NIILM University International Journal of Applied and Behavioural Sciences (IJABS)

ISSN: 3048-9083 Vol.03, Issue 01, Jan-Jun 2026

Quantum Cryptography: Securing the Digital Future

Neelam

Assistant Professor, Department of Physics, Dr. B.R. Ambedkar Govt. College Kaithal

DOI: https://doi.org/10.70388/ijabs250159

Received on Nov 06, 2025

Accepted on Dec 15, 2025

Published on Jan 05, 2026

Abstract

In the modern digital era, where cyber-attacks, data breaches, and digital spying threaten global security, conventional cryptographic systems face increasing challenges. The rapid development of quantum computing has amplified these threats by undermining the security foundations of classical encryption algorithms such as RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography), both of which depend on the computational hardness of factorization and discrete logarithmic problems. Quantum cryptography, rooted in the principles of quantum mechanics, introduces a transformative approach that ensures theoretically unbreakable security. This paper explores the theoretical foundations, current technological developments, challenges, and future prospects of quantum cryptography. It emphasizes the transition from mathematical security to physical security, highlighting quantum key distribution (QKD), quantum random number generation, and post-quantum cryptographic frameworks. The study concludes that quantum cryptography is not merely a futuristic ideal but a necessary evolution for safeguarding the digital future in a quantum-enabled world.

Keywords: Quantum Cryptography, Quantum Key Distribution, QKD, Cyber security, Post-Quantum Cryptography, Quantum Communication, Quantum Computing.

1. Introduction

The digital revolution has interconnected the world in ways once unimaginable, enabling seamless data exchange, global financial transactions, and communication across vast distances. However, this connectivity comes at the cost of vulnerability. Conventional cryptographic systems such as RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography) depend on the mathematical intractability of specific problems, like integer factorization and discrete logarithms. With the emergence of quantum computing, these problems are no longer computationally secure, as quantum algorithms such as Shor's algorithm can solve them exponentially faster than classical methods [1].

Quantum cryptography presents a paradigm shift from computational to physical security. It leverages the fundamental principles of quantum mechanics—specifically, the superposition and no-cloning theorem—to ensure that eavesdropping attempts are not only detectable but also impossible without disturbing the system [2]. This property offers an unprecedented level of security for information transmission, particularly through quantum key distribution (QKD).

This paper explores the theoretical framework, technological progress, limitations, and prospective advancements of quantum cryptography, underscoring its indispensable role in ensuring secure communication in the quantum era.

2. Theoretical Background

Quantum cryptography is built upon three foundational pillars of quantum mechanics:

a) **Superposition**: A quantum system can exist in multiple states simultaneously until it is measured.
b) **Entanglement:** Two or more particles can become correlated such that the state of one instantaneously determines the state of the other, regardless of distance.
c) **No-Cloning Theorem**: It is impossible to create an identical copy of an arbitrary unknown quantum state [3].

2.1 Quantum Key Distribution (QKD)

At the heart of quantum cryptography lies QKD, a method that enables two parties (commonly referred to as Alice and Bob) to share a secret cryptographic key with absolute

security. The most renowned QKD protocol is the BB84 protocol, proposed by Bennett and Brassard in 1984 [4].

In BB84, photons are polarized in four possible states—horizontal, vertical, diagonal, and anti-diagonal. Any attempt by an eavesdropper (Eve) to intercept and measure these photons introduces detectable errors, alerting Alice and Bob to the intrusion.

