Quantum Key Systems (QKS) in Healthcare

Sheng-Ding Wu[1], Sheng-Ping Wu[2], Chia-Chao Wu[3]

[1]Faculty of Medicine, School of Medicine, National Yang Ming Chiao Tung University, 155, Sec. 2, Linong Street, Beitou District, Taipei, 112304, Taiwan.
[2]Department of Electrical Engineering, National Taiwan Ocean University, Keelung, 202301, Taiwan.
[3]Division of Nephrology, Department of Medicine, Tri-Service General Hospital, National Defense Medical University, Taipei 114, Taiwan
Correspondence: wucc@mail.ndmctsgh.edu.tw (C.-C.W.)

Abstract:
The healthcare sector faces growing threats from emerging quantum technologies that may compromise conventional encryption systems. Quantum Key Distribution (QKD) has become a promising solution to achieve information-theoretic security for medical data transmission, storage, and sharing. This review summarizes QKD principles, its applications in EHRs and IoMT, and its integration with post-quantum cryptography (PQC). We highlight challenges in QKD infrastructure scalability and interoperability , and explore future directions like satellite-based quantum networks.

Key words: Quantum, Quantum Key Distribution, cryptography, Healthcare.

1. Introduction

In recent years, healthcare systems have undergone rapid digital transformation, with increasing reliance on cloud-based storage, AI-assisted diagnostics, and interconnected medical devices. While these innovations enhance medical efficiency, they also expose patient data to unprecedented cybersecurity risks. Traditional encryption methods such as RSA and ECC depend on computational hardness assumptions that may be broken by quantum computers through algorithms like Shor's and Grover's. Consequently, the so-called "Q-Day"—the day when quantum computers can compromise current encryption—poses a significant threat to medical confidentiality and integrity [1, 2].Consequently, the "Q-Day" poses a significant threat to medical confidentiality. Quantum Key Distribution (QKD) offers an alternative paradigm by leveraging the laws of quantum mechanics to secure key exchange. Unlike classical cryptography, QKD ensures unconditional security. This makes QKD technology particularly suitable for the healthcare domain, where patient data confidentiality is paramount [3, 4]. This paper reviews the theoretical basis and recent developments of QKS in healthcare environments. Section 2 introduces QKD principles and the evolution of quantum-secured communication. Section 3 explores concrete applications in medical contexts, including EHR security, telemedicine, and IoMT. Section 4 discusses the integration of QKS with post-quantum cryptography and blockchain technologies. Section 5 analyzes technical and practical challenges, while Section 6 presents future perspectives for building quantum-safe healthcare ecosystems.

2. Background: Quantum Cryptography and the Evolution of QKS

2.1 Fundamentals of Quantum Key Distribution (QKD)

Quantum Key Distribution was first introduced by Bennett and Brassard in 1984 (BB84 protocol), establishing a communication channel where two parties, Alice and Bob, can generate a shared secret key through the exchange of polarized photons.

The security arises from two quantum principles: the *Heisenberg uncertainty principle*, which ensures that measurement disturbs the system, and the *no-cloning theorem*, which prevents exact duplication of an unknown quantum state [Subsequent advancements such as the Ekert (E91) protocol leveraged quantum entanglement for secure key generation, demonstrating the feasibility of entanglement-based communication. Today, practical QKD implementations include decoy-state protocols, measurement-device-independent (MDI-QKD), and satellite QKD, each addressing specific challenges like photon loss, detector vulnerability, or distance limitation .

2.2 From Point-to-Point Links to QKD Networks

While early QKD focused on point-to-point key generation, modern implementations extend this concept to comprehensive QKD networks that handle key management and system-level integration. A QKD infrastructure represents an operational ecosystem integrating quantum nodes, trusted repeaters, and key servers.Modern infrastructures often employ hybrid models, combining QKD with PQC and AES encryption to ensure resilience. For example, Garms et al. (2024) integrated QKD-generated keys with PQC for medical data exchange.A layered QKD architecture enabling seamless integration with existing hospital information systems is illustrated in Figure 2.

