Challenges and Advancements in Quantum Cryptography: Standardization, Security Risks, and Practical Implementations

Yasmin Makki Mohialden[1], Muhanad Tahrir Younis[1], Saba Abdulbaqi Salman[2], Ethar Abdul Wahhab Hachim[1] and Muthana S. Mahdi[1]

[1]Department of Computer Science, College of Science, Mustansiriyah University, 10052 Baghdad, Iraq
[2]Department of Computer Science, College of Education, Al-Iraqia University, 10001 Baghdad, Iraq
ymmiraq2009@uomustansiriyah.edu.iq, mty@uomustansiriyah.edu.iq, sabasalman2019@gmail.com, ethar201124@uomustansiriyah.edu.iq, muthanasalih@uomustansiriyah.edu.iq

Keywords: Communication Security, Cryptographic Algorithms, Post-Quantum Cryptography (PQC), Quantum Computing Threats, Quantum Cryptography, Quantum Key Distribution (QKD), Quantum-Resistant Encryption.

Abstract: The advancement of quantum computing poses a direct threat to classical cryptographic systems, necessitating the adoption of quantum-resistant encryption techniques to maintain data integrity, confidentiality, and trust in digital communications. This study presents a comprehensive evaluation of Quantum Key Distribution (QKD) protocols - specifically BB84, E91, and B92 - alongside post-quantum cryptographic algorithms, including lattice-based, hash-based, and multivariate-quadratic systems. These techniques represent two complementary approaches: QKD leverages quantum mechanical principles for secure key exchange, while PQC reinforces classical cryptography against quantum threats using novel mathematical constructs. A comparative analysis is conducted focusing on security robustness, computational efficiency, and deployment scalability. Real-world constraints such as infrastructure limitations, key management complexity, and algorithmic overhead are also critically examined. The paper also investigates the standardization efforts led by NIST, ISO, and ETSI, highlighting current challenges to global adoption, including the lack of interoperability frameworks and varying readiness levels across industries. The findings underscore the need for hybrid cryptographic models that integrate classical and quantum-resistant mechanisms, offering a pragmatic path forward as quantum capabilities mature. Future directions include integrating quantum cryptography with cloud security, advancing homomorphic encryption, and developing quantum-safe blockchain technologies. These innovations are crucial for building resilient cybersecurity infrastructures capable of supporting next-generation applications such as secure edge computing, confidential AI model sharing, and tamper-proof digital ledgers. This research provides timely insights into the evolving cryptographic landscape and emphasizes the urgency of preparing for the quantum future through interdisciplinary collaboration and proactive technological adaptation.

1 INTRODUCTION

RSA and ECC utilize prime number decomposition and discrete logarithm resolution as key encryption elements due to their mathematical complexity [1]. Encryption techniques are crucial for digital data protection, as they require long periods to decipher traditional computers [2]. Quantum computing disrupts traditional encryption methods with Shor's algorithm, enabling efficient integer factorization and making RSA and ECC vulnerable to hacks [3]. Grover's algorithm reduces symmetric key cryptography's security levels by half, necessitating key length extension. Quantum developments necessitate the development of encryption methods that resist quantum security threats, utilizing quantum mechanics principles instead of computational hardness assumptions [4]. Quantum Key Distribution (QKD) is a key application that uses quantum physics concepts for proof-based protection, enabling users to establish secure shared keys and monitor security breaches through detectable disturbances [5]. QKD offers strong security but implementation is limited due to hardware, high costs, and scalability issues. PQC develops classical encryption algorithms for QKD systems, and NIST standardizes lattice-based, hash-based, multivariate-quadratic schemes, and code-based cryptographic systems [6]. The global business sector is pushing for the establishment of quantum encryption standards, which are currently being evaluated by NIST ISO and ETSI entities, to ensure security, scalability, and interoperability of these new encryption mechanisms [6]. Quantum computing significantly alters traditional cryptographic systems, such as RSA and ECC, by enabling faster problem-solving on powerful quantum computers. This breaks the security guarantees of these methods, making them vulnerable to decryption. As a result, transitioning to quantum-resistant cryptographic algorithms is crucial to maintain data confidentiality and integrity in the post-quantum era [7]. The research will review quantum cryptography work through three significant areas including Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) and quantum attack methods in Section 2. The core principles of quantum cryptographic protocols receive detailed examination in Section 3 together with their implementation obstacles and performance limitations and compatibility with modern cryptographic systems. The study concludes through Section 4 by presenting a summary of essential findings together with potential research paths to achieve quantum-resistant security implementation in practical applications.

