QMail: Hybrid Quantum Secure Email Client Application

Achal K A[1][0009-0007-0372-3991], S Pranav Roy[2][0009-0000-7414-6908], Rudraraju Satvik Varma[3][0009-0007-2145-6786]

[1,2,3]Presidency University, Bengaluru, Karnataka, India
achalacharya07@gmail.com, roy.sugavasi@gmail.com, satvikvarma03@gmail.com

Abstract. The emergence of commercial quantum computers is inevitable and only a matter of time given the rapid progress made by companies such as IBM, Google, and Microsoft. Commercialization of quantum computers threatens current encryption methods that have worked effectively up until now however, with the advent of Shor's and Grover's algorithms (quantum algorithms) for breaking current encryption methods, this compromises confidentiality, integrity and authenticity. Securing communication channels must be a top priority, and since email is the most widely used communication method, it must be addressed first. QMail, a Quantum Secure Email Client Application (QSECA), is designed to withstand both classical and quantum-level attacks. It uses a hybrid architecture of both Quantum Key Distribution (QKD) for the session key and Post-Quantum Cryptography (PQC) for authentication and metadata protection, innovating on top of existing QSECA. The prototype we have made features a user-friendly interface to choose between three levels of encryption, including OTP. The results we obtained show that QMail ensures end-to-end security and provides protection against adversaries with quantum capabilities. The results we obtained show that QMail ensures end-to-end security and provides protection against adversaries with quantum capabilities. We have established QMail as a foundation for a scalable, quantum-safe communication platform which is a step towards secure communication in the era of 6G and quantum internet.

Keywords: Quantum Key Distribution (QKD), Post-quantum cryptography (PQC), Hybrid Cryptography, Quantum-Resistant Communication, Secure Email Systems, One-Time Pad (OTP), Kyber KEM, Quantum Internet, 6G Security, Key management, AI- AI-assisted encryption, End-to-End Encryption.

1 INTRODUCTION

Email remains the most used communication system by companies and governments. Over the decade, it has evolved from desktop-based systems to cloud-based systems, which are supported worldwide. In our study, all the technologies that the email uses,

like cloud servers, mobile synchronization, better interfaces, and AI-based spam filters, are recently developed technologies over the past decade. While the rest technological stack for emails grew significantly over the decade, cryptographic changes were never made. Emails still use traditional methods like RSA and ECC, which can not protect the data from quantum attacks over time. From studying Shor's and Grover's algorithms, we could understand that performing factorization of large integers and probabilistic searches could be done really fast with better confidentiality, integrity, and authenticity [1]-[3].

With the growing understanding of quantum computing, it introduced the "Harvest Now, Decrypt later" concept in short HNDL. This concept explains how encrypted communications of today can be stored and decrypted later when quantum systems become available. To counter this, researchers around the world started to work on two promising approaches: The Quantum Key Distribution (QKD) and Post Quantum Cryptography (PQC). QKD inherits principles of quantum mechanics along the way from the no-cloning theorem to secure key exchange, which helps in intrusion detection by changing the quantum signals [3], [9], [10]. On the other hand, the PQC algorithm works based on complex mathematical problems (such as lattice-based and hash-based schemes) that are computationally not solvable even for quantum computers [5].

The standardization of PQC algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium was solely led by the National Institute of Standards and Technology (NIST). These algorithms serve as strong foundations for post-quantum security frameworks [5]. From our research, we found that QKD provides the best security, but has a few drawbacks, such as the need for specialized hardware to generate keys and complex implementations. This makes the use of QKD harder at the current time. PQC, being a software, does not have the same issue as QKD and provides smooth and easy implementations, but lacks an in-built mechanism for intrusion detection. So, by combining them, it gives rise to a hybrid architecture that provides balance between scalability and quantum resilience [6], [7].

From our research on current encrypted email services like ProtonMail, we discovered that it provides excellent security through end-to-end encryption, but ProtonMail still uses traditional cryptographic methods. The main drawback of this is that it does not connect to existing software like Gmail and does not have a multiple-level encryption system [4]. Researchers, namely Basha and Saiteja, attempted to integrate quantum and post-quantum security, calling it the QSECA [1]. Sharon et al [2] created a Quantum Messaging Application that stuck to simulated environments, and this could not determine any real-world deployment.

