SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I11P114

Volume 13 Issue 11, 232-247, November 2026
© 2026 Seventh Sense Research Group®

Original Article

Lightweight RLWE-based Mutual Authentication with Traffic Digital Lock for Quantum-Resistant Healthcare IoT Networks

Catherin Sonia S[1], T. Jaya[2]

[1,2]*Department of ECE, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India.*

[1]*Corresponding Author: catherinsonia03@gmail.com*

Received: 23 September 2026 Revised: 31 October 2026 Accepted: 05 November 2026 Published: 27 November 2026

Abstract *- The evolution of quantum computing threatens the security of conventional public-key cryptographic schemes by compromising the computational hardness assumptions underlying existing authentication protocols (Nguyen et al. 2021).The healthcare Internet of Things (IoT) networks require efficient post-quantum authentication mechanisms for protecting sensitive medical data while operating under robust computational and resource constraints. This paper proposes a Modified Ring Learning with Errors (MRLWE)-based Mutual Authentication with Traffic Digital Lock (MRMA-TDL) framework for quantum-resistant healthcare IoT networks. The proposed authentication protocol is developed over an optimized RLWE parameter set carefully designed through offline QAOA-assisted parameter optimization. Also, to assure endurance against device impersonation, replay, and clone-device attacks, a Traffic Digital Lock (TDL) is merged to generate a novel behavioral signature from communication characteristics, including packet size, transmission frequency, and communication delay, during device registration. In addition, an offline Quantum Approximate Optimization Algorithm (QAOA) is employed to optimize RLWE parameters by minimizing authentication latency and cryptographic key size while maintaining the required security level. Security analysis confirms that the proposed protocol achieves robust resistance against impersonation, behavioral spoofing, replay, and clone-device attacks under the RLWE hardness assumption. Experimental results achieves an authentication latency of 6.9 ms, a throughput of 890 authentications/s, an authentication acceptance rate of 99.8%, and a clone-device detection accuracy of 97%, outperforming existing post-quantum authentication approaches in terms of computational efficiency and behavioral attack detection. The proposed framework further reduces communication overhead and storage requirements while maintaining statistically consistent performance over 100 independent simulation runs. These results indicate that the proposed MRMA-TDL framework yields an efficient, scalable, and quantum-resistant authentication solution for next-generation healthcare IoT networks.*

Keywords *- Ring Learning with Errors, Module Learning with Errors, Modified RLWE-based Mutual Authentication, Traffic Digital Lock, Internet of Things, Lightweight authentication, Quantum Approximate Optimization Algorithm, Behavioral attack detection, Clone device detection.*

1. Introduction

As quantum computers continue to improve, there is a real threat to the current public-key cryptographic systems such as RSA, Diffie–Hellman (DH) and Elliptic Curve Cryptography (ECC) (Aljebry & Barnawi, 2026). Existing authentication and key establishment methods are vulnerable to a quantum adversary, as quantum algorithms are able to efficiently solve the mathematical problems that underlie these cryptosystems, notably Shor's algorithm. For Healthcare Internet of Things (H-IoT) systems, where wearable sensors, medical devices and medical gateways are constantly sharing trust-sensitive patient-related information over heterogeneous communication networks, this threat is very significant. Maintaining patient confidentiality, integrity, authenticity and availability of medical information is critical for correct diagnosis, timely clinical decisions, and patient privacy. Despite their widespread use, the processing power, memory, energy and communication bandwidth of H-IoT devices remain limited, and they are unable to run computationally intensive cryptographic protocols (Zhou et al. 2018). Plus, healthcare IoT networks face a variety of cyber-attacks such as replay attacks, impersonation attacks, man-in-the-middle attacks, device cloning attacks, and behavioral spoofing attacks. Given this background, lightweight post-quantum authentication protocols that offer robust cryptographic security with low computational complexity, minimal communication expenses, and energy-efficient operation (Yavuz et al. 2025) are needed. The two

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

key research areas to address quantum threats are Quantum Cryptography and Post-Quantum Cryptography (PQC) (Suhail et al. 2020). Quantum Key Distribution (QKD) is an information-theoretic-secure method, but is restricted by the need for specialized hardware, high implementation costs, and limited scalability to large-scale IoT deployments. PQC is in contrast, a practical software-oriented solution involving computational problems that are thought to be intractable even for quantum computers (Kumar et al. 2021). Recognizing its significance, the National Institute of Standards and Technology (NIST) has standardized a few PQC algorithms for future cryptographic deployment. In particular, lattice-based cryptography is one of the most attractive methods among those listed above, due to its rigorous security properties and its efficiency and capability of being applied to systems with limited resources.

Algorithms, such as NIST-standardized CRYSTALS-Kyber and CRYSTALS-Dilithium, and schemes, including FrodoKEM and Saber, are based on the hardness of the Learning with Errors (LWE), Ring Learning with Errors (RLWE), and Module Learning with Errors (MLWE) problems. While there are ways to make lattice-based cryptography quantum-resistant, the direct adoption of existing authentication protocols based on RLWE and MLWE in healthcare IoT systems is still difficult (Boorghany et al. 2015). While the schemes based on MLWE usually have higher computational complexity, larger memory needs, and larger key sizes, the schemes based on RLWE are still highly dependent on the choice of parameters.

Unfeasible choices of polynomial degree, modulus size or error distribution can substantially impact the authentication latency and/or degrade the desired security level. Furthermore, most of the existing lattice-based authentication schemes are based on cryptographic authentication without addressing the threats that behavioral attacks can pose, like device cloning, replay, spoofing and exceptional communication patterns (Upadhyaya et al. 2025). The challenges these come with encourage the improvement of quantum-resistant, efficient, and behavioral verification authentication systems.

In order to address these issues, this paper introduces an Offline QAOA-Optimized Modified RLWE-based Mutual Authentication with Traffic Digital Lock (MRMA-TDL) framework for resource-limited healthcare IoT networks. The framework proposes an optimized RLWE formulation, minimizing computation overhead without compromising post-quantum security. During system design, an offline Quantum Approximate Optimization Algorithm (QAOA) is implemented to evaluate optimal parameters for the RLWE, including the degree of the polynomial, the size of the modulus, and the distribution of errors, which not only leads to offline parameter optimization but also minimizes the authentication latency, the communication overhead, and the size of the authentication cryptographic key without increasing the online computational complexity.

