*Journal of Information & Optimization Sciences*
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 10, pp. 3731–3740
DOI : 10.47974/JIOS-2498

# Quantum-resilient security for cross-border healthcare data exchange

Shilpa C. Patil [§]
*Department of Critical Care Medicine*
*Krishna Institute of Medical Sciences*
*Krishna Vishwa Vidyapeeth (Deemed to be University)*
*Karad 415539*
*Maharashtra*
*India*

Veerendra Yadav [†]
*Department of Computer Science & Engineering*
*Noida International University*
*Greater Noida 201312*
*Uttar Pradesh*
*India*

Swati Shivkumar Shriyal *
*Department of Artificial Intelligence*
*Vishwakarma University*
*Pune 411048*
*Maharashtra*
*India*

Chittireddy Amarendar Reddy [‡]
*Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)*
*Vardhaman College of Engineering*
*Shamshabad*
*Hyderabad 501218*
*Telangana*
*India*

[§] *E-mail:* drshilpapatil22@gmail.com
[†] *E-mail:* veerendra.yadav@niu.edu.in
* *E-mail:* swati.shriyal@vupune.ac.in (Corresponding Author)
[‡] *E-mail:* amarendar_vce1644@vardhaman.org

© Taru Publications

Prasanth Varasala [@]
*Department of Electronics & Communication Engineering*
*Pragati Engineering College*
*Kakinada 533437*
*Andhra Pradesh*
*India*

Vijay Suresh Karwande [#]
*Department of Computer Engineering*
*Sandip Institute of Technology and Research Centre*
*Nashik 422213*
*Maharashtra*
*India*

**Abstract**

As health information crosses from one healthcare domain or infrastructure to another, robust confidentiality, authentication, and integrity of the electronic medical records are crucial. This study aims to present a hybrid post-quantum encryption and authentication scheme for secure medical data exchange across the border using lattice-based encryption. The framework integrates a session-key establishment mechanism based on ML-KEM, AES-256-GCM for medical-data encryption, a digital signature scheme based on ML-DSA, integrity check based on hash function and identity-bound transaction metadata. It takes into account the mathematical security model involving key encapsulation, signature verification, adversarial advantage, communication overhead and processing cost. This shows that the proposed framework takes around 0.47ms for key encapsulation, 0.55ms for decapsulation and 0.94ms for digital signing, using simulation-based evaluation. The assumed end-to-end processing time is 83.91ms for a medical record of 50 MB, and the security related communication overhead falls off to about 0.011% when the size of the medical record increases. The results of the analysis show that quantum-resistant protection can be implemented with a moderate computational and communication overhead in cross-border healthcare settings.

***Subject Classification:*** *Primary 93A30, Secondary 49K15.*

***Keywords:*** *Post-quantum cryptography, Medical data exchange, Lattice cryptography, ML-KEM, Healthcare security.*

## 1. Introduction

The sharing of Electronic Health Records (EHRs), diagnostic reports, prescriptions, lab results, and medical images are all integral components of digital health care. With cross-border healthcare, this exchange becomes more complex as medical information can traverse various healthcare networks, cloud

[@] *E-mail:* **prasanthvarasala@outlook.com**
[#] *E-mail:* **vijayskarwande@gmail.com**

platforms, security domains, and national healthcare systems. Cryptographic security is essential for protecting information that is long-lived and sensitive to the present and future quantum-capable attacks.

### 1.1 *Digital and Cross-Border Healthcare Security Requirements*

Patient information is easier to store, retrieve, and share in cloud-based healthcare systems, while also posing problems with authentication, confidentiality, key management, and impersonation. The concerns have been mitigated with secure eHealth authentication mechanisms that use cryptographic key generation and minimize key exchange operations between healthcare participants [1]. This is further complicated by the proliferation of IoT devices, since medical sensors, wearables, gateways, hospital servers and monitoring platforms are constantly communicating with each other, passing sensitive information. Post-quantum authentication has thus been investigated for healthcare IoT application scenarios with limited resources, where traditional public-key schemes might be susceptible to quantum attacks [2].