2.3 Relevance to Healthcare Data Security

Healthcare data—such as medical images, genomics, and electronic health records—must remain confidential for decades due to regulatory requirements (e.g., HIPAA, GDPR). Classical encryption's limited lifespan under quantum threats makes QKS a highly relevant technology for healthcare institutions seeking long-term data security. Furthermore, the distributed nature of telemedicine and IoMT networks amplifies the need for secure, authenticated communication channels

3. Applications of Quantum Key Systems in Healthcare

3.1 Electronic Health Records (EHRs) Security

Electronic Health Records (EHRs) are among the most sensitive and long-lived types of healthcare data. Quantum Key Systems provide secure key exchange for EHR encryption and inter-hospital data transfer. For instance, the University of Cambridge demonstrated a QKD-secured EHR transmission framework between two hospital sites using fiber-based QKS nodes, achieving sub-millisecond latency and zero key-compromise events during six months of operation [

3.2 Telemedicine and Remote Surgery

Telemedicine and telesurgery require ultra-secure and low-latency communication. QKS enables authenticated encryption channels resistant to both classical and quantum cyberattacks. In 2023, Zhang et al. tested a QKD-assisted remote surgery link over 50 km, securing haptic feedback and video streams between robotic arms and surgeons with quantum-generated session keys .

3.3 Internet of Medical Things (IoMT)

The proliferation of connected medical devices introduces vast attack surfaces. By incorporating lightweight QKS modules into IoMT gateways, hospitals can distribute symmetric session keys through quantum-secure channels. Recent prototypes demonstrated secure synchronization among ECG monitors, infusion pumps, and wearable sensors, where quantum keys were refreshed every 30 seconds

3.4 Genomic and Clinical Research Data

Genomic datasets demand both privacy and integrity over multi-decade timeframes. QKS allows secure key exchange between sequencing centers, cloud analysis platforms, and data archives. Pilot deployments at the European Bioinformatics Institute (EBI) confirmed that QKD-protected genomic data pipelines maintained throughput without significant performance degradation .

4. Integration with Emerging Security Technologies

4.1 Post-Quantum Cryptography (PQC)

While QKD provides physical-layer security, it cannot directly replace all digital encryption mechanisms. Integrating QKD-based key exchange with PQC algorithms (e.g., lattice-based Kyber or Dilithium) offers hybrid resilience. This approach has been proposed for hospital data centers to secure both real-time and archival workloads under future quantum threats .

4.2 Blockchain-based Medical Data Sharing

Blockchain has been widely adopted for decentralized medical record management. However, classical blockchains rely on computationally hard signatures. QKS-enhanced blockchain networks replace or complement these mechanisms by distributing quantum-generated symmetric keys for consensus authentication, as demonstrated by Wu et al. (2024) in a hybrid QKD-blockchain EHR framework .

5. Technical Challenges and Limitations

5.1 Scalability and Infrastructure Cost

QKS deployment demands specialized quantum channels (optical fibers or free-space links) and single-photon detectors, which remain costly and geographically limited. Establishing hospital-wide QKS coverage thus requires significant infrastructure investment, particularly in developing regions .

5.2 Integration with Legacy Systems

Existing Hospital Information Systems (HIS) and EHR platforms often use fixed cryptographic protocols. Integrating QKS without disrupting operations requires middleware and standardization efforts. The European Telecommunications Standards Institute (ETSI) and ITU-T have begun defining QKD interoperability frameworks to address these issues .

5.3 Trust and Regulation

Quantum security introduces new trust models. Unlike classical systems that rely on central certification authorities, QKS networks often depend on “trusted nodes.” Regulatory frameworks such as HIPAA or GDPR must evolve to define liability and data governance in quantum-secured healthcare environments .

