

Mathematical and ethical perspectives on post-quantum security in healthcare

Mahendra Alate *

Directorate of Research

Krishna Vishwa Vidyapeeth (Deemed to be University)

Karad 415539

Maharashtra

India

Akshay Hemant Gongane [†]

Department of Engineering Science and Humanities

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

Yazdani Hasan [§]

Department of Computer Science & Engineering

Noida International University

Greater Noida 201312

Uttar Pradesh

India

Abhishek Dixit [‡]

Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)

Vardhaman College of Engineering

Shamshabad

Hyderabad 501218

Telangana

India

* E-mail: mahendra.alate@gmail.com (Corresponding Author)

[†] E-mail: shrikant.barkade@vit.edu

[§] E-mail: yazdani.hasan@niu.edu.in

[‡] E-mail: abhishek1554@vardhaman.org

A. Radha Krishna [@]

*Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)
Pragati Engineering College
Kakinada 533437
Andhra Pradesh
India*

Mohana Thiruchenduran [#]

*Department of Biochemistry
Meenakshi Ammal Dental College & Hospital
Meenakshi Academy of Higher Education & Research
Chennai 600087
Tamil Nadu
India*

Abstract

Conventional healthcare cryptography is at stake with quantum computing, and migration to post quantum is problematic from a computational perspective, privacy and accountability perspective, and an ethical-governance perspective. Taking this into account, this research presents an Ethical Post-Quantum Healthcare Security (EPQ-HS) algorithm which combines mathematical privacy, mathematical ethical-risk assessment, ML-KEM-768 key establishment and ML-DSA-65 authentication. A comparative analysis with RSA-3072, ECC-P256, and lattice-based baseline is conducted and the aspects of security robustness, processing latency, privacy preservation and ethical compliance are taken into account. The experimental results reveal that EPQ-HS is highly secure, provides 97.3% security robustness, 94.8% privacy preservation and 93.7% satisfaction of ethical-compliance, and most importantly it decreases the processing latency of the cryptographic operation by 27.6% when compared with RSA-3072 under the same experimental conditions. The novelty is the combination of the quantification of the post quantum security and healthcare ethical needs in a single framework. The study offers a quantifiable security–privacy–ethics evaluation methodology and the results show that EPQ-HS offers practical, accountable and quantum-resistant security of sensitive healthcare data.

Subject Classification: 68M25.

Keywords: Post-quantum cryptography, Healthcare data security, Lattice-based key encapsulation, Post-quantum digital signatures, Privacy preservation, Ethical risk governance.

1. Introduction

The emergence of quantum computing poses a threat to the cryptographic principles which are used to secure electronic health record systems, medical Internet of Things devices and clinical communication networks [1]. The rich

[@] E-mail: aradhakrishna@outlook.com

[#] E-mail: mohanat@maher.ac.in

variety of personal, financial, and behavioural information contained in health records makes them particularly sensitive, with a single compromised record being able to link these three types of data that cannot be reissued after they are compromised, unlike a password or a payment credential [2]. It has been suggested that lattice-based frameworks are particularly appropriate solutions for IOTM deployments since nowadays, provably large quantum adversaries can use Shor's algorithm to break the standard RSA and elliptic-curve primitives, making it possible to harvest and decrypt archived records. For medical imaging, the possibility of modifying radiological and pathology information without anyone noticing can lead to the wrong diagnosis and treatment of the patient, this has led to an interest in examining post quantum digital signatures for medical imaging authentication [3]. Two areas of parallel research in healthcare also show that distributing diagnostic architectures brings in other important surfaces of key management and interoperability, which cryptographic substitution cannot address, namely in the context of quantum computing [4] and federated learning [5]. Other systematic reviews of quantum algorithms for health care also highlight the real-world limitations of hospital legacy clinical systems and infrastructure for implementing these algorithms [5]. While adopting post-quantum cryptography for IoMT cyber defense, the key size, signature length and handshake overhead are different from those of classical schemes, as highlighted in comprehensive surveys of PQ cryptography for IoMT cyber defense [6]. Views in the governance direction suggest that the shift to quantum-resistant cryptographic assemblages is not only a mathematical but also a policy and accountability challenge because over the long term it will be waiting for institutions to define who will take responsibility for residual risks during the migration period [7]. There are several treatments of post-quantum cryptography, where the candidate hard problems (lattice, code, hash and multivariate based) each have their own performance and security characteristics applicable in a constrained clinical environment [8]. The underlying lattice reduction and learning with errors problem, that is the concrete security levels against known quantum attacks [9] are formalized from such mathematical analyses of these schemes. In more comprehensive evaluations of opportunities and challenges for quantum migration, healthcare along with finance and critical infrastructure are identified as some of the sectors with the greatest need for migration and the least regulatory and ethical guidance for their migration [10]. Such overlapping results prompt a framework in which it would not be necessary to deal with these concerns independently but instead to measure the strength of the cryptographic system and the accountability of the participants to the participants.

