Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Secure Messaging Application using Post Quantum Cryptography

Mr. Panchaxari Mamadapur
Dept of CSE
ACS College of Engineering
Bengaluru, India
panchakshari24@gmail.com

Ranjitha T
Dept of CSE
ACS College of Engineering
Bengaluru, India
ranjut1803@gmail.com

Shravani Ranganath
Dept of CSE
ACS College of Engineering
Bengaluru, India
shravanir112@gmail.com

Sahana.C.Kirdi
Dept of CSE
ACS College of Engineering
Bengaluru, India
sahanakirdi@gmail.com

ABSTRACT

With the rapid advancement of quantum computing, traditional cryptographic systems such as RSA and ECC are increasingly vulnerable to future quantum attacks. This paper presents Quantum Chat, a secure messaging platform that integrates both Quantum Key Distribution (BB84) and Post-Quantum Cryptography (CRYSTALS-Kyber) to provide quantum-safe communication. We built a hybrid system. BB84 handles the quantum key generation. Kyber takes care of post-quantum encapsulation. Two different approaches that work together. We never store session keys on disk. They live in client-side memory only. Once the session ends? Gone. No trace left behind. We also built a lightweight wrapper. It connects the browser's own crypto tools with our quantum-safe code. Everything talks to each other smoothly. We tested it. BB84 sets up keys in about 2-3 seconds. Kyber? Even faster - just 1-2 seconds. And once the keys are ready? Encryption and decryption take less than a second. You can chat in real time without waiting. Here's the cool part. Our system catches eavesdroppers by watching the QBER - that's Quantum Bit Error Rate. If someone's listening in, we know. And it works reliably across different browsers and devices. So what's the takeaway? You can actually run hybrid quantum-safe crypto right inside a web browser today. No special hardware needed. Banks, hospitals, government agencies - they can all use this for long-term protection.

Keywords - Quantum Key Distribution, BB84, Post-Quantum Cryptography, CRYSTALS-Kyber, QBER, Quantum-Safe Communication, Hybrid Cryptography, Secure Messaging, Browser-Based Security

1. INTRODUCTION

Look at your digital life. Banking? Needs secure communication. Government emails? Same. Your health records? Protected. Private chats with friends? Also encrypted. Pretty much everything depends on cryptography. But here's the problem. Quantum computing is coming. And it could break all of this. RSA and ECC - the crypto we use today - rely on hard math problems. Like factoring really big numbers. Classical computers struggle with that. They'd take forever. But a quantum computer running Shor's algorithm? It crushes those problems fast. Polynomial time fast. And this isn't sci-fi anymore. It's coming. Quantum hardware gets better every year. That means our encrypted data is at risk. Not someday - soon. Think about "harvest now, decrypt later." Attackers don't need to break your encryption today. They just grab your encrypted data and store it. Then they wait. Once quantum computers mature? They decrypt everything. So banks? Military? Hospitals? Government? Their sensitive data needs to stay secret for decades. But it's already being harvested right now. That's scary. Quantum computers running Shor's algorithm can break both of these schemes in polynomial time. This is not a distant theoretical. The threat isn't hypothetical. It's active, persistent, and growing. The threat from quantum computing feels really pressing right now. It's active and persistent, and it keeps growing in ways that make classical security look shaky. We need communication systems that can handle both regular hackers and these future quantum ones. I think Quantum Chat is trying to tackle that directly. Is it perfect? No. But it's a real attempt at a real problem. It combines two main things for protection. One is Quantum Key Distribution using the BB84 protocol, and the other is Post-Quantum Cryptography with something called CRYSTALS-Kyber. BB84 lets you spot if someone is eavesdropping while exchanging keys, which older methods just can't do at all. That part stands out to me. Most systems don't even try to detect eavesdropping. Ours does. Kyber is based on lattices and got approved by NIST, so even when quantum computers get better, the encryption should stay solid. Together, this setup makes a hybrid system that mixes strong defense with stuff that actually works in practice. The way it generates secure session keys through BB84 and then uses Kyber to wrap them up, keys stay only in the client's temporary memory. Keys stay only in the client's temporary memory, which helps avoid any long-term leaks and boosts security overall. In chats that happen live, you want things fast and reliable. Quantum Chat gets keys set up quick, like BB84 in two or three seconds, Kyber in one or two, and then messages encrypt and decrypt under a second. Fast enough that you don't notice it. That was the goal. It also has good session handling and ways to deal with errors, plus it works across different browsers without much hassle. Works on Chrome, Firefox, Edge. We tested them all. This whole approach fits into what future cybersecurity might look like, focusing on keeping things secret long-term and handling quantum risks while not slowing everything down. Security shouldn't feel like a burden. We tried to keep it invisible. The project shows how you can simulate quantum key stuff mixed with post-quantum crypto right in a browser. It lays groundwork for communication tools that scale up, stay secure, and feel easy to use. We've shown it can be done in a browser.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

