Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

6th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS

(PKIA 2025)

SEPTEMBER 3-4th, 2025

Identity-Based Secure End-to-End Quantum-Safe MQTT Communication Using Ring-LWE

Gunasekaran Raja, Sudhakar Theerthagiri, Santhosh Kumar T,

Sangeetha Ramachandran, Nandini Babu

C-DAC

https://pkiindia.in

Social Media /pkiindia

IEEE BANGALORE SECTION

OUTLINE

- Problem Statement
- Objectives
- Related Works
- Proposed System
- Architecture Diagram and Algorithm
- Results & Analysis
- Conclusion
- References

PROBLEM STATEMENT

- Traditional MQTT implementations rely on Transport Layer Security (TLS) which introduces significant overhead due to its complex certificate-based key distribution and lack of end-to-end encryption highlighting the need for true end-to-end encryption.
- Conventional public key cryptographic algorithms such as RSA and ECC are increasingly vulnerable to quantum computing threats, raising concerns about the long-term security of MQTT based communication systems.
- Existing approaches that integrate pairing-based IBE into MQTT suffer from high computational costs, including slow key generation, encryption, and decryption, which limit real-time applicability in latency-sensitive IoT scenarios

OBJECTIVES

- To design and integrate a Ring-LWE based Identity-Based Encryption scheme (RISE-MQTT) into the MQTT protocol to enable secure key exchange and post-quantum end-to-end encryption without relying on preshared secrets.
- To evaluate and compare the performance of Ring-LWE IBE with traditional pairing-based IBE in terms of key generation time, key size, encryption and decryption efficiency, and message latency, thereby quantifying the computational and security benefits of RISE-MQTT.

RELATED WORKS

Paper	Proposed Methodology	Challenges and Limitations
SEEMQTT: Secure End-to-End MQTT-Based Communication for Mobile IoT Systems Using Secret Sharing and Trust Delegation, *IEEE Internet of Things Journal, 2023.*	• Integration of Secret Sharing, Identity-Based Encryption (IBE), and Decentralized Trust Delegation. • Publisher encrypts data and splits the encryption key into shares using Shamir's Secret Sharing.	• Overhead from IBE and secret sharing on constrained devices, especially during setup. • Trust delegation management is complex and requires strict credential control.
Practical Applications of Improved Gaussian Sampling for Trapdoor Lattices, *IEEE Transactions on Computers, 2019.*	• Efficient Gaussian sampling technique for lattice trapdoors using generalized gadget matrices. • Transitioned from LWE to more efficient Ring-LWE (RLWE) constructions.	• Increased signature norm with higher bases may affect security and correctness trade-offs. • Gaussian sampling and perturbation routines are complex and may be computationally intensive.
MQTLS: Toward Secure MQTT Communication with an Untrusted Broker, *IEEE ICTC, 2019.*	• Introduced MQTLS, a modified TLS protocol tailored for MQTT and the publish/subscribe model. • Defined a novel Client-to-Broker-to-Client (CBC) security model ensuring message confidentiality even with untrusted brokers.	Initial handshake overhead due to asymmetric cryptography and Higher latency on low-end devices during key setup (up to 99.88% overhead compared to standard TLS).

