Proceedings of CONF-MPCS 2025 Symposium: Leveraging EVs and Machine Learning for Sustainable Energy Demand Management
DOI: 10.54254/2753-8818/2025.GL23411

Quantum Security: An Overview of Quantum Cryptography

Yiheng Chen

College of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou, China
cyh897572022@163.com

Abstract: Recent years have witnessed a furious race for quantum technologies in both academia and industry, driven by the rapid progress in quantum cryptography. The traditional cryptography faces the risk of being deciphered. Thus, traditional ways of transmitting information are not safe anymore. For those reasons, future information transmission needs to use quantum cryptography. This paper explores the two most important ways to achieve quantum security: Quantum Key Distribution and Post Quantum Cryptography. This study also investigates the synergistic integration of these two methodologies within quantum security systems, including their background, current mainstream technology, the encountered problems, some ways to solve them and future directions. Through the method of literature review, the paper finds that Quantum Key Distribution and Post Quantum Cryptography are important in protecting information security in the future, but they are still imperfect and have many problems that need to be solved, including technical immaturity, interoperability constraints, and scalability bottlenecks that demand global cooperation.

Keywords: Quantum Cryptography, Introduction Quantum Security, Quantum Key Distribution, Post Quantum Cryptograph

1. Introduction

Modern encryption methods for sending information mainly use asymmetric encryption systems, which rely on complex math problems to keep data secure, especially the difficulty of breaking down large numbers into their prime factors and solving discrete logarithm problems. Nevertheless, the sustained integrity of such cryptosystems faces existential risks due to exponential advancements in semiconductor technology and computational methodologies. This imperative becomes particularly acute given the advent of quantum computing systems capable of executing Shor's polynomial-time factorization algorithm and Grover's quadratic speedup search technique, which collectively jeopardizes conventional public-key infrastructure (PKI) systems. To address these emergent threats, two distinct cryptographic countermeasures have gained prominence: Quantum Key Distribution (QKD) which harnesses quantum mechanical principles (e.g., no-cloning theorem and quantum entanglement) to generate information-theoretically secure and Post-Quantum Cryptography (PQC) which develops classical algebraic constructs resistant to quantum cryptanalysis and classical decryption methodologies [1]. Furthermore, the integration of QKD and PQC within a unified system is also a promising strategy for achieving complementary security advantages that leverages QKD's information-theoretic security alongside PQC's convenience to better defend against cryptographic threats.

DOI: 10.54254/2753-8818/2025.GL23411

This article examines the foundational principles and evolution of Quantum Key Distribution and Post-Quantum Cryptography, analyzes persistent challenges in their implementation, outlines prospective research, and systematically investigates the potential synergies and methodologies for constructing frameworks that enhance cryptographic infrastructures through the integration of these two technologies. Additionally, it provides a theoretical reference for the further development of quantum cryptography.

2. Quantum Key Distribution

2.1. Background

QKD is a method used to securely exchange cryptographic keys between two parties, utilizing the principles of quantum mechanics. Unlike traditional cryptographic methods relying on computational hardness assumptions, QKD leverages the inherent properties of quantum mechanics to achieve secure key exchange, even in the presence of eavesdroppers. QKD systems, leveraging quantum mechanical principles such as photon polarization and the no-cloning theorem, demonstrate unparalleled efficacy in securing static high-security government networks with fiber-optic backbone architectures, achieving provable information-theoretic security [2].

QKD protocols rely on quantum states of photons to encode information, which cannot be cloned or measured without altering the state due to the no-cloning theorem and the Heisenberg uncertainty principle. These quantum properties allow the communicating parties to detect the presence of an eavesdropper through the measurement disturbances it would cause. The well-known QKD protocol is BB84, developed by Charles Bennett and Gilles Brassard in 1984, which uses photon polarization states to transmit secret keys. The team of Peter W. Shor makes simple proof of security of the BB84 through entanglement purification and Calderbank-Shor-Steane (CSS) codes [3].

Unlike discrete-variable QKD protocols, continuous-variable QKD (CV-QKD) utilizes the continuous properties of quantum systems (such as the quadratures of light) to perform key distribution. CV-QKD systems are particularly attractive for use in fiber-optic networks due to their ability to operate over longer distances with less sensitivity to losses. Hou-Manchin's team proposes a digital synchronization procedure for a modern CV-QKD system with a locally generated local oscillator for coherent reception; their approach could be used in various CV-QKD systems, Meanwhile, it paves the way for cost-effective QKD solutions [4].