2 RELATED WORKS

This review reviews research on Quantum Key Distribution, Post-Quantum Cryptography, and Quantum Attacks, focusing on recent breakthroughs and analyzing existing knowledge gaps.

Theoretical investigations of Quantum Key Distribution (QKD) security introduced the trade-off between protection strength and security expenses while also identifying weaknesses regarding anonymity and accuracy during 2019. Post-Quantum Cryptography (PQC) became the research focus after 2021 when NIST reviewed their standards about encryption resistance transition difficulties and practical implementation limitations. Quantum Public-Key Encryption (QPKE) was introduced in 2023, presenting new security requirements. The Variation Quantum Attacker (VQAA) demonstrated its superiority in 2022, targeting AES encryption even though implementation challenges exist. In 2024, international standards were set for quantum cryptography, despite technical barriers to scalability. The evolution of quantum cryptography from 2019 to 2024 is illustrated in Figure 1 and Table 1.

Table 1: Comparison of previous researches in quantum cryptography.

Ref.	Main Focus	Key Contributions	Advantages	Limitations
[8]	Information-Theoretic Secure Quantum Cryptography	Defined and analyzed concealment in quantum cryptography	Provided insights into security trade-offs	Issues with anonymity and accuracy
[9]	Quantum Circuit Optimization for AES	Reduced Toffoli circuits by 88% for AES encryption	Improved efficiency of quantum circuits	High complexity in large-scale systems
[10]	NIST PQC Standards	Reviewed post-quantum cryptography challenges	Supported the transition to PQC	Lacked practical implementation details
[11]	Quantum Cryptography Network Optimization for AES	Reduced qubit usage and T-depth for AES	Improved quantum encryption performance	Complex circuit design challenges
[12]	Variational Quantum Attacker (VQAA) on AES	Proposed a quantum attack technique for AES	Demonstrated potential to outperform Grover's algorithm	Difficult to apply in real-world settings
[13]	Quantum Public-Key Encryption (QPKE)	Developed new QPKE encryption models	Expanded theoretical foundations of QPKE	Lacks information-theoretic security guarantees
[14]	Quantum Cryptography and National Security	Analyzed challenges and global standardization	Promoted quantum encryption standardization efforts	Significant obstacles in achieving global adoption

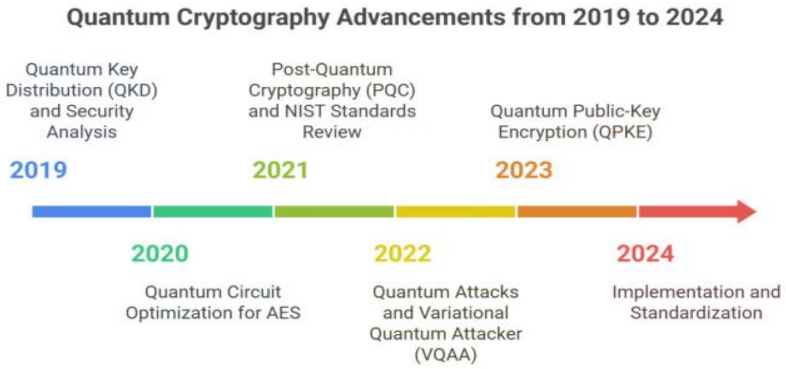
Quantum Cryptography Advancements from 2019 to 2024
Quantum Key Distribution (QKD) and Security Analysis
2019
Post-Quantum Cryptography (PQC) and NIST Standards Review
2021
Quantum Public-Key Encryption (QPKE)
2023
2020
Quantum Circuit Optimization for AES
2022
Quantum Attacks and Variational Quantum Attacker (VQAA)
2024
Implementation and Standardization

Figure 1: The evolution of quantum cryptography from 2019 to 2024.