Long term confidentiality of medical records is also needed. Data stolen today might be relevant for decades to come, thus presenting a “harvest-now, decrypt-later” risk. Therefore, migration to post-quantum healthcare should take into account cryptographic algorithms, interoperability, infrastructure modifications, key management, and preservation of data integrity and security in both storage and transmission [3]. Authentication also is critical, because the fact that data is encrypted doesn't mean that an entity is a legitimate physician, hospital, lab or medical service. Thus, quantum-resistant primitives have been used for authentication in e-health environment based on IoT [4]. The same problems can occur in cloud healthcare, where records can be processed outside the originating institution. A quantum resistant authentication and key-agreement protocols can help in establishing protected sessions before confidential records are released [5].

### 1.2 *Post-Quantum Lattice Protection of medical Data*

Lattice-based cryptography is a natural fit for healthcare communication as it can be designed to provide post-quantum key establishment and authentication that relies on computational problems that are believed to be safe from known quantum attacks. The lattice-based three-party authenticated key agreement has shown its applicability for interactions between multiple medical IoT-entities [6]. Permissioned blockchain architectures have also been used together with post-quantum crypto operations to allow distributed transactions on the blockchain, and secure health data sharing [7].

Records moving through multiple systems are a place where integrity is very important. Unapproved changes to prescriptions, diagnoses, lab values, or clinical reports can affect clinical decisions. Post-quantum authentication with the assistance of blockchain has been investigated to ensure verifiable data provenance and resistance against threats from quantum computers [8]. Hybrid cryptography is a pragmatic solution where symmetric cryptography is used to

secure medical data (assuming it is large), and post-quantum cryptography is used to secure session keys and authentication information. Hybrid encryption along with anti-quantum signatures has been studied for the security of EHRs confidentiality and source authenticity [9].

Groups of physicians, laboratories, devices and administrative entities may also be involved in healthcare communication. Lattice-based group authentication can be used to verify authorized members in such settings and to offer post-quantum security [10]. The recently introduced lattice-based IoMT security protocols incorporate several cryptographic tools into single schemes for the protection of interconnected healthcare entities including encryption, authentication, key establishment, and message verification [11].

### 1.3 *Research Gap and Proposed Cross-Border Framework*

The majority of the studies that have been conducted so far focus on particular applications, like IoMT, cloud healthcare, blockchain systems, or communication in local medical devices. Cross-border medical-data exchange presents a broader trust issue, as institutions involved can have varying infrastructures, administrative authorities and security policies. Protected communication is important for quantum-resistant protocols for distributed and digital-twin healthcare, and exchange of medical records across jurisdictions needs more attention. In view of these problems, this study proposes a lattice-based post-quantum hybrid encryption and authentication system for secure cross-border medical-data exchange. The shared secret for the session is established by ML-KEM, medical records are then encrypted using AES-256-GCM, and ML-DSA is used to provide post-quantum source authentication. Cryptographic hashing is used to associate the protected document with sender, receiver, time and access-policy information. The two main goals of the study are: (1) developing a mathematical post-quantum framework to integrate lattice-based key encapsulation, authenticated symmetric encryption, digital signatures, hashing, and identity-bound transaction information; (2) evaluating key generation, key encapsulation, key decapsulation, signing and verification, communication overhead, processing time, latency, and throughput.

The proposed work present a foundation for post-quantum healthcare security, and for cross-border medical sharing, the four aspects of confidentiality, authentication, integrity and long-term quantum security with a practical communication performance must be taken into account simultaneously.

## 2. Lattice-Based Post-Quantum Cryptographic Framework

The proposed architecture secures medical records that are sent across healthcare institutions from different countries and makes them quantum resistant. It is a hybrid of lattice-based ML-KEM to secure key establishment and AES-256-GCM for bulk-data encryption. This division prevents the use of quantum capable opponents in the encryption of the session key, while omitting the public key encryption of entire medical files, which is a complex operation.