To reinforce protocol dependability, a lightweight Traffic Digital Lock (TDL) mechanism designs a behavioral signature using communication attributes such as packet size, transmission frequency, and communication delay. During authentication, the observed communication behavior is compared with the registered behavioral profile to detect cloned devices, replay attacks, spoofing attempts, and abnormal communication patterns. More importantly, a lightweight digital signature mechanism ensures message authenticity and integrity. The security of the proposed protocol is formally analyzed under the Bellare–Rogaway adversarial model, demonstrating resistance against replay, impersonation, chosen-ciphertext, algebraic, behavioral, and quantum-enabled attacks. In this study, the term Modified RLWE-based Mutual Authentication (MRMA) does not denote a modification of the underlying RLWE hardness assumption. As an alternative, it refers to an authentication-oriented construction instantiated using standard RLWE primitives and extended through certificate-based device registration, fresh ephemeral authentication values, session-bound key derivation, and behavioral validation. Consequently, the security foundation remains the conventional RLWE problem, while the modification lies in the protocol-level organization of RLWE operations for lightweight mutual authentication in resource-constrained healthcare IoT environments. The principal contributions of this work are summarized as follows:

1. An RLWE-based mutual authentication framework, termed MRMA, is developed for resource-constrained healthcare IoT systems. The protocol combines certificate-based registration, fresh ephemeral RLWE values, bidirectional authentication, and session-bound key establishment while retaining the conventional RLWE hardness assumption.
2. A lightweight Traffic Digital Lock (TDL) layer is incorporated for behavioral authentication. The TDL establishes a device-specific communication profile using packet size, transmission frequency, and communication delay and uses runtime behavioral deviation to identify cloned devices and spoofing attempts.
3. An offline QAOA-assisted parameter-selection mechanism is formulated for the MRMA protocol. Candidate RLWE configurations are evaluated using a multi-objective cost function incorporating authentication latency, key size, throughput, and authentication reliability under a minimum post-quantum security constraint. Since optimization is performed before deployment, no QAOA-related computational overhead is introduced into online authentication.

4. A formal security analysis and systematic performance evaluation are provided. The cryptographic protocol is analyzed under the Bellare–Rogaway adversarial model (Cagalj et al. 2006), while TDL effectiveness is evaluated independently through behavioral attack-detection metrics. Comparative and ablation analyses quantify the security-performance trade-off introduced by each component of the proposed framework.

The remainder of this paper is organized as follows. Section 2 reviews recent lattice-based authentication schemes for IoT environments. Section 3 presents the mathematical preliminaries of lattice-based cryptography. Section 4 describes the proposed MRMA-TDL framework. Section 5 provides the formal security analysis. Section 6 presents the experimental evaluation and comparative performance analysis. Finally, Section 7 concludes the paper and discusses future research directions.

2. Related Work

2.1. Foundations of Lattice-based Post-Quantum Cryptography

Lattice-based cryptography has become one of the principal approaches for constructing post-quantum security mechanisms because its underlying computational problems are believed to remain difficult for both classical and quantum adversaries. Lyubashevsky [1] introduced an efficient lattice-based signature scheme without trapdoors, demonstrating the practicality of lattice constructions for post-quantum digital signatures.

Liu et al. [2] subsequently surveyed lattice-based digital-signature techniques and highlighted their security properties and implementation potential. Lindner and Peikert [3] investigated parameter selection, key-size optimization, and lattice-reduction attacks for Learning with Errors (LWE)-based encryption, demonstrating that appropriate cryptographic parameter selection is essential for achieving a suitable balance between security and implementation overhead. The theoretical basis for Ring Learning with Errors (RLWE) was further established by Lyubashevsky, Peikert, and Regev [4], who related average-case RLWE instances to hard lattice problems. RLWE reduces the arithmetic dimensionality through polynomial-ring operations and is consequently attractive for computationally constrained applications. Practical lattice-based schemes have further demonstrated the feasibility of post-quantum cryptography. Bos et al. [5] presented CRYSTALS-Kyber, a module-lattice-based key-encapsulation mechanism, while Alkim et al. [6] proposed NewHope, an RLWE-based post-quantum key-exchange scheme.

These works provide important cryptographic foundations and practical benchmarks for the RLWE-based authentication mechanism considered in this study.

2.2. Lattice-based Authentication and Key Agreement for IoT

Beyond encryption and key establishment, lattice-based cryptography is increasingly investigated for mutual authentication. Bellare and Rogaway [7] established a formal framework for analyzing entity authentication and session-key security, which provides a basis for evaluating resistance against impersonation and active adversaries. Shahidinejad et al. [8] proposed lattice-based authenticated key-exchange protocols with provable security, demonstrating that quantum-resistant mutual authentication and session-key establishment can be constructed from lattice-hardness assumptions. For resource-constrained IoT environments, Fathenojavan et al. [9] proposed a lightweight lattice-based authentication protocol intended to reduce processing requirements while providing resistance to replay, impersonation, and man-in-the-middle attacks.

Gagan Kumar et al. [10] subsequently developed a post-quantum lightweight IoT authentication scheme combining lattice cryptography with hash-based operations. Huang et al. [11] introduce an RLWE-based privacy-preserving authentication mechanism for Industrial IoT in which edge computing is used for reducing the processing burden on constrained devices. These approaches demonstrate the applicability of lattice cryptography to lightweight authentication; however, their primary emphasis remains cryptographic identity verification and session-key establishment rather than behavioral validation of the authenticated device.

2.3. Post-Quantum and Lightweight Authentication for Healthcare IoT

Authentication for healthcare IoT requires not only strong security but also low computation, storage, and communication overhead. Meng et al. [12] proposed an authentication protocol for eHealth systems that protects sensitive medical information while considering the resource limitations of healthcare devices. Ahmad and Jagatheswari [13] developed a lattice-based three-party authenticated key-agreement protocol for Medical IoT involving users, gateways, and medical sensing devices. Their work demonstrated the feasibility of post-quantum session-key establishment in healthcare-oriented IoT environments.