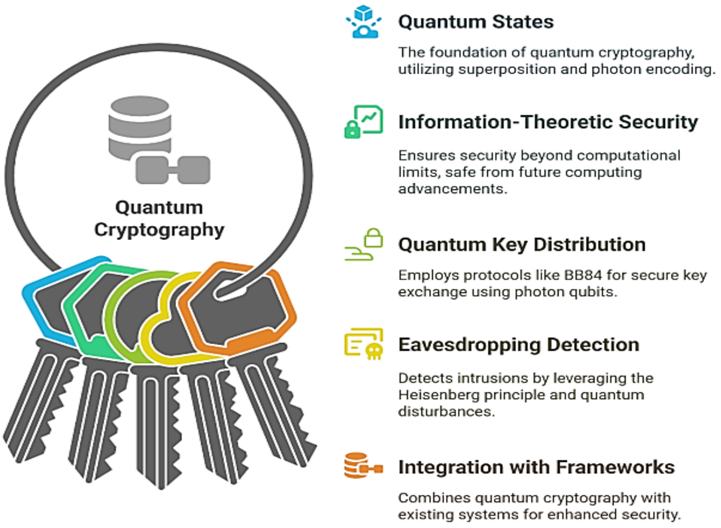
Quantum Cryptography
Quantum States
The foundation of quantum cryptography, utilizing superposition and photon encoding.
Information-Theoretic Security
Ensures security beyond computational limits, safe from future computing advancements.
Quantum Key Distribution
Employs protocols like BB84 for secure key exchange using photon qubits.
Eavesdropping Detection
Detects intrusions by leveraging the Heisenberg principle and quantum disturbances.
Integration with Frameworks
Combines quantum cryptography with existing systems for enhanced security.

Figure 2: The basic principles of quantum cryptography 2024.

Despite advancements in quantum cryptography, several research gaps persist, notably the need for practical implementation of Post-Quantum Cryptography (PQC) algorithms beyond theoretical frameworks and addressing the scalability and high infrastructure costs hindering large-scale Quantum Key Distribution (QKD) deployment. Further research is needed to explore hybrid cryptographic models that integrate QKD and PQC for enhanced cybersecurity, alongside optimizing quantum attack techniques like VQAA to improve their real-world applicability. Future research should therefore prioritize the practical integration of quantum cryptography, focusing on enhancing PQC implementation, developing hybrid security solutions that bridge quantum and classical cryptography, and overcoming the deployment challenges currently facing QKD technologies.

3 FUNDAMENTALS OF QUANTUM CRYPTOGRAPHY

Quantum cryptography is a groundbreaking field that leverages quantum mechanics to secure communication. Unlike traditional cryptographic methods, which rely on mathematical complexity, quantum cryptography provides information-theoretic security based on fundamental quantum principle. The most widely studied application of quantum cryptography is Quantum Key Distribution (QKD), which enables two parties to exchange cryptographic keys securely over an insecure channel [15], [16].

3.1 Key Principles of Quantum Cryptography

This section explains the basic principles and concepts of quantum cryptography. Figure 2 summarizes these principles [17], [18].

3.1.1 Quantum States

Quantum cryptography encodes information using quantum states of photons, leveraging principles such as superposition and the no-cloning theorem. In superposition, a quantum bit (qubit) exists in multiple states simultaneously until measured. The o-cloning theorem ensures that an unknown quantum state cannot be copied without disturbing it, which forms the basis of quantum cryptographic security [19].

3.1.2 Information-Theoretic Security

Unlike classical cryptographic systems, which rely on computational hardness assumptions (e.g., factorization in RSA), quantum cryptography provides security guarantees that do not depend on computational power. Even an adversary with infinite computing capacity cannot extract useful information from intercepted quantum states without detection [17].

3.1.3 Quantum Key Distribution (QKD)

QKD is one of the most well-known applications of quantum cryptography. The BB84 protocol, developed by Bennett and Brassard in 1984, is the first and most widely studied QKD scheme. It allows two parties (Alice and Bob) to exchange photon-polarized qubits over an insecure quantum channel. By comparing measurement results over a classical channel, they can establish a shared secret key, while any eavesdropping attempts by Eve introduce detectable anomalies. The following steps represent the procedure of the algorithm working:

1) Preparation. Alice randomly selects a sequence of bits and a sequence of polarization bases (rectilinear or diagonal), and encodes each bit onto a photon.
2) Transmission. Alice transmits polarized photons to Bob through a quantum channel.
3) Measurement. Bob randomly selects a basis (rectilinear or diagonal) to measure each photon.
4) Public Discussion. Alice and Bob use a public classical channel to share their chosen bases.
5) Key Sifting. They discard bits with different bases, leaving the remaining bits as the sifted key.
6) Error Checking and Privacy Amplification. The team uses error correction and privacy amplification to create a secure final key, detecting and eliminating potential Eve interference.

