engineering proceedings

MDPI

Proceeding Paper

Post-Quantum Crystal-Kyber Group-Oriented Encryption Scheme for Cloud Security in Personal Health Records †

Zhen-Yu Wu [1] and Chia-Hui Liu [2,*]

[1] Department of Maritime Information and Technology, National Kaohsiung University of Science and Technology, Kaohsiung 81143, Taiwan; hkwu668@nkust.edu.tw
[2] Department of Electronic Engineering, National Formosa University, Huwei Township 632301, Taiwan
* Correspondence: liuch@nfu.edu.tw
† Presented at the 8th Eurasian Conference on Educational Innovation 2025, Bali, Indonesia, 7–9 February 2025.

Abstract

As medical technology develops and digital demands grow, personal health records (PHRs) are becoming more patient-centered than before based on cloud-based health information exchanges. While enhancing data accessibility and sharing, these systems present privacy and security issues, including data breaches and unauthorized access. We developed a post-quantum, group-oriented encryption scheme using the Crystal-Kyber Key encapsulation mechanism (KEM). Leveraging lattice-based post-quantum cryptography, this scheme ensures quantum resilience and chosen ciphertext attack security for layered cloud PHR environments. It supports four encryption modes: individual, group, subgroup-specific, and authorized subgroup decryption, meeting diverse data access needs. With efficient key management requiring only one private key per user, the developed scheme strengthens the privacy and security of PHRs in a future-proof, flexible, and scalable manner.

Keywords: group-oriented encryption; personal health records (PHRs); lattice-based cryptography; post-quantum security

check for updates

Academic Editors: Teen-Hang Meen, Chun-Yen Chang and Cheng-Fu Yang

Published: 6 August 2025

Citation: Wu, Z.-Y.; Liu, C.-H. Post-Quantum Crystal-Kyber Group-Oriented Encryption Scheme for Cloud Security in Personal Health Records. *Eng. Proc.* **2025**, *103*, 6. https://doi.org/10.3390/engproc2025103006

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

As medical technology advances and digital transformation progresses, personal health records (PHRs) are evolving to be patient-centered, cloud-based health information exchange models. By centralizing health data in cloud data centers, PHR systems enable patients to access, manage, and control their personal health information anytime, facilitating efficient medical information sharing and collaboration while improving healthcare quality and efficiency. At the same time, cloud-based PHR systems offer healthcare institutions operational flexibility and cost-effectiveness, reducing reliance on dedicated data centers. However, this evolution comes with significant privacy and security risks, including data breaches, unauthorized access, and insider misuse, which threaten patient privacy rights and the integrity and credibility of medical data [1,2]. Current privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, provide safeguards for traditional healthcare entities but leave gaps when applied to emerging cloud-based PHR service providers. This regulatory insufficiency exacerbates privacy and security concerns [3].

Beyond these challenges, the rapid development of quantum computing presents a potential threat to traditional encryption methods. Leveraging its superposition and entanglement properties, quantum computers solve complex mathematical problems, such

as those underlying Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC) algorithms in an exceptionally short time. This renders existing encryption mechanisms ineffective in future quantum computing environments. To ensure the confidentiality and integrity of PHR systems in the face of quantum computing, it is imperative to adopt quantum-resistant encryption technologies [4]. Furthermore, as PHR systems are used by diverse user groups, differences in roles and data access permissions, such as those between physicians and nurses, become prominent. Traditional single-layer encryption models struggle to accommodate these varied needs, requiring system designs that balance flexibility with efficiency.

To address these challenges, we developed a post-quantum, group-oriented encryption system based on the Crystal-Kyber Key encapsulation mechanism (KEM). This system employs lattice-based post-quantum cryptography, offering quantum resilience and chosen ciphertext attack (CCA) security, making it appropriate for hierarchical cloud PHR environments. It incorporates four flexible encryption modes: individual designated decryption, group broadcast decryption, designated subgroup decryption, and authorized subgroup broadcast decryption. These modes accommodate diverse data access needs, such as team-wide announcements, private messages for individual patients, and data sharing within specific subgroups [5]. Additionally, the system allows users to manage a single private key for all encryption modes, reducing the risks associated with operational complexity and mismanagement while enhancing usability.