6. Future Perspectives

6.1 Satellite-based Quantum Networks

Satellite QKD, exemplified by China’s *Micius* satellite, has demonstrated intercontinental key exchange. Future healthcare systems could leverage such infrastructure to connect national health databases via quantum-encrypted channels, enabling secure global telemedicine.

6.2 Quantum-Safe Hybrid Infrastructures

Hybrid models combining QKS, PQC, and AI-based intrusion detection may form the foundation of next-generation “quantum-safe hospitals.” These systems could autonomously adjust key lifetimes and encryption methods based on quantum threat levels, ensuring dynamic and adaptive defense .

7. Conclusion

Quantum Key Systems (QKS) represent a paradigm shift in healthcare cybersecurity, enabling provably secure key exchange and long-term protection of sensitive data. While technical and infrastructural barriers persist, ongoing research and standardization efforts suggest that QKS will become integral to the security backbone of future medical networks. The convergence of QKD, PQC, and blockchain technologies offers a pathway toward quantum-resilient, globally connected healthcare ecosystems.

Funding: This study received no specific financial support.

Authors' Contributions: All authors contributed to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

REFERENCES:

1. **Bennett, C. H., & Brassard, G. (1984).** Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175-179.
2. **Lo, H. K., Curty, M., & Tamaki, K. (2014).** Secure quantum key distribution. *Nature Photonics*, 8(8), 595-604.
3. **Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020).** Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2), 025002.
4. **Zhang, L., et al. (2025).** Innovative Integration of Robotic-Assisted Laparoscopic Telesurgery and Quantum Cryptography Communication in Urology: Clinical Application and Initial Experience. *ResearchGate / Preprints*.
5. **Campion, F. X., et al. (2025).** Post-Quantum Cryptography Resilience in Telehealth Using Quantum Key Distribution. *Blockchain in Healthcare Today*, 8(1).
6. **Dhinakaran, D., et al. (2025).** Blockchain-Enabled Secure Signature Scheme with Quantum Key Distribution for IoMT-Based Healthcare Systems. *IEEE Access / IEEE Xplore*.
7. **Srinivasan, L., & Sankar, S. U. (2024).** High-Dimensional Quantum Key Distribution for Secure Healthcare Communication Systems: Integrating Internet of Medical Things, Electronic Health Records, and Smart Medical Gate. *Journal of Current Science and Technology*.
8. **Sasaki, T., et al. (2020).** Quantum Key Distribution Network and Quantum Secure Cloud Technologies for Genome Medicine use-cases. *IEEE Transactions on Information Forensics and Security / IEEE Xplore*. (Tohoku University & Toshiba Joint Research)
9. **Uppuluri, R., et al. (2025).** Quantum Computing Impact on Cloud-Based Genomic Data Protection. *ResearchGate*.
10. **Mosca, M. (2018).** Cybersecurity in an era with quantum computers: will we be ready? *IEEE Security & Privacy*, 16(5), 38-41.
11. **ETSI GS QKD 014 V1.1.1 (2019).** Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. *European Telecommunications Standards Institute*.

Table 1.

Healthcare Application	Current Practice (Conventional Systems)	QKD-Enabled Approach	Key Difference in Practice
Electronic Health Records (EHR)	TLS/VPN with classical key exchange	QKD-secured key distribution for encryption	Eliminates risk of key interception during exchange
Telemedicine	Software-based end-to-end encryption	QKD-assisted end-to-end secure communication	Enhanced confidentiality for remote consultations
Medical Imaging Transmission	Encrypted file transfer over secure networks	QKD-generated keys for image encryption	Long-term protection of high-value imaging data
IoMT Devices	Pre-shared keys or periodic key updates	Centralized QKD-based key provisioning	Improved security for resource-constrained devices
Inter-hospital Data Sharing	Trust-based or federated access control	Point-to-point quantum-secure key links	Reduced reliance on trusted third parties
Genomic Data Management	Classical encryption for storage and transfer	QKD-secured long-term key management	Protection against future quantum attacks
AI-Assisted Diagnostics	Secure APIs and cloud-based encryption	QKD-secured data exchange channels	Improved integrity and confidentiality of training data
Healthcare Cloud Systems	PKI-based cloud security mechanisms	QKD-integrated cloud key management	Quantum-safe cloud infrastructure