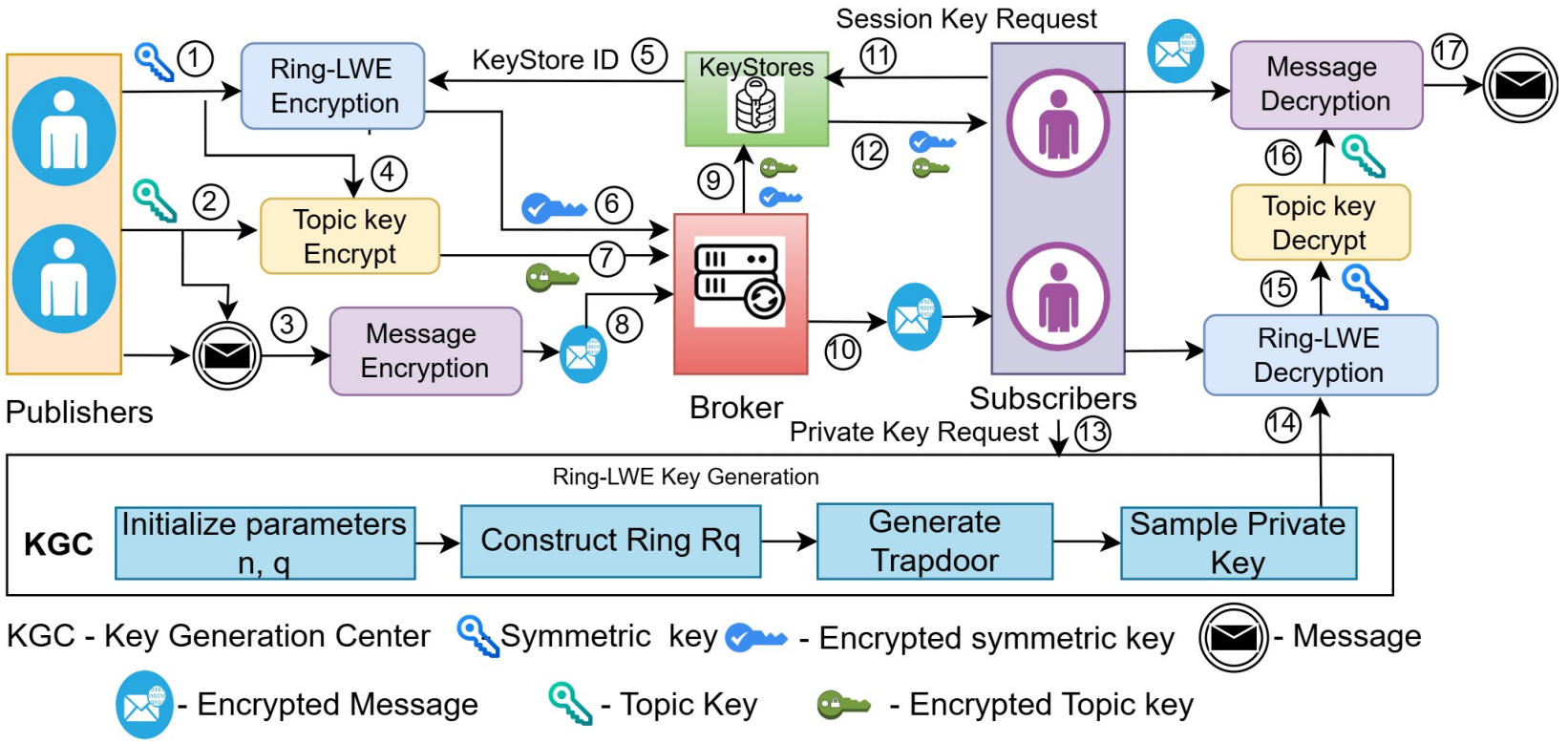
RELATED WORKS

Paper	Proposed Methodology	Challenges and Limitations
"MQTT-I: Achieving End-to-End Data Flow Integrity in MQTT, *IEEE Transactions on Dependable and Secure Computing, 2024.*	• Introduced MQTT-I protocol using Merkle Hash Trees to ensure end-to-end data flow integrity in the presence of an untrusted broker. • Ensures completeness, correctness, weak and strong liveness of MQTT message streams without requiring pre-shared keys.	• Higher initial overhead in comparison to standard MQTT due to Merkle tree construction and signature generation. • Not suitable for low QoS.
Securing the IoT Application Layer From an MQTT Protocol Perspective: Challenges and Research Prospects, *IEEE Communications Surveys & Tutorials, 2024.*	• Presented a comprehensive survey of MQTT protocol vulnerabilities and categorized them into flaws in protocol specification and implementation. • Proposed a classification of attacks and defenses by analyzing links between protocol features, vulnerabilities, and real-world threats.	• Weak built-in security in MQTT, making IoT systems highly vulnerable. • Widespread misconfiguration of MQTT brokers and inconsistent adherence to security best practices by vendors.
Assessment of the Impact of Hybrid Post-Quantum Cryptography on the Performance of the MQTT Communication Protocol, *IEEE Symposium on Internet of Things (SIoT), 2023.*	• Evaluated MQTT with hybrid TLS (classical + post-quantum crypto) using DILITHIUM and FALCON. • Measured CPU, memory, and data overhead in mutual and broker-only authentication..	• Increased overhead in memory, CPU, and network data, especially with DILITHIUM. • FALCON offers better performance for constrained environments.