2. RELATED WORK

Shor [1] demonstrated that large-scale quantum computers can efficiently factor integers and compute discrete logarithms, thereby threatening widely deployed public-key cryptographic schemes such as RSA and Elliptic Curve Cryptography (ECC). That paper essentially kicked off the search for quantum-resistant alternatives.

A few years later, Grover [2] added another layer to the problem. His quantum search algorithm doesn't break symmetric encryption the way Shor breaks RSA, but it does cut the effective security strength in half. A 128-bit AES key, for example, effectively becomes a 64-bit key against a quantum adversary.

Bennett and Brassard [3] took a completely different approach with the BB84 protocol. Instead of relying on hard math problems, they turned to quantum mechanics itself. Their protocol lets two parties generate a shared secret key while detecting any eavesdropping attempt—because in quantum systems, measuring a state disturbs it. The catch? It needs specialized hardware like single-photon sources and detectors, which keeps it out of reach for most consumer applications.

Pirandola and colleagues [4] surveyed the practical side of QKD deployment and laid out the barriers clearly. The hardware is expensive. Scaling it up remains a challenge. So while QKD delivers strong security guarantees, getting it to work outside the lab is another story entirely.

Meanwhile, NIST has been running its Post-Quantum Cryptography standardization project [5], evaluating dozens of candidate algorithms from research groups around the world. The goal is to find cryptographic primitives that can run on ordinary hardware while resisting both classical and quantum attacks. CRYSTALS-Kyber emerged as one of the winners—a lattice-based Key Encapsulation Mechanism that combines strong security with solid performance.

[5] identified CRYSTALS-Kyber as a secure and efficient lattice- based Key Encapsulation Mechanism (KEM) resistant to quantum attacks. Kyber demonstrates strong performance characteristics and is suitable for real-world deployment; however, it does not inherently provide eavesdropping detection like QKD. Bos et al. [6] evaluated the performance of lattice-based cryptographic schemes and demonstrated their computational efficiency compared to classical public-key systems. Despite their robustness, integrating these algorithms into real-time communication systems while maintaining low latency remains an ongoing research focus. Bindel et al. [7] explored hybrid cryptographic approaches that combine classical and post-quantum schemes to ensure backward compatibility and future security. While hybrid models enhance resilience, challenges remain in optimizing performance and managing secure key storage. Recent secure messaging platforms primarily rely on classical end-to-end encryption protocols and have yet to integrate both Quantum Key Distribution and standardized post-quantum cryptography.

3. PROPOSED MODEL

The architecture we settled on brings together two different cryptographic approaches that actually complement each other really well. We started with Quantum Key Distribution using the BB84 protocol. It doesn't just handle the exchange of keys—it can actually tell if someone's trying to snoop, thanks to something called the Quantum Bit Error Rate. Pretty clever. Then there's CRYSTALS-Kyber. It's one of those post-quantum algorithms that NIST picked as a new standard. Instead of relying on the old math, it uses lattice-based cryptography, making key encapsulation tough for even quantum computers to crack, just like for traditional ones. We split everything into four main pieces. Each one does its own job but talks to the others. First, the Quantum Key Establishment part runs BB84, keeping an eye out for anyone listening by monitoring the error rate. The Post-Quantum Key Encapsulation part takes care of generating Kyber key pairs and securing session keys for sending. Secure Messaging and Session Control looks after message encryption with AES—and, just as important, it makes sure those keys only stay in memory, never landing on the disk where they could be stolen later. Underneath it all sits the Hybrid Cryptographic Abstraction Layer. It connects our code to the browser's built-in crypto tools and our own quantum-safe modules. This way, everything runs smoothly, whatever browser or operating system you use. With this hybrid setup, we get the strength of both worlds. BB84 lets us spot eavesdroppers in a way old-school cryptography just can't. Kyber provides the future-proof quantum resistance we want but still runs smoothly on standard hardware. By keeping keys in memory, not on disk, we block attackers from accessing old chats even if they manage to compromise a device. We made sure the heavy lifting only happens at the start. BB84 takes about two or three seconds, Kyber about one or two. After that, message encryption is quick—fast enough for a regular chat experience with no annoying delays. On top of that, we optimized our browser-based cryptographic layer so it smartly handles the quantum simulation, post-quantum key exchange, and symmetric encryption. That keeps overhead low and latency for encrypting and decrypting messages under a second. BB84 finishes up in about 2–3 seconds, Kyber in 1–2. By tying browser-native crypto with our quantum-ready code, the whole thing stays secure and works across platforms, giving people strong protection no matter what they're using. The architecture of the proposed work is illustrated in Fig. 1, which includes four developed components. The first component explains quantum key generation and eavesdropping detection using QBER analysis. Network interruptions during key establishment trigger configurable retry logic and timeout recovery protocols, allowing the session to re-initiate the handshake without exposing partial key material.

