Rakheeba Taseen

Rakheeba Taseen-QMail Research Paper (2).pdf

Quick Submit

Quick Submit

Presidency University

Document Details

Submission ID
trn:oid:::1:3407720804

Submission Date
Nov 12, 2025, 1:46 PM GMT+5:30

Download Date
Nov 12, 2025, 2:11 PM GMT+5:30

File Name
QMail_Research_Paper_2.pdf

File Size
336.0 KB

6 Pages

3,131 Words

18,173 Characters

5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography

Match Groups

18 Not Cited or Quoted 5%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

2% Internet sources
4% Publications
1% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **18** Not Cited or Quoted 5%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

2% Internet sources
4% Publications
1% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Publication	"Quantum Protocols in Blockchain Security", Springer Science and Business Medi... 1%
2	Student papers	Presidency University <1%
3	Publication	Prateek Singhal, Pramod Kumar Mishra, Mokhtar Mohammed Hasan. "Quantum ... <1%
4	Publication	Sushil Kumar Singh, Rajendrasinh B. Jadeja, Ashish Khanna, Pushan Kumar Dutta,... <1%
5	Internet	avasant.com <1%
6	Internet	www.cysecurity.news <1%
7	Internet	www.mdpi.com <1%
8	Internet	quantumzeitgeist.com <1%
9	Internet	www.igi-global.com <1%
10	Internet	eprint.iacr.org <1%

QMail: Hybrid Quantum Secure Email Client Application

Achal K A
B.Tech CSE
Presidency University
Bengaluru, India
achalacharya07@gmail.com

S Pranav Roy
B.Tech CSE
Presidency University
Bengaluru, India
roy.sugavasi@gmail.com

Rudraraju Satvik Varma
B.Tech CSE
Presidency University
Bengaluru, India
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. It poses a threat to current encryption algorithms, which are effective today but will be obsolete to Shor's and Grover's algorithms (Quantum algorithms), compromising 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 features a user-friendly interface to choose between three levels of encryption, including OTP. The results show that QMail ensures end-to-end security and provides resilience against adversaries with quantum capabilities. QMail establishes a foundation for a scalable, quantum-safe communication platform and 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.

I. INTRODUCTION

Email remains the most used communication system by companies and governments. Over the decade, it 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].

It was solely the NIST who standardised PQC algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium, which will serve as a strong foundation for post-quantum security frameworks [5]. We found from our research that

QKD is the most secure protocol; however,it has some drawbacks in terms of the generation of keys through specialized hardware and its complexity of implementation. These make the use of QKD difficult at present. In contrast to QKD, PQC is a software-based solution and does not suffer from the same issues as the above-mentioned disadvantages of QKD. Although PQC may provide smooth and simple implementations, there are no inherent mechanisms within this solution for intrusion detection. Therefore, when these two are combined, they create a hybrid architecture that creates balance between scalability and quantum resilience [6] [7].

Based on our research about the current use of encrypted services (like ProtonMail) for sending Email, we found that ProtonMail has great security capabilities through its use of end-to-end encryption; however, while ProtonMail uses traditional cryptographic techniques, it is not able to interface with current software such as Gmail and it does not have an multi-layered encryption system in place [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.

II. LITERATURE SURVEY

The advancement of quantum computing has shown growth in major research into quantum communication systems. The QSECA developed by Basha and Saiteja [1], uses a hybrid model of operation to provide secure email client applications for users who require secure end-to-end email communications by utilizing Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). The hybrid model utilized for the QSECA is an initial implementation that used both PQC and a user-friendly interface; however, it was limited in its ability to use actual quantum keys via simulation. 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. The above was an example of a demonstration that there is both technically viable and logically viable means to co-exist in a backward-compatible hybrid PKCS model.

More in-depth analysis has been done on this topic by Mumtaz and Guizani [8], and Manzalini [9] which have shown that QKD and PQC are foundational technologies for future generation 6G networks, and will be used as part of the infrastructure for quantum Internet. In addition, they have demonstrated how AI, QC, and Network Security will converge. Dutta and Bhuyan [10] have demonstrated how QCP's such as BB84 and E91 are relevant to practical, tamper evident data exchange.

Collectively, these studies demonstrate that it is possible to integrate QKC and PQC into a hybrid model, and represents the best practical and logical route forward towards post-quantum communications. The insights from prior prototypes, standardisation efforts, and network research can help directly in QMail's hybrid QKD/KEM architecture.

