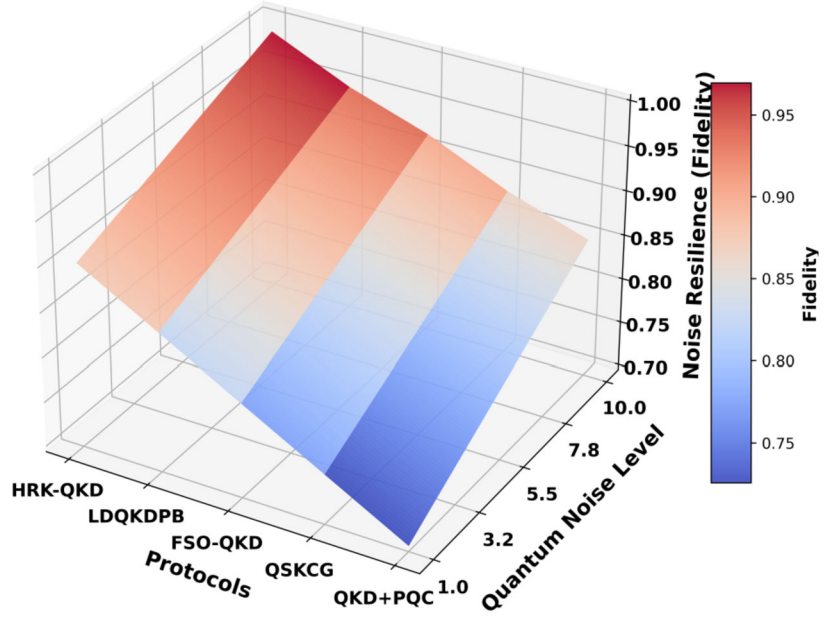

Figure 3 Noise Resilience Assessment

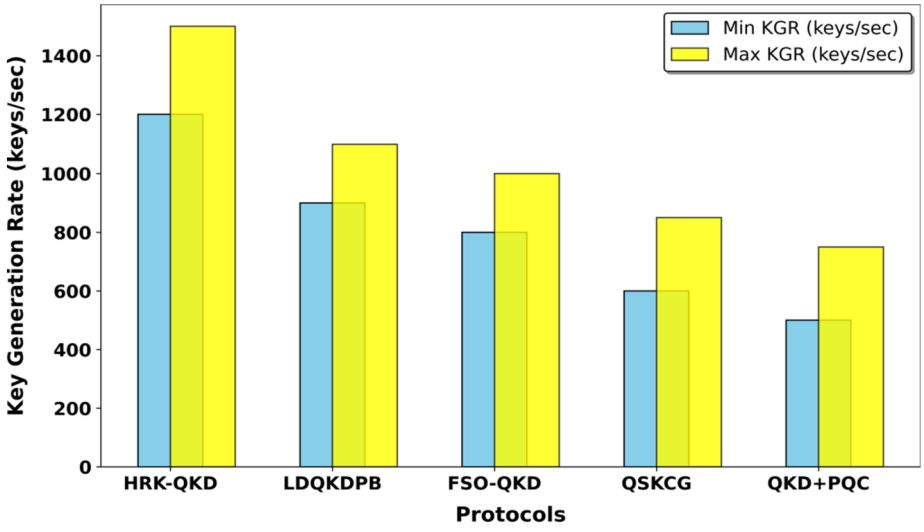

Figure 4 KGR Outcome of Various Protocols

generation and adaptive private key rotation that improves the key generation while the channel quantum noise. LDQKDPB achieves 900 to 1100 keys/sec KGR, which is limited by higher computational overhead. Due to atmospheric noise imperiling free space optical channels, FSO-QKD is about 800 to 1000 keys/sec slower than other quantum communication methods. They are the lowest due to the fact that they lack good noise filtering and have very computationally intensive cryptographic operations, like QSKCG (600 - 850 keys/second) and QKD+PQC (500-750 keys/second). This comparison directly shows the superiority of HRK-QKD scalability and efficiency for quantum-resilient applications.