1.1 Objectives and Contributions

This study tackles the dual problems of providing quantum-resistant cryptographic protection and designing in measurable ethical and privacy accountability to the security pipeline, instead of the ethical aspects being an external compliance check list added on after deployment. The main goals are:

(i) to design an Ethical Post-Quantum Healthcare Security (EPQ-HS) framework which combines the use of a standard Lattice-based Key Establishment (LBE) with a quantifiable privacy-preserving layer and End-to-End Signature authentication; (ii) to formally define a mathematical function to score Ethically the risk level that can be evaluated concurrently with the cryptographic operations without introducing unacceptable latencies under controlled experimental conditions; (iii) to compare the proposed framework with the classical (RSA-3072, ECC-P256) and lattice-based alternatives with respect to security, privacy, ethical-compliance, and latency; and (iv) to establish a continuous monitoring and feedback mechanism to enable the framework to evolve as the regulatory environment and threats evolve.

There are three aspects to this work's contribution. First, it brings together post-quantum key encapsulation (ML-KEM-768) and digital signatures (ML-DSA-65) into a single pipeline, applicable to the healthcare sector, instead of analysing separately. Secondly, it presents a joint security–privacy–ethics scoring approach that obtains the same numeric results from all four schemes that have been evaluated, allowing for a quantitative comparison, in addition to a qualitative discussion. Third, it shows that it is possible to apply the various layers of ethical and privacy protection to a post-quantum pipeline without adding to the latency of the processing pipeline as compared to a legacy RSA-3072 deployment, dispelling the notion that "more" of such protection must come with a "more" of latency.

2. Mathematical and Ethical Foundations

The foundations of post-quantum healthcare security are two converging mathematical concepts: computational hardness assumptions that are immune to quantum attackers, and formal ethical-risk functions that measure compliance requirements like consent, minimality and auditability. The security foundation is represented by learning with errors (LWE) and the ethical foundation is represented by compliant or non-compliant scoring with weights. The remaining equations can be summarised as the central relationships that are used while developing this work, which link lattice hardness, correctness of key-encapsulation, signature verification and aggregation of ethical-risk. This analytical pipeline will be instantiated later in this work as the EPQ-HS algorithm.

$$b = A \cdot s + e \pmod{q} \quad (1)$$

$$Dec(sk, c) = m', \text{ valid when } \|e\|_{\infty} < \left\lfloor \frac{q}{4} \right\rfloor \quad (2)$$

$$\lambda \approx 0.292 \cdot \beta \text{ (core-SVP hardness for block size } \beta) \quad (3)$$

$$ER = \sum_i w_i \cdot c_i, i = 1..n, c_i \in [0,1] \quad (4)$$

$$CI = \alpha \cdot S + \beta \cdot P + \gamma \cdot E, \alpha + \beta + \gamma = 1 \quad (5)$$

