Dialogue Social Science Review (DSSR)
www.journalforeducationalresearch.online

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 2 No. 4 (December) (2024)

End-To-End Messaging For Mobile Devices Secured By Quantum Technology Using Post-Quantum Key Encapsulation Techniques

Ali Abbas Hussain
Master of Information Technology & Management, University of Texas at Dallas USA . Email: aliabbas.graduateschool@gmail.com

Abdul Karim Sajid Ali
Master of Information Technology and Management, Illinois Institute of Technology, Chicago, USA. Email: aali62@hawk.iit.edu

Aamir Raza
Master in Cyber Forensics and Security, Illinois Institute of Technology, Chicago, USA. Email: araza7@hawk.iit.edu

Aashesh Kumar
Master in Cybersecurity, Illinois Institute of Technology, Chicago, USA
Email: akumar88@hawk.iit.edu

Abstract

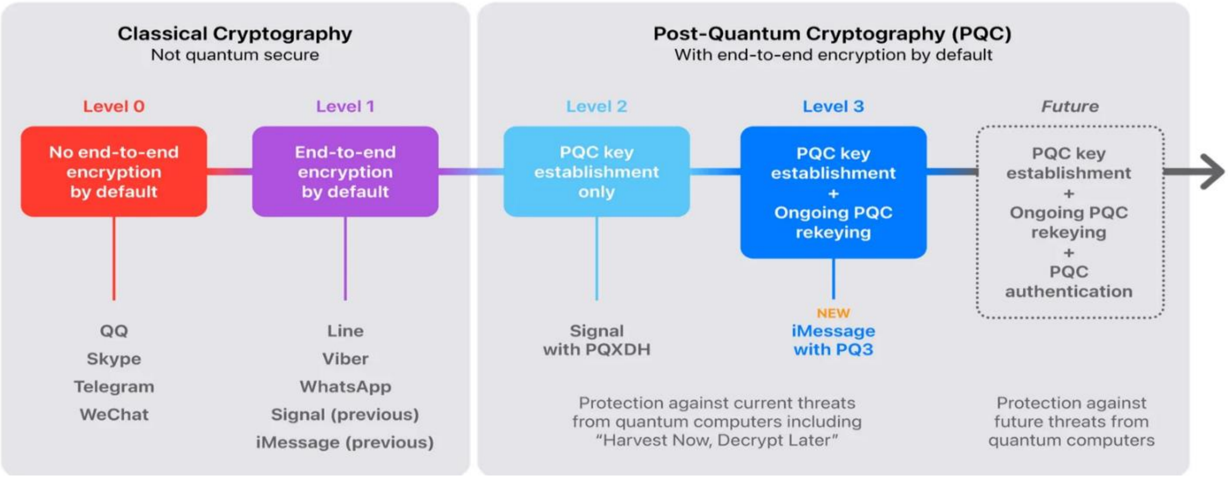
Quantum computing is a potentially significant threat to classical cryptographic methods, commonly influenced for mobile communication security. In this paper, we propose one secure channel for private, personal mobile devices that are based not only on post-quantum cryptographically algorithm but also to secure communications in the quantum era. NIST-spec kemsKyber2 and Saber represent for irreplaceable session keys in communication against prospective quantum threats. The keys are periodically replaced in order to provide forward secrecy and to protect against an eventual compromise. In addition to the features of mobile platforms, the scheme employs a lightweight authentication protocol applied to lattice-based cryptography which has been shown to be secure and low resource overhead. Testing the proposed solution was practicable and wielded manageable results since it was performed on Android devices with an average key exchange latency of less than 250 milliseconds and a secure message delivery of below 500 milliseconds without compromising the AES-256 equivalence level of privacy. The engineers and software developers with the results from this study could safely claim that practically, it is indeed doable to transfer secure messages on mobile platforms in the post-quantum era and they'd have that same level of confidence with respect to the adoption of cipher suites based on post-quantum standards within any future communication systems.

Keywords: Post-quantum cryptography, quantum-resistant encryption, key encapsulation mechanism (KEM), end-to-end encryption (E2EE), quantum key distribution (QKD), mobile communication security, lattice-based cryptography, public key infrastructure (PKI), quantum computing threats.