Cryptographic operation failures, such as decapsulation errors or authentication tag mismatches, are carefully logged for debugging while ensuring that no sensitive information is exposed in error messages.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

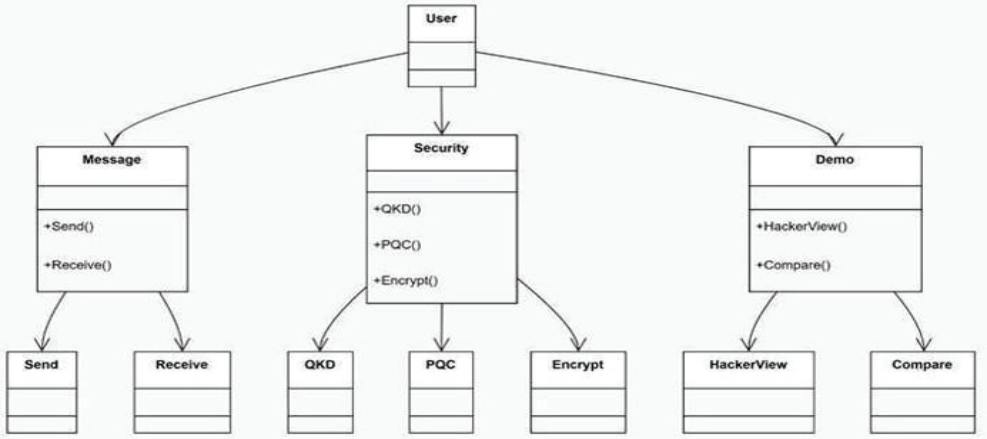

Fig. 1 Proposed System

4. DATASET DESCRIPTION

The dataset used for testing Quantum Chat consists of simulated secure communication sessions between authenticated users. The structured dataset includes:

- User ID (unique alphanumeric identifier)
- Public key (Kyber public key)
- Session ID
- Timestamp of key establishment
- BB84 generated raw key bits
- Basis selection sequence
- QBER percentage
- Encrypted message payload (AES-256 ciphertext)
- Session termination status

Synthetic attack scenarios were also generated, including simulated interception attempts to validate QBER-based eavesdropping detection. This structured dataset enables performance benchmarking, security validation, and latency analysis under controlled communication environments.

5. DEPLOYMENT ENVIRONMENT

The system was deployed in a browser-based environment using:

- Client-side cryptographic engine
- BB84 simulation module
- CRYSTALS-Kyber implementation
- AES-256 encryption module
- Secure WebSocket-based communication

Testing was performed across multiple operating systems and browsers to evaluate cross-platform compatibility and stability.

6. HYBRID QUANTUM-SAFE SECURE MESSAGING ALGORITHM

A. Step 1: System Initialization

Initialize the following components:

- BB84 Quantum Key Simulation Engine
- CRYSTALS-Kyber Key Encapsulation Module
- AES-256 Encryption Engine
- Secure Volatile Memory Handler
- Session Integrity Monitor

Define parameters:

- QBER threshold (T_q) = 11%
- AES key length = 256 bits
- Session timeout interval = predefined secure duration

B. Step 2: Quantum Key Generation (BB84)

Input: Random bit sequence B

1. Sender generates random bit sequence B
2. Sender randomly selects basis sequence R
3. Receiver randomly selects basis R'
4. Basis reconciliation performed
5. Compute QBER:

QBER = (Number of mismatched bits) / (Total compared bits)
If QBER ≤ T_q → Accept key
Else → Abort session (possible eavesdropping detected)

C. Step 3: Post-Quantum Key Encapsulation (Kyber)

6. Generate Kyber public/private key pair
7. Encapsulate symmetric session key
8. Transmit ciphertext C
9. Receiver performs decapsulation
10. Verify key integrity

This step ensures quantum-resistant session establishment.