The developed scheme enhances privacy and security while ensuring operational efficiency and stability for cloud-based PHR systems. By optimizing ciphertext design and encryption/decryption processes, this scheme maintains low spatial and computational complexity during large-scale data transmissions, significantly reducing transmission costs. Furthermore, its adaptability to quantum computing environments enables a robust, flexible, and scalable solution for data security and privacy protection in the future. This scheme can be used to develop secure and compliant cloud-based PHR systems, addressing the pressing challenges of modern healthcare data management.

2. Related Work

2.1. Cryptosystem

The rapid development of information technology and advancements in data transmission and communication have significantly influenced daily life. However, the increase in data volume and transmission frequency has also raised security concerns. To ensure the safety of information, cryptosystems are used to address confidentiality, authentication, integrity, and non-repudiation. Currently, cryptosystems are categorized into symmetric and asymmetric types.

Symmetric cryptosystems, also known as private key cryptosystems or one-key cryptosystems, use the same key for encryption and decryption. Symmetric cryptosystems include the Data Encryption Standard (DES) [6] and the International Data Encryption Algorithm (IDEA) [7]. Symmetric cryptosystems have challenges, such as key distribution and management. In multi-party communication scenarios, the number of keys increases exponentially with the number of users, complicating management and raising the risk of errors or loss. Additionally, because the same key is used for encryption and decryption, symmetric systems lack non-repudiation, as senders can deny having sent specific messages.

Asymmetric cryptosystems, or public key cryptosystems, use a pair of public and private keys for encryption and decryption. These systems overcome limitations of symmetric cryptosystems by eliminating the need for shared keys and offering non-repudiation through digital signature techniques. The algorithms include RSA [8], ElGamal [9], and

ECC [10]. However, asymmetric systems typically have higher computational complexity, making them slower compared to symmetric systems [11]. For instance, RSA is approximately 1000 times slower than DES [12]. To enhance the reliability of public key systems, public key infrastructure (PKI) provides a trusted third-party mechanism to certify public keys, ensuring their authenticity and security [13].

2.2. Post-Quantum Cryptography

The advent of quantum computing poses a severe threat to traditional encryption methods, such as RSA and ECC, which rely on mathematical problems that quantum computers can efficiently solve. Post-quantum cryptography aims to address this challenge by developing encryption methods based on new mathematical foundations that are resistant to quantum attacks. Crytsal-Kyber, a module lattice-based encryption scheme, is one of the leading candidates for post-quantum cryptography. Its core mechanism, the key encapsulation mechanism (KEM), consists of key generation, encapsulation, and decapsulation.

The security of Crytsal-Kyber is based on lattice-based cryptography for the learning with errors (LWEs) problem and its extensions. The mathematical structure of lattices provides strong resistance against quantum attacks [14,15]. Crytsal-Kyber improves efficiency and security through the use of Ring-LWE and Module-LWE designs, which optimize computational performance and provide additional flexibility [16]. In applications, Crytsal-Kyber offers the following advantages:

- Quantum resistance: Based on the problems faced in lattice-based cryptography, it provides robust protection against quantum attacks.
- High efficiency: The ring-based polynomial structure enhances encryption and decryption speeds, making it suitable for large-scale data transmission.
- Implicit rejection mechanism: This mechanism returns pseudo-random keys instead of error messages during ciphertext verification failures, preventing side-channel attacks [17].
- Resource efficiency: Crystal-Kyber reduces ciphertext size, making it ideal for embedded devices and resource-constrained environments [18].
- Due to its exceptional security and performance, Crystal-Kyber is used in the standardization process for post-quantum cryptography as it plays a critical role in ensuring data security and communication privacy in a quantum computing era.

3. Crystal-Kyber-Based Group Encryption

We developed a group encryption scheme based on the Crystal-Kyber post-quantum cryptographic algorithm. The scheme consists of three main processes: key generation (KeyGen), key encapsulation (Encaps), and key decapsulation (Decaps). These processes collaboratively ensure secure key generation, ciphertext encapsulation, and shared key recovery.