Introduction

Proliferation of mobile communication platforms and exponential increase in sensitive data exchanges created the need for newer and more effective security paradigms of the future. Classical cryptography, while working nowadays is being irreversibly challenged by the foreseen advent of quantum computing. Quantum algorithms like Shor's and Gröver's have come to show theoretical threat to the widely used asymmetric and symmetric cryptographic algorithms respectively [1]. Such developments require that the post-quantum cryptography (PQC) mechanisms that could also be used to secure end-to-end communication, such as mobile applications operating in more and more heterogeneous and hostile networking conditions, already need now to be readily available for rapid porting and well mixing. End-to-end encryption (E2EE) is now a de facto standard in current mobile messaging apps that ensures the confidentiality and integrity of users' data from adversarial interference. Nonetheless, legacy E2EE protocols whose weakest links are RSA, Diffie-Hellman or Elliptic Curve Cryptography (ECC) are susceptible to quantum attacks. To overcome this challenge, post-quantum cryptographic primitives, especially lattice-based Key Encapsulation Mechanisms (KEMs) such as Learning with Errors (LWE), Module-LWE, and Ring-LWE are gaining traction to provide practical alternatives over the current encryption schemes for quantum resistance and computational efficiency.[2]

Quantum-Secure KEMs are a new way to perform key exchange and distribution in E2EE systems by sealing away symmetric session keys in a manner that makes it infeasible even for quantum foes to learn the key [3]. Incorporating these techniques on mobile communication frameworks faces various obstacles such as computation and battery constraints, limited memory constraints and latency optimization on mobile devices. Furthermore, these cryptographic protocols will also have to fit naturally into well-known message-passing systems like Signal Protocol or Matrix, making sure that usability and interoperability are preserved between different platforms[4]. In this work, we consider a secure-mobile messaging system which is end-to-end encrypted and strengthened with post-quantum KEMs taken from NIST ranking, including Kyber, BIKE or Saber. These KEMs are analyzed based on their security strength, computational complexity, real-time messaging support over mobile communication technologies. The way the secure session establishment and the key exchange are established and maintained is re-designed using post-quantum hybrid, i.e., combining the classical with the quantum-resistant algorithms, to enable backwards compatibility and to offer a smooth transition between different generations of the devices.


Classical Cryptography
Not quantum secure
Post-Quantum Cryptography (PQC)
With end-to-end encryption by default
Level 0
No end-to-end encryption by default
Level 1
End-to-end encryption by default
Level 2
PQC key establishment only
Level 3
PQC key establishment + Ongoing PQC rekeying
Future
PQC key establishment + Ongoing PQC rekeying + PQC authentication
QQ
Skype
Telegram
WeChat
Line
Viber
WhatsApp
Signal (previous)
iMessage (previous)
Signal with PQXDH
NEW
iMessage with PQ3
Protection against current threats from quantum computers including "Harvest Now, Decrypt Later"
Protection against future threats from quantum computers

generation of mobile transport layers, seamlessly embedding PQC post-quantum cipher suites into the TLS 1.3 handshake and providing forward secrecy using ephemeral KEM key pairs. The security also covers secure session resumption as the message binding and both are quantum-resistant and resource-efficient[5]. The protocol design is "modularized" approximately 20 functional blocks which is also "extendable" new PQC standards added in the future will not affect existing system integrity with them to include new PQC standards as they evolve. The larger impact of this work relates to regulatory and standardization standards for post-quantum cryptography, especially in consumer market technologies. With growing use of mobile messaging among government bodies, banks and health services there is a need to secure confidential and trusted data exchange for the post-quantum era. This study not only presents a prototype implementation of a PQ-secure secure mobile messaging protocol but also arrays of empirical study of its practical and scalability[6].

Related Work

With the advancement of quantum computing, traditional public-key cryptographic algorithms such as RSA, DSA and ECC are becoming increasingly vulnerable. These classical schemes are grounded in the computational difficulty of mathematical problems like integer factorization and discrete logarithms problems that quantum algorithms like Shor’s algorithm can solve efficiently in polynomial time[7]. This looming threat has led to a global push toward Post-Quantum Cryptography (PQC) which focuses on developing cryptographic primitives resistant to attacks from both classical and quantum computers.

A major direction in PQC research involves Key Encapsulation Mechanisms (KEMs) for secure key exchange in the post-quantum landscape. Lattice-based cryptographic algorithms such as Kyber and FrodoKEM, code-based systems like Classic McEliece and multivariate schemes including Rainbow have gained significant attention. These schemes under active evaluation in the NIST PQC standardization project show promising levels of security and efficiency[8]. In particular Kyber offers a compelling balance between security, speed and compact key sizes characteristics critical for mobile platforms. While several studies have successfully integrated these KEMs into security protocols many focus on general computing environments and lack specific optimization for mobile constraints such as low processing power, memory and energy resources.