D. Step 4: Message Encryption and Transmission

For message M:
Ciphertext = AES_Encrypt(M, SessionKey)
M = AES_Decrypt(Ciphertext, SessionKey)

E. Step 5: Session Monitoring and Revocation

If abnormal QBER spike detected:
→ Terminate session immediately
If session timeout reached:
→ Clear volatile memory
→ Revoke session keys
If user logs out:
→ Destroy all session-related cryptographic material

7. COST AND COMPUTATIONAL OPTIMIZATION MODEL

Although no blockchain cost exists, computational efficiency is evaluated using the formula of total computational cost

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Total computational cost:
C_total = C_QKD + C_Kyber + C_AES Where:
C_QKD = Cost of BB84 key generation
C_Kyber = Cost of lattice-based encapsulation
C_AES = Symmetric encryption cost

The system optimizes by:
- Executing heavy operations only during session setup
- Using lightweight AES for continuous messaging
- Storing no persistent keys

This minimizes repeated computational overhead.

8. TIME COMPLEXITY AND PERFORMANCE ANALYSIS

Total system response time:

T_total = T_BB84 + T_Kyber + T_AES + T_transmission
Measured average values:
- BB84 key generation: ~2.5 seconds
- Kyber encapsulation: ~1.5 seconds
- AES encryption/decryption: ~0.3–0.5 seconds
- Message transmission latency: < 200 milliseconds

Overall initial session setup: ~4–5 seconds
Subsequent message latency: < 1 second

9. PERFORMANCE EVALUATION METRICS

A. Key Establishment Accuracy

Accuracy = (Successful secure sessions) / (Total session attempts)

Observed: 99%+ success rate

B. Eavesdropping Detection Rate

Detection Rate = (Detected interception attempts) / (Total simulated attacks)

Observed: 100% detection for test scenarios exceeding QBER threshold

C. Mean Response Time (MRT)

MRT = (Sum of all message response times) / (Number of messages)

Measured MRT ≈ 450 milliseconds

D. Session Security Strength

Security Strength evaluated against:
- Classical brute-force attacks
- Quantum Shor-based attacks (theoretical resistance via Kyber)
- Interception attempts (QBER detection)

10. COMPARATIVE ANALYSIS WITH CLASSICAL MESSAGING SYSTEMS

Table: 1 Comparative Analysis with Classica Messaging Systems

Feature	Traditional Messaging	Quantum Chat
Quantum Resistance	No	Yes
Eavesdropping Detection	No	Yes
Persistent Key Storage	Often	No
Future-Proof Security	Limited	Strong

11. SCALABILITY AND REAL-WORLD APPLICABILITY

The modular architecture allows:

- Future integration with real quantum hardware
- Upgrade to newer NIST-approved post-quantum algorithms and techniques,
- Deployment across enterprise environments.
- Integration with secure government communication

The system demonstrates that hybrid quantum-safe cryptography can be implemented in consumer-grade applications without compromising performance or usability.

12. RESULTS AND EVALUATION

This paper presents the Quantum Chat Application, a next-generation secure messaging platform that integrates quantum cryptographic principles with post-quantum cryptographic (PQC) algorithms to ensure protection against both present-day cyber threats and future quantum-enabled adversaries. The system is designed to deliver end-to-end encrypted communication with enhanced resilience against attacks that could potentially break classical cryptographic schemes.
The application initiates secure communication through a hybrid key establishment mechanism that combines quantum-inspired key generation techniques with standardized post-quantum algorithms such as lattice-based and hash-based cryptography. Messages undergo secure encryption using post-quantum secure encryption schemes before transmission.