2.1. System Model and Cross-Border Communication Architecture

Suppose it is a source healthcare institution $H_s$ in country $C_s$ and a receiving healthcare institution $H_{\mathrm{r}}$ in country $C_{\mathrm{r}}$. A medical transaction holds the medical record and context data to relate the record to a particular cross-border transaction. The transaction is formed as eq.1

$$D = M \parallel ID_{\mathrm{p}} \parallel ID_{\mathrm{s}} \parallel ID_{\mathrm{r}} \parallel T \parallel P \tag{1}$$

where, $D$ is the full transaction, $M$ is the medical record, $ID_{\mathrm{p}}$ is a pseudo-identifiable patient identity, $ID_{\mathrm{s}}\ and\ ID_{\mathrm{r}}$ are identities of the source and receiving institutions, T is the time of the transaction, $P$ is the appropriate access policy and $\parallel$ is the concatenation operation. A digest of the transaction is then created as in eq.2:

$$h^{\mathrm{D}} = H(D) \tag{2}$$

where, $h^{\mathrm{D}}$ is the fixed-length transaction digest and $H(\cdot)$ is a cryptographic hash function. The digest will tie the medical information to its respective identities, policy and timestamp.

2.2. *Lattice-Based Key Generation, B. ML-KEM Key Encapsulation*

The key-establishment stage is ML-KEM, which is a protocol whose security is related to the computational hardness of Module Learning With Errors. The simplified form of its underlying noisy lattice relation is shown in eq.3:

$$t = A \cdot s + e\ mod\ q \tag{3}$$

where A refers to a public matrix over a finite polynomial ring, s is a secret vector, e is a small error vector, t is part of a public-key information and q is a chosen modulus. Recovery of s from the publicly available information is difficult because of the error term. The receiving institution creates its ML-KEM key pair and the source encapsulates a shared secret as in eq.4:

$$(pk_{\mathrm{r}}, sk_{\mathrm{r}}) \leftarrow KeyGen(1^{\mathrm{l}}), \quad (c_{\mathrm{k}}, z) \leftarrow Encaps(pk_{\mathrm{r}}) \tag{4}$$

This is because the public key $\mathrm{pk_r}$ and the private key $sk_{\mathrm{r}}$ are those of the receiver, l refers to a security parameter, $c_k$ is the KEM ciphertext, and $z$ is the shared secret obtained as a result of encapsulation. Next, a transaction specific encryption key is obtained from the shared secret as shown in eq.5:

$$K_{\mathrm{m}} = KDF(z \parallel ID_{\mathrm{s}} \parallel ID_{\mathrm{r}} \parallel T \parallel h^{\mathrm{D}}) \tag{5}$$

Where, $K_m$ is a 256-bit session key and $KDF(\cdot)$ is the key-derivation function. The institution identities, timestamp and transaction digest tie $K_m$ to one medical-data exchange.

2.3. *Proposed Hybrid Medical-Data Encryption*

Because EHRs and medical images may be large, AES-256-GCM is used to encrypt the actual medical record, and ML-KEM is used to protect key established as eq.6:

$$(C_{\mathrm{m}}, \tau) = AES - GCM_{\mathrm{km}}(M, N, AD) \tag{6}$$

Where, $C_m$, the encrypted medical record, along with a tag $\tau$ and a unique nonce $N$, and $AD$, authenticated transaction metadata. The receiving institution first reconstructs the shared secret by applying ML-KEM decapsulation and then decrypts $C_m$. If the record is altered, a bad authentication tag is generated, and the record is rejected. Therefore, the scheme brings a mix of quantum resistant key establishment and workable authenticated encryption of large cross-border healthcare data.