QKD's built-in eavesdropping detection mechanism, using quantum properties like the no-cloning theorem and Heisenberg's uncertainty principle, prevents attacker Eve from intercepting or measuring quantum states during transmission, causing detectable disturbances in the key reconciliation process [19], [20].

3.1.4 Eavesdropping Detection

A significant advantage of QKD is its built-in mechanism for detecting eavesdropping. When an attacker (Eve) attempts to measure quantum states in transit, the quantum system is disturbed due to Heisenberg’s uncertainty principle.

This disruption manifests as errors in key reconciliation, alerting Alice and Bob to the presence of an intruder [19].

3.1.5 Integration with Classical Cryptographic Frameworks

Integrating Quantum Key Distribution (QKD) into classical cryptographic frameworks presents challenges due to architectural incompatibilities, as classical systems rely on computational hardness assumptions [21]. Hybrid models propose using QKD for secure key generation while maintaining classical encryption for data transmission, addressing key management concerns in traditional protocols. Interoperability issues arise from timing, error handling, and authentication differences in quantum-compliant systems, necessitating hash-based or one-time pad schemes to prevent man-in-the-middle attacks. Infrastructure upgrades are also necessary, including quantum channels (fiber-optics or satellites), quantum repeaters, and integration modules with classical networks.

Current efforts focus on developing middleware that can bridge classical internet protocols with quantum communication layers. These challenges highlight the need for standardized APIs, quantum-aware protocols, and dedicated hardware, all of which are subjects of ongoing research and standardization led by NIST, ETSI, and ITU-T [22].

3.2 Quantum Key Distribution (QKD) Protocols

QKD protocols differ in their implementation approaches, ranging from polarization-based schemes (BB84, B92) to entanglement-based systems (E91, BBM92). Table 2 summarizes the key QKD protocols, mechanisms, and security features [23], [24].

3.2.1 Quantum Cryptographic Algorithms

Post-Quantum Cryptography (PQC) is a field that uses lightweight algorithms to secure resource-constrained devices like IoT nodes and embedded systems. These algorithms are designed to resist quantum attacks while maintaining computational and energy efficiency.

Notable examples include NTRU, a lattice-based encryption algorithm, and SPHINCS+, a stateless hash-based signature scheme. Ascon, selected by NIST for lightweight cryptography, provides an efficient and secure encryption framework for small devices. These schemes are crucial in extending quantum-safe protections to real-world systems operating under strict performance constraints. Incorporating these algorithms in future security standards will improve the viability of quantum-resilient infrastructure in enterprise and edge-computing environments [25].

3.3 Challenges in QKD Deployment

Despite its theoretical advantages, the real-world deployment of QKD faces several obstacles. Table 3 briefly illustrates these obstacles [26].

3.3.1 Technological Limitations

QKD requires specialized quantum hardware such as single-photon sources and highly sensitive detectors. Current fiber-based QKD systems are limited in range (~100 - 200 km) without quantum repeaters [26].

3.3.2 Scalability and Cost Issues

Large-scale deployment of QKD networks is expensive and requires dedicated optical infrastructure. Satellite-based QKD systems (e.g., China’s Micius satellite) offer potential solutions but remain costly [26].

3.3.3 Key Management and Integration Challenges

Hybrid cryptographic models (QKD + PQC) are required to facilitate the transition without overhauling existing security infrastructure. Secure authentication mechanisms are necessary to prevent man-in-the-middle attacks [27].

3.4 Future Directions in Quantum Cryptography

To overcome these challenges, future research should focus on the following key areas [27]:

- Developing high-efficiency and cost-effective quantum hardware to support longer-distance and more accessible QKD systems.
- Advancing quantum repeaters and satellite-based QKD to extend the range of secure communication.
- Exploring and integrating hybrid cryptographic models that combine Quantum Key Distribution (QKD) with Post-Quantum Cryptography (PQC).
- Enhanced compatibility with existing security network.
- Enhancing network-layer and quantum network security to support real-world and large-scale adoption of QKD technologies.