3.1. Parameter Definitions:

- q: A prime modulus defining the range of ciphertext and keys.
- k: The dimension of the lattice, influencing ciphertext size and security.
- $A \in Z_q^{k \times k}$: A modular lattice matrix forming the foundational structure.
- R_q: A polynomial ring modulo q, used in lattice computations.
- $s, e \in R_q^k$: Private and error vectors are essential for private key generation.

3.2. Key and Ciphertext Structure:

- Public Key (*pk*): Consists of t (a compressed value derived from the lattice) and ρ (a random seed).
- Private Key (*sk*): Consists of a private lattice vector s.
- Ciphertext (c): Comprises two parts (u, v), derived through modular lattice operations.

Additionally, secure hash functions H and G are utilized as follows:

- $H : 0,1^* \rightarrow 0,1^{256}$: Produces a fixed 256-bit hash from arbitrary-length inputs.
- $G : 0,1^* \rightarrow \left(0,1^{256}, R_q^k\right)$: Generates a random 256-bit string and a lattice vector.

3.3. Encryption Process Design

The encryption system operates through the following steps.

Step 1: KeyGen creates public and private keys for the group.

- Input: Security parameter λ.
- Output: Public key $pk = (t, \rho)$, private key $sk = s$.
- Procedures:

Step.1.1: Generate random seeds ρ, σ from $0, 1^{256}$.
Step.1.2: Construct the modular lattice matrix A using ρ.
Step.1.3: Generate private vector s.
Step.1.4: Generate error vector e using σ.
Step.1.5: Compute the compressed value: $t = Compress_q\ (A \cdot s + e, d_t)$.
Step.1.6: Output $pk = (t, \rho)$ and $sk = s$.

Step 2: In Encaps, the sender encrypts a message and generates a ciphertext and shared key.

- Input: Public key $pk = (t, \rho)$.
- Output: Ciphertext $c = (u, v)$, with shared key K.
- Procedures:

Step.2.1: Randomly generate a message $m \in 0, 1^{256}$.
Step.2.2: Compute K and r using hash functions: $(K, r) = G(H(pk), m)$.
Step.2.3: Encrypt m using Kyber CPA encryption to produce (u, v).
Step.2.4: Derive the shared key K as $H(K, H(c))$.
Step.2.5: Output $c = (u, v)$ and K.

Step 3: In Decaps, the receiver decrypts the ciphertext to recover the shared key.

- Input: Private key $sk = s$, ciphertext $c = (u, v)$.
- Output: Shared key K.
- Procedures:

Step.3.1: Decrypt c using sk to recover m': *Kyber.CPA.Dec* $(s, (u, v))$.
Step.3.2: Recompute K' and r': $(K', r') = G(H(pk), m')$.
Step.3.3: Validate ciphertext consistency by re-encrypting m':
$(u', v') =$ *Kyber.CPA.Enc* $((t, \rho), m'; r')$.
Step.3.4: If $(u', v') = (u, v)$, return $K = H(K', H(c))$; otherwise, return a pseudo-random key: $K' = H(z, H(c))$, where z is a random seed.

4. Security Analysis

We analyzed the security of the developed Crystal-Kyber-based group encryption scheme. The analysis was conducted based on its resilience against quantum attacks, chosen ciphertext attacks, impersonation, and data integrity threats.

4.1. Resilience to Quantum Computing Attacks

The security of Crystal-Kyber is built on the module LWE (MLWE) problem, which is widely recognized in the academic community as computationally difficult, even with the assistance of quantum computers. The difficulty of MLWE lies in the inability of attackers to reverse-engineer private parameters from modular lattice structures obscured by random noise, making such computations infeasible.

- Defense against quantum algorithms: Crystal-Kyber's reliance on high-dimensional algebraic structures ensures that algorithms like Shor's algorithm, which have the potential for long-term data protection leaks in traditional cryptosystems, are ineffective. This guarantees robust security even in a future quantum computing era.
- Advantages for long-term data protection: The quantum-resistant nature of Crystal-Kyber is ideal for applications requiring prolonged data protection, such as PHRs. The sensitive nature of PHR data necessitates safeguarding against attacks over extended periods.