To overcome these challenges, we developed an application that could run on three levels of encryption (TLS, PQC + AES-256, and One-Time Pad OTP + Simulated QKD) and provide the user with easier access to quantum-level security. We plan to allow the user to log in through Gmail, which provides the user with more accessibility.

This could be used as a model to work on future upcoming technologies like 6G and quantum systems.

2 LITERATURE SURVEY

The advancement of quantum computing has shown growth in major research into quantum communication systems. Basha and Saiteja [1] designed the Quantum Secure Email Client Application (QSECA), which functions and lives in a hybrid model by using Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) to provide secure end-to-end email communications. This initial implementation supported a hybrid encryption with a user-friendly interface, but only through simulated quantum keys. Sharon et al. [2] created a Quantum Encrypted Messaging Application using simulated quantum key management and PQC for authentication purposes, providing evidence of quantum secure messaging.

G. S. Parvathi et al.[3] designed a QKD-based secure email model which ensures confidentiality and integrity through quantum-generated keys combined with encryption. Though effective, the system did not have live hardware validation, as well as large-scale performance evaluations. Proton Technologies [4] created ProtonMail, an end-to-end encrypted email service based on OpenPGP and AES-256. This helped establish a strong privacy base, but it can still be compromised by a quantum attack based on dependence on classical cryptography. The National Institute of Standards and Technology (NIST) was responsible for ingesting PQC [5]. This included formalising algorithms such as CRYSTALS Kyber and CRYSTALS Dilithium as secure post-quantum standards. These developments are a step towards the practical use of hybrid cryptographic schemes, bringing together classical and post-quantum. Ghashghaei et al. [6] also improved QKD systems by introducing authenticated encryption algorithms based on PQC into settings that are based on classical channels, demonstrating proof of concept to show that it could be used with a similar performance. Stebila et al. [7] extended this work by using the hybrid key establishment in TLS and SSH. This was a demonstration signal that there is not only a technical avenue to coexist if you can use backwards-compatible hybrid PKCS, but that it can also logically coexist.

Broader analyses done by Mumtaz and Guizani [8] and Manzalini [9] identified that QKD and PQC as foundational elements of next-generation 6G and for quantum internet infrastructures. They managed to highlight the convergence of artificial intelligence, quantum communication, and network security. Dutta and Bhuyan [10] further unified the theoretical and implementation perspectives of quantum communication protocols such as BB84 and E91, emphasizing their relevance to practical, tamper-evident data exchange.

Collectively, these studies confirm that integration of QKC and PQC within a hybrid framework is possible and is the most practical and logical path towards post-quantum communication. The insights from prior prototypes, standardisation efforts, and network research can help directly in QMail's hybrid QKD/KEM architecture.

3 METHODOLOGY

We designed QMail to be a hybrid cryptographic email client that uses a PQC algorithm and simulated QKD to send and receive end-to-end encrypted emails. We focused on building a secure system architecture, multiple encryption levels, and a key management process to ensure that the requirements of a quantum-secure email can be met.

The hybrid approach of QMail is meant to be practical, efficient, and secure against both classical and quantum threats. The different levels of encryption ensure both a convenient encryption standard and maximum security. We designed QMail to work with the current infrastructure and be scalable in the future.

3.1 System Architecture

The three essential components of QMail are a React.js frontend component, a FastAPI backend component, and a PostgreSQL database. The frontend comprises a simple yet functional UI to help compose and view messages, while the backend runs the complex tasks of encryption, key exchange, and Gmail API integration with OAuth 2.0. The database stores device encryption keys, message metadata, and session tokens with access controls.

We deployed the 3 components independently as 3 different services on Render Cloud Service. This allows easier access to scale and modify each service with precision.