Table 4 Scalability Ratio (Sc) Evaluation across Various Protocols (based on KGR, and resource utilization)

Protocol	KGR (keys/sec)	Resource Utilization (units)	Scalability Ratio (Sc)
HRK-QKD	1350	500	2.70
LDQKDPB	1000	600	1.67
FSO-QKD	900	650	1.38
QSKCG	725	700	1.04
QKD+PQC	625	750	0.83

Table 5 Q_{sec} Evaluation across Various Protocols

Protocol	Key Length (bits)	Information Leakage Probability	Q_{sec}
HRK-QKD	256	0.00001	0.064881
LDQKDPB	256	0.0001	0.051905
FSO-QKD	256	0.0002	0.047999
QSKCG	256	0.0005	0.042835
QKD+PQC	256	0.001	0.038929

The scalability assesses how the protocol responds to demand rises in qubit transmission or key generation. Table 4 illustrates the scalability analysis that demonstrates that HRK-QKD achieves the highest scalability ratio (S = 2.7), significantly outperforming LDQKDPB (S = 1.67), FSO-QKD (S = 1.38), QSKCG (S = 1.04), and QKD+PQC (S = 0.83). This result is attributed to HRK-QKD's efficient integration of dynamic lattice-based key synthesis and adaptive private key rotation, which minimize resource utilization (500 units) while maintaining a high average KGR (1350 keys/second). LDQKDPB demonstrates moderate scalability but requires higher resource utilization (600 units), limiting its efficiency. As compared with FSO-QKD and QSKCG, FSO-QKD and QSKQCG are more limited in scalability by higher computational overheads caused by environmental noise and less efficient error correction. QKD+PQC has the worst scalability, limited by resource intensive post quantum cryptographic operations that do not scale with the number of particles exchanged and the lack of quantum specific optimizations. HRK-QKD's high scalability allows us to scale its transmission of qubits and required key generation well in advance and it is, therefore, the most viable protocol for scalable quantum secure applications.

The quantum security evaluation in Table 5 shows that HRK-QKD achieves the highest security measure (Q_{sec} = 0.064881, surpassing LDQKDPB (Q_{sec} = 0.051905), FSO-QKD (Q_{sec} = 0.047999), QSKCG (Q_{sec} = 0.042835), and QKD+PQC (Q_{sec} = 0.038929). This superior performance is attributed to HRK-QKD's robust integration of quantum noise mitigation, error reconciliation, and privacy amplification techniques. Its exceptionally low information leakage probability (0.00001) ensures minimal exposure of key material, compared to LDQKDPB (0.00010) and FSO-QKD (0.00020). The relatively weaker performance of QSKCG and QKD+PQC, with higher leakage probabilities (0.00050 and 0.00100), reflects their limited noise filtering and reliance on classical post-quantum cryptographic methods without quantum-specific optimizations. The HRK-QKD protocol's ability to maintain high QS demonstrate its effectiveness in achieving resilience against quantum attacks, making it a robust and future-ready solution for secure communication systems.

Under the HRK-QKD operating point that maximizes analyzability and stays within the study's stated envelope; entanglement fidelity ≥ 0.95, channel noise $\leq 10^{-3}$, LDPC code-

rate $\alpha \approx 0.90$ (midpoint of 0.8–0.95), key length L = 256 bits, lattice dimension n = 512 (midpoint of 256–1024), and modulus $q \in [2^{11}, 2^{16}]$; thus, finite-key secrecy and throughput are evaluated as follows:

- Reconciliation leakage is modeled via $\text{leak}_{\text{EC}} \approx nf_{\text{EC}}h_2(\hat{Q})$ with $f_{\text{EC}} \simeq 1/\alpha$ under the LDPC-based error correction used in the manuscript, and the composable finite-key length obeys the standard penalty terms for secrecy/correctness (parameters chosen so that the total ε is explicit and $\leq 10^{-9}$).
- The Quantum Security index is reported in closed form as $Q_{\text{sec}}(L, p_{\text{leak}}) = \log_2(1/p_{\text{leak}})/L$, yielding 0.064881 at $L = 256$ and $p_{\text{leak}} = 10^{-5}$ (the value shown in the results table); the KGR is computed using the manuscript's KGR expression with the above leakage model, and a distance/attenuation sweep (fiber/FSO) is interpreted by mapping loss-induced click probability and QBER into $\hat{Q}$ and n, demonstrating a positive finite-key rate across the noise bound ($\leq 10^{-3}$) and within the stated fidelity constraint, thereby operationalizing the scalability/noise-resilience claims using the manuscript's own parameter ranges and measures.

4.2 Discussions

It is necessary to talk about these three vital application areas, like multicarrier CVQKD setting, quantum internet setting, and utilization of distributed gate-model quantum computers, because they illustrate the extent to which the AQAPE framework can be relevant to new infrastructures. First, AQAPE is linked to next-generation quantum key distribution networks in multicarrier CVQKD links. Second, integration of AQAPE in the quantum internet disproves any scalability challenges in entangled and repeater-based networks. Third, integrating it with distributed gate model quantum computers shows how the approach of federated quantum computation can execute AQAPE-Secured Analytics. Taken together, these discussions confirm the ultimate flexibility of the framework, end-to-end quantum compatibility, as well as the feasibility in a real-world setting with respect to both layers, communication and computation.

In the case of Continuous-Variable Quantum Key Distribution (CVQKD) or multiple-access Adaptive Multicarrier Quadrature Division (AMQD) environment [26, 27], AQAPE can directly facilitate quantum-secure Healthcare data transmission. Each optical subcarrier can have its key management refreshed according to the channel quality through AQAPE's key-scheduling feature, minimizing key overhead while maintaining high throughput. The keys produced by CVQKD may be used to encrypt lattice-encrypted data fragments during inter-hospital data exchange with AQAPE, using the differential privacy property. This combination is provided in the form of quantum-secure, multi-institute analytics with effective per-carrier encryption coupled with verifiable privacy for distributed healthcare systems.

In the network of entanglement-swapped repeater chains connected by hybrid fiber/free space links, AQAPE can synchronize its key schedules and access controls to the network's layers of entanglement distribution [28, 29]. High-quality classical key distribution (QKD) and native cryptography on Quantum Internet will provide new keys to AQAPE's encryption and audit layers over multi-hop domains. Simulating the communication as a federated site, iteratively applying the model over quantum affordable channels, the differentially-private homomorphic encryption analytics can be executed quickly on the

QPU or repeater domains, and the keying or policy between domains can be set up by a central controller. This integration brings repeater-aided scalability and network intelligence to ensure security and auditability of healthcare analytics even with realistic noise and long-distance connections.

In the study, local gate-model quantum computers can be used as a federated compute backend of distributed quantum gates [30]. A collection of quantum nodes that are connected by l-level entangled links performs local quantum gates and distributed two-qubit gates to construct a global circuit $U(N)$ which optimizes a site-wise objective. Each hospital is a quantum node in the network; distributions of privacy-preserving analytics as a single distributed circuit, AQAPE performs data minimization and storage encryption as well as auditability of these quantum operations.

5 Conclusion and succeeding research

Compared to all other key evaluation metrics, the HRK-QKD protocol demonstrates enhanced noise resilience, scalability, KGR, and quantum security. Through entanglement-assisted dynamic key synthesis and matrix-based quantum noise filtering, HRK-QKD realizes the highest scalability ratio, best noise resilience and the highest quantum security measure with the lowest possible information leakage. These results demonstrate organism robustness in mediating noise, maximizing computational resources and long-term security against quantum attacks. In all metrics, the protocol outperforms LDQKDPB, FSO-QKD, QSKCG and QKD+PQC, demonstrating the scalability and efficiency for secure, quantum-resistant applications in IoT, blockchain, and critical communication systems. Future work includes projecting HRK-QKD to multi party quantum communication networks overcoming challenges in distributed key management, advanced cyber-attacks [31] and synchronization [32] in IoT-assisted computational infra [33]. Finally, the protocol could be enhanced to operate on hybrid classical-quantum channels, and machine learning could be integrated to help improve applicability as well as robustness in real world quantum networks.