The continued evolution of quantum-safe encryption technologies will play a crucial role in securing communication systems against emerging quantum threats.

3.5 Applications and Limitations of Quantum Cryptography

Although secure key exchange is the primary use of quantum cryptography, it also has potential applications in secure communication systems and authentication processes. Table 3 shows these applications, while Table 4 illustrates the limitations of quantum cryptography [28].

3.6 Measurement Techniques for Testing Quantum Cryptography

Evaluating the performance and security of quantum cryptographic systems requires precise measurement techniques to ensure reliability, efficiency, and robustness against attacks.

This section discusses key metrics used to assess the effectiveness of quantum cryptographic protocols and their practical deployment.

3.7 Challenges in Quantum Cryptographic Performance Evaluation

While QKD and PQC offer strong security, their performance evaluation presents specific challenges. Table 4 briefly summarizes these challenges [29].

- QKD highly depends on physical conditions, such as optical fiber quality and atmospheric interference.
- PQC requires extensive computational resources and rigorous security proofs to ensure resistance to quantum attacks.
- Hybrid cryptographic systems must balance performance trade-offs between quantum and classical encryption models [30].

3.8 Future Research Directions

To enhance quantum cryptographic performance testing, future research should focus on:

- Developing advanced security proofs to validate the resilience of new quantum cryptographic protocols.
- Improving QKD key generation rates for real-world deployment.
- Optimizing hybrid cryptographic approaches to balance security and efficiency.

Table 2: Notable quantum key.

Protocol	Introduced	Mechanism	Security Features
BB84 Protocol	1984 (Bennett and Brassard)	Uses photon polarization (horizontal, vertical, and diagonal states) for key encoding	Detects eavesdropping through quantum disturbance
E91 Protocol	(1991) (Ekert)	Based on quantum entanglement Two parties share entangled photon pairs.	Uses Bell's inequalities to detect eavesdropping
BBM92 Protocol	1992	Hybrid of BB84 and E91; uses entangled photon pairs.	Inherits security features of BB84 and E91
B92 Protocol	1992	Simplified version of BB84; uses non-orthogonal quantum states.	More straightforward implementation, but more vulnerable to attacks
Decoy State Protocol	2003	Introduces multiple intensity levels to detect photon-number splitting attacks	Prevents attackers from exploiting weak pulses

Table 3: Applications of quantum cryptography.

Aspect	Applications	Details
Secure Communication	Provides theoretically unbreakable encryption for confidential communication	Prevents eavesdropping in diplomatic, corporate, and defense communications
Key Distribution (QKD)	Enables secure exchange of cryptographic keys over insecure channels.	Resistant to interception due to the no-cloning theorem
Financial Transactions	Enhances security in online banking, credit card transactions, and digital payments	Protects against man-in-the-middle attacks and quantum-enabled cyber threats
Military and Government	Secures classified communication for intelligence agencies, military operations, and diplomatic exchanges	Ensures tamper-proof data transmission in national security networks
Healthcare Data Security	Safeguards electronic medical records (EMRs) and patient data from breaches	Ensures compliance with HIPAA, GDPR, and other data protection regulations
Critical Infrastructure	Protects smart grids, transportation systems, and IoT networks from cyber threats	Ensures resilient security in power grids, autonomous vehicles, and industrial automation
Scientific Research	Facilitates secure data exchange in quantum networks and high-performance computing research.	Used in secure cloud computing, AI model protection, and collaborative projects.

Table 4: Limitations of quantum cryptography.

Aspect	Challenges	Details
High Cost	Expensive implementation due to the need for specialized quantum hardware	Requires quantum key distribution (QKD) devices, quantum repeaters, and dedicated fiber-optic infrastructure.
Distance Limitations	Limited to short distances without quantum repeaters or satellite-based QKD	Current fiber-based QKD systems work within ~100–200 km range without signal degradation.
Complexity	Requires advanced technical expertise for deployment and maintenance.	Needs integration with existing cryptographic protocols and secure key management systems
Technological Maturity	Still an emerging technology, with ongoing research required to improve efficiency.	Adoption is hindered by limited commercial availability and ongoing experimental developments.
Environmental Sensitivity	Quantum signals are highly vulnerable to noise, signal loss, and atmospheric conditions.	Requires ultra-low temperature environments and stable transmission media
Integration Challenges	Difficult to incorporate into traditional cryptographic frameworks	Requires hybrid cryptographic approaches combining QKD with post-quantum cryptography (PQC)
Limited Adoption	Deployment is slow due to cost, infrastructure, and technical barriers.	Adoption in industries remains restricted to research, government, and military applications.