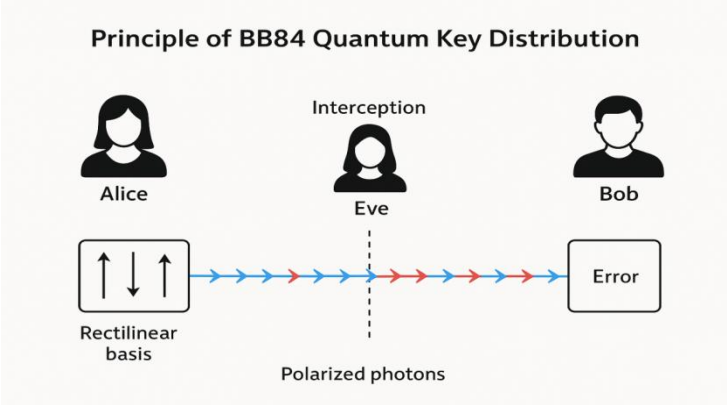

Diagram 1: Principle of BB84 Quantum Key Distribution

Description: A schematic showing Alice sending polarized photons to Bob using two bases (rectilinear and diagonal). Eve's interception disturbs photon polarization, creating detectable errors in the key comparison stage.

2.2 Quantum Entanglement-Based Protocols

Another class of QKD systems uses quantum entanglement, The E91 protocol which was proposed by Artur Ekert in 1991, utilizes pairs of entangled photons shared between Alice and Bob [5]. The security of E91 arises from the violation of Bell's inequalities—demonstrating quantum correlations that cannot be explained by classical physics.

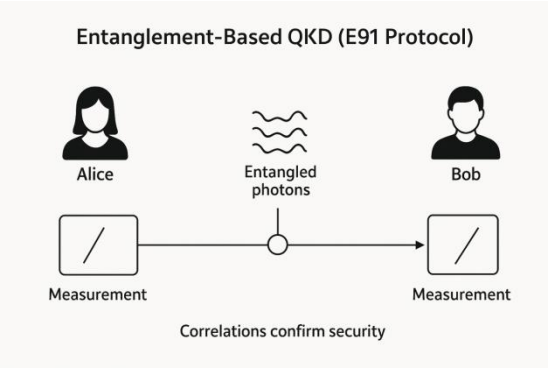

Diagram 2: "Entanglement-Based QKD (E91 Protocol)": Two entangled photons are generated at a central source and distributed to Alice and Bob. Measurement correlations confirm security if Bell's inequalities are violated.

2.3 Quantum Random Number Generation (QRNG)

Randomness is a vital component in cryptography. Traditional pseudo-random number generators (PRNGs) rely on deterministic algorithms and can be predicted. QRNGs exploit the inherent unpredictability of quantum measurements—such as photon arrival times or spin states—to generate truly random numbers [6].

3. Current Developments

Quantum cryptography has transitioned from theoretical constructs to practical systems deployed in real-world settings.

3.1 Commercial QKD Systems

Companies like ID Quantique (Switzerland) and Toshiba (Japan) have developed commercial QKD products that integrate with existing fiber-optic infrastructure. The Swiss Quantum Network demonstrated long-term, field-deployed QKD between Geneva and Lausanne [7].

3.2 Satellite-Based Quantum Communication

A major breakthrough occurred with China's Micius satellite, launched in 2016, which successfully established satellite-to-ground QKD links over 1200 km [8]. This experiment marked a pivotal step toward global quantum communication networks.

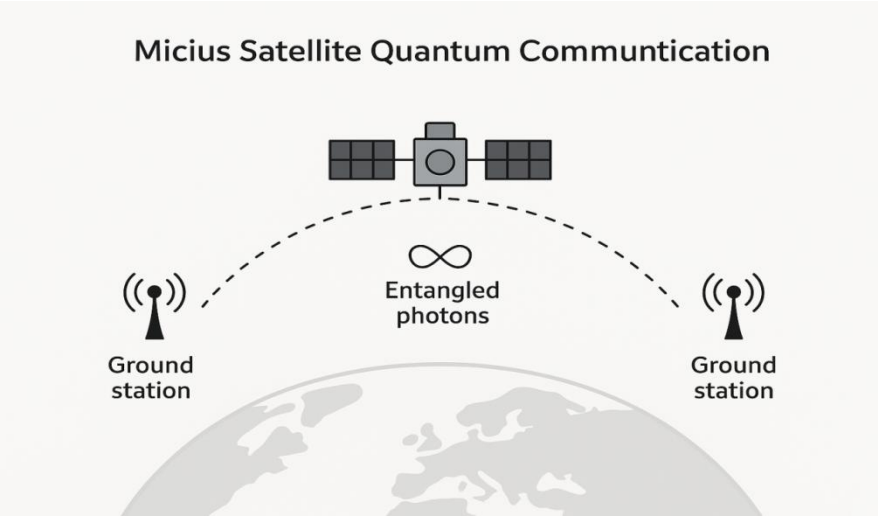

Diagram 3:

Title: "Micius Satellite Quantum Communication"

Description: The Micius satellite distributes entangled photons between two distant ground stations, demonstrating secure intercontinental key exchange.

3.3 Quantum Networks and the Quantum Internet

Efforts are underway to interconnect multiple QKD nodes into quantum-secure networks. The European Quantum Communication Infrastructure (EuroQCI) and the U.S. Quantum Internet Blueprint both aim to establish nationwide quantum communication frameworks [9]. These initiatives represent early stages of a future quantum internet, combining classical and quantum channels for hybrid data transmission.

3.4 Post-Quantum Cryptography (PQC)

While QKD requires specialized hardware, PQC focuses on developing classical cryptographic algorithms resistant to quantum attacks. The National Institute of Standards and Technology (NIST) are currently standardizing post-quantum algorithms, including lattice-based and hash-based schemes [10].

Quantum cryptography and PQC are complementary—one offering physical-layer security, the other ensuring quantum-safe computation.

4. Challenges and Limitations

Despite its promise, quantum cryptography faces several significant challenges that must be addressed for large-scale deployment.

4.1 Technological Limitations

Quantum systems are highly sensitive to environmental noise and photon losses. Maintaining coherence over long distances requires ultra-low temperature detectors and precise optical alignment. Fiber-based QKD systems currently achieve secure transmission up to approximately 400 km, beyond which signal degradation becomes significant [11].

4.2 Cost and Infrastructure Requirements

The integration of QKD into existing communication systems demands specialized hardware—single-photon sources, detectors, and optical stabilizers—which increases cost.

Moreover, global deployment would require hybrid infrastructures combining terrestrial and satellite links.

4.3 Key Rate and Speed Constraints

Compared to classical cryptography, QKD systems have lower key generation rates. The balance between transmission distance and key rate remains a key research area, with current experiments achieving megabit-per-second rates over metropolitan distances [12].

4.4 Standardization and Interoperability

Different QKD implementations often lack standardized protocols, which complicates interoperability between systems from various manufacturers. The European Telecommunications Standards Institute (ETSI) and ITU-T are developing guidelines for QKD network integration [13].

4.5 Security Assumptions and Attacks

Although theoretically unbreakable, practical QKD systems can be vulnerable to side-channel attacks such as detector blinding or Trojan-horse attacks [14]. Continuous testing and hardware-level countermeasures are essential to maintain security integrity.

5. Future Perspectives

Quantum cryptography is on the cusp of transforming cybersecurity. Future research focuses on scalability, integration, and performance optimization.

5.1 Toward the Quantum Internet

The next milestone is the establishment of a global quantum internet, where quantum and classical nodes co-exist. Researchers are developing quantum repeaters—devices capable of extending entanglement over long distances without measurement—to overcome current range limitations [15].

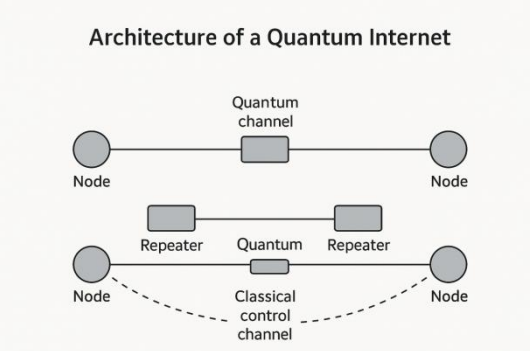

Diagram 4:

Title: "Architecture of a Quantum Internet"

Description: Nodes connected through quantum channels using repeaters for entanglement swapping, with classical control channels for data synchronization.