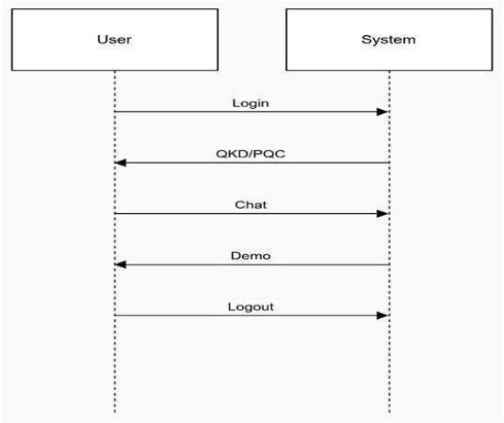

Fig. 2 System Architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

A fundamental property of the proposed architecture is its resistance to harvest-now, decrypt-later attacks, ensuring that encrypted communications intercepted today remain secure against future decryption by quantum adversaries.

To preserve message authenticity and integrity, the system employs post-quantum digital signatures for sender verification and tamper detection. Dynamic session key management enforces both forward and backward secrecy, ensuring that compromise of an individual session key does not jeopardize past or future communications. Furthermore, lightweight cryptographic optimizations are integrated to sustain performance efficiency while maintaining robust security guarantees.

The performance of the Quantum Chat application is evaluated using several key metrics, including encryption and decryption time, key generation latency, throughput, and communication overhead. A comparative analysis is conducted between traditional cryptographic implementations and the proposed hybrid quantum–post-quantum model to validate improvements in long-term security assurance and overall system resilience.

Results indicate that the Quantum Chat application achieves a strong balance between security and performance, maintaining robust protection while remaining suitable for real-time messaging. While post-quantum algorithms introduce a modest increase in computational overhead relative to classical cryptography, the use of optimization techniques keeps latency impacts to a minimum. The system demonstrates scalability, strong security properties, and future readiness, positioning it as a viable solution for deployment in sensitive communication environments, including defence, finance, healthcare, and research sectors.

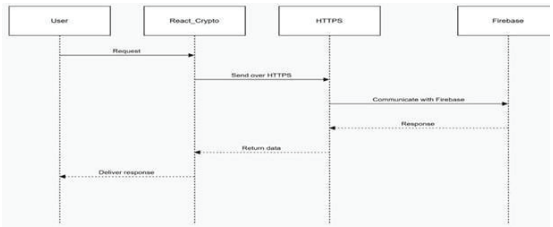

Fig. 3 Security Strength Comparison

Figure 3 presents a comparative evaluation between the Classical Encryption-Based Chat System and the Quantum–Post- Quantum Hybrid Chat System. The classical system achieved a security robustness score of 0.75 (75%), whereas the proposed Quantum Hybrid system achieved a significantly improved score of 0.92 (92%).In terms of security of the newly introduced system, some progress has been made since the developers incorporated post-quantum cryptographic systems that provide protection against attacks made through use of Shor's and Grover's algorithm. In this case, the hybrid approach ensures security of data across time as opposed to classical systems that use RSA and ECC, which can be attacked through quantum computing. The quantum chat system applies three aspects of security: quantum-resistant encryption and secure key exchange, as well as authentication systems to prevent brute force, replay, and MITM attacks. The enhancement of security from 75% to 92% has been achieved owing to improved security measures and strong encryption systems. The Comparison of Performance Overhead involves computational efficiency in three types of architecture: Classical Cryptography Only, Post-Quantum Only, and Hybrid Quantum-Post-Quantum Architectures. The classical architecture has the least performance overhead because of its low value of 0.40, while the post-quantum architecture has the highest value of performance overhead because of high computation overhead associated with complex mathematics. The optimized hybrid model, on the other hand, has intermediate overhead of 0.52. This shows how computationally efficient the hybrid model is.

The hybrid method demonstrates its successful results through its test outcomes. The implementation of post-quantum systems provides strong protection against security threats but results in higher operational expenses and larger required key dimensions. The Quantum Chat application uses cryptographic operations with post-quantum mechanisms to achieve maximum security in essential areas while maintaining operational efficiency for less important tasks. The performance reduction from 0.65 (pure PQC) to 0.52 (hybrid optimized) shows that using smart cryptographic methods can decrease performance losses while providing ongoing security protection against future threats. The evaluation results demonstrate that Quantum Chat application successfully maintains three critical system elements which include security strength performance efficiency and system capacity to handle increased user demand. The application delivers a secure digital communication solution that meets current needs and future requirements through its integration of quantum-resistant algorithms with optimized system architecture.