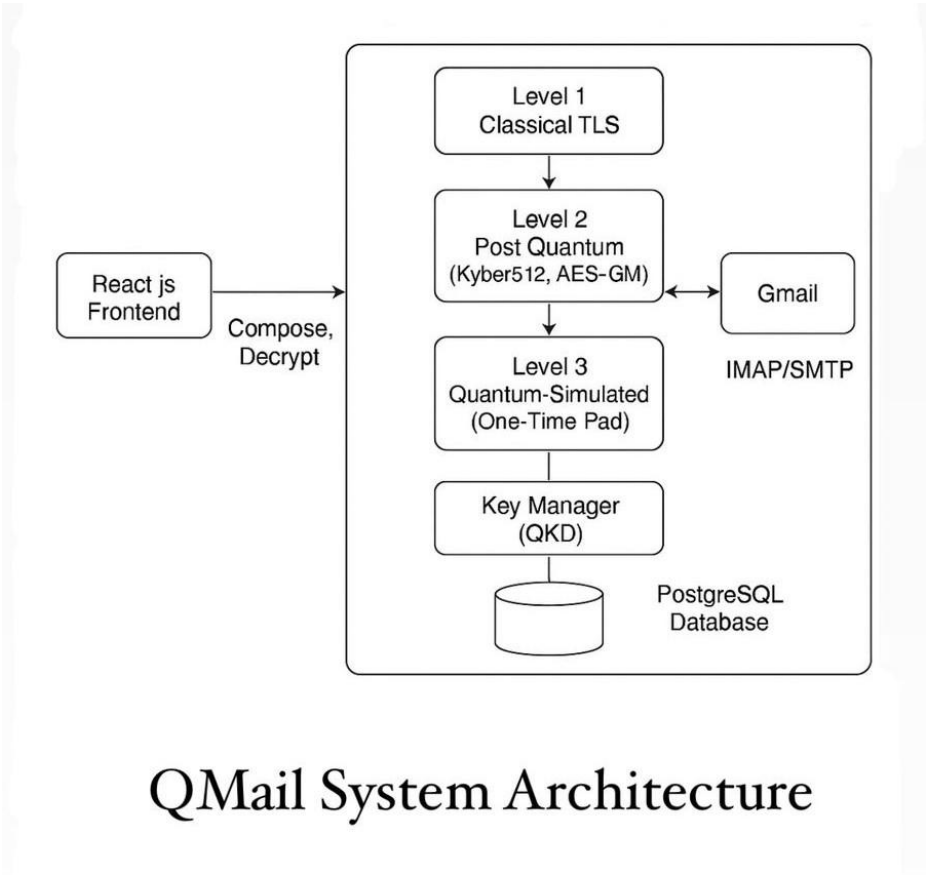

Fig. 1. QMail System Architecture

3.2 Encryption Framework

We divided QMail's encryption service into 3 different levels:

a. Level 1: Standard TLS Communication - Uses Gmail's built-in TLS for general, non-sensitive communication.

b. Level 2: Post Quantum Encryption - It uses CRYSTALS Kyber512 PQC algorithm for key encapsulation and AES-256 GCM for message encryption.

c. Level 3: One-Time Pad (OTP) with simulated QKD - A simulated quantum key exchange that generates OTP Keys. Each OTP can only be used once, and then it is discarded; this achieves security and mimics QKD principles.

3.3 System Implementation

We used the following technology stack in building QMail:

a. Frontend: React 18, TypeScript, Vite, Tailwind CSS.
b. Backend: Python's FastAPI framework and liboqs-python library for Kyber512 Post-Quantum cryptography.
c. Database: PostgreSQL with SQLAlchemy ORM.
d. Authentication: Google OAuth 2.0 (server-side flow), with an encrypted token stored in the database.
e. Deployment: Render Cloud Services.

On the backend side, we ensured it supports a zero-knowledge backend architecture, in which the private keys do not leave the client's device. Furthermore, Decryption only happens on the browser side of the application, relying on WebAssembly cryptographic libraries to ensure security. This protects end-to-end confidentiality and works perfectly with Gmail APIs.