III. METHODOLOGY

We have developed QMail as an email client using a hybrid method for providing end-to-end

encryption of emails via a PQC (Post Quantum Cryptography) algorithm and simulated QKD (Quantum Key Distribution).

Our primary focus was on developing a hybrid secure system architecture which would provide multi-level encryption capabilities and a key management function in order to meet the needs of an email system that is secure against classical and quantum attacks.

Our hybrid approach to QMail is intended to provide a practical solution to users that will be both efficient and secure against all possible threats.

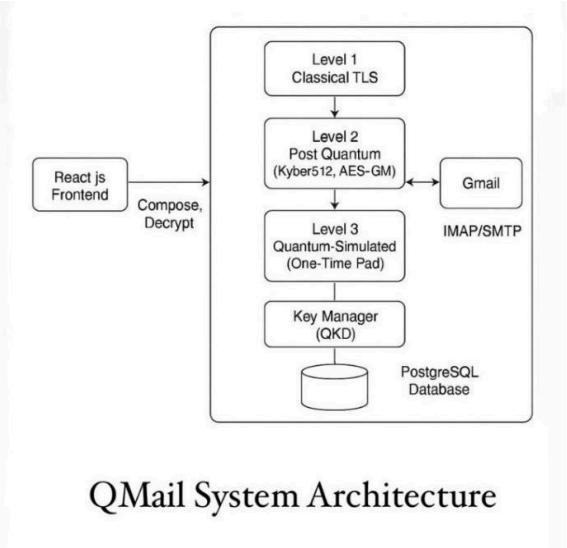
By having multiple layers of encryption we have provided two goals; first, the user has a convenient encryption standard to use, second, the overall security of the system is maximized.

QMail is intended to be compatible with the existing infrastructure of most Internet Service Providers and to also be scalable to support future developments.

A. System Architecture

The three core components for QMail include a React.js frontend component, a FastAPI backend component, and a PostgreSQL database. The frontend contains an easy-to-use yet functional user interface to assist in writing and viewing emails; the backend handles all of the complex functions including encryption, key exchange, and connection to Gmail via the Gmail API using OAuth 2.0. The database stores device encryption keys, message metadata, and session tokens along with access controls.

Each of the three components were run separately as individual applications on the Render Cloud Services platform. The separate nature of the three provides better ability to scale or make modifications to each application individually.



QMail System Architecture

B. Encryption Framework

QMail's encryption service was split into three levels of encryption:

level 1 - Standard TLS communications

uses Gmail's standard TLS communications for normal or low sensitivity email communication;

level 2 - post quantum encryption

uses a PQC (post quantum cryptography) algorithm called "CRYSTALS Kyber512" for the generation of keys and aes-256-gcm for encrypting messages;

level 3 - one-time pad (otp) using simulated qkd

uses a simulated quantum key exchange to generate an otp (one time pad), each otp is only usable once and after that is deleted from memory; provides confidentiality similar to qkd.

C. System Implementation

We chose a number of technologies to create our version of Qmail as follows:

a. Frontend - The front end will be created using: React 18, Typescript, Vite and tailwindcss.

b. Backend - fast api (python) will be our server side framework and we will also use liboqs-python for post-quantum kyber512 server-side cryptography support.

c. Database - PostgreSQL will be our database and we will use SQLAlchemy to handle our data storage needs.

d. Authentication - We will use google oauth 2.0 for our server side authentication flow and will then store the encrypted token in our database.

e. Deployment - Our application is hosted at render cloud services. To add additional server-side functionality to provide a completely zero-knowledge backend we implemented the following: to keep the client from transmitting their private keys across the internet. To allow decryption to occur only on the client-side of the application using web assembly based cryptographic libraries for both decryption and rendering. This provides the user with complete end-to-end confidentiality while allowing them to interact with the Gmail APIs.

D. 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 +Simulted QKD	Maximum theoretical security	Pre-generated OTP, XOR cipher, single-use enforcement

E. 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.

F. 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.

IV. 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.

A. 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.

B. Deployment Summary

The 3 components of QMail are deployed on

Render in the following services:
- Frontend: qmail-frontend.onrender.com
- Backend: qmail-backend.onrender.com
- 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.

C. 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.

D. 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.

E. 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

V. 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 practical currently 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.

VI. 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.

VII. 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, 2024, pp. 211–216.

[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, 2021, doi: 10.1049/qtc2.12021

[9] A. Manzalini, "Quantum Communications in Future Networks and Services," *Quantum Reports*, vol. 2, no. 1, pp. 221–232, 2020, doi: 10.3390/quantum2010014

[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