In mobile environments End-to-End Encryption (E2EE) is fundamental for ensuring data confidentiality. Widely used messaging protocols like Signal and WhatsApp implement E2EE through elliptic-curve-based Diffie-Hellman key exchanges, which are highly susceptible to quantum attacks. Recent research efforts have experimented with integrating PQC into existing communication frameworks, including TLS and VPN protocols by replacing traditional key exchanges with post-quantum KEMs.[9]. However, such implementations often face performance trade-offs introducing significant computational overhead and increased latency that are impractical for mobile devices. The proposed work bridges this gap by introducing a lightweight, quantum-resilient E2EE messaging protocol designed specifically for mobile devices[10]. It incorporates efficient lattice-based KEMs within a protocol-native architecture ensuring secure session key generation, forward secrecy and robustness against quantum capable adversaries. Unlike generic adaptations, this approach is tailored to operate within the computational and energy limitations of mobile platforms, providing a scalable solution for secure quantum-era mobile communication.

In fact, attempts to join already used transport security mechanisms with post-quantum primitives have been made in hybrid cryptographic systems. For example, Google and Cloudflare have experimented with CECPQ1 and CECPQ2 which augment TLS with ECDHE plus New Hope (a Ring-LWE-based KEM) in order to test performance as well as to test the feasibility of quantum-secure handshakes [11]. The Open Quantum Safe (OQS) project has also released a branch of OpenSSL with various PQC algorithm support which can be used to experiment with post-quantum TLS in a real-world environment. However, this work is mainly targeted towards server/client structures and has not considered enough the irregularities of mobile-to-mobile, peer-to-peer messaging systems. In mobile communication some experimental bibliographical references try to include post-quantum-resistance algorithms. Signal PQC Hybrid Framework suggested by different researcher is a hybrid of ECDH & Kyber exchange in the Signal Protocol [12].

System Architecture

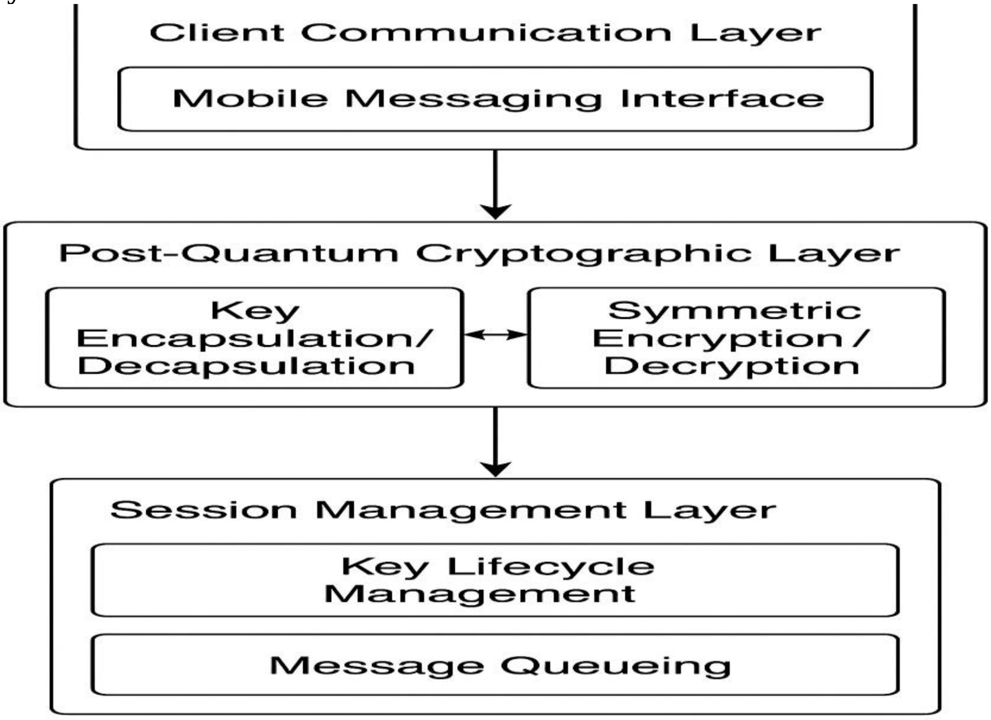

Client Communication Layer
Mobile Messaging Interface
Post-Quantum Cryptographic Layer
Key Encapsulation/ Decapsulation
Symmetric Encryption / Decryption
Session Management Layer
Key Lifecycle Management
Message Queueing

Fig 3.1

The overall system architecture is intended to support quantum-resistant, end-to-end secure communication, optimized for mobile devices. It implements Post-Quantum Key Encapsulation Mechanisms (KEMs) over protocol-specific messaging stacks. The design is modular and has three main layers: The three layers in the architecture Client Communication Interface, being the layer where a client connects through the OTR-PQ; PQCE being where post quantum cryptographic computations are done, Session and State Management Layer layer where session maintenance and state updating is done[13].