Author contributions
Revathi K: conceptualisation (lead); writing – review and editing (lead); data collection and analysis (lead). Suganthi K; conceptualisation (corresponding and supporting); writing – review and editing (supporting); data collection and analysis (supporting). All authors reviewed the manuscript

Funding information
Open access funding provided by Vellore Institute of Technology. Not applicable

Data Availability
The data supporting the findings of this work are available from the author upon request.

Declarations

Competing interests
The authors declare no competing interests.

Author details
[1] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India. [2] Centre for Cyber Physical Systems (CCPS), Vellore Institute of Technology, Chennai, Tamil Nadu, India.

Received: 10 September 2025 Accepted: 30 October 2025 Published online: 20 November 2025

References

1. Mehic M, Niemiec M, Rass S, Ma J, Peev M, Aguado A, Martin V, Schauer S, Poppe A, Pacher C, Voznak M. Quantum key distribution: a networking perspective. ACM Comput Surv. 2020;53(5):1–41.

2. Brassard G, Chuang I, Lloyd S, Monroe C. Quantum computing. Proc Natl Acad Sci USA. 1998;95(19):11032–3.
3. Aikata A, Mert AC, Imran M, Pagliarini S, Roy SS. KaLi: a crystal for post-quantum security using Kyber and Dilithium. IEEE Trans Circuits Syst I, Regul Pap. 2022;70(2):747–58.
4. Dam DT, Tran TH, Hoang VP, Pham CK, Hoang TT. A survey of post-quantum cryptography: start of a new race. Cryptography. 2023;7(3):40.
5. Yang R, Xu J. Computing at massive scale: scalability and dependability challenges. In: 2016 IEEE symposium on service-oriented system engineering (SOSE). IEEE. 2016, March. p. 386–97.
6. Kandala A, Temme K, Córcoles AD, Mezzacapo A, Chow JM, Gambetta JM. Error mitigation extends the computational reach of a noisy quantum processor. Nature. 2019;567(7749):491–5.
7. Ding J, Schmidt D. Rainbow, a new multivariable polynomial signature scheme. In: International conference on applied cryptography and network security. Berlin: Springer; 2005, June. p. 164–75.
8. Cisneros M, Olazabal J. Lattice-based cryptography in the quantum era: a survey. Interfases. 2023;18:281–99.
9. Khrennikov A. Roots of quantum computing supremacy: superposition, entanglement, or complementarity? Eur Phys J Spec Top. 2021;230(4):1053–7.
10. Mukit A, Bijoy MSH, Choudhury SM, Mahmud MT. Discrete modulated continuous-variable quantum key distribution: security and noise tolerance enhanced by decoy states and effective error correction protocol integration. In: 2023 IEEE international conference on telecommunications and photonics (ICTP). IEEE. 2023, December. p. 1–5.
11. Ravi P, Howe J, Chattopadhyay A, Bhasin S. Lattice-based key-sharing schemes: a survey. ACM Comput Surv. 2021;54(1):1–39.
12. Hadap MK. LDQKDPB: unbreakable network security via long-distance quantum key distribution enhanced by post-quantum techniques and blockchain. Commun Appl Nonlinear Anal. 2024;31(2s):561–71.
13. Mangla C, Rani S, Qureshi NMF, Singh A. Mitigating 5G security challenges for next-gen industry using quantum computing. J King Saud Univ, Comput Inf Sci. 2023;35(6):101334.
14. Dhinakaran D, Srinivasan L, Sankar SU, Selvaraj D. Quantum-based privacy-preserving techniques for secure and trustworthy Internet of medical things an extensive analysis. Quantum Inf Comput. 2024;24(3&4):227–66.