Riya et al. [14] proposed an encryption scheme for Internet of Medical Things applications to provide secure communication under constrained operating conditions. These studies establish the importance of lightweight and post-quantum authentication in healthcare networks. Nevertheless, authentication is predominantly based on cryptographic credentials; device communication behavior is generally not incorporated as an independent authentication factor. This limitation is important in scenarios involving cloned or compromised devices that may possess valid credentials.

2.4. Behavioral and Clone-Device Verification

Behavioral and device-level security mechanisms provide an additional means of identifying compromised, spoofed, or cloned IoT devices. Hameed et al. [15] proposed a context-aware mechanism for clone-node detection in IoT, demonstrating the usefulness of device-context information for distinguishing legitimate and duplicated nodes. More recently, Upadhyaya et al. [16] investigated behavioral fingerprinting for identifying false devices in IoT networks, reinforcing the observation that cryptographic validity alone may not always be sufficient for establishing device legitimacy. Julaihi et al. [17] presented a comprehensive authentication taxonomy for IoMT and emphasized the importance of lightweight authentication mechanisms in resource-constrained medical environments. Intelligent network-security approaches have also demonstrated the effectiveness of behavior-related attributes. Altamimi et al. [18] employed interpretable AI and feature optimization for intrusion detection in smart infrastructures, while Chaurasiya et al. [19] investigated feature-selection and explainable-AI techniques for DDoS detection in IoT networks. Although these approaches improve behavioral anomaly and attack detection, they generally operate independently of lattice-based post-quantum mutual authentication.

2.5. QAOA-Assisted Cryptographic Parameter Optimization

Selection of RLWE parameters directly affects cryptographic security, computational cost, key size, and authentication latency. Existing lattice-based authentication mechanisms generally employ predetermined parameter configurations instead of dynamically evaluating several feasible configurations before deployment. Blekos et al. [20] provide a detailed review of the Quantum Approximate Optimization Algorithm (QAOA), including its cost-Hamiltonian formulation, variational parameters, optimization mechanisms, and implementation considerations. Their study demonstrates the suitability of QAOA for solving constrained discrete optimization problems. Waseem et al. [21] investigated quantum-assisted optimization and security in AI-driven healthcare, indicating the potential role of quantum-classical optimization in healthcare-related security applications. However, the literature considered in this manuscript does not provide an integrated approach in which QAOA is employed offline to select RLWE parameters specifically for lightweight mutual authentication while jointly considering latency, key size, throughput, authentication reliability, and a minimum post-quantum security requirement. Recent studies have further investigated lightweight implementation and quantum-resistant authentication for heterogeneous IoT environments. Kundi et al. [22] developed AxRLWE, a multilevel approximate Ring-LWE co-processor designed for lightweight IoT applications, demonstrating that RLWE arithmetic can be optimized for constrained hardware platforms. Siddiqui et al. [23] proposed a lightweight PUF–PKI digital-certificate authentication mechanism for IoT, highlighting the importance of efficient certificate-based device authentication. Wang [24] presented an R-LWE- and QIBE-based identity-authentication mechanism for quantum-resistant IoT devices, further demonstrating the applicability of ring-lattice techniques to secure device authentication. Yavuz et al. [25] proposed LiteQSign, a lightweight quantum-safe signature framework for heterogeneous IoT applications, emphasizing reduced computational and communication overhead for constrained devices. Although these approaches improve lightweight post-quantum security, they do not jointly integrate RLWE-based mutual authentication, behavioral traffic verification, and QAOA-assisted parameter optimization, which forms the principal motivation for the proposed MRMA-TDL framework.

2.6. Research Gap Analysis

The reviewed literature indicates three principal research gaps. First, existing lattice-based IoT and healthcare authentication protocols predominantly concentrate on cryptographic identity verification and session-key establishment, with limited consideration of behavioral device verification. Second, clone-device and behavioral-fingerprinting mechanisms are typically implemented as independent detection mechanisms rather than as part of the post-quantum mutual-authentication decision. Third, RLWE parameter selection is normally fixed or treated separately from the authentication architecture, despite its direct influence on latency, key size, throughput, and security. Consequently, an integrated lightweight framework combining post-quantum mutual authentication, behavioral device validation, and resource-aware parameter selection remains insufficiently investigated. The proposed MRMA-TDL framework addresses this gap by integrating certificate-bound RLWE mutual authentication with a Traffic Digital Lock (TDL) based on packet size, transmission frequency, and communication delay, together with offline QAOA-assisted RLWE parameter selection. The objective is not to modify the RLWE hardness assumption, but to achieve protocol-level and system-level integration suitable for resource-constrained healthcare IoT environments. This motivation is consistent with the manuscript's stated research gap and proposed architecture.

3. Mathematical Preliminaries

3.1. Lattice Theory

Lattice-based cryptography derives its security from computational problems that remain intractable even in the presence of quantum computers. A lattice is a discrete additive subgroup of the Euclidean space generated by integer linear combinations of a set of linearly independent basis vectors. Let

$$B = \{b_1, b_2, \ldots, b_n\} \quad R^m \tag{1}$$

be a basis consisting of n linearly independent vectors. The lattice generated by B is defined as

$$L(B) = \{\sum_{i=1}^{n} z_i b_i : z_i \in Z\} \quad (2)$$

A lattice admits infinitely many equivalent basis representations. Consequently, lattice basis reduction algorithms, such as the Lenstra–Lenstra–Lovász (LLL) algorithm, are employed to obtain shorter and nearly orthogonal basis vectors that facilitate efficient computation while preserving the lattice structure (Craps et al. 2022). Post-Quantum Cryptography (PQC) is based on the theoretical groundwork of computational hardness of lattice problems such as the Shortest Vector Problem (SVP), Closest Vector Problem (CVP), and Shortest Independent Vector Problem (SIVP) (Buser et al. 2022).