4 CONCLUSIONS

Traditional cryptographic methods are increasingly vulnerable to quantum computing threats, necessitating the adoption of quantum-resistant standards. Core approaches, such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC), offer vital protection. To ensure a secure transition, organizations must proactively develop quantum-resilient infrastructures, guided by evolving standards from bodies like NIST, ISO, and ETSI. The integration of classical and next-generation encryption frameworks will define the execution phase. Unified international policies and governmental support are essential in addressing quantum-enabled cyber threats. Furthermore, innovations in post-quantum techniques, including homomorphic encryption and secure blockchain integration, are pivotal for safeguarding sensitive data. While challenges remain, continued interdisciplinary research and global collaboration will fortify cryptographic systems in the quantum era. Global coordination is crucial, with unified international policies and robust governmental support necessary to effectively address quantum-enabled cyber risks. At the same time, advancements in post-quantum techniques such as fully homomorphic encryption, lattice-based cryptography, and secure blockchain integration will be key to protecting sensitive information in the long term. While challenges related to performance, interoperability, and deployment persist, sustained interdisciplinary research and international collaboration will be crucial for strengthening cryptographic ecosystems in the quantum era.

ACKNOWLEDGMENTS

The authors thank Mustansiriyah University (https://uomustansiriyah.edu.iq in Baghdad, Iraq) for its support in the present work.

REFERENCES

[1] S. Sharma, K. Ramkumar, A. Kaur, T. Hasija, S. Mittal, and B. Singh, “Post-quantum cryptography: A solution to the challenges of classical encryption algorithms,” in Modern Electronics Devices and Communication Systems. Singapore: Springer, 2023, pp. 23–38, doi: 10.1007/978-981-19-6383-4_3.

[2] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, “Elliptic curve cryptography: Applications, challenges, recent advances, and future trends: A comprehensive survey,” Computer Science Review, vol. 47, p. 100530, 2023, doi: 10.1016/j.cosrev.2022.100530.

[3] C. Easttom, “Quantum computing and cryptography,” in Modern Cryptography: Applied Mathematics for Encryption and Information Security. Cham, Switzerland: Springer, 2022, pp. 397–407.

[4] Y. Baseri, V. Chouhan, and A. Hafid, “Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols,” Computers & Security, vol. 142, p. 103883, 2024, doi: 10.1016/j.cose.2024.103883.

[5] F. Opiłka, M. Niemiec, M. Gagliardi, and M. A. Kourtis, “Performance analysis of post-quantum

cryptography algorithms for digital signature," Applied Sciences, vol. 14, no. 12, p. 4994, 2024, doi: 10.3390/app14124994.

[6] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure," arXiv, 2024, Art. no. 2404.10659, doi: 10.48550/arXiv.2404.10659.

[7] R. Cyriac, S. Eswaran, S. Selvarajan, and D. Yuvaraj, "Quantum computing in cryptographic systems," International Journal of Advanced IT Research and Development, vol. 1, no. 1, pp. 18–24, 2024.

[8] C.-Y. Lai and K.-M. Chung, "Quantum encryption and generalized Shannon impossibility," Designs, Codes and Cryptography, vol. 87, pp. 1961–1972, 2019, doi: 10.1007/s10623-018-00597-3.

[9] B. Langenberg, H. Pham, and R. Steinwandt, "Reducing the cost of implementing the advanced encryption standard as a quantum circuit," IEEE Transactions on Quantum Engineering, vol. 1, pp. 1–12, 2020, doi: 10.1109/TQE.2020.2965697.

[10] K. Kan and M. Une, "Recent trends on research and development of quantum computers and standardization of post-quantum cryptography," Monetary and Economic Studies, pp. 77–108, 2021.

[11] Z. Li et al., "Novel quantum circuit implementation of advanced encryption standard with low costs," Science China Physics, Mechanics & Astronomy, vol. 65, p. 290311, 2022, doi: 10.1007/s11433-022-1921-y.