3.4 Encryption Workflow

In each level of encryption, different steps are taken to achieve encryption. They are as follows:

Level	Algorithm used	Purpose	Encryption flow state
1	TLS (Gmail)	Basic Encryption	Direct Gmail API pass-through
2	Kyber 512+ AES 256-GCM	Post-quantum encryption	Kyber key encapsulation → HKDF → AES encryption
3	OTP + Simulated QKD	Maximum theoretical security	Pre-generated OTP, XOR cipher, single-use enforcement

3.5 Deployment and Testing

We have hosted QMail on Render Cloud Service platform as 3 separate services for frontend, backend, and database.

However, since it has been deployed as different services on a free cloud platform, there is a significant startup time for all the services to be up and running.

Currently, the testing phase checks the consistency of encryption and decryption, group communication, token management, and prevents OTP reuse between multiple devices and Gmail accounts.

3.6 Key Management and Authentication

The QMail's Key Manager (KM) manages key registration, OTP generation, and secure key wrapping with Kyber.

Users' accounts are associated with Google's OAuth-based authentication, and still retain the zero-knowledge architecture, which ensures the users' safety and protection.

Encryption and decryption happen on the client side using a secure WebAssembly cryptography library. This implies end-to-end security and that the usage of QMail ensures maximum security.

4 RESULTS AND FINDINGS

We have successfully created QMail to deliver the system requirements of a secure end-to-end quantum-resistant email client application. The prototype is hosted and deployed on Render Cloud. The performance is consistent and is proven to be both scalable and user-friendly.

4.1 Functional Results

The testing we have done showed that all the key features of QMail work as intended. Users can log in using Google OAuth 2.0 (users' Gmail ID), which uses session tokens and automatically refreshes in the background. Mails can be sent over all three layers of encryption (standard TLS, post-quantum using Kyber512 + AES-GCM, and OTP with simulated QKD.

The decryption takes place on the client-side, following the zero-knowledge architecture. Furthermore, the group emails run smoothly using the shared AES-256 keys that are individually distributed to each member through Kyber encryption. We intentionally did not implement the level 3 encryption for group messages, as securely distributing unique keys for all the users is highly resource-intensive and requires more computations. The inbox also displays "Quantum Protected"; this will help users easily identify the level of protection for each message.

4.2 Deployment Summary

The 3 components of QMail are deployed on Render in the following services:

a. Frontend: qmail-frontend.onrender.com
b. Backend: qmail-backend.onrender.com
c. Database: Managed PostgreSQL instance

The environment is free and guarantees auto-scaling, enforced HTTPS, and availability. Environment variables, which include Google OAuth, session keys, and database connection information, are stored securely on the platform.

4.3 Security and Performance

The Kyber512 algorithm gives strong post-quantum protection from RSA quantum attacks, while the AES-256-GCM cipher provides data integrity.

The Level 3 OTP encryption is meant for extreme safety via OTP and simulated QKD, both of which are unattainable by attack. Usually used for short but important emails.

It is also worth noting that each email sent is encrypted with a unique key, which guarantees email security while also limiting threats to security. In real-time use, the operation of the system's security is stable.

4.4 Key findings

a. Quantum-safe Communication:
The hybrid use of PQC algorithms and simulated QKD manages to achieve strong defence against all types of cyber-attacks.

b. User Privacy:
The client-side decryption adds end-to-end security and ensures the user data is not compromised.

c. Performance and Usability:
QMail provides multiple levels for the user to send and receive messages. This adds to the easier usage of the application. Furthermore, it adds to the performance as emails can be sent based on their importance.

d. Scalable Design:
The QMail right now provides security using simulated QKDs. This can always be scaled to use keys generated by quantum hardware systems when they are commercially available. It can be used as a foundation to build higher security measures and applications, like for 6G.

e. Seamless Integration:
QMail works with Gmail's API and OAuth for user login. This shows that PQC algorithms can be added to existing platforms.

4.5 Quantitative Results

The following scenarios were verified successfully:

Test Case	Expected outcome	Result
OAuth Flow	Successful login and token refresh	Passed
PQC Encryption	Correct decryption with the recipient's key	Passed
OTP Reuse Prevention	Unique OTP per message	Passed
Token Persistence	All group members decrypt the message	Passed
Group Encryption	Valid session over 1+ hour	Passed

5 CONCLUSION

The QMail system successfully illustrates the use of Post-Quantum Cryptography (PQC) and simulated Quantum Key Distribution (QKD) in a real email communication system. It achieves a balance between quantum resilience, usability, and system scalability by blending a Kyber-based key encapsulation, AES-GCM encryption, and One-Time Pad (OTP) for higher security levels.