## 3. Post-Quantum Authentication and Security Analysis

During the authentication step, the origin, integrity and freshness of each encrypted medical transaction is checked prior to releasing the record to the receiving institution. ML-DSA is used for post-quantum digital signatures, hash verification, ML-KEM decapsulation, AES-256-GCM authentication are successive verifications for record recovery.

### 3.1 *ML-DSA-Based Digital Signature and Identity Authentication*

The source institution first creates an ML-DSA signing key pair for authentication is shown in eq.7:

$$(pk_s{}^g, sk_s{}^g) \leftarrow SigKeyGen(1^l) \tag{7}$$

where, $pk_s{}^g$ is the public verification key, $sk_s{}^g$ is the private signing key and l is the chosen security parameter. The secret key is kept by the source healthcare institution while the verification key is given to the authorized receivers. Prior to signing, a digest is computed from the encrypted record and its transaction information shown in eq.8:

$$h_s = H(C_m \parallel c_k \parallel \tau \parallel ID_s \parallel ID_r \parallel T \parallel P) \tag{8}$$

where, $h_s$ is the signing digest, $C_m$ is the encrypted medical record, $c_k$ is the ML-KEM ciphertext, $\tau$ is the AES-GCM authentication tag and $ID_s, ID_r, T, and\ P$ are the identity of the sender, the identity of the receiver, the time stamp and the access policy, respectively. A source applies its signature $h_s$ and the receiver verifies the signature shown in eq.9:

$$\sigma = Sign(sk_s{}^g, h_s), \quad v = Verify(pk_s{}^g, h'_s, \sigma) \tag{9}$$

where, $\sigma$ is the ML-DSA signature, $h'_s$ is the digest that is computed independently by the receiver, and v is a verification result, in which $v = 0$ means that the digest is not verified and $v = 1$ means that the digest is verified. The transaction only occurs when $v = 1$.

### 3.2 *Integrity Verification & Secure medical-data Recovery*

Once successful it authenticates, the receiver decapsulates and reconstructs the transaction specific key as shown in eq.10:

$$z' = Decaps(sk_r, c_k), \quad K'_m = KDF(z' \parallel ID_s \parallel ID_r \parallel T \parallel h^D) \tag{10}$$

where, $z'$ is the recovered shared secret, $sk_r$ is the private key of the ML-KEM receiver, and $K'_m$ is the reconstructed AES-256 session key. By attaching the key to information for a transaction, the recovered secret cannot be used directly

for another transaction that is unrelated to the medical exchange. Medical-data recovery is done by authenticated individuals as

$$M' = AES - GCM - Dec_{\mathrm{k}}{}'_{\mathrm{m}}(C_{\mathrm{m}}, N, AD, \tau), \quad if\ \tau' = \tau \tag{11}$$

Here, $M'$ is the recovered medical record, $N$ the nonce, $AD$ authenticated metadata and $\tau'$ the locally verified authentication tag. Tag mismatch has been considered as modification, which is rejected immediately.

3.3 *Mathematical Security and Computational Analysis.*

The combined adversarial advantage can be used to represent the overall security:

$$Adv_{\mathrm{p}}(\mathcal{A}) \leq Adv^{\mathrm{KEM}}(\mathcal{A}) + Adv^{\mathrm{DsA}}(\mathcal{A}) + Adv^{\mathrm{GcM}}(\mathcal{A}) + Adv^{\mathrm{H}}(\mathcal{A}) \tag{12}$$

were, the $\mathcal{A}$ stands for an adversary, while the $Adv_{\mathrm{p}}$ is the adversary's success advantage overall. The rest of these terms refer to the benefits of ML-KEM, ML-DSA, AES-GCM and the hash function. If these individual probabilities are negligible, then successful key recovery, forgery of signatures or undetectable modification of ciphertexts is still not feasible. The concatenated verification sequence offers confidentiality, source authentication, integrity, replay resistance, and post-quantum security for cross-border medical-data transactions.