[12] Z. Wang, S. Wei, G.-L. Long, and L. Hanzo, "Variational quantum attacks threaten advanced encryption standard based symmetric cryptography," Science China Information Sciences, vol. 65, p. 200503, 2022, doi: 10.1007/s11432-022-3511-5.

[13] K. Barooti et al., "Public-key encryption with quantum keys," in Theory of Cryptography Conference. Cham, Switzerland: Springer, 2023, pp. 198–227, doi: 10.1007/978-3-031-48624-1_8.

[14] S. Subramani and S. K. Svn, "Review of security methods based on classical cryptography and quantum cryptography," Cybernetics and Systems, vol. 56, no. 3, pp. 302–320, 2025, doi: 10.1080/01969722.2023.2166261.

[15] S. Pirandola et al., "Advances in quantum cryptography," Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012–1236, 2020, doi: 10.1364/AOP.361502.

[16] X. Tan, "Introduction to quantum cryptography," in Theory and Practice of Cryptography and Network Security Protocols and Technologies. Norderstedt, Germany: BoD – Books on Demand, 2013, pp. 111–145.

[17] F. Grasselli, Quantum Cryptography: From Key Distribution to Conference Key Agreement. Cham, Switzerland: Springer, 2021.

[18] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," in Proc. 4th Int. Conf. on Opto-Electronics and Applied Optics (OPTRONIX), Kolkata, India, 2017, pp. 1–7, doi: 10.1109/OPTRONIX.2017.8350006.

[19] M. S. Sharbaf, "Quantum cryptography: An emerging technology in network security," in Proc. IEEE Int. Conf. on Technologies for Homeland Security (HST), Waltham, MA, USA, 2011, pp. 13–19, doi: 10.1109/THS.2011.6107841.

[20] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Physical Review Letters, vol. 85, p. 441, 2000, doi: 10.1103/PhysRevLett.85.441.

[21] L.-J. Wang et al., "Experimental authentication of quantum key distribution with post-quantum cryptography," npj Quantum Information, vol. 7, p. 67, 2021, doi: 10.1038/s41534-021-00400-7.

[22] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions," Optics Express, vol. 26, no. 18, pp. 24260–24273, 2018, doi: 10.1364/OE.26.024260.

[23] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839–894, 2022, doi: 10.1109/COMST.2022.3144219.

[24] A. I. Nurhadi and N. R. Syambas, "Quantum key distribution protocols: A survey," in Proc. 4th Int. Conf. on Wireless and Telematics (ICWT), Nusa Dua, Bali, Indonesia, 2018, pp. 1–5, doi: 10.1109/ICWT.2018.8527822.

[25] N. Yang, Y. Tian, Z. Zhou, and Q. Zhang, "A provably secure collusion-resistant identity-based proxy re-encryption scheme based on NTRU," Journal of Information Security and Applications, vol. 78, p. 103604, 2023, doi: 10.1016/j.jisa.2023.103604.

[26] L. C. Alvarez and P. C. Caiconte, "Comparison and analysis of BB84 and E91 quantum cryptography protocols security strengths," International Journal of Modern Communication Technologies and Research, vol. 4, no. 9, pp. 12–21, 2016.

[27] S. Salman, Y. M. Mohialden, A. Abdulhameed, and N. M. Hussien, "A novel method for Hill cipher encryption and decryption using Gaussian integers implemented in banking systems," Iraqi Journal for Computer Science and Mathematics, vol. 5, no. 1, pp. 277–284, 2024, doi: 10.52866/ijcsm.2024.05.01.019.

[28] H. R. Shakir, "Secure selective image encryption based on wavelet domain, 3D-chaotic map, and discrete fractional random transform," International Journal of Intelligent Engineering & Systems, vol. 16, no. 6, pp. 965–980, 2023, doi: 10.22266/ijies2023.1231.80.

[29] S. A. Yassir and H. R. Shakir, "Hybrid image encryption technique for securing color images transmitted over cloud networks," International Journal of Intelligent Engineering & Systems, vol. 16, no. 6, pp. 850–862, 2023, doi: 10.22266/ijies2023.1231.70.

[30] C. Portmann and R. Renner, "Security in quantum cryptography," Reviews of Modern Physics, vol. 94, p. 025008, 2022, doi: 10.1103/RevModPhys.94.025008.