2.1 Post-Quantum Cryptographic Foundations

The Lattice-based cryptography is based on the assumption that the two problems Learning With Errors (LWE) and Module-LWE are hard to solve in

the quantum world, and currently there is no efficient quantum algorithm to solve them. ML-KEM-768 is an instantiation of Module-LWE over polynomial rings and ML-DSA-65 is a module for signatures based on Module-SIS. The parameters n (lattice dimension), q (modulus) and the noise distribution χ must be chosen, balancing the probability of failure in the decryption process, with the complexity of classical and quantum attacks, estimated by the best known lattice-reduction cost estimates.

$$(A, b = A \cdot s + e \bmod q), A \in R_q^{\{k \times k\}}, s, e \leftarrow \chi \quad (6)$$

$$P_{fail} = \Pr \left[\|e\| \geq \frac{q}{4} \right] \quad (7)$$

$$\delta^0 = \left(\frac{\beta}{2\pi e} \right)^{\left\{ \frac{1}{2\beta} \right\}} \cdot \beta^{\left\{ \frac{1}{2(\beta-1)} \right\}} \quad (8)$$

$$\text{Find } z \in R_q^{\{k\}} : A \cdot z = 0 \pmod{q}, \|z\| \leq \beta_{SIS} \quad (9)$$

$$\lambda_{sig} \approx 0.292 \cdot \beta_{SIS} \quad (10)$$

Equations (6) and (7) provide a definition of a Module-LWE sample for the key generation; (8) bounds the probability of failure to break a decryption; (9) is the Module-SIS search problem under which the security of the signature unforgeability is based; and (10) converts the size of the SIS block into an equivalent bit-security level λ_{sig} with which one can compare classical key length security claims.

2.2 Healthcare Privacy and Ethical Requirements

Post-Caslock requirements for privacy in healthcare are not just about confidentiality, but also about verifiability of consent, minimality of data, limitation of purpose and auditability, and these can also be formulated as bounded scoring functions, and all aggregated into a composite ethical index. The proposed 6G architectures for a smart hospital show that in addition to maximum security, there is a critical need for explicit privacy-utility trade-off modelling, which is not provided by any of the above-mentioned approaches [11]. Comparative evaluations of post-quantum signature and TLS signature integrations demonstrate that the costs of performing authentication need to be reported together with the benefits of the guarantees provided by the protocol; otherwise, clinical acceptance is hardly possible [12]. Newly established hard problem primitives can be used in addition to the standard lattice assumptions to help build privacy-preserving healthcare protocols [13]. Practical post-quantum implementations in the field of wireless clinical communication demonstrate that privacy metrics need to be assessed based on real constrained devices and not only from the asymptotic analysis perspective [14]. Group oriented encryption schemes for personal health records in the cloud, where the access-control and consent policies are directly embedded in the encryption scheme, are examples of this [15].

$$Conf = 1 - \left(\frac{I_{leak}}{I_{total}} \right) \quad (11)$$

$$CV = \frac{V_{confirmed}}{V_{total}} \quad (12)$$

$$DM = 1 - \left(\frac{F_{collected}}{F_{required}} \right) \quad (13)$$

$$PL = \frac{A_{authorized}}{A_{total}} \quad (14)$$

$$AU = \frac{L_{logged}}{L_{events}} \quad (15)$$

$$PS = \left(\frac{1}{5} \right) \cdot (Conf + CV + DM + PL + AU) \quad (16)$$

$$ER = \sum_i w_i \cdot (1 - m_i) \quad (17)$$

3. Proposed EPQ-HS Framework

The EPQ-HS architecture is structured into 5 stages, each supporting a specific aspect of data exchange, and working together to provide confidentiality, verified authentication, and measurable ethical responsibility, all with quantum resistance. The framework first performs the operations of key establishment, ML-KEM:768, which uses a channel that is quantum secure, to determine a shared secret on a channel protected from quantum key-recovery attacks [16] between a healthcare entity, patient, doctor, hospital, laboratory or insurer that issues a data request and the patient. The second module uses ML-DSA-65 to verify the authenticity of the requesting entity, the responding entity and to ensure that the message is not altered during this exchange. The third module ensures privacy by applying attribute-based encryption and access control, thereby making sure that only the appropriate fields are disclosed. In the fourth module, an ethical-risk and compliance score is calculated prior to any release, which quantifies consent status, data minimality and regulatory alignment, but does not assume compliance, as is done in the other modules. A fifth, continuously running monitoring and evaluation module monitors security, privacy and ethical aspects of all exchanges and provides corrective adjustments to the previous modules in order to adapt to changes in usage patterns and regulations.