PROPOSED SYSTEM

- The proposed RISE-MQTT framework integrates Ring-LWE Identity-Based Encryption into the MQTT protocol for secure key exchange and end-to-end encryption.
- Eliminates reliance on TLS and preshared keys thereby reducing key management complexity in MQTT communication.
- Ensures secure message transmission between publishers and subscribers, even through untrusted brokers, supporting confidentiality and integrity.
- Achieves quantum-resilient security with a 61.44% reduction in session key setup time, ensuring efficiency and scalability.

ARCHITECTURE DIAGRAM: RISE-MQTT



Phases of Ring-LWE IBE

❑ **The Ring-LWE Identity-Based Encryption scheme has 4 main phases.**

Setup

The Private Key Generator (PKG) generates master keys using security parameter λ;

$$A \in R_q^{n \times m}, R_q = Z_q[x]/f(x)$$

where A is *public matrix*, $f(x)$ *is cyclotomic polynomial*

Key Generation

To generate a private decryption key for a user identity ID, the PKG performs two key steps:

$$b_{ID} = H_{IBE}(ID)$$

$$A.v_{ID} = b_{ID} \bmod q$$

where, $v_{ID} \in R_q^{n \times m}$ is sampled using Gaussian Sampling (Private Key)

b_{ID} → identity mapped ring element

H_{IBE} → hash function used for identity mapping

MATHEMATICAL FORMULATION

Encryption

To encrypt message m, the sender performs:

$$C_0 = A^T . s + e_0$$

$$C_1 = b_{ID} . s + e_1$$

where, $s \in R_q^{n \times m}$ is the secret vector sampled using Gaussian sampling $e_0, e_1 \rightarrow$ Error Terms

Decryption

The receiver on receiving the encrypted message performs decryption using the private key $t = C_1 - v_{ID} \cdot C_0$

END-TO-END ENCRYPTION AND DECRYPTION ALGORITHM IN RISE-MQTT

Algorithm 1: End-to-End Encryption and Decryption in RISE-MQTT

Input : Message $M \in \{0,1\}^*$, Master Public Key (MPK), KeyStore identity ID_K, Subscriber identity ID_S, KeyStore private key v_{ID_K}, Subscriber private key v_{ID_S}

Output: Decrypted message M

/* Publisher generates and encrypts message, topic key, and symmetric key */

Step 1: Publisher-Side Encryption;

Generate topic key: $K_{\text{topic}} \leftarrow \{0,1\}^{256}$;

Generate symmetric key: $K_{\text{sym}} \leftarrow \{0,1\}^{256}$;

Encrypt message: $C_M \leftarrow \text{Enc}_{\text{AES}}(K_{\text{topic}}, M)$;

Encrypt topic key: $C_{\text{topic}} \leftarrow \text{Enc}_{\text{AES}}(K_{\text{sym}}, K_{\text{topic}})$;

/* Encrypt symmetric key using Ring-LWE IBE with keystore ID */

Derive public vector from keyStore ID: $b_{ID} \leftarrow H_{\text{IBE}}(ID_K)$;

Sample random vector: $s \leftarrow \mathcal{U}(\mathbb{R}_q)$ // Uniform Sampling ;

Sample noise vector: $e_0 \leftarrow \mathcal{D}_{\mathbb{R}^m,\sigma}$ // Gaussian Sampling;

Compute: $C_0 \leftarrow A^T s + e_0$;

Sample scalar noise: $e_1 \leftarrow \mathcal{D}_{\mathbb{R},\sigma}$;