5.2 Integration with Artificial Intelligence and Cloud Security

Quantum cryptography can be integrated with AI-driven security systems for adaptive threat detection. Quantum-secure cloud storage using distributed QKD ensures end-to-end confidentiality for data hosted in multi-cloud environments [16].

5.3 Miniaturization and Chip-Scale Quantum Devices

Advancements in photonic integration are leading to chip-based QKD modules that could be embedded in everyday devices like smartphones and IoT sensors. This development could democratize quantum security for mass markets [17].

5.4 Policy and Global Cooperation

Quantum cryptography's success requires coordinated international standards and collaborations. Governments and organizations, including the Quantum Flagship Program (EU) and Quantum Information Science Initiative (U.S.), are investing heavily in secure quantum communication research [18].

6. Conclusion

Quantum cryptography represents a paradigm shift from mathematically based to physically guaranteed security. Its reliance on the laws of quantum mechanics provides unmatched resilience against both classical and quantum computational threats. While technical and economic challenges remain, rapid advancements in QKD systems, satellite networks, and post-quantum algorithms signal an imminent transition toward a quantum-secure digital world.

As the boundaries between classical and quantum technologies blur, quantum cryptography will form the cornerstone of global cybersecurity infrastructure—ensuring that the future of digital communication remains private, reliable, and fundamentally secure.

References:

1. Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, *68*(21), 3121–3124. https://doi.org/10.1103/PhysRevLett.68.3121
2. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*.
3. Boaron, A. et al. (2021). Chip-integrated quantum key distribution. *Optica*, *8*.
4. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, *67*(6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661
5. ETSI. GS QKD 011, *Quantum key distribution: Security framework*. (2023).
6. European Commission. (2024). *Quantum flagship programme*.
7. Herrero-Collantes, M., & Garcia-Escartin, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics*, *89*(1), Article 015004. https://doi.org/10.1103/RevModPhys.89.015004
8. IBM. (2024). Quantum. *Quantum-safe cloud security* [IBM Research white paper].
9. Kimble, H. J. (2008). The quantum Internet. *Nature*, *453*(7198), 1023–1030. https://doi.org/10.1038/nature07127
10. Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., & Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, *4*(10), 686–689. https://doi.org/10.1038/nphoton.2010.214
11. National Institute of Standards and Technology. (2023). *Post-quantum cryptography standardization process*.
12. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, *12*(4), 1012–1236. https://doi.org/10.1364/AOP.361502
13. Quantique, I. D. (2010). *Swiss quantum network demonstration*.
14. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer*

Science, IEEE (pp. 124–134). IEEE Comput. Soc. Press. https://doi.org/10.1109/SFCS.1994.365700

15. Toshiba research Europe, *High-speed QKD demonstration*. (2022).
16. United States Department of Energy. (2020). *Quantum Internet blueprint*.
17. Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, *299*(5886), 802–803. https://doi.org/10.1038/299802a0
18. Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., Li, G.-B., Lu, Q.-M., Gong, Y.-H., Xu, Y., Li, S.-L., Li, F.-Z., Yin, Y.-Y., Jiang, Z.-Q., Li, M., . . . Pan, J.-W. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*, *356*(6343), 1140–1144. https://doi.org/10.1126/science.aan3211
19. Rani, P., & Bhardwaj, R. (2025). The Future of Innovation: How emerging technologies are shaping tomorrow. *International Journal of Applied and Behavioral Sciences*, *2*(1), 181–186. https://doi.org/10.70388/ijabs250117
20. Swarna, T. (2024). A study on the dominance of digital transaction over M3 money supply transactions. *Edumania-An International Multidisciplinary Journal*, *02*(04), 194–220. https://doi.org/10.59231/edumania/9083