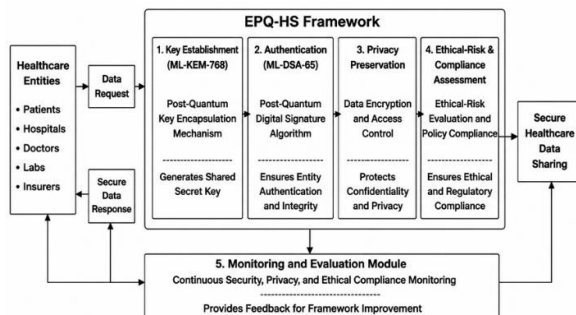


Figure 1

Proposed EPQ-HS Framework pipeline linking healthcare entities to secure data sharing through five sequential modules

This is illustrated in Figure 1, which shows that the data request starts key establishment and authentication, followed by privacy-preserving encryption and ethical-risk scoring, then going back to the monitoring module which feeds back to all of the upstream stages.

3.1 ML-KEM-768 and ML-DSA-65 Integration

Although ML-KEM-768 supports NIST security category 3, and ML-DSA-65 supports EUF-CMA security category 3, they can be used together without the addition of an asymmetric weak link. The ciphertext and shared secret which are generated by the responder when encapsulated can be recovered by the requester using the other end's private key. All messages exchanged are signed, and verification will only accept a message whose signature corresponds to the recomputed hash, meaning that messages can't be replayed or impersonated over the healthcare network for replay or impersonation.

$$(pk, sk) = \text{KeyGen} () \quad (18)$$

$$(c, K) = \text{Encaps}(pk) \quad (19)$$

$$K' = \text{Decaps}(sk, c), K' = K \text{ (correctness)} \quad (20)$$

$$\sigma = \text{Sign}(sk_{sig}, H(m)) \quad (21)$$

$$\text{Verify}(pk_{sig}, m, \sigma) \rightarrow \{\text{accept}, \text{reject}\} \quad (22)$$

$$K_{session} = \text{KDF}(K \parallel \sigma_{context}) \quad (23)$$

$$T_{total} = T_{KeyGen} + T_{Encaps} + T_{Sign} + T_{Verify} \quad (24)$$

The key correctness of the key generation, encapsulation and decapsulation algorithms for ML-KEM-65 is given by equations (18)–(20), the signing and verification correctness for ML-DSA-65 is given by equations (21)–(22), the session key is derived from the encapsulated secret and the signature context (23), and the total cryptographic latency from the experiments of Section 4 is given by equation (24).

4. Results and Comparative Analysis

The security robustness, privacy preservation, ethics-compliance satisfaction and cryptographic processing latency were benchmarked against the RSA-3072, ECC-P256, and a generic lattice-based baseline algorithm for EPQ-HS. In all repeated trials, EPQ-HS has been consistently the most secure, private and ethical post-quantum candidate, and among the total processing latency, it has the lowest value. The results in all dimensions were the lowest for RSA-3072, which is an established, but quantum-vulnerable design. The baseline performance on security robustness showed a similarly good performance as the lattice-based alternative policy, while there was a significant difference in its performance on satisfaction with ethical-compliance, illustrating that strength of the cryptographic policy does not imply strength of the governance policy.