3.2. RLWE Hardness Assumption

The proposed authentication protocol is built on the Ring Learning with Errors (RLWE) assumption, which is quantum-resistant and has much lower computational complexity than Learning with Errors (LWE) (Lyubashevsky et al. 2013). The polynomial ring is defined as

$$R_q = Z_q[x]/(x^n+1) \quad (3)$$

Where

- n denotes the polynomial degree,
- q represents the modulus, and
- Rq denotes the quotient polynomial ring.

Given a uniformly distributed polynomial

$$a(x) \leftarrow R_q, \quad (4)$$

a secret polynomial

$$s(x) \leftarrow \chi, \quad (5)$$

and an error polynomial

$$e(x) \leftarrow \chi, \quad (6)$$

The RLWE sample is generated as

$$b(x)=a(x)s(x)+e(x) \pmod q \quad (7)$$

The RLWE decision problem consists of distinguishing the pair,

$$(a(x),b(x)) \quad (8)$$

From a uniformly random pair over R_q. Under appropriate parameter selection, solving this problem is computationally equivalent to solving worst-case lattice problems, thereby providing resistance against both classical and quantum adversaries (Borges et al. 2020).

3.3. Relationship between MLWE and RLWE

Module Learning WITH Errors (MLWE) operates over a module R_q^k of rank k, whereas RLWE corresponds to the rank-one case. Hence,

$$R_q^1 = R_q \quad (9)$$

The proposed framework therefore employs an RLWE-based construction rather than a higher-rank MLWE formulation. This choice is motivated by the reduced arithmetic dimensionality associated with polynomial-ring operations, which is advantageous for constrained IoT platforms. The rank-one relation is used only to explain the design choice and is not claimed as a new cryptographic reduction in this work.

3.4. Bellare–Rogaway Authentication Model

The security of the proposed MRMA-TDL protocol is evaluated using the Bellare–Rogaway (BR) authentication model (Cagalj et al. 2006). The BR model formalizes the capabilities of an adversary interacting with protocol participants through oracle queries. The adversary is permitted to (Cagalj et al. 2006):

- Intercept authentication messages,
- Modify transmitted packets,
- Replay previous sessions,
- Initiate concurrent sessions,
- Impersonate legitimate devices.

The protocol is considered secure if the adversary cannot (Cagalj et al. 2006):

1 Distinguish the established session key from a random value,
2 Impersonate a legitimate participant,
3 Violate mutual authentication,
4 Compromise session-key freshness.

The BR model therefore provides a rigorous framework for analyzing authentication correctness and session-key security under active adversarial conditions (Cagalj et al. 2006).

3.5. Notation

Table 1 summarizes the principal symbols used throughout the paper.

Table 1. Notation

Symbol	Description
R_q	Polynomial ring
n	Polynomial degree
q	Modulus
χ	Error distribution
a(x)	Public polynomial
s(x)	Secret polynomial
e(x)	Error polynomial
b(x)	RLWE sample
TDL_i	Traffic Digital Lock

δ_i	Behavioral threshold
Θ	Parameter set
K_{sess}	Session key

4. Proposed MRMA-TDL Framework

4.1. System Architecture

Figure 1 elaborates the architecture of the proposed Modified RLWE-based Mutual Authentication with Traffic Digital Lock (MRMA-TDL) framework, which merges offline QAOA-assisted parameter optimization, RLWE-based mutual authentication, behavioral traffic verification, and certificate-based trust management for secure Healthcare IoT communication. The system consists of four principal entities: the IoT device, IoT gateway/server, Central Certificate Authority (CCA), and the Traffic Digital Lock (TDL) module. The CCA computes one-time certificate generation and public-key certification, while the QAOA optimizer operates offline to analyze an optimal RLWE parameter set before deployment. During online operation, authentication is jointly determined through cryptographic verification and behavioral traffic validation, providing resistance against both classical and quantum-enabled attacks, while maintaining low computational overhead for memory-limited IoT devices.

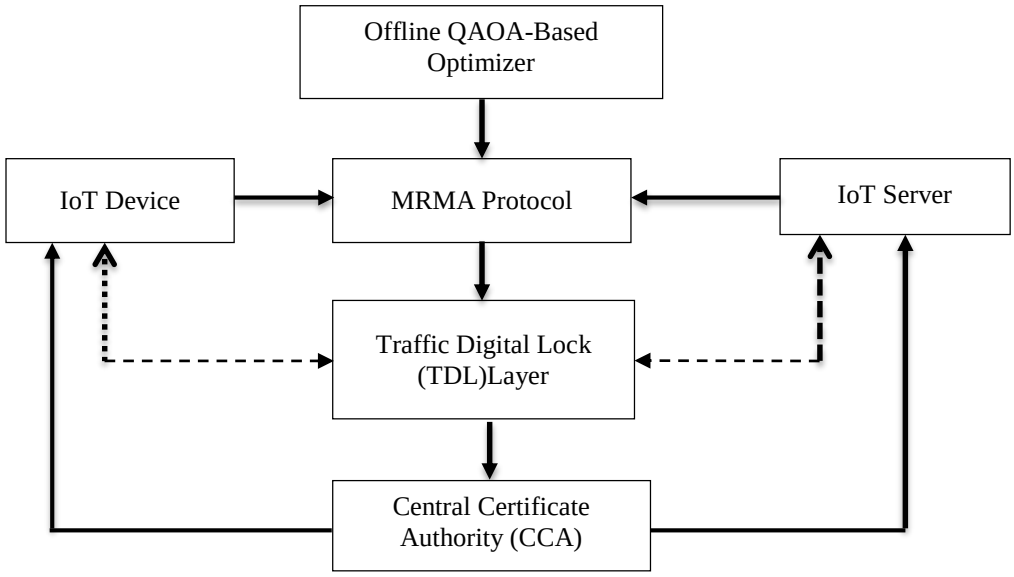

Fig. 1 Proposed MRMA-TDL system architecture

4.2. Protocol-Level Modification Introduced in MRMA

The suggested MRMA scheme upholds the already existing RLWE arithmetic yet reconfigures its application for bi-directional authentication. The main changes at the protocol level are: 1) certificate-bound RLWE public keys for the persistent device identity; 2) ephemeral RLWE values independently generated by the device for each authentication session; 3) bidirectional challenge verification; 4) explicit binding of the session key to the identities of the peer devices and to the new data contributed by the peer devices; and 5) pre-authentication decision made through post-cryptographic TDL validation. Consequently, MRMA is not a single encryption or key exchange primitive based on RLWE, but rather integrates identity binding, freshness, mutual verification, and behavioral validation into a single authentication workflow.