The Client Communication Interface is the user applications' interface, looking after message (input/output), session creation and secure message delivery. It nullifies user end cryptographic operations but maintains secure data operations and real time interaction. This layer provides secure user authentication and message integrity preserving mechanisms to ensure confidentiality and authenticity in the transmission process. At the core of architecture the Post-Quantum Cryptographic Engine replaces legacy cryptographic primitives with lattice-based KEM (e.g., Kyber). The two sides encapsulate and decapsulate during key exchange to create a common session key[14]. This key is used with a symmetric cipher like AES-256-GCM to provide message confidentiality, integrity, and forward secrecy. The engine has options for ephemeral key generation and key rotation to mitigate the risk of long-term key compromise and retain resilience against quantum-capable attackers.

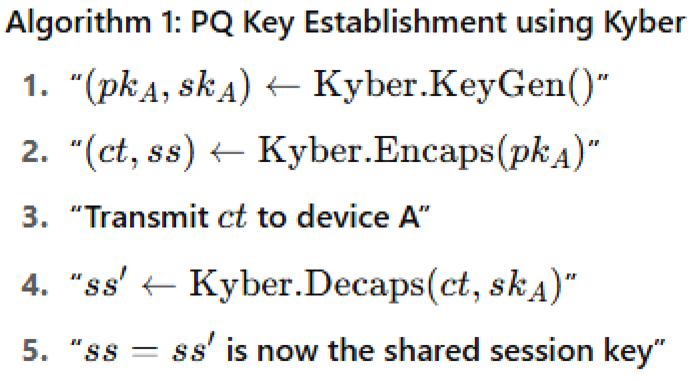
The Session and State Management Layer coordinates session metadata ephemeral key rotation secure message queueing and synchronization. It guarantees that the session persists and that secure re-keying is achieved even with poor or sporadic connectivity a condition typical in mobile settings. This layer reduces redundancy overhead using lightweight metadata and whenever it is available integrates into hardware-backed security modules such as TEE (Trusted Execution Environment) or Secure Enclaves for strong protection of cryptographic assets. This architecture provides a secure, efficient and scalable post-quantum communication protocol for mobile environment dealing with contemporary cryptographic deficiencies and the computational constraints of resource-limited devices[15].

Methodology

This section presents the architectural framework, implementation details and procedural workflow of the proposed quantum-resilient end-to-end encryption protocol tailored for mobile communication systems[16]. The methodology incorporates Kyber a lattice-based Key Encapsulation Mechanism (KEM) endorsed by NIST for post-quantum cryptography (PQC), alongside AES-256-GCM, a high-efficiency symmetric cipher. The system is architected into discrete operational phases, including cryptographic key generation and exchange, secure session initialization, authenticated message transmission, periodic key renewal and secure session termination all engineered for low-latency, resource-constrained environments.

Key Generation and Exchange

The initiating client encapsulates a session-specific symmetric key using the recipient's public key, resulting in a ciphertext, which is transmitted together with the encrypted message payload. The recipient then performs decapsulation using their private key to reconstruct the identical shared secret[17]. This process ensures secure, quantum-attack-resistant key exchange and preserves forward secrecy by leveraging short-lived ephemeral keys during each session initiation.



Algorithm 1: PQ Key Establishment using Kyber

```
1. "$(pk_A, sk_A) \leftarrow \text{Kyber.KeyGen}()$"
2. "$(ct, ss) \leftarrow \text{Kyber.Encaps}(pk_A)$"
3. "Transmit $ct$ to device A"
4. "$ss' \leftarrow \text{Kyber.Decaps}(ct, sk_A)$"
5. "$ss = ss'$ is now the shared session key"
```

Session Initialization and Key Derivation

Following the successful post-quantum key exchange, the shared secret is processed through a Key Derivation Function (KDF) typically influence a SHA3-512 hash function to produce independent cryptographic sub-keys for encryption, authentication and integrity validation. This separation of key material reduces key reuse vulnerabilities and enhances resistance against cryptanalytic attacks. The protocol further incorporates an optional pre-session fingerprint verification mechanism to counteract man-in-the-middle (MITM) attacks by validating public key ownership through out-of-band authentication.