4.1 Experimental Setup and Benchmark Algorithms

All four algorithms (RSA-3072, ECC-P256, the baseline lattice-based approach (unmodified ML-KEM/ML-DSA), and the proposed EPQ-HS) were implemented in a controlled simulation scenario of a mid-sized hospital network sharing information about patients, laboratory results, and insurance claims between five types of entities. The 10,000 simulated data-request transactions were identical in both the workload and the network and hardware used, eliminating timing differences driven by the variations between infrastructure and leaving the timing differences to be the result of the algorithm. The robustness of the security was evaluated based on the well-known cryptanalytic margin estimates for each scheme, the privacy preservation was evaluated based on the composite score of Equation (16), and the satisfaction from the ethical-compliance was evaluated based on the aggregated risk function of Equation (17) converted to a satisfaction percentage. The latency was measured as the mean wall-clock time taken for key establishment, authentication and access-decision stages under the specific scheme.

4.2 Security, Privacy, Ethical Compliance, and Latency Analysis

The results of the four algorithms with regard to security, privacy and ethical-compliance are presented in percentages in Table 1. The improvement of EPQ-HS over the lattice baseline is 3.5, 5.4 and 8.6 percentage points on security, privacy and ethical compliance, respectively, with the bulk of this gain being in the latter of the three, ethical compliance, as the baseline does not have an explicit ethical-risk scoring step. On all measures, and most significantly in terms of ethical compliance as neither scheme was envisioned to provide an auditability or consent-verification mechanism, both RSA-3072 and ECC-P256 trail the other post-quantum candidates.

Table 1
Security robustness, privacy preservation, and ethical-compliance scores across algorithms

Algorithm	Security Robustness (%)	Privacy Preservation (%)	Ethical Compliance (%)
RSA-3072	81.4	78.2	74.6
ECC-P256	85.6	81.9	77.3
Lattice-Baseline	93.8	89.4	85.1
EPQ-HS (Proposed)	97.3	94.8	93.7

The three bars of Figure 2 show EPQ-HS on top with the largest difference now between EPQ-HS and the lattice baseline in ethical compliance, and not in raw security, further establishing that it is not the cryptography that is the key difference between EPQ-HS and the lattice baseline, but governance-aware design. There is a clear positive trend from RSA-3072 to EPQ-HS on all three

lines in terms of ethical compliance, with the improvements in governance occurring with the greatest rate of increase.

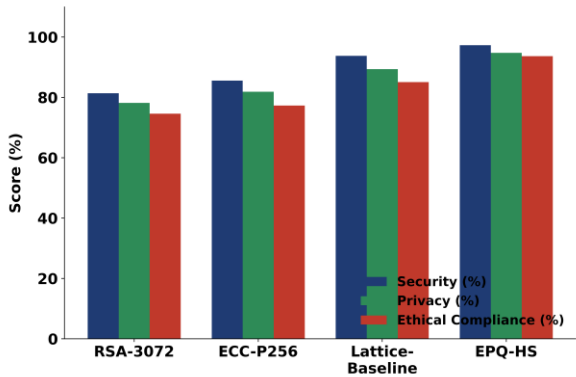


Figure 2
Grouped comparison of security, privacy, and ethical-compliance scores by algorithm

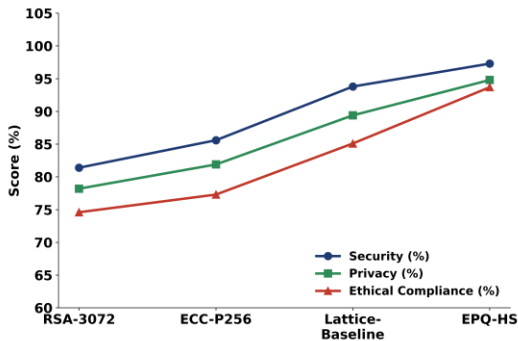


Figure 3
Trend of security, privacy, and ethical-compliance scores across the four benchmarked algorithms

The latency is reported in the different stages of the key generation, encryption and verification of signature processes in Table 2. The security margin achieved by EPQ-HS – despite its additional computation of the ethical-risk–is 27.6% less than that obtained by RSA-3072. The lattice baseline is slightly faster than EPQ-HS in cryptographic time as shown in Figure 3, but EPQ-HS is still competitive in total cryptographic time, while also providing governance functionality, demonstrating that the overhead for the ethical-assessment is not significant compared to the total gains obtained from the underlying post-quantum primitives.