4.3. Offline QAOA-based Parameter Optimization

Unlike traditional lattice-based authentication schemes, which usually rely on fixed cryptographic parameters, the proposed framework optimizes the parameters before deployment. The optimization problem is formulated over the candidate parameter set

$$\Theta = \{n, q, \chi\} \quad (10)$$

where

- n denotes the polynomial degree.
- q denotes the modulus.
- χ represents the error distribution.

The objective is

$$\Theta=\arg\frac{min}{\theta}(w_1L+w_2K-w_3T-w_4A) \quad (11)$$

subject to Security(Θ) $\geq$ 128 bits.

Here,

- L = authentication latency
- K = key size
- T = throughput
- A = authentication acceptance rate

The optimization problem is encoded as a Quadratic Unconstrained Binary Optimization (QUBO) model and solved using the Quantum Approximate Optimization

Algorithm (QAOA) (Waseem et al. 2026). Since optimization is performed offline, no additional computational burden is introduced during authentication. The optimized parameter set is subsequently used throughout the MRMA protocol.

5. Proposed MRMA Scheme-based Cryptosystem

The proposed MRMA scheme-based cryptosystem is a post-quantum public-key encryption technique founded on the Ring Learning with Errors (RLWE) assumption, deemed secure against quantum computer attacks (Zheng et al. 2025), as shown in Table 2. This cryptosystem relies on the difficulty of solving RLWE, which is thought to be impervious to quantum attacks. The noise obstructs attackers from retrieving s or m, even when they observe numerous ciphertexts.

Table 2. Proposed MRMA framework-based cryptosystem

Algorithm 3: Proposed MRMA Scheme-based cryptosystem

Input parameters:

- n: Degree of the cyclotomic ring, $R = Z_q[x]/(x^n+1)$
- q: Modulus (Typically, a large prime $q \equiv 1 \bmod 2^n$)
- $Rq = Z_q[x] / (x^n+1)$
- χ: Error distribution (e.g., discrete Gaussian over R)

Key generation:

Private key:

- Choose a secret polynomial, $s \leftarrow \chi \in R_q$

Public key:

- Choose $a \leftarrow R_q$
- Sample error $e \leftarrow \chi$
- Compute $b = a.s + e \ R_q$
- Public key (a, b)
- Private key: s

Encryption (Encrypt message $m \ \{0,1\}^n$):

- Sample ephemeral secret polynomials: r, e_1, $e_2 \leftarrow \chi \in R_q$
- Encode $m \in \{0,1\}^n$ as polynomial $m(x) \ R_q$
- Compute ciphertext: $u = a.r + e_1 \in R_q$; $v = b.r + e_2 + [\frac{q}{2}] \ m \ R_q$
- Ciphertext (u, v)

Decryption:

Compute: $v - u. s = b. r + e_2 + [\frac{q}{2}] \ m - a. r. s - e_1. s$

Since $b = a.s + e$, it simplifies to: $v - u. s = e. r + e_2 - e_1. s + [\frac{q}{2}] \ m$

Use noise bound to recover message $m \in \{0,1\}^n$:

If the coefficient is closer to $0 \rightarrow m = 0$; If the coefficient is closer to $\frac{q}{2} \rightarrow m = 1$

5.1. Proposed Modified RLWE-based Mutual Authentication (MRMA) Scheme for IoT Systems

The proposed Modified RLWE-based Mutual Authentication (MRMA) Scheme consists of three successive phases: registration of the IoT device certificate, registration of the IoT server certificate, and a mutual authentication protocol between the device and the server. Initially, each IoT device solicits and obtains a digital certificate from the Certificate Authority (CA). Likewise, the IoT server obtains its certificate from the Certificate Authority (CA) (Siddiqui et al. 2022). These certificates are crucial for implementing a secure mutual authentication mechanism with lattice-based cryptography. In this scenario, the IoT device generates a public-private key pair and transmits its public key to the CA. The CA subsequently links the device's identity to its public key through a signed hash and generates a certificate that ensures the device's authenticity in future interactions.

5.2. MRMA-TDL Operational Workflow

The operational workflow of the proposed MRMA-TDL has 3 layers as shown in Figure 2: QAOA-based parameter optimization, RLWE-based mutual authentication, and Traffic Digital Lock (TDL) behavioral verification. The novel method is constructed to achieve secure device registration, authentication, cloning detection, and final authentication decision.

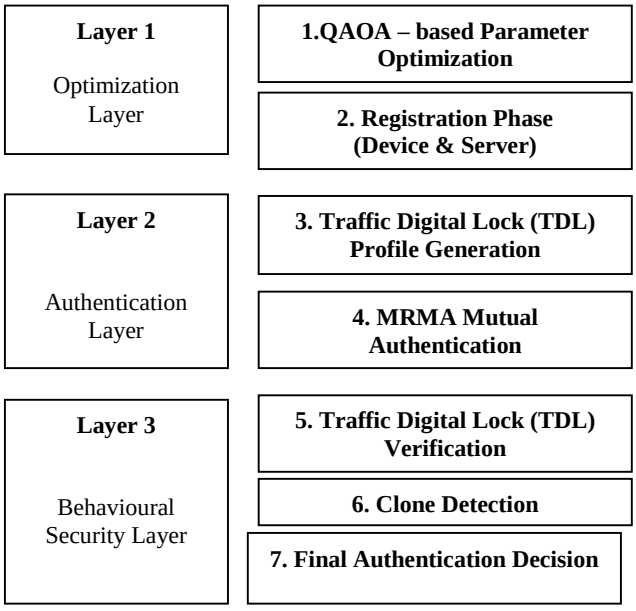

Fig. 2 Layered authentication workflow diagram

5.3. IoT Server Certificate Registration

Figure 3 explains certificate registration procedure for the IoT server within a lattice-based cryptography architecture. The process begins with the initialization of essential parameters: the cyclotomic ring R_q, an error distribution χ, a public ring element a, and a secret key κ held by the CA. The