2.2. Challenges and current technology development

Although QKD is theoretically secure, several challenges remain to be addressed, particularly the high cost, limitations in key rates and transmission distances. Potential solutions to these challenges include quantum repeaters and ground-to-satellite QKD [5]. One of the most important studies presents a QKD experiment based on quantum entanglement, led by the University of Science and Technology of China. The research utilizes the "Micius" satellite to distribute entangled photon pairs, overcoming the traditional 100-kilometer distance limitation of ground-based QKD. The satellite carried a high-efficiency entangled photon source and transmitted entangled photon pairs to ground stations in Delingha, Qinghai, and Xinjiang. The physical distance between the two stations was 1,120 kilometers, with a total link loss of 56-71 dB. Compared to previous experiments, the ground stations were equipped with a new 1.2-meter telescope and optimized optical paths, improving single-link efficiency by 3 dB and increasing the total two-photon distribution efficiency by four times. Entanglement-based QKD is source-independent, eliminating the need to trust the photon source. The ground stations employed time-frequency domain filtering, detector monitoring circuits, and free-running modes to ensure fair sampling and actual security. Thus, the Bell test yielded an S-value of 2.56±0.07, confirming high-quality entanglement. This method can generate 6,208 initial

DOI: 10.54254/2753-8818/2025.GL23411

compatible events during 3,100 seconds of effective time. After filtering and error correction, 372 secure key bits were obtained. The key rate was 0.12 bits per second under finite key conditions, with a quantum bit error rate as low as 4.5%. The satellite-based solution demonstrated an 11-order-of-magnitude improvement in link efficiency compared to commercial ultra-low-loss fibers. This breakthrough extends the practical QKD security distance from the hundred-kilometer to the thousand-kilometer range, without requiring trusted relays [6].

Another study analyzes the performance of subcarrier quantum key distribution (SCW QKD) in classical dense wavelength division multiplexing (DWDM) channels, focusing on the impact of spontaneous Raman scattering (SpRS) noise. The research compares continuous wave (CW) and pulsed laser source modes, evaluating their performance under SpRS noise and varying classical receiver sensitivities. Results show that SpRS significantly increases the quantum bit error rate (QBER), particularly over long distances. The pulsed mode outperforms CW mode, achieving a longer maximum distance for secure key generation. Thus, optimizing laser modulation and receiver sensitivity can enhance SCW QKD's compatibility with high-speed DWDM networks, supporting the integration of quantum-classical communication systems [7].

2.3. Emerging application domains

QKD leverages quantum mechanical principles to distribute keys securely, making it inherently resistant to quantum computing threats. Thus, it’s particularly suitable for the following areas.

In secure communication networks, QKD enables the secure exchange of cryptographic keys, providing end-to-end security for communication protocols like TLS/SSL. QKD guarantees that any eavesdropping attempt on the key exchange will be detected. For highly sensitive government and military communications, QKD ensures that cryptographic keys are exchanged securely without the need for traditional key management systems vulnerable to quantum attacks. Financial services benefit from QKD's cryptographic robustness, as it provides secure banking systems and digital transactions, offering an unbreakable solution for key exchange that is immune to the decryption capabilities of quantum computers. Furthermore, as for cloud computing, QKD ensures quantum-safe encryption for cloud data, protecting sensitive information during key exchange.

These applications illustrate QKD's potential to revolutionize security in a post-quantum world, providing long-term protection against quantum computing threats.

3. Post-Quantum Cryptography

3.1. Background

Post-Quantum Cryptography refers to cryptographic algorithms designed to be secure against the capabilities of quantum computers. As quantum computers have the potential to break widely used cryptographic systems, such as RSA and ECC, there is a strong push towards developing new cryptographic protocols (PQC) that can withstand quantum attacks. The two most prominent families of algorithms in PQC are hash-based cryptography and lattice-based cryptography.

The first is Hash-Based Cryptography leveraging the security of cryptographic hash functions, unlike traditional cryptographic systems that rely on the difficulty of factoring large integers or solving discrete logarithm problems, hash-based schemes focus on the one-way nature of hash functions, which remains even in the presence of quantum computation. To enhance the standard of Hash-Based Cryptography, the National Institute of Standards and Technology (NIST) guidelines specify two hash-based stateful signature schemes and their multi-tree variants. The first one is Leighton-Micali Signature System based on Winternitz one-time signatures (OTS) and a Merkle tree structure. Hierarchical Signature System (HSS) supports multi-layer tree structures to enhance key capacity. The second one is Extended Merkle Signature Scheme (XMSS), which combines

DOI: 10.54254/2753-8818/2025.GL23411

Winternitz OTS+ with an enhanced Merkle tree structure and uses prefixes and bitmasks for improved security. XMSS-MT allows hierarchical management of signature keys [8].