4.2. Defense Against Chosen Ciphertext Attacks

Crystal-Kyber employs implicit rejection mechanisms and ciphertext validation for CCA. These techniques mitigate the risks associated with tampered or malicious ciphertexts by generating pseudo-random keys instead of revealing decryption errors.

- Implicit rejection mechanism: When an invalid ciphertext is encountered during decryption, the scheme outputs a pseudo-random key rather than indicating an error. This prevents attackers from deducing any useful information about the decryption process.
- Tampering resistance: By withholding feedback on the validity of the ciphertext, the scheme thwarts side-channel analysis and replay attacks. This significantly enhances security by reducing opportunities for attackers to exploit cryptographic vulnerabilities.

4.3. Resistance to Impersonation Attacks

Impersonation attacks aim to forge a valid ciphertext to impersonate legitimate users and gain access to shared keys or sensitive data. The developed scheme incorporates the following measures to respond to these threats.

- Unique key pairs: Each member's public–private key pair is randomly generated and intrinsically linked to the modular lattice structure. Attackers, even if they possess the public key, cannot forge a valid ciphertext without the corresponding private key.
- CCA: The decryption process includes a consistency check to validate whether the ciphertext originates from authorized users. Any tampering or forgery attempts are detected and rejected.
- Mitigation of consequences: Even if attackers submit a forged ciphertext, the system only returns a pseudo-random key, ensuring no sensitive data or shared keys are leaked.

4.4. Data Integrity and Tamper Resistance

Crystal-Kyber ensures data integrity and protects against tampering attacks through the mathematical properties of its ciphertext structure and consistency validation.

- Ciphertext integrity protection: The encryption process embeds cryptographic parameters and random noise within the ciphertext. Any attempt to tamper with the ciphertext disrupts its structure, resulting in decryption failure.
- Tamper detection: If a ciphertext is illegally modified, the system identifies anomalies during consistency checks and rejects the decryption request. A pseudo-random key is returned instead, preventing attackers from obtaining valuable information.

5. Conclusions

The Crystal-Kyber-based group encryption scheme developed in this study shows its value in PHR systems, particularly in ensuring data security and addressing the flexible needs of group applications. Built upon the post-quantum cryptographic framework of the MLWE problem, this scheme leverages the mathematical properties of modular lattices, making it resistant to attacks from classical and quantum computers. This robustness offers a reliable countermeasure against potential threats posed by future advancements in quantum computing. Through mechanisms such as implicit rejection and ciphertext consistency checks, the scheme effectively defends against tampering and impersonation attacks, ensuring that intercepted or modified ciphertexts cannot expose sensitive data or enable replay attacks.

To accommodate the demands of group applications, the developed Crystal-Kyber encryption scheme is designed to meet the diverse access needs of different members. The system allows senders to define decryption scopes based on group structure and data sensitivity, such as assigning differential access privileges to doctors, patients, and nurses in medical environments. This enhances operational flexibility and fosters collaboration and data sharing within medical teams. Furthermore, the scheme simplifies key management by requiring each group member to manage only a single private key for all encryption and decryption operations. This reduces the risk of operational errors and mitigates potential data breaches caused by complex key management processes.

During data transmissions, the Crystal-Kyber scheme ensures data integrity by introducing random noise to ciphertexts, preventing tampering or forgery. When inconsistencies in the ciphertext are detected, the scheme avoids providing explicit decryption failure feedback and instead returns a pseudo-random key. This approach effectively prevents attackers from exploiting error feedback for side-channel attacks. Additionally, the Crystal-Kyber scheme outperforms previous alternative encryption techniques in terms of computational efficiency and ciphertext size, making it particularly well-suited for cloud-deployed PHR systems that handle large volumes of data and support multi-user access.

The developed Crystal-Kyber group encryption scheme meets the current requirements for the data privacy and security of PHR systems and provides robust protection against future quantum computing threats. It efficiently addresses individual data encryption needs while supporting flexible group data access management, offering critical information for secure data sharing and collaboration in healthcare. As global data privacy regulations become increasingly stringent, this scheme provides a balanced solution for security, efficiency, and flexibility, enabling healthcare institutions to advance toward a more digital, patient-centered future.