## 4. Results

The proposed PQ Hybrid Scheme lists the time to generate, encapsulate and decapsulate as 0.64ms, 0.47ms and 0.55ms respectively. The signing and verification time are 0.94 ms and 0.31 ms, respectively, which is only slightly higher than ML-KEM-768 + ML-DSA-65. This extra processing relates to the inclusion of cross-border transaction and authentication data in the proposed security procedure as shown in Table 1.

**Table 1**
**Cryptographic Performance Comparison**

| Cryptographic Scheme | Key Generation (ms) | Encapsulation (ms) | Decapsulation (ms) | Signing (ms) | Verification (ms) |
|---|---|---|---|---|---|
| ML-KEM-512 + ML-DSA-44 | 0.42 | 0.31 | 0.39 | 0.68 | 0.21 |
| ML-KEM-768 + ML-DSA-65 | 0.61 | 0.45 | 0.53 | 0.91 | 0.29 |
| Proposed PQ Hybrid Scheme | 0.64 | 0.47 | 0.55 | 0.94 | 0.31 |

The security overhead of the proposed scheme is 5,741 bytes, with a 1,184-byte public key, a 1,088-byte KEM ciphertext, and a 3,309-byte signature. That's just 64 bytes more than ML-KEM-768 + ML-DSA-65, due to the transaction metadata. This overhead provides sender-receiver identification, policy

information, and other cross-border transaction parameters without significantly adding to the amount of information that is transmitted in the record shown in Table 2.

**Table 2**

**Communication and Storage Overhead**

| Scheme | Public Key (Bytes) | Ciphertext/KEM Data (Bytes) | Signature (Bytes) | Metadata (Bytes) | Total Security Overhead (Bytes) |
|---|---|---|---|---|---|
| ML-KEM-512 + ML-DSA-44 | 800 | 768 | 2,420 | 96 | 4,084 |
| ML-KEM-768 + ML-DSA-65 | 1,184 | 1,088 | 3,309 | 96 | 5,677 |
| Proposed PQ Hybrid Scheme | 1,184 | 1,088 | 3,309 | 160 | 5,741 |

As the medical-record size goes up, processing time goes up (from 5.02ms for 1MB to 83.91ms for 50MB) and throughput goes up (from 53.8 MB/s to 165.2 MB/s). Transmission latency at a 50 MB record is up to 302.6 ms, but the relative security overhead is only 0.011%, which is lower compared to 0.55% at 10 MB. The results show that the fixed cryptographic overhead is relatively small with increasing size of the medical record transferred as shown in Table 3.

**Table 3**

**Medical Data Transmission Performance**

| Medical Record Size | Encryption Time (ms) | Total Processing Time (ms) | Transmission Latency (ms) | Throughput (MB/s) | Total Overhead (%) |
|---|---|---|---|---|---|
| 1 MB | 2.14 | 5.02 | 18.6 | 53.8 | 0.55 |
| 5 MB | 8.73 | 11.65 | 42.4 | 117.9 | 0.11 |
| 10 MB | 16.91 | 19.86 | 71.8 | 139.3 | 0.055 |
| 25 MB | 40.82 | 43.79 | 158.7 | 157.5 | 0.022 |
| 50 MB | 80.94 | 83.91 | 302.6 | 165.2 | 0.011 |

## 5. Discussion and Conclusion

The experimental analysis focuses on the proposed post-quantum framework in terms of cryptographic execution time, overhead in communication, and performance in medical-data transmission. The results serve as a quantitative foundation to evaluate its appropriateness for secure cross-country healthcare data exchange. The results show that the proposed post-quantum hybrid scheme can be used to provide cross-border medical-data protection with moderate cryptographic cost. The time for generating keys is 0.64ms and the time for encapsulating is 0.47ms, which means that there is no

significant processing delay if lattice-based key establishment is used. This is useful when transferring EHRs, diagnostic files and medical images because the fixed security overhead will be proportional smaller for larger medical records.