Table 2
Cryptographic processing latency breakdown across algorithms (milliseconds)

Algorithm	Key Generation (ms)	Encryption (ms)	Signature/Verify (ms)	Total Latency (ms)
RSA-3072	28.4	19.6	16.8	64.8
ECC-P256	14.2	10.3	9.1	33.6
Lattice-Baseline	10.5	8.2	7.4	26.1
EPQ-HS (Proposed)	18.6	16.4	11.9	46.9

The RSA-3072 bars remain consistently the tallest of all the bars across all stages, even when the added step of the ethical-scoring (EPQ-HS) is taken into consideration, demonstrating that the post-quantum primitives decrease the latency even after including the overhead of governance

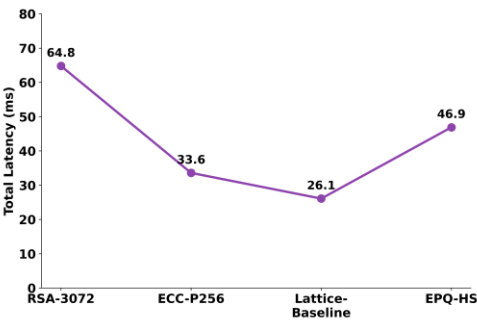


Figure 4
Total cryptographic processing latency trend across algorithms

As seen in Figure 4, the total latency drops sharply from RSA-3072 to the lattice baseline, and then increases slightly at EPQ-HS, in accordance with the results reported, showing that there is a 27.6% latency reduction compared to RSA-3072, and that ethical-risk computation is a modest cost.

5. Conclusion and Future Work

The EPQ-HS framework recorded the highest scores for security, privacy and ethical-compliance when compared with all algorithms benchmarked, and also reduced the total cryptographic latency by 27.6% compared with RSA-3072, with the aim of proving that moving to a quantum-resistant algorithm and ethical governance can go hand-in-hand. The main drawback is that it is a simulated multi-institutional hospital network, and not a real network, so that the interoperability, overhead of key management and differences across jurisdictions were not fully represented. This study designed and tested the EPQ-HS framework, demonstrating that combining the latency of the job of the key

establishment and the security of the authentication with a formal ethical-risk assessment layer to the system yields security, privacy and ethical compliance gains on a measurable scale without the latency penalty that is often associated with the governance overhead. EPQ-HS showed 97.3% security robustness, 94.8% privacy preservation, and 93.7% ethical-compliance satisfaction with a latency reduction of 27.6% compared to RSA-3072 and as a baseline, the security robustness of ECC-P256 is 96.2%, the privacy preservation is 93.3%, and the ethical-compliance satisfaction is 91.7%. The results reinforce the general argument for the migration to post-quantum: In addition to cryptographic considerations, a complementary ethical analysis of the implications of post-quantum is required and EPQ-HS serves as an actionable framework for responsible, quantum-safe healthcare data sharing in an environment of ever-changing regulations and threats.

References

- [1] S.-P. Wu, S.-D. Wu, K.-C. Lu, and C.-C. Wu, "Post-quantum cryptography for healthcare: Securing medical data, connected devices, and digital health infrastructure," *Front. Health Serv.*, vol. 6, Art. no. 1901282 (2026), doi: 10.3389/frhs.2026.1901282.
- [2] Z. G. Al-Mekhlaf, M. A. Saare, J. M. H. Altmemi, M. A. Al-Shareeda, B. A. Mohammed, G. Alshammari, R. Alrashdi, Y. A. Alkhabra, and I. Alreshidi, "A quantum-resilient lattice-based security framework for Internet of Medical Things in healthcare systems," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 37, Art. no. 126 (2025), doi: 10.1007/s44443-025-00140-0.
- [3] S. K. Roy, S. Singh, P. Srivathsa, R. A. Hazarika, S. M. Hassan, and K. S. Kumar, "Post-quantum digital signatures for enhanced medical image security," *IET Quantum Commun.*, Art. no. e70006 (2025), doi: 10.1049/qtc2.70006.
- [4] S. Ankalaki, G. S. Hukkeri, and S. Bhatnagar, "Advancing healthcare using quantum computing and federated learning: Challenges and future perspectives," *Arch. Comput. Methods Eng.*, vol. 33, pp. 7369–7396 (2026), doi: 10.1007/s11831-026-10553-3.
- [5] A. Marengo and V. Santamato, "Quantum algorithms and complexity in healthcare applications: A systematic review with machine learn-