server's cryptographic credentials are produced by selecting a secret polynomial s_i and an error term t from χ, and then generating the public key as $b=a \cdot s_i + t$. The key pair (a, b), together with the secret key and error term, is stored on the IoT server. The CA then processes the public key, assigns a unique identity ID_i, containing device-specific metadata ED, and stores a timestamp T_g. It builds a hash of the identity, public key, metadata, and timestamp. The generated certificate, $Cert_i$, which includes all these elements, is digitally signed by the CA. Finally, the certificate is sent to the IoT server, which keeps the complete set of credentials (s_i, b, a, ID_i, ED). This procedure guarantees secure and verifiable pre-deployment registration inside a post-quantum secure framework as shown in Table 3.

Table 3. IoT server registration framework

Algorithm 4: IoT Server Certificate Registration (Pre-deployment)
General Input parameters: ● $R_q = Z_q[x] / (x^n + 1)$: cyclotomic ring ● χ: Error distribution (e.g., Discrete Gaussian) ● $a \in R_q$: Public ring element ● CertID, Cert Server: Certificates of IoT Devices and IOT Server, respectively ● s_u, s_l: Secret polynomials of device and server ● $b_u = a. s_u + e_u$, $b_l = a. s_l + e_l$ Public keys of device/server ● ID_u, ID_l: Unique identities ● ED_u, ED_l: Embedded device information ● t,w,z: Security tags from CAC ● H: Collision-resistant hash function
Input parameters: Public parameter: $a \in R_q$, Error distribution: χ ,CAC secret key: S_{CAC}
Step 1. Key Generation: ● Choose secret polynomial $sl \leftarrow \chi$ ● Sample error $t_1 \leftarrow \chi$ ● Compute public key: $b_l = a. s_l + t_1 \in R_q$ Step 2. Public key pair: (a, b_l) Step 3. Store in IoT Server: {sl, b_l,a,t_1} Step 4. Send PublicKey b_l to CAC Step 5. CAC Side Processing: ● Assign: Identity ID_l , Embedded info ED_l, Tag t ● Compute hash: h = H(b_l, t , ED_l) ● Generate Certificate: Cert1 = { b_l, ID_l, t, ED_l} ● Generate a signed certificate: $Seri_l$ = {b_l, ID_l , t, ED_l, z} Step 6. Transmit certificate Certi to IoT Server Step 7. IoT Server Final Store: {s_l , b_l , a, z, ID_l, t, ED_l}

5.4. IoT Device Certificate Registration

Likewise, a lattice-based cryptographic approach is used to handle the registration process of the IoT device. The first step of IoT device is to generate a secret polynomial and an error term from an error distribution χ , as shown in Figure 4. After that, the device computes the public key, as $b_u = a.s_u + e$. The secret key, public key and public parameters are stored in the device before transmission. The public key is then transmitted to the Certificate Authority (CA). Upon receipt of the public key, the Certificate Authority (CA) provides the device with an identity IDu, unique to the device, as well as device-specific information ED and creates security tags: witness w and tag t. It creates a secure hash to generate a digitally signed certificate. The signed certificate is returned to the IoT device with the signed certificate. The device, in turn, retains the complete set of information: (s_u, b_u, a, ID_u, t, w, ED, b_{CAC}) as shown in Table 4.

Table 4. IoT device certificate registration framework

Algorithm 5: IoT Device Certificate Registration (Pre-deployment)
Input Parameters: Public parameter: $a \in R_q$, Error distribution, χ, CAC secret key s_{CAC} Step 1. Key Generation: ● Choose secret polynomial $su \leftarrow \chi$, Sample error $eu \leftarrow \chi$ ● Compute public key: $bu = a. s_u + e_u \in R_q$ Step 2: Public Key Pair: (a, b_u) Step 3: Store in IoT server: {s_u, b_u, a, z} Step 4: Send Public key bu to CAC Step 5: CAC Side Processing ● Assign: Identity, ID_u, Embedded info, ED_u, Tag t, witness ● Compute hash: h = H (H (b_u, ED_u)) ● Generate Certificate: Certu = {H = {h, t, w, ED_u}} ● Generate Signed Certificate: Seriu= {b_u, w, ID_u, t, w, z} Step 6: Transmit Certificate Certu to IoT Device Step 7: IoT Device Final Store: {s_u,b_u,a,z,ID_u,t,w,ED_u,b_{CAC}}

5.5. Modified RLWE-based Mutual Authentication Algorithm

The Modified RLWE-Based Mutual Authentication Algorithm promises a secure, efficient method for authentication (Huang et al. 2024). The mutual authentication process relies on the fact that both the IoT device (D_u) and the server (S_u) have completed their certificate registration and possess the necessary credentials. These include public-private key pairs, digital certificates, and system parameters such as the ring R_q, modulus q, generator a, and a collision-resistant hash function H (.). In Step 1, the IoT device commences the authentication request by generating random ephemeral secrets r, e_1, e_2. χ R_q. Also, $u_1 = a. r + e_1$ and $u_2 = b_u . r + e_2 + [\frac{q}{2}]$. m, where m is a session-specific random bit string represented as a polynomial. The device transmits the message Msg_1 = {u_1, u_2, $Cert_u$} to the server. In Step 2, the IoT server verifies the device's certificate $Cert_u$ using CAC information. It then

computes $v = u_2 - s \cdot u_1$, where s is the server's secret key, and recovers the message m′ using a decoding algorithm. If the certificate and decoded message are valid, the process continues. In Step 3, the server responds by generating its own random ephemeral secrets r′, $e_1^{'}$,$e_2^{'}$ and computing,

$$u_1^{'} = a.\, r' + e_1^{'} \quad (11)$$

$$u_2^{'} = b_u.\, r' + e_2^{'} + [\tfrac{q}{2}].\, m' \quad (12)$$

The server then sends the message, $Msg_2 = \{u_1^{'}, u_2^{'}, Cert_s\}$ to the device. In Step 4, the IoT device verifies the server's certificate $Cert_s$, computes $v' = u_2^{'} - s_u.u_1^{'}$ Moreover, decodes v′ to retrieve message m_3. Upon successful verification, mutual authentication is confirmed as shown in Table 5.

$$SK = H(m \parallel ID_u \parallel ID_s) \quad (13)$$

This session key is unique to the interaction and secure, authenticated communication, offering resistance against quantum and classical attacks alike (Wang, 2024).

