EDITORIAL

Inaugural Editorial of the *Journal of Quantum Cryptography*

Syed Sajid Ullah[1,2,*]

[1] Department of Information and Communications Technology, University of Agder, 4898 Grimstad, Norway
[2] Center for Cybersecurity Cluster, School of Computer Science, The University of Sydney, Sydney, Australia

Dear Readers,

It is both my privilege and honor to introduce our new journal, the *Journal of Quantum Cryptography*, a peer-reviewed publication dedicated to advancing secure communication in the quantum age. This journal serves as a vital platform for researchers, practitioners, and policymakers working at the intersection of quantum mechanics and cryptographic science. Our mission is to foster innovation, promote interdisciplinary collaboration, and accelerate the development of quantum-secure cryptographic solutions that are resilient against future threats posed by quantum computing.

Over the past few decades, cryptography has evolved significantly from classical symmetric and asymmetric algorithms rooted in number-theoretic hardness assumptions to advanced frameworks designed to withstand quantum attacks. Traditional encryption schemes such as RSA, ECC, and Diffie-Hellman, which underpin much of today's digital security infrastructure, are now increasingly vulnerable due to the emergence of quantum algorithms like Shor's, which can efficiently solve the integer factorization and discrete logarithm problems [1].

This paradigm shift has triggered a global race to develop and deploy cryptographic mechanisms that remain secure even in the presence of quantum adversaries. Two primary approaches have emerged: post-quantum cryptography (PQC), which relies on classical but quantum-resistant mathematical problems, and quantum cryptography, particularly quantum key distribution (QKD), which leverages the principles of quantum mechanics to achieve information-theoretic security [2].

While standardization efforts led by organizations such as NIST and ETSI are accelerating the adoption of PQC, the transition presents significant technical, operational, and strategic challenges for governments and enterprises alike [1]. At the same time, QKD and other quantum-based protocols continue to be explored for their unique ability to offer unconditional security grounded in physical laws rather than computational complexity [3].

Journal of Quantum Cryptography is committed to publishing high-quality research that addresses both theoretical and practical aspects of this evolving landscape. We welcome contributions that explore novel cryptographic primitives, composable security models, hybrid cryptographic systems, implementation challenges, and policy implications,

Submitted: 21 June 2025
Accepted: 23 June 2025
Published: 29 June 2025

Vol. 1, **No.** 1, 2025.
10.62762/JQC.2025.237610

***Corresponding author:**
Syed Sajid Ullah
sajidullah718@gmail.com

Citation
Ullah, S. S. (2025). Inaugural Editorial of the Journal of Quantum Cryptography. *Journal of Quantum Cryptography*, 1(1), 1–4.

ensuring that the journal remains at the forefront of the transition toward a secure quantum future.

The Evolution of Quantum Cryptography and Integration with Emerging Technologies

Quantum cryptography has evolved significantly from its theoretical inception to practical implementation over the past few decades. Its foundation was laid in the early 1970s by Stephen Wiesner, who introduced the concept of quantum money—a precursor to modern quantum cryptographic techniques [4].

This vision was later expanded upon by Bennett and Brassard in 1984 with the proposal of the BB84 protocol, the first practical Quantum Key Distribution (QKD) scheme [5]. This groundbreaking work established the basis for secure communication using the principles of quantum mechanics, particularly leveraging the Heisenberg uncertainty principle and the no-cloning theorem to ensure information-theoretic security [6].

Since then, QKD has moved beyond theory into real-world deployments. Experimental QKD networks have been successfully implemented across metropolitan areas, and satellite-based systems—most notably China's Micius mission—have demonstrated long-distance quantum communication on a global scale [7]. These developments highlight the feasibility of integrating quantum cryptographic protocols into existing infrastructure, while also identifying key technical and operational challenges that must be addressed for widespread adoption.

Post-Quantum Cryptography

While quantum cryptography relies on the physical properties of quantum states to achieve security, post-quantum cryptography (PQC) focuses on developing classical algorithms that remain secure against attacks by both classical and quantum computers [8]. Recognizing the imminent threat posed by quantum computing to traditional public-key cryptosystems (e.g., RSA and ECC), the National Institute of Standards and Technology (NIST) initiated the Post-Quantum Cryptography Standardization Project. Promising candidates include lattice-based, hash-based, code-based, and multivariate polynomial schemes. These approaches are being standardized to ensure long-term data protection in a post-quantum world.

It is crucial to distinguish between quantum cryptography and PQC: the former leverages quantum mechanics to provide unconditional security, while the latter adapts classical cryptographic principles to resist quantum attacks. Both fields play complementary roles in securing future digital infrastructures.

Integration with Emerging Technologies

As quantum cryptography matures, its integration with cutting-edge technologies presents both transformative opportunities and significant challenges:

Artificial Intelligence (AI)

AI plays a critical role in optimizing quantum cryptographic protocols, detecting anomalies in quantum channels, and advancing cryptanalysis. Machine learning models can enhance error correction, improve key generation rates, and identify potential eavesdropping attempts by analyzing quantum channel behavior in real time [9]. Furthermore, AI-driven simulations aid in designing robust QKD protocols resilient to various attack vectors.