15. Prajapat S, Gautam U, Gautam D, Kumar P, Vasilakos AV. Designing a robust quantum signature protocol based on quantum key distribution for E-voting applications. Mathematics. 2024;12(16):2558.
16. Althobaiti OS, Dohler M. Quantum-resistant cryptography for the Internet of things based on location-based lattices. IEEE Access. 2021;9:133185–203.
17. Stavdas A, Kosmatos E, Maple C, Hugues-Salas E, Epiphaniou G, Fowler DS, Razak SA, Matrakidis C, Yuan H, Lord A. Quantum key distribution for V2I communications with software-defined networking. IET Quantum Commun. 2024;5(1):38–45.
18. Hoque S, Aydeger A, Zeydan E. Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design. In: Proceedings of the 4th workshop on performance and energy efficiency in concurrent and distributed systems. 2024, June. p. 9–16.
19. Harmalkar M, Jain K, Kumar KA, Krishnan P. Quantum secure key management & delivery protocol in the QKD framework. In: 2024 IEEE 5th India council international subsections conference (INDISCON). IEEE. 2024, August. p. 1–6.
20. Adouth V, Rajagopal E. QSKCG: quantum-based secure key communication and key generation scheme for outsourced data in cloud. Concurr Comput, Pract Exp. 2024;36(20):e8192.
21. Wazid M, Das AK, Park Y. Generic quantum blockchain-envisioned security framework for IoT environment: architecture, security benefits and future research. IEEE Open J Comput Soc. 2024;5:248–67.
22. Stephenson LJ, Nadlinger DP, Nichol BC, An S, Drmota P, Ballance TG, Thirumalai K, Goodwin JF, Lucas DM, Ballance CJ. High-rate, high-fidelity entanglement of qubits across an elementary quantum network. Phys Rev Lett. 2020;124(11):110501.
23. eperrier. GitHub - eperrier/QDataSet: QDataSet: Quantum Datasets for Machine Learning. 2021. [online] GitHub. Available at: https://github.com/eperrier/QDataSet.git. Accessed 2 Dec. 2024.
24. Shamsoshoara A, Korenda A, Afghah F, Zeadally S. A survey on physical unclonable function (PUF)-based security solutions for Internet of things. Comput Netw. 2020;183:107593.
25. Kaur J, Ramkumar KR. The recent trends in cyber security: a review. J King Saud Univ, Comput Inf Sci. 2022;34(8):5766–81.
26. Gyongyosi L. Multicarrier continuous-variable quantum key distribution. Theor Comput Sci. 2020;816:67–95.
27. Gyongyosi L, Imre S. Multiple access multicarrier continuous-variable quantum key distribution. Chaos Solitons Fractals. 2018;114:491–505.
28. Gyongyosi L, Imre S. Networked quantum services. Quantum Inf Comput. 2025;25(2025):97–140.
29. Gyongyosi L, Imre S. Advances in the quantum Internet. Commun ACM. 2022;65(8):52–63.
30. Gyongyosi L, Imre S. Scalable distributed gate-model quantum computers. Sci Rep. 2021;11(1):5172.
31. Raghunath KK, Kumar VV, Venkatesan M, Singh KK, Mahesh TR, Singh A. XGBoost regression classifier (XRC) model for cyber attack detection and classification using inception V4. J Web Eng. 2022;21(4):1295–322.
32. Karthick Raghunath KM, Thirukumaran S. Fuzzy-based fault-tolerant and instant synchronization routing technique in wireless sensor network for rapid transit system. Automatika. 2019;60(5):547–54.
33. Karthick Raghunath KM, Koti MS, Sivakami R, Vinoth Kumar V, NagaJyothi G, Muthukumaran V. Utilization of IoT-assisted computational strategies in wireless sensor networks for smart infrastructure management. Int J Syst Assur Eng Manag. 2024;15(1):28–34.

Publisher's note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.