Table 5. MRMA framework

Algorithm 6: Modified RLWE-based Mutual Authentication Algorithm
Participants: IoT Devices D_u, IoT Server Su Assumptions: Each participant has already registered and holds: Public Key: $b \in R_q$, Secret Key: $s \in R_q$ Certificate: Cert = {b, ID, t, ED…}, System parameters: Ring Rq, Modulus q, Generator a, Hash Function H ()
Step 1: IoT Device → IoT Server (Authentication Request)
Input from IoT Device: Stored s_u, b_u, a, z, ID_u, t_u, w, ED_u, b_{CAC} Procedure: 1. Choose random ephemeral secrets: r, e_1, $e_2 \leftarrow \chi\, R_q$ 2. Compute: $u_1 = a.r + e_1 \in R_q$, $u_2 = b_a \cdot r + e_2 + [\frac{q}{2}].\, m \in R_q$ where m is a session-specific random bit string encoded as a polynomial 3. Send message to server: $Msg_1 = \{u_1, u_2, Cert_u\}$
Step 2: IoT Server → Verifies IoT Device Input at server: Own: s_s, b_s, $Cert_s$, Received: u_1, u_2, $Cert_u$ Procedure: 1. Verify Certificate Certu using stored CAC info bCAC 2. Compute: $v = u_2 - s_s \cdot u_1$ 3. Recover message: m′ = Decode (v) based on threshold $[\frac{q}{2}]$ 4. If the message is valid and the certificate check passes, proceed.
Step 3: IoT Server → IoT Devices (Authentication Request)
Procedure:
1. Choose random ephemeral secrets: r′, $e_1^{'}$, $e_2^{'} \leftarrow \chi\, R_q$ 2. Compute: $u_1^{'} = a.\, r' + e_1^{'}$; $u_2^{'} = bu.\, r' + e_2^{'} + [\frac{q}{2}].\, m_s$ 3. Send response: $Msg2 = \{u_1^{'}, u_2^{'}, Cert_s\}$
Step 4: IoT Device → Verifies Server
Procedure: 1. Verify certificate, Certs 2. Compute: $v' = u_2^{'} - s_u \cdot u_1^{'}$ 3. Recover: $m_s^{'}$ = Decode (v′) 4. If valid, mutual authentication is successful
Session Key Derivation: Both entities can derive a common session key: $SK = H(m \parallel m_s \parallel ID_u \parallel ID_s)$

A QAOA-assisted parameter optimization framework is constructed for systematically tuning the cryptographic parameters of the Modified RLWE-based Mutual Authentication (MRMA) scheme. The algorithm constructs a discrete parameter space of candidate polynomial degrees, moduli, and noise distributions, and formulates parameter selection as a constrained multi-objective optimization problem balancing authentication latency, throughput, Authentication Acceptance Rate (AAR), and key size under fixed post-quantum security requirements. The optimization problem is also encoded as a Quadratic Unconstrained Binary Optimization (QUBO) model (Turnip et al. 2025) and mapped to a cost Hamiltonian in the QAOA framework (Zhou et al. 2020). A hybrid quantum-classical loop iteratively updates the variational parameters to find near-optimal configurations. The optimized parameters thus obtained are used offline for the instantiation of the MRMA protocol, which improves the computational efficiency significantly without incurring any additional runtime overhead or loss of the RLWE-based security guarantees.

6. Security Analysis

6.1. Simulation Environment

The proposed MRMA-TDL authentication framework was implemented in Python 3.11 using NumPy, SciPy, and Python cryptographic libraries. The offline QAOA-assisted parameter optimization was executed using the Qiskit Aer Simulator. Experiments were performed on an Intel Core i7-based workstation equipped with 16 GB RAM and 512 GB SSD storage, as shown in Table 6. The simulated healthcare IoT environment consisted of 25–100 heterogeneous devices, including wearable ECG sensors, pulse oximeters, blood-pressure sensors, glucose monitors, temperature sensors, gateway nodes, authentication servers, and a trusted Certificate Authority (CA). The evaluation considered both legitimate and malicious devices performing replay, impersonation, relay, message-modification, behavioral spoofing, and clone-device attacks. Each experiment was repeated 100 independent times, and the reported values correspond to the sample mean. For repeated-run analysis, standard deviation and 95% confidence intervals were computed to quantify execution variability.

Table 6. Experimental parameters

Parameter	Value
Programming Language	Python 3.11
Numerical Libraries	NumPy, SciPy
Quantum Simulator	Qiskit Aer
Processor	Intel Core i7
RAM	16 GB
Storage	512 GB SSD
Number of IoT Devices	25–100
Simulation Runs	100
Attack Models	Replay, MITM, Impersonation, Clone, Behavioral Spoofing
Evaluation Metrics	Latency, Throughput, AAR, Clone Detection

Let x_i represent the result obtained during the ith execution, and N =100 represent the total represent the total number of independent simulation runs. The sample mean is computed as

$$\underline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \,, \tag{14}$$

while the sample standard deviation is

$$s= \sqrt{\frac{1}{N-1}\ \sum_{i=1}^{N}\left(x_i - \underline{x}\right)^2} \tag{15}$$

The corresponding 95% Confidence Interval (CI) is

$$\underline{x} \pm 1.96\ \frac{s}{\sqrt{N}} \tag{16}$$

Statistical reporting provides insight into execution stability and allows a fair comparison among competing authentication schemes, as shown in Table 7.