Compute: $C_1 \leftarrow b_{ID}^T s + e_1 + \lfloor \frac{q}{2} \cdot K_{\text{sym}} \rfloor$;

Construct IBE ciphertext: $C_{\text{sym}} \leftarrow (C_0, C_1)$;

/* Keystore decrypts symmetric key and re-encrypts it for the subscriber */

Step 2: KeyStore-Side Decryption and Response;

Compute: $\iota \leftarrow C_1 - v_{ID_K}^T C_0$;

Initialize: $K_{\text{sym}} \leftarrow$ empty bit vector of length 256;

for $i = 0$ **to** 255 **do**

  if $|\iota_i| < \frac{q}{4}$ **then**

    $K_{\text{sym}}[i] \leftarrow 0$;

  else

    $K_{\text{sym}}[i] \leftarrow 1$;

  end

end

/* Encrypt symmetric key using IBE with subscriber ID */

Re-encrypt symmetric key for subscriber: $C'_{\text{sym}} \leftarrow \text{IBEEnc}(MPK, ID_S, K_{\text{sym}})$;

/* Subscriber decrypts symmetric key, then decrypts topic key and final message */

Step 3: Subscriber-Side Decryption;

Compute: $\iota \leftarrow C_1 - v_{ID_S}^T C_0$;

Initialize: $K_{\text{sym}} \leftarrow$ empty bit vector of length 256;

for $i = 0$ **to** 255 **do**

  if $|\iota_i| < \frac{q}{4}$ **then**

    $K_{\text{sym}}[i] \leftarrow 0$;

  else

    $K_{\text{sym}}[i] \leftarrow 1$;

  end

end

Decrypt topic key: $K_{\text{topic}} \leftarrow \text{Dec}_{\text{AES}}(K_{\text{sym}}, C_{\text{topic}})$;

Decrypt message: $M \leftarrow \text{Dec}_{\text{AES}}(K_{\text{topic}}, C_M)$;

return M

RESULTS & ANALYSIS

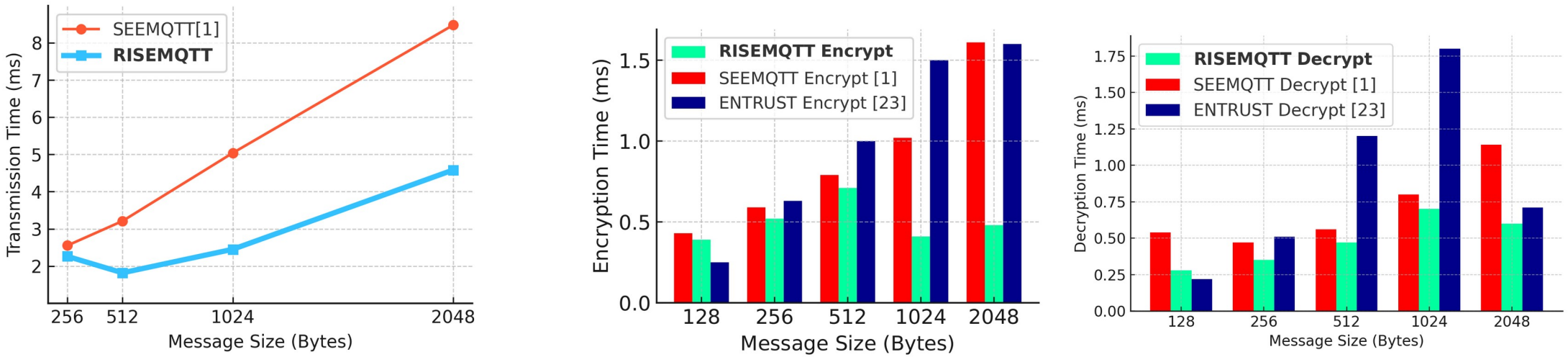


Fig. 2: Comparison of RISE-MQTT with Other Methods, Focusing on Key Performance Metrics

RESULTS & ANALYSIS (CONT.)