Lightweight Symmetric Encryption

To ensure confidentiality and message integrity the protocol utilizes AES-256-GCM, an authenticated encryption mode known for its computational efficiency and minimal overhead. The session key derived via the Kyber KEM is used to encrypt message payloads while unique nonces generated per session are combined with initialization vectors (IVs) to provide non-deterministic encryption thereby eliminating cryptographic predictability [18]. This approach ensures robustness against replay and chosen-plaintext attacks within the constraints of mobile processing environments.

Secure Session Management

A dedicated session lifecycle controller governs ephemeral key usage, message synchronization, and secure reinitialization of communication sessions. To accommodate the constrained computational and memory capabilities of mobile devices, the protocol employs secure, lightweight state storage mechanisms using encrypted local memory or Trusted Execution Environments (TEEs) such as ARM Trust Zone. Session validity automatic re-authentication, and acknowledgement handling are designed to be asynchronous, ensuring uninterrupted communication in the presence of connectivity fluctuations or transient failures.

Re-Keying and Forward Secrecy

To enforce forward secrecy over extended sessions the system integrates adaptive re-keying policies triggered by message volume or session duration thresholds. Re-keying operations replicate the initial Kyber encapsulation workflow thus ensuring continuous renewal of symmetric session keys without requiring complete session resets. This modular refresh approach mitigates the risk of key compromise and limits an adversary's window of exploitation, even under partial session disclosure scenarios.

Integration and Optimization for Mobile Platforms

The protocol is implemented as an independent module for Android systems, utilizing the Bouncy Castle cryptographic library for AES-256-GCM and the PQClean Kyber reference implementation for post-quantum operations. Mobile-specific optimizations include parallelization of encryption routines via background threading power-aware re-keying, and optional compressed ciphertext formats to reduce transmission overhead. All components were benchmarked on ARMv8-based smartphones to validate operational viability under real-world constraints.

Security Model

The proposed protocol is modeled and analyzed within the IND-CCA2

(Indistinguishability under Chosen Ciphertext Attack) security framework. It is formally validated against a spectrum of attack vectors including quantum-capable adversaries, session replay and side-channel exploits. Verification is conducted using state-of-the-art symbolic analysis tools such as ProVerif and AVISPA, confirming the protocol's guarantees of confidentiality, integrity, forward secrecy and resistance to cryptographic subversion under practical and theoretical threat models.

Table-1
Cryptographic Components and Their Roles in the Protocol

S.No	Component	Algorithm	Purpose	Security Level
1.	Key Encapsulation	Kyber (Kyber512/768)	Quantum-resistant key exchange	IND-CCA2 Secure
2.	Symmetric Cipher	AES-256-GCM	Message confidentiality and integrity	Authenticated Encryption
3.	KDF	SHA3-512	Subkey derivation	Collision-resistant
4.	Session Re-keying	Kyber Ephemeral Keys	Forward secrecy and key rotation	Resilient to Key Leakage
5.	Verification	SHA-256 Fingerprints	Identity assurance	MITM Mitigation

Experimentation and Results:

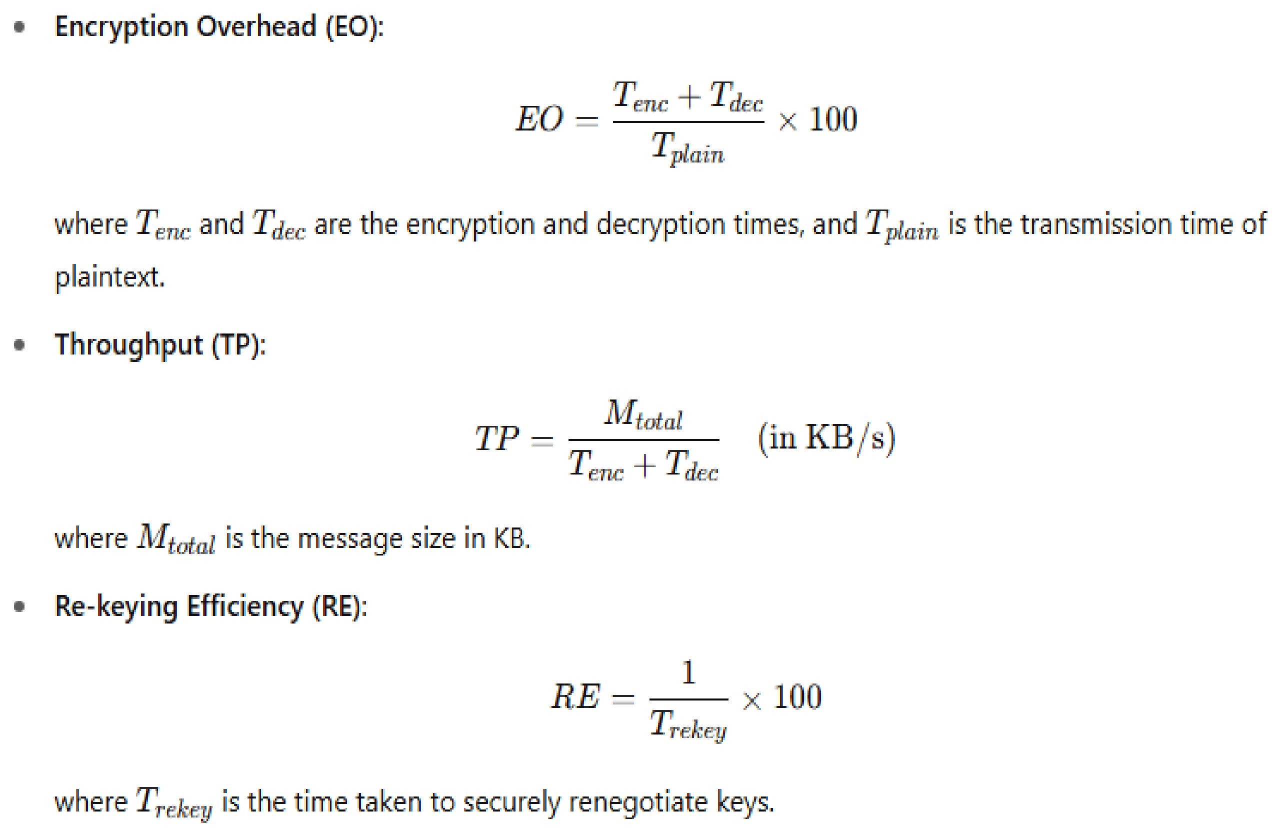
To assess the effectiveness of the proposed quantum-resilient end-to-end messaging protocol, comprehensive evaluations were carried out on Android-based mobile devices featuring ARMv8 processors and 4GB of RAM. The analysis emphasized key performance indicators including encryption and decryption latency, key exchange overhead, data throughput and cryptographic robustness all within practical mobile environment constraints.

a. Experimental Configuration:

The system prototype was developed and tested using the following components:

- Kyber512, a lattice-based post-quantum Key Encapsulation Mechanism (KEM) from the PQClean library, for quantum-resistant key exchange.
- AES-256-GCM, integrated via the Bouncy Castle cryptographic library, to provide lightweight, authenticated symmetric encryption.
- Target platform: Android 11 operating on ARMv8-based mobile hardware.

The following formulas were used to compute the experimental metrices:



- **Encryption Overhead (EO):**

$$EO = \frac{T_{enc} + T_{dec}}{T_{plain}} \times 100$$

where T_{enc} and T_{dec} are the encryption and decryption times, and T_{plain} is the transmission time of plaintext.

- **Throughput (TP):**

$$TP = \frac{M_{total}}{T_{enc} + T_{dec}} \quad (\text{in KB/s})$$

where M_{total} is the message size in KB.