Table 7. Statistical summary of experimental results

Metric	Mean	Std. Dev.	95% CI
MRMA Latency (ms)	6.50	≈0.28	6.45–6.56
MRMA-TDL Latency (ms)	6.90	≈0.31	6.84–6.96
MRMA Throughput (auth/s)	900	≈17	896.6–903.4
MRMA-TDL Throughput (auth/s)	890	≈18	886.5–893.5
MRMA AAR (%)	99.2	≈0.15	99.17–99.23
MRMA-TDL AAR (%)	99.8	≈0.08	99.78–99.82
MRMA Clone Detection (%)	88	≈1.4	87.7–88.3
MRMA-TDL Clone Detection (%)	97	≈0.75	96.85–97.15

6.2. Bellare–Rogaway Adversarial Model

Considering a probabilistic polynomial-time adversary $\mathcal{A}$, with full control over the communication channel. Following the BR framework, $\mathcal{A}$ may issue the following oracle queries:

- Execute: Observe honest protocol executions.
- Send: Inject, replay, or modify protocol messages.
- Reveal: Obtain session-specific values of completed sessions.
- Test: Distinguish a real session output from a random value.

The adversary's objective is to impersonate a legitimate participant, cause incorrect authentication, or distinguish a valid authentication transcript from a random one with non-negligible probability.

6.3. Game 0: Real Protocol Execution

Game 0 corresponds to the real execution of the MRMA protocol between a legitimate IoT device and the authentication server. Public parameters are generated according to the RLWE setting, and each authentication session uses fresh ephemeral secret polynomials and noise samples. The decisions are based on correct RLWE decoding and certificate validation. Let Pr[Succ0] be the probability that $\mathcal{A}$ breaks authentication for the real-world IoT deployments.

6.4. Game 1: Elimination of Replay Attacks

In the first game, modify the protocol to reject any authentication transcript that tries to reuse stale session identifiers, timestamps or ephemeral RLWE components. Since each session in MRMA employs fresh randomness and session-specific values, replayed messages fail verification deterministically. The adversary's view in Game 1 is indistinguishable from Game 0 except with negligible probability:

$$|\Pr[\mathrm{Succ}_1] - \Pr[\mathrm{Succ}_0]| \le \varepsilon_{\mathrm{replay}} \tag{17}$$

Where ε_{replay} is negligible.

6.5. Game 2: Resistance to Impersonation and MITM Attacks

In Game 2, consider the adversaries attempting impersonation or Man-in-the-Middle (MITM) attacks by injecting forged authentication messages. Abort the game if the adversary successfully authenticates without possessing

the correct secret polynomial or producing a valid RLWE-based authentication transcript. Any adversary that succeeds in this game can be used to construct a distinguisher that separates RLWE samples from uniformly random ring elements. Thus,

$$|Pr[Succ_2] - Pr[Succ_1]| \leq \varepsilon_{RLWE} \quad (18)$$

Where ε_{RLWE} is negligible under the RLWE hardness assumption (Brakerski et al. 2013).

6.6. Game 3: Chosen-Ciphertext and Transcript Manipulation Attacks

In Game 3, the adversary is allowed adaptive manipulation of authentication ciphertexts and protocol transcripts. Due to the presence of RLWE noise and ephemeral randomness, any modification causes decoding failure with overwhelming probability.

Replacing valid authentication transcripts with uniformly random ring elements does not change the adversary's view under the RLWE assumption. Therefore,

$$|Pr[Succ_3]| = \frac{1}{3} \quad (19)$$

6.7. Game 4: Quantum Attack Model (Shor-Enabled Adversary)

In Game 4, the adversary is granted access to quantum computational capabilities, including Shor's algorithm. Although Shor's algorithm effectively compromises RSA and ECC through the resolution of integer factorization and discrete logarithms, it offers no benefit when applied to RLWE-based constructions (Zen & 10, 2025). These latter constructions are predicated on lattice problems that are not amenable to reduction to the aforementioned algebraic structures. Consequently, the adversary's probability of success remains unaffected.

$$|Pr[Succ_4] - Pr[Succ_3]| \leq \varepsilon_{quantum} \quad (20)$$

Where $\varepsilon_{quantum}$ is negligible.

6.8. Overall Security Bound

By combining the above game transitions, the overall advantage of any polynomial-time adversary in breaking the MRMA authentication protocol is bounded as:

$$Adv_{MRMA}(.) \leq \varepsilon_{replay} + \varepsilon_{RLWE} + \varepsilon_{quantum} \quad (21)$$

Which is negligible. Therefore, the proposed MRMA scheme achieves provable security against replay, impersonation, MITM, chosen-ciphertext, and quantum attacks under the RLWE assumption in the Bellare–Rogaway model (Blake-Wilson⋆⋆ & Menezes, 1999).

7. Performance Analysis

This section calculates the computational efficiency, authentication and security within the healthcare IoT environment. Implementation is done using Python 3.11, and the QAOA parameter optimization is done using Qiskit Aer Simulator to model the communication behavior of wearable medical devices, including ECG, Pulse Oximeter, body temperature, blood pressure, and glucose monitoring sensors. Evaluation is done in an IoT environment to identify legitimate devices, malicious devices, authentication servers, and gateway nodes in both active and passive settings. Performance evaluation is based on 100 independent simulations, and average results are calculated.

The evaluation metrics are secret key size, throughput, authentication latency, Authentication Acceptance Rate (AAR), decryption accuracy and clone detection. The proposed framework, MRMA-TDL protocol, is compared with RLWE-NewHope and MLWE-Kyber to assess its suitability for resource-constrained environments. Further analysis shows the effect of polynomial degree on cryptographic parameters and performance of integrating Traffic Digital Lock (TDL) Mechanism with RLWE-based mutual authentication for enhancing security against cloning and behavioral spoofing attacks.

7.1. RLWE

As can be seen in Figure 3, in RLWE-NewHope schemes, the secret key size and processing time are affected by the degree of the polynomial and the secret key size and computational cost increase as the degree of the polynomial increases from 256 to 1024.

The trade-off between security strength and resource consumption is addressed. At the higher end of polynomial degree, memory and processing resource requirements affect resource-constrained healthcare IoT devices (Kundi et al. 2021).