Blockchain and Distributed Ledger Technologies (DLTs)

Blockchain systems, which rely heavily on digital signatures and hashing, face existential threats from quantum attacks. Integrating quantum-resistant signature schemes or QKD-based authentication into DLTs ensures transaction integrity and long-term trust in decentralized environments [10]. Quantum-enhanced blockchains may offer superior resistance to tampering and unauthorized access, especially in high-security applications such as financial transactions and supply chain management.

6G Networks

The next generation of mobile communications, 6G, will demand ultra-secure, low-latency communication layers capable of supporting massive device connectivity [11]. Quantum-secure encryption and QKD can serve as foundational components for securing these networks, particularly in scenarios involving critical infrastructure, IoT ecosystems, and autonomous systems. Ensuring compatibility between quantum cryptographic solutions and 6G network architectures remains an active area of research.

Digital Twin and Metaverse Applications

In immersive environments such as digital twins and the metaverse, securing virtual identities, interactions, and sensitive data becomes increasingly important [12]. Quantum-resistant encryption and secure key exchange mechanisms can protect user

privacy and prevent identity spoofing. Additionally, quantum-based authentication methods can ensure the integrity of digital assets and interactions within these complex, dynamic systems.

Edge and Fog Computing Architectures

Edge and fog computing require lightweight cryptographic primitives to secure data processing at the network periphery without compromising performance [14]. Quantum-secure algorithms tailored for constrained devices, along with compact QKD implementations, offer promising solutions [13]. However, challenges related to resource limitations, latency, and interoperability must be carefully addressed to enable scalable deployment.

The *Journal of Quantum Cryptography* invites original research articles, comprehensive reviews, technical notes, and insightful commentaries that contribute to the advancement of this transformative field. We welcome interdisciplinary studies that bridge theory and practice, as well as applied research in domains such as finance, healthcare, defense, and smart cities.

We look forward to receiving your valuable contributions and embarking on this exciting journey together. Let us shape the future of secure communication in the quantum age.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

The author declares no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] 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. [CrossRef]

[2] Subramani, S., & SVN, S. K. (2025). Review of security methods based on classical cryptography and quantum cryptography. *Cybernetics and Systems, 56*(3), 302-320. [CrossRef]

[3] Portmann, C., & Renner, R. (2022). Security in quantum cryptography. *Reviews of Modern Physics, 94*(2), 025008. [CrossRef]

[4] Wiesner, S. (1983). Conjugate coding. *ACM Sigact News, 15*(1), 78-88. [CrossRef]

[5] Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography, 78*, 351-382. [CrossRef]

[6] Singh, H. (2025). 9 Future Directions and Challenges, Quantum Supremacy, and Beyond. In *Quantum Technology Applications, Impact, and Future Challenges* (pp. 141). CRC Press.

[7] Imran, M., Altamimi, A. B., Khan, W., Hussain, S., & Alsaffar, M. (2024). Quantum Cryptography for Future Networks Security: A Systematic Review. *IEEE Access*. [CrossRef]

[8] Fathalla, E., & Azab, M. (2024). Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations. *IEEE Access*. [CrossRef]

[9] Radanliev, P. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology, 15*(1), 4. [CrossRef]

[10] Khodaiemehr, H., Bagheri, K., & Feng, C. (2023). Navigating the quantum computing threat landscape for blockchains: A comprehensive survey. *Authorea Preprints*. [CrossRef]

[11] Saeed, M. M., Saeed, R. A., Hasan, M. K., Ali, E. S., Mazha, T., ... & Hamam, H. (2025). A comprehensive survey on 6G-security: physical connection and service layers. *Discover Internet of Things, 5*(1), 28. [CrossRef]

[12] Tang, A. (2025). *Safeguarding the Future: Security and Privacy by Design for AI, Metaverse, Blockchain, and Beyond*. CRC Press.

[13] Lohachab, A., Lohachab, A., & Jangra, A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. *Internet of Things, 9*, 100174. [CrossRef]

[14] Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. *IEEE Internet of Things Journal, 8*(6), 4132-4156. [CrossRef]

Syed Sajid Ullah received his Master's degree in computer science from Hazara University, Pakistan, and earned his Ph.D. through a joint program between Villanova University, USA, and the University of Agder, Norway. He is currently a researcher at the Department of Information and Communication Technology at the University of Agder (UiA), Grimstad, Norway. Soon, he will be joining the University of Sydney as an Assistant Professor.
Dr. Sajid is an active member of the academic community, having

authored over 100 publications in high-impact journals. He serves as an editor for IEEE Access, PeerJ Computer Science, Sensors, and Scientific Reports and is on the editorial boards of several reputable journals. He also contributes regularly as a reviewer for more than 30 esteemed publications.

His research focuses on cryptography, blockchain, access control, post-quantum cryptography, network security, information-centric networking, named data networking, and the Internet of Things (IoT). Additionally, he plays a key role in the NIST-funded project on quantum cryptography and named data networking. (Email: sajidullah718@gmail.com)