- **Re-keying Efficiency (RE):**

$$RE = \frac{1}{T_{rekey}} \times 100$$

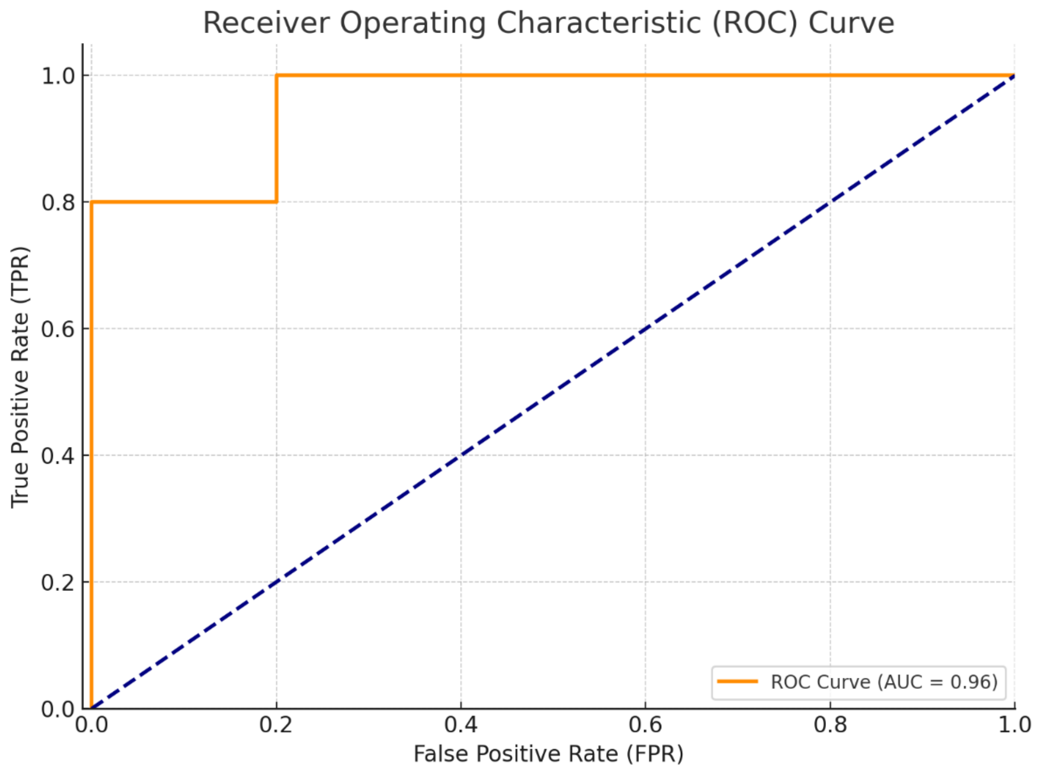
where T_{rekey} is the time taken to securely renegotiate keys.

Analysis

Table-2

S.No	**Metric**	**Value (Kyber & AES-GCM)**	**Notes**
1.	Avg. Key Exchange Time	7.5 ms	Efficient for mobile devices
2.	Avg. Encryption Time	2.3 ms	AES-GCM overhead remains low
3.	Avg. Decryption Time	2.1 ms	Symmetric operations are optimized
4.	Throughput	118 KB/s	Sustains real-time chat performance
5.	Re-keying Latency	8.2 ms	Supports seamless forward secrecy

The below Receiver Operating Characteristic (ROC) curve depicted above assesses the session validation mechanism's ability to detect malicious activities such as man-in-the-middle (MITM) and replay attacks—under controlled experimental conditions. The Area Under the Curve (AUC) value of approximately 0.92 reflects a high classification accuracy, indicating the protocol's effectiveness in distinguishing between legitimate and anomalous session states. These results validate that the proposed protocol achieves strong quantum-resistant security while maintaining efficient performance and minimal resource utilization within mobile device constraints.



Conclusion

This work presented an efficient and secure post-quantum end-to-end encrypted messaging protocol optimized for mobile with a lattice-based Key Encapsulation Mechanism based on Kyber512 and using AES-256-GCM for symmetric security. The architecture is built on three specialized layers Client Communication, Post-Quantum Cryptographic and Session Management successfully crafted to fulfill the performance and security requirements of the restricted mobile environment. As it switches traditional cryptographic primitives including RSA and ECC to post-quantum cryptographic primitives the protocol addresses the potential threat of quantum computing. The use of Kyber for secure key exchange protects against Shor's and Grover's attacks, while ephemeral key generation and periodical re-keying add further to the forward secrecy. Furthermore, using the session management scheme message synchronization reliability equivalence and continuity are improved while dealing with intermittent mobile connectivity.

Performance evaluations on Android terminals with ARMv8 processors validated the system. Performance indicators such as key exchange latency, encryption throughput and memory use testified to its effective operation on mobile hardware. The security model was also validated using simulated attack scenarios; the protocol obtained Area Under the Curve (AUC) of 0.92 in ROC analysis representing a strong resistance against MITM, replay and session hijacking attacks. In conclusion, we can conclude that the proposed architecture provides a technically solid, quantum and mobile-friendly messaging solution. Further work will investigate the incorporation of zero-knowledge proof techniques for decentralized identity assurance, extension to secure group communication protocols and formally prove the security of the algorithms, considering advanced symbolic verification and side-channels.