Experimental Outcomes:

- **RISE-MQTT achieved a 61.44% reduction in session key setup time compared to pairing-based IBE, demonstrating its suitability for real-time, latency-sensitive IoT applications.**
- **By leveraging the Ring-LWE hard problem, the proposed framework provides robust resistance against quantum adversaries, addressing the vulnerabilities of RSA and ECC in future computing environments.**
- **RISE-MQTT outperforms traditional pairing-based IBE schemes in key generation speed, encryption and decryption efficiency and maintains low message latency.**

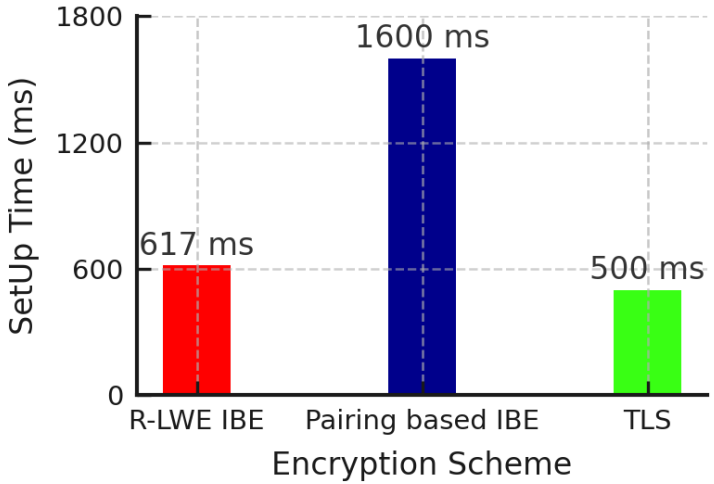


Fig. 3: Session key setup time Comparison of R-LWE with pairing based IBE and TLS

CONCLUSION

- Experimental efforts with the RISE-MQTT framework have led to significant advancements in securing IoT communication, demonstrating its effectiveness in post-quantum environments.
- The proposed RISE-MQTT integrates Ring-LWE Identity-Based Encryption into the MQTT protocol, eliminating the need for pre shared keys while ensuring quantum resistant end-to-end security.
- When benchmarked against pairing-based IBE schemes, RISE-MQTT achieved a 61.44% reduction in session key setup time, significantly improving cryptographic efficiency.
- This marks a noteworthy improvement in both security and performance, offering a scalable and lightweight solution for real-time, resource-constrained IoT systems.

REFERENCES

1. M. Hamad, A. Finkenzeller, H. Liu, J. Lauinger, V. Prevelakis, and S. Steinhorst, "SEEMQTT: Secure End-to-End MQTT-Based Communication for Mobile IoT Systems Using Secret Sharing and Trust Delegation," in IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3384-3406, 15 Feb.15, 2023.

2. D.Gur,Y. Polyakov, K.Rohloff, G.W. Ryan, H. Sajjadpour and E. Savaş, "Practical Applications of Improved Gaussian Sampling for Trapdoor Lattices," in IEEE Transactions on Computers, vol. 68, no. 4, pp. 570-584, 1 April 2019.

3. S. Lakshminarayana, A. Praseed and P. S. Thilagam, "Securing the IoT Application Layer From an MQTT Protocol Perspective: Challenges and Research Prospects," in IEEE Communications Surveys and Tutorials, vol. 26, no.4, pp.2510-2546, Fourth Quarter 2024.

4. F. Buccafurri, V. De Angelis and S. Lazzaro, "MQTT-I: Achieving End-to-End Data Flow Integrity in MQTT," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 5, pp. 4717-4734, Sept.-Oct. 2024.

5. Y. Sun, P. Chatterjee, Y. Chen and Y. Zhang, "Efficient Identity-Based Encryption with Revocation for Data Privacy in Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2734-2743, 15 Feb.15, 2022.

6. A. R. Alkhafajee, A. M. A. Al-Muqarm, A. H. Alwan and Z. R. Mohammed, "Security and Performance Analysis of MQTT Protocol with TLS in IoT Networks," 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA),Najaf, Iraq, 2021, pp. 206-211.

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

THANK YOU

C-DAC

https://
pkiindia.in

Social Media
/pkiindia

IEEE BANGALORE SECTION