Then there is Lattice-Based Cryptography. Lattice-based cryptographic schemes are considered one of the most promising approaches in the post-quantum era due to their resilience against quantum attacks. The security of lattice-based schemes is based on the hardness of problems such as the Short Integer Solution (SIS) problem and other related lattice problems. These problems have not been efficiently solved by quantum algorithms, making lattice-based cryptography a strong candidate for post-quantum cryptographic systems. Lattice-based algorithms can be widely applied in areas like public-key encryption, key exchange protocols, and digital signatures.

Both approaches are key technologies for secure communications against quantum computing threats. Hash-based schemes focus on the simplicity and efficiency of hash functions while lattice-based schemes offer broader capabilities. These two algorithms represent the cutting edge of research in post-quantum cryptography and are the main methods in the transition to quantum-resistant cryptographic standards.

3.2. Challenges and current technology development

Although demonstrating robustness against quantum algorithms, it still faces significant challenges. The two primary obstacles are algorithm efficiency bottlenecks and immature standardization.

PQC algorithms face challenges such as large key sizes, oversized signatures, and high computational complexity. Moreover, the signature generation in PQC systems is often significantly slower than in classical alternatives, leading to slower overall performance. These inefficiencies hinder widespread deployment, particularly in resource-constrained environments or applications with strict latency and bandwidth requirements. Additionally, the standardization process remains immature. While the National Institute of Standards and Technology (NIST) is finalizing the post-quantum cryptography standards, no definitive set of algorithms has been adopted. The withdrawal of notable contenders like Rainbow-based schemes has intensified institutional hurdles in building enduring post-quantum cryptographic frameworks amid shifting security paradigms.

To solve the challenges, many methods were proposed. Consider SPHINCS+. As a stateless, quantum-resistant signature scheme selected by NIST for standardization, SPHINCS+ offers robust security but suffers from high computational overhead, limiting its practical adoption. To address this, a team led by Ziheng Wang has introduced significant breakthroughs through GPU-accelerated implementations, notably the CUSPX Framework, which enhances the efficiency of SPHINCS+. The CUSPX framework employs a multi-level parallelism approach, utilizing algorithmic, data, and hybrid parallelism, extended with task parallelism, enabling large-scale parallel execution across over 10,000 GPU cores. Key innovations include parallel Merkle tree construction and load balancing techniques for the WOTS+ and FORS trees, optimizing resource utilization and mitigate workload imbalances in hybrid parallelism. Hence, performance improvements are significant, with CUSPX achieving a latency of 0.67 MS per signature on an RTX 3090 GPU, outperforming FPGA and CPU implementations by 18.5×. The system's throughput reaches 1.15 million signatures per second, demonstrating high efficiency. The low-latency, high-throughput capabilities of CUSPX make it suitable for real-time applications and high-demand environments [9].

Another team supposed that cryptographic migration will take decades, requiring early planning for systems with long lifespans, like automotive and infrastructure. With NIST's PQC standardization nearing completion, this team recommends hash-based signatures (HBS) and hybrid encryption combining classical and PQC algorithms. And the enterprises must inventory cryptographic assets, test candidate algorithms, and support the standardization process [10].

DOI: 10.54254/2753-8818/2025.GL23411

3.3. Emerging application domains

Post-Quantum Cryptography is essential for securing various sectors against the potential threats posed by quantum computers. Key applications of PQC include the following domains.

First is secure communication networks, in which PQC ensures the security of protocols like TLS or SSL. For cloud computing and data storage, PQC provides quantum-safe encryption, protecting data confidentiality and privacy across industries like healthcare, finance, and government. Within financial services and digital currencies, PQC can secure digital transactions, blockchain technologies, and cryptocurrencies by replacing vulnerable algorithms with quantum-resistant alternatives. Additionally, PQC supports secure digital identity management and authentication systems, preventing unauthorized access to sensitive personal and organizational data.

These applications highlight the broad potential of PQC in safeguarding sensitive data and communications in the quantum era.

4. Hybrid security architecture collaborative deployment QKD and PQC

4.1. Synergistic QKD-PQC co-deployment framework

Standalone Quantum Key Distribution faces limitations due to its reliance on pre-shared keys for classical channel authentication, which introduces key management complexity and security risks associated with trusted relays as user scales increase. In contrast, Post-Quantum Cryptography offers quantum-secure authentication that, when integrated with Public Key Infrastructure (PKI), supports dynamic, pre-shared-key-free initial identity verification.

This paper proposes that a hybrid framework employs multi-layered architecture. At the quantum layer, QKD is responsible for generating information-theoretically secure keys. The classical cryptography layer utilizes PQC for initial authentication, certificate exchange, and key negotiation protocols. A dedicated Key Management System (KMS) dynamically orchestrates the integration between these layers, ensuring a seamless key lifecycle: PQC establishes initial identity authentication and negotiates short-term session keys, while QKD generates long-term, high-security keys for encrypting core business data.