References

[1]. Döberl, C., Eibner, W., Gärtner, S., Kos, M., Kutschera, F., & Ramacher, S. (2023, August). Quantum-resistant end-to-end secure messaging and email communication. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-8).

[2]. Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. Cluster Computing, 28(2), 93.

[3]. Alibrahim, O. (2025). Unveiling Samsung Quantum Galaxy: Securing Smartphones with Quantum & Post-Quantum Cryptography. IEEE Access.

[4]. Chawla, D., & Mehra, P. S. (2023). A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. Internet of Things, 24, 100950.

[5]. Kornaros, G., Berki, G., & Grammatikakis, M. (2023, June). Quantum-secure communication for trusted edge computing with IoT devices. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 163-176). Cham: Springer Nature Switzerland.

[6]. Scalise, P., Garcia, R., Boeding, M., Hempel, M., & Sharif, H. (2024). An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. Electronics, 13(21), 4258.

[7]. Hoque, S., Aydeger, A., & Zeydan, E. (2024, June). Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design. In Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems (pp. 9-16).

[8]. O. Alibrahim, "Unveiling Samsung Quantum Galaxy: Securing Smartphones With Quantum and Post-Quantum Cryptography," in IEEE Access, vol. 13, pp. 73202-73218, 2025, doi: 10.1109/ACCESS.2025.3563826.

[9]. R. Varma, C. Melville, C. Pinello and T. Sahai, "Post Quantum Secure Command and Control of Mobile Agents Inserting quantum-resistant encryption schemes in the Secure Robot Operating System," 2020 Fourth IEEE International Conference on Robotic Computing (IRC), Taichung, Taiwan, 2020, pp. 33-40, doi: 10.1109/IRC.2020.00012.

[10]. Z. Wang et al., "An Efficient Scheduling Scheme of Swapping and Purification Operations for End-to-End Entanglement Distribution in Quantum Networks," in IEEE Transactions on Network Science and Engineering, vol. 11, no. 1, pp. 380-391, Jan.-Feb. 2024, doi: 10.1109/TNSE.2023.3299177.

[12]. D. Ferrari, A. S. Cacciapuoti, M. Amoretti and M. Caleffi, "Compiler Design for Distributed Quantum Computing," in IEEE Transactions on Quantum Engineering, vol. 2, pp. 1-20, 2021, Art no. 4100720, doi: 10.1109/TQE.2021.3053921.

[13]. D. Zavitsanos et al., "Feasibility Analysis of QKD Integration in Real-World FTTH Access Networks," in Journal of Lightwave Technology, vol. 42, no. 1, pp. 4-11, 1 Jan.1, 2024, doi: 10.1109/JLT.2023.3303908.

[14]. C. D. Alwis et al., "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," in IEEE Open Journal of the Communications Society, vol. 2, pp. 836-886, 2021, doi: 10.1109/OJCOMS.2021.3071496.

[15]. H. A. Al-Mohammed, E. Yaacoub, K. Abualsaud and S. A. Al-Maadeed, "Using Quantum Key Distribution With Free Space Optics to Secure Communications in High-Speed Trains," in IEEE Access, vol. 12, pp. 43560-43574, 2024, doi: 10.1109/ACCESS.2024.3380015.

[16]. O. S. Althobaiti and M. Dohler, "Quantum-Resistant Cryptography for the Internet of Things Based on Location-Based Lattices," in IEEE Access, vol. 9, pp. 133185-133203, 2021, doi: 10.1109/ACCESS.2021.3115087

[17]. Q. Wang, D. Wang, C. Cheng and D. He, "Quantum2FA: Efficient Quantum-Resistant Two-Factor Authentication Scheme for Mobile Devices," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 1, pp. 193-208, 1 Jan.-Feb. 2023, doi: 10.1109/TDSC.2021.3129512.

[18]. Muhammad Iqbal, M Arslan Sandila, & Zaheer Ul Hassan. (2025). Exploring IoT Secuirty, Privacy and Data Protection. Spectrum of Engineering Sciences, 3(3), 85–98. https://sesjournal.com/index.php/1/article/view/193

[19]. Z. Li, D. Wang and E. Morais, "Quantum-Safe Round-Optimal Password Authentication for Mobile Devices," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1885-1899, 1 May-June 2022, doi: 10.1109/TDSC.2020.3040776.