We have used a three-component architecture, a zero-knowledge backend, and client-side decryption to preserve the principle of data privacy while providing a simple ability to interface with Gmail and other cloud-based email services.

This research we have conducted serves as proof of concept that assesses the possibility of a hybrid cryptographic architecture to support modern communication system security from emerging quantum threats.

While Level 3 encryption (OTP + QKD) offers the highest theoretical level of security, it is not currently practical for larger or group communication due to the generation and distribution of OTPs. As a result, Level 2 encryption using PQC is the most practical solution for scalable email transmission that aims to be quantum safe.

6 FUTURE SCOPE

As new versions of QMail are released, the site could become a fully fledged quantum-integrated email site, incorporating real QKD hardware and PQC commercial standards accepted by NIST. This could enhance the site with features, like AI-based anomaly detection for security monitoring via alerts based on real-time phishing or intrusion attempts.

We can expect the services to be migrated to a larger cloud provider or a private cloud to either scale it or make it more secure. Furthermore, we can implement anti-screenshot and device-bound technology, adding more layers of security.

Future generations of supporting enterprise-level deployment, multi-user collaboration, and cross-platform integration adoption will improve its usability and scalability. Plus, the future integration of blockchain-based software for identity management and QRNGs will further increase users' trust, transparency, and true quantum randomness in the key distribution process.

Currently, we have evidence that QMail is indeed bridging research-based cryptography advancements and developments to real-life implementation through quantum secure communication systems and positioning for future 6G network development, along with the quantum internet.

ACKNOWLEDGEMENT

Thank you to Dr. Joseph Michael Jerard V, Professor, School of Computer Science and Engineering at Presidency University for providing us with continuing guidance, feedback and support during our research.

REFERENCES

1. Basha, M. S. H., & Saiteja, P. "Quantum Secure Email Client Application." *Journal of Nonlinear Analysis and Optimisation*, vol. 16, no. 1, (2025).
2. R. G. Sharon, A. S. Kumar, and A. Mayan, "Quantum Encrypted Messaging Application: Harnessing Quantum Mechanics for Secure Communication," in *2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*, Dehradun, India, pp. 211–216 (2024).
3. G. S. Parvathi, K. N. Reddy, K. Harini, and K. Akshaya, "Revolutionizing Email Security with Quantum Key Distribution for Enhanced Data Protection in Communication Systems," Journal of Computational Analysis and Applications, vol. 33, no. 8, pp. 1426–1437, (2024).
4. Proton Technologies AG, "ProtonMail Security Features," Whitepaper, 2023.

5. NIST, “Post-Quantum Cryptography Standardization,” National Institute of Standards and Technology, (2023).
6. A. Ghashghaei, A. A. Ahmadi, A. Sadeghi, and M. Esmaeili, “Enhancing the Security of Classical Communication with Post-Quantum Authenticated-Encryption for QKD,” Computers, vol. 13, no. 7, p. 163, MDPI, (2025).
7. D. Stebila, T. K. D. Nguyen, and M. Mosca, “Prototyping Post-Quantum and Hybrid Key Exchange and Authentication in TLS and SSH,” in Proc. 2nd NIST PQC Standardization Conference, Gaithersburg, MD, USA, (2019).
8. S. Mumtaz and M. Guizani, "An overview of quantum computing and quantum communication systems," *IET Quantum Communication*, vol. 2, no. 3, pp. 136–138, doi: 10.1049/qtc2.12021 (2021).
9. A. Manzalini, "Quantum Communications in Future Networks and Services," *Quantum Reports*, vol. 2, no. 1, pp. 221–232, doi: 10.3390/quantum2010014 (2021)
10. H. Dutta and A. K. Bhuyan, *“Quantum Communication: From Fundamentals to Recent Trends, Challenges and Open Problems,”* arXiv preprint arXiv:2406.04492, (June 2024)