Author Contributions: Conceptualization, Z.-Y.W. and C.-H.L.; methodology, Z.-Y.W.; software, Z.-Y.W.; validation, Z.-Y.W. and C.-H.L.; formal analysis, Z.-Y.W.; investigation, Z.-Y.W.; resources, C.-H.L.; data curation, Z.-Y.W.; writing: original draft preparation, Z.-Y.W.; writing: review and editing, C.-H.L.; visualization, Z.-Y.W.; supervision, C.-H.L.; project administration, C.-H.L.; funding acquisition, C.-H.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Science and Technology Council, Taipei, Taiwan, under grant number NSTC 113-2635-E-150-001.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Marouf, I.; Saighi, A.; Kouah, S.; Laboudi, Z. *E-Health Cloud Based Systems: A Survey on Security Challenges and Solutions*; Springer: Cham, Switzerland, 2023; Volume 783, pp. 224–229.
2. Javed, W.; Aabid, F.; Danish, M.; Tahir, H.; Zainab, R. *Role of Blockchain Technology in Healthcare: A Systematic Review*; IEEE: New York, NY, USA, 2021; pp. 1–8.
3. Alberts, C.J.; Dorofee, A. HIPAA and information security risk: Implementing an enterprise-wide risk management strategy. In Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05), Kaohsiung, Taiwan, 5–8 July 2005.
4. Li, S.; Chen, Y.; Chen, L.; Liao, J.; Kuang, C.; Li, K.; Liang, W.; Xiong, N. Post-Quantum Security: Opportunities and Challenges. *Sensors* **2023**, *23*, 8744. [CrossRef] [PubMed]
5. Du, C.; Bai, G.; Chen, H. Towards Efficient Implementation of Lattice-Based Public-Key Encryption on Modern CPUs. In Proceedings of the IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 1230–1236.
6. *FIPS PUB46-3*; Specification for the Data Encryption Standard (DES). National Institute of Standards and Technology: Gaithersburg, MD, USA, 1999.
7. Leong, M.P.; Cheung, O.Y.H.; Tsoi, K.H.; Leong, P.H.W. A Bit-serial implementation of the international data encryption algorithm IDEA. In Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines, Napa Valley, CA, USA, 17–19 April 2000; pp. 122–131.
8. Diffie, W.; Hellman, E. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
9. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [CrossRef]
10. Koblitz, N. Elliptic Curve Cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
11. Baumer, D.L.; Earp, J.B.; Payton, F.C. Privacy of medical records: IT implications of HIPAA. *ACM Comput. Soc.* **2000**, *30*, 40–47. [CrossRef]
12. RSA Laboratories. *RSA Algorithm Technical Specifications*; RSA Security Inc.: Burlington, MA, USA, 2004.
13. Guajardo, J.; Paar, C. *Efficient Algorithms for Elliptic Curve Cryptosystems*; Springer: Berlin/Heidelberg, Germany, 1997. [CrossRef]
14. Richter, M.; Bertram, M.; Seidensticker, J.; Tschache, A. A Mathematical Perspective on Post-Quantum Cryptography. *Mathematics* **2022**, *10*, 2579. [CrossRef]
15. Chen, L.; Moody, D.; Regenscheid, A. *NIST Post-Quantum Cryptography Standardization: A Preliminary Report*; NIST: Gaithersburg, MD, USA, 2019.
16. Cherkaoui Dekkaki, K.; Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies* **2024**, *12*, 241. [CrossRef]
17. Streit, S.; De Santis, F. Post-Quantum Key Exchange on ARMv8-A: A New Hope for NEON Made Simple. *IEEE Trans. Comput.* **2017**, *67*, 1651–1662. [CrossRef]
18. Bos, J.; Costello, C.; Ducas, L.; Mironov, I.; Naehrig, M.; Nikolaenko, V.; Raghunathan, A.; Stebila, D. Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), New York, NY, USA, 24–28 October 2016; pp. 1006–1018.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.