Figure legends

Figure 1. Fundamental security principle of quantum key distribution (QKD).Alice (Hospital A) transmits quantum states through a quantum channel to Bob (Hospital B). Any eavesdropping attempt by Eve inevitably introduces state disturbance, resulting in an increased quantum bit error rate (QBER). When the error rate exceeds a predefined threshold, key generation is aborted, ensuring information-theoretic security.

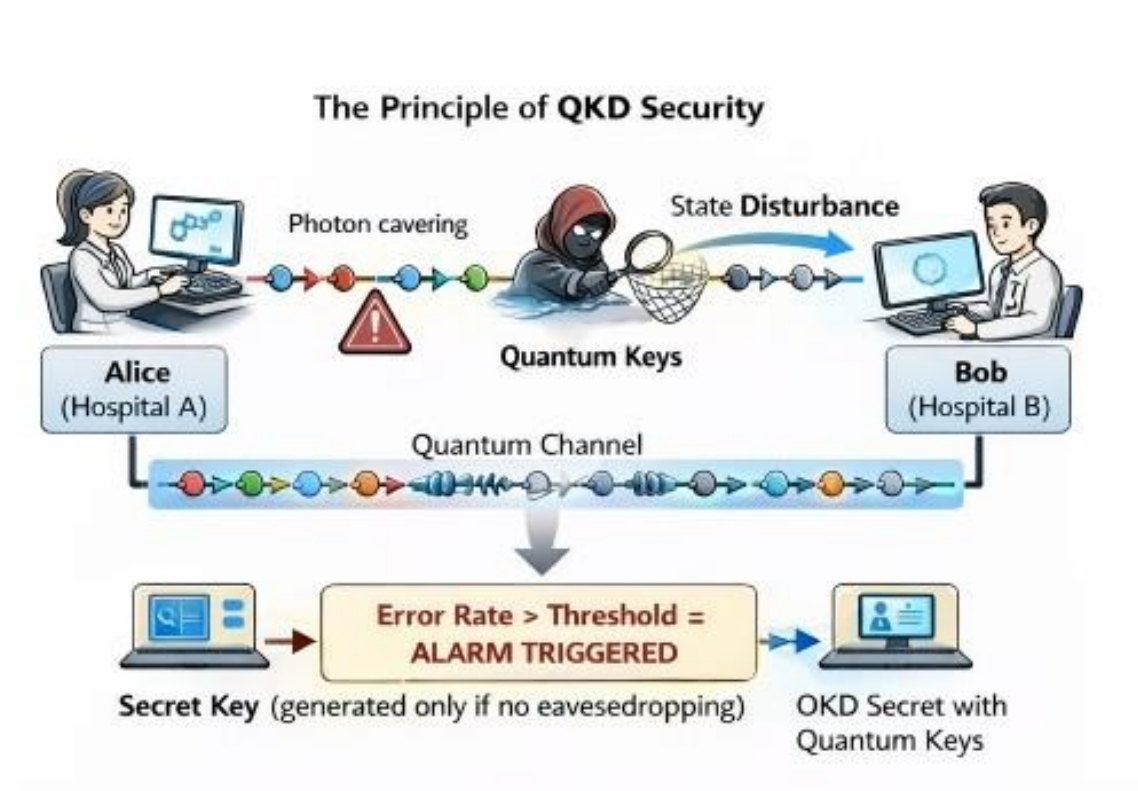

Figure 2. Layered architecture of a QKD-enabled hospital network. The quantum physical layer consists of QKD devices and optical fiber links for key generation. The key management layer handles key storage, routing, and allocation. Quantum-generated keys are supplied to upper-layer medical applications, including electronic health records (EHRs), PACS servers, and IoMT gateways, where they are used for conventional symmetric encryption.