The framework draws design inspiration from the “Jinan Metropolitan QKD Network,” where optical switches replace traditional trusted relays, and PQC authentication secures inter-node communication [11]. Moreover, integrating PQC algorithms into QKD devices’ ARM chips reduces key sizes to the kilobyte level and achieves authentication latencies below 100 ms. In metropolitan network scenarios, dynamic PQC-based routing minimizes the number of trusted relays, thereby reducing both operational costs and the attack surface.

4.2. Future prospects

Looking forward, further algorithmic optimizations are essential to enhance this hybrid QKD-PQC system’s efficiency, particularly in signature generation and verification—to support larger-scale networks. Standardization compatibility must also be promoted, ensuring that emerging PQC algorithms interoperate seamlessly with established QKD protocols. Additionally, integrating satellite-based QKD with ground-based PQC authentication could enable a unified quantum internet, enhancing the security of critical infrastructure sectors such as finance and energy.

Future research should focus on developing integrated devices that support simultaneous QKD transmission and PQC co-processing, exploring novel hybrid authentication protocols to reduce communication rounds, and designing joint defense mechanisms that leverage QKD’s physical security and PQC’s logical security to counter quantum relay attacks.

DOI: 10.54254/2753-8818/2025.GL23411

5. Conclusion

Quantum Key Distribution and Post-Quantum Cryptography, despite their distinct theoretical foundations rooted in quantum physics and mathematical complexity respectively, collectively constitute dual pillars for safeguarding information infrastructure against quantum computing threats. Meanwhile, PQC algorithms—particularly lattice-based and hash-based schemes standardized by NIST—are optimized for dynamic commercial environments, where their polynomial-time computational efficiency aligns with mobile network constraints in 5G/6G deployments. Therefore, for situations with high requirements for easy adaptation and compatibility, PQC can be appropriately incorporated.

This paper systematically evaluates quantum security challenges through literature review, elucidating QKD-PQC integration paradigms across protocol layers. While QKD excels in long-term key provisioning for critical national infrastructure, PQC mechanisms dominate agile authentication in IoT ecosystems and vehicular networks. Nevertheless, the analysis remains insufficient in quantifying performance benchmarks against hybrid attacks.

While the theoretical framework and conceptual conclusions are grounded in comprehensive academic discourse, the findings remain subject to limitations inherent to non-empirical research, notably the absence of experimental validation and data to substantiate cryptographic performance metrics.

Future advancements are projected to transcend current sector-specific limitations. People should advance interdisciplinary quantum cryptography research across physics, computer science, and information theory to expand its applications. Only through interdisciplinary collaboration, global cooperation, and sustained investment can a quantum security network covering a wide area be built, providing a solid barrier for data sovereignty and privacy protection in the post-quantum era.

References

[1] *Mehic, M., Michalek, L., Dervisevic, E., Burdiak, P., Plakalovic, M., Rozhon, J., ... & Voznak, M. (2023). Quantum cryptography in 5G networks: A comprehensive overview. IEEE Communications Surveys & Tutorials, 26(1), 302-346.*

[2] *Jian-Wei, P. (2024). Quantum information technology: Current status and prospects. Acta Physica Sinica, 73(1).*

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

[4] *Chin, H. M., Jain, N., Andersen, U. L., Zibar, D., & Gehring, T. (2022). Digital synchronization for continu ous-variable quantum key distribution. Quantum Science and Technology, 7(4), 045006.*

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

[6] *Yin, J., Li, Y. H., Liao, S. K., Yang, M., Cao, Y., Zhang, L., ... & Pan, J. W. (2020). Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature, 582(7813), 501-505.*

[7] *Kiselev, F., Goncharov, R., Veselkova, N., Samsonov, E., Kiselev, A. D., & Egorov, V. (2021). Performance of subcarrier-wave quantum key distribution in the presence of spontaneous Raman scattering noise generated by classical DWDM channels. Journal of the Optical Society of America B, 38(2), 595-601.*

[8] *Cooper, D. A., Apon, D. C., Dang, Q. H., Davidson, M. S., Dworkin, M. J., & Miller, C. A. (2020). Recommendation for stateful hash-based signature schemes. NIST Special Publication, 800(208), 800-208.*

[9] *Wang, Z., Dong, X., Chen, H., Kang, Y., & Wang, Q. (2024). CUSPX: Efficient GPU Implementations of Post-Quantum Signature SPHINCS+. IEEE Transactions on Computers.*

[10] *Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), 237-243.*

[11] *Yang, Y. H., Li, P. Y., Ma, S. Z., Qian, X. C., Zhang, K. Y., Wang, L. J., ... & Pan, J. W. (2021). All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. Optics express, 29(16), 25859-25867.*