The present work proposes a lattice based post-quantum solution consisting of the ML-KEM, ML-DSA and AES-256-GCM for exchanging medical data securely and verifiably across the nation boundaries. The total processing time is 83.91 ms for 50 MB medical record, and the security overhead is 0.011% for the relative one. These results show a fair trade-off between security against quantum attacks and transmission costs. Future research can investigate the framework with actual hospital communication environments, mixed medical-data formats and multi-country communication networks. Key rotation, certificate management, patient controlled authorization, interoperability of FHIR based systems, and formal protocol verification in more quantum and network attack models are additional topics for further evaluation.

## References

[1] B. Mohinder Singh and J. Natarajan, "A novel secure authentication protocol for eHealth records in cloud with a new key generation method and minimized key exchange," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 7, Art. no. 101629 (2023), doi: 10.1016/j.jksuci.2023.101629.

[2] M. Adeli, N. Bagheri, H. R. Maimani, S. Kumari, and J. J. P. C. Rodrigues, "A post-quantum compliant authentication scheme for IoT healthcare systems," *IEEE Internet Things J.*, vol. 11, no. 4, pp. 6111–6118 (Feb. 2024), doi: 10.1109/JIOT.2023.3309931.

[3] M. SaberiKamarposhti, K.-W. Ng, F.-F. Chua, J. Abdullah, M. Yadollahi, M. Moradi, and S. Ahmadpour, "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data," *Heliyon*, vol. 10, no. 10, Art. no. e31406 (2024), doi: 10.1016/j.heliyon.2024.e31406.

[4] K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, S. Mussiraliyeva, and A. Chehri, "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems," *Internet Things*, vol. 27, Art. no. 101228 (2024), doi: 10.1016/j.iot.2024.101228.

[5] A. N. E. Bahache, N. Chikouche, and S. Akleylek, "Securing cloud-based healthcare applications with a quantum-resistant authentication and key agreement framework," *Internet Things*, vol. 26, Art. no. 101200 (2024), doi: 10.1016/j.iot.2024.101200.

[6] A. Ahmad and S. Jagatheswari, "Lattice-based three party authenticated key agreement scheme in medical IoT for post-quantum

environment," *IEEE Access*, vol. 12, pp. 157247–157259 (2024), doi: 10.1109/ACCESS.2024.3483971.

[7] T. Zhukabayeva, A. U. Rehman, N. Tariq, and E. Benkhelifa, "Hyperledger Fabric-based post quantum cryptography for healthcare application using discrete event simulation," *IEEE Access*, vol. 12, pp. 192482–192493 (2024), doi: 10.1109/ACCESS.2024.3513153.

[8] L. Soni, H. Chandra, and D. S. Gupta, "Post-quantum attack resilience blockchain-assisted data authentication protocol for smart healthcare system," *Softw. Pract. Exp.*, vol. 54, no. 11, pp. 2170–2190 (Nov. 2024), doi: 10.1002/spe.3336.

[9] S. Alsubai, A. Alqahtani, H. Garg, M. Sha, and A. Gumaei, "A blockchain-based hybrid encryption technique with anti-quantum signature for securing electronic health records," *Complex Intell. Syst.*, vol. 10, pp. 6117–6141 (2024), doi: 10.1007/s40747-024-01477-1.

[10] S. Prajapat, G. Thakur, P. Kumar, A. K. Das, S. S. Jamal, and W. Susilo, "Designing lattice-enabled group authentication scheme based on post-quantum computing in healthcare applications," *Comput. Electr. Eng.*, vol. 123, Art. no. 110028 (2025), doi: 10.1016/j.compeleceng.2024.110028.

[11] C. Deshpande, C. Ramtirthkar, T. A. Wani, V. K. Bhosale, M. Gulhane, and K. S. Kumar, "Topology and knot theory applications in quantum field theory," *Journal of Interdisciplinary Mathematics,* vol. 28, no. 6, pp. 2281–2287 (2025), doi: 10.47974/JIM-2370.

*Received March, 2026*