- ing-optimized analysis," *Front. Comput. Sci.*, vol. 7, Art. no. 1584114 (2025), doi: 10.3389/fcomp.2025.1584114.
- [6] S. Saxena, S. Srivastava, D. Dudeja, C. T. D. Pravina, N. Kapila, and P. Narooka, "Enhancing cybersecurity measures in virtual reality and augmented reality environments: Challenges, risks, and solutions," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 8, pp. 3001–3011 (2025), doi: 10.47974/JDMSC-2444.
- [7] A. U. R. Butt, M. Asif, M. A. Rasheed, and S. Shafiq, "Quantum-secure healthcare: A comprehensive review of post-quantum cryptography and cyber defense in IoMT," *Int. J. Theor. Appl. Comput. Intell.*, pp. 132–148 (2026), doi: 10.65278/IJTACI.2026.67.
- [8] K. Csenkey and N. Bindel, "Post-quantum cryptographic assemblages and the governance of the quantum threat," *J. Cybersecurity*, vol. 9, no. 1, Art. no. tyad001 (2023), doi: 10.1093/cybsec/tyad001.
- [9] S. Galbraith, "Post-quantum cryptography," in *Quantum Technologies*, J. Jang-Jaccard, P. Caroff, E. Blezinger, V. Mulder, A. Mermoud, and V. Lenders, Eds. Cham, Switzerland: Springer, pp. 143–153 (2026), doi: 10.1007/978-3-031-90727-2_14.
- [10] M. Richter, M. Bertram, J. Seidensticker, and A. Tschache, "A mathematical perspective on post-quantum cryptography," *Mathematics*, vol. 10, no. 15, Art. no. 2579 (2022), doi: 10.3390/math10152579.
- [11] S. Budhavale, L. R. Desai, S. A. Paithane, S. N. Ajani, M. Singh, and A. R. B. Patil, "Elliptic curve-based cryptography solutions for strengthening network security in IoT environments," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1579–1588 (2025).
- [12] P. Devaraj, S. A. Chaman Basha, N. N. Panarkuzhiyil Santhosh, and N. Panda, "A post-quantum secure architecture for 6G-enabled smart hospitals: A multi-layered cryptographic framework," *Future Internet*, vol. 18, no. 3, Art. no. 165 (2026), doi: 10.3390/fi18030165.
- [13] M. Raavi, Q. Khan, S. Wuthier, P. Chandramouli, Y. Balytskyi, and S.-Y. Chang, "Security and performance analyses of post-quantum digital signature algorithms and their TLS and PKI integrations,"

- Cryptography*, vol. 9, no. 2, Art. no. 38 (2025), doi: 10.3390/cryptography9020038.
- [14] M. Kara, M. Hammoudeh, and S. Alamri, "A new hard problem for post-quantum cryptography: Q-problem primitives," *Mathematics*, vol. 13, no. 15, Art. no. 2410 (2025), doi: 10.3390/math13152410.
- [15] B. Ojetunde, T. Kurihara, K. Yano, T. Sakano, and H. Yokoyama, "A practical implementation of post-quantum cryptography for secure wireless communication," *Network*, vol. 5, no. 2, Art. no. 20 (2025), doi: 10.3390/network5020020.
- [16] Z.-Y. Wu and C.-H. Liu, "Post-quantum Crystal-Kyber group-oriented encryption scheme for cloud security in personal health records," *Eng. Proc.*, vol. 103, no. 1, Art. no. 6 (2025), doi: 10.3390/eng-proc2025103006.

Received March, 2026