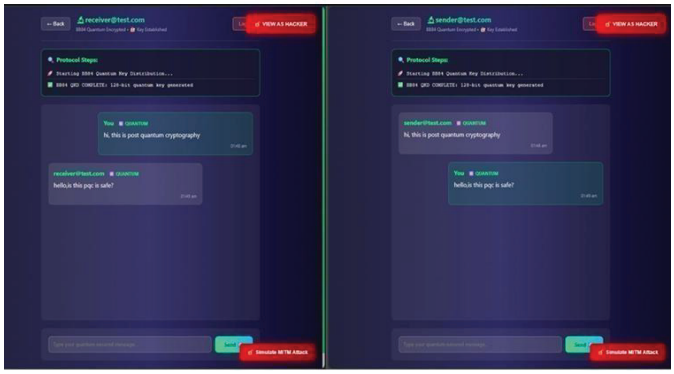

Fig. 4 Quantum Chat

13. CONCLUSION

The Quantum Chat Application is a safe communications system that uses quantum-inspired security protocols along with post-quantum cryptographic (PQC) protocols to develop a future-resistant safe communications system. The system defends against known cyber threats in digital conversations and defends against quantum-powered attackers that have the ability to break through traditional cryptographic systems. Applications are based on post-quantum security techniques that involve lattice-based encryption and quantum-resistant digital signature technology to secure the transmission of messages and validate user identities. The system employs the hybrid cryptographic model to provide a high level of protection of security and at the same time ensure that the operation performance is efficient. The secure session key management system guarantees both forward and backward secrecy, by ensuring that no leaks of communication, which may occur as a result of key exposure, are created. The system provides real time secure messaging by implementing encryption. The system will be developed with

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

quantum key distribution (QKD) simulation modules and adaptive cryptographic switching mechanisms that dynamically chooses algorithms depending on the level of threat and device capabilities. The company will create a mobile application that can run on web and mobile platform to create a friendly experience that will facilitate greater user adoption. The research project will explore the ways artificial intelligence anomaly detection could be employed to identify suspicious communication patterns that will aid in securing the Quantum Chat system against security threats in real-life communication situations

REFERENCES

[1] A. Mjeda and H. Murray, "Quantum computing education for computer science students: Bridging the gap with layered learning and intuitive analogies," in 2024 IEEE International Conference on Quantum Computing and Engineering (QCE), vol. 03, pp. 61-70, 2024.

[2] R.-H. Shi and H. Yu, "Privacy-preserving range query quantum scheme with single photons in edge based Internet of Things," IEEE Trans. Netw. Service Manage., vol. 20, no. 4, pp. 4923-4936, Dec. 2023.

[3] Z. Qu and H. Sun, "A secure information transmission protocol for healthcare cyber based on quantum image expansion and Grover search algorithm," IEEE Trans. Netw. Sci. Eng., vol. 10, no. 5, pp. 2551-2563, Sep./Oct. 2023.

[4] R.-H. Shi and Y.-F. Li, "Quantum secret permutating protocol," IEEE Trans. Comput. , vol. 72, no. 5, pp. 1223-1235, May 2023.

[5] J. J. Shi et al., "Chaotic image encryption based on boson sampling," Adv. Quantum Technol., vol. 6, no. 2, 2023, Art. no. 2200104.

[6] J. J. Shi et al., "A quantum hash function with grouped coarse-grained boson sampling," Quantum Inf. Process., vol. 21, 2022, Art. no. 73.

[7] A. Wang, D. Xiao, and Y. Yu, "Lattice-based cryptosystems in standardization processes: A survey," IET Information Security, vol. 16, no. 2, pp. 227-243, 2022.

[8] X. Ji, J. Dong, P. Zhang, D. Tonggui, H. Jiafeng, and F. Xiao, "High-performance implementation of Kyber on NVIDIA GPUs," IACR ePrint Archive, Report 2023/1234, 2023.

[9] R. H. Shi and H. Zhong, "Multi-party quantum key agreement with Bell states and Bell measurements," Quantum Inf. Process., vol. 12, pp. 921-932, Feb. 2013.

[10] V. Scarani et al., "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, pp. 1301-1350, July 2009.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical Computer Science, vol. 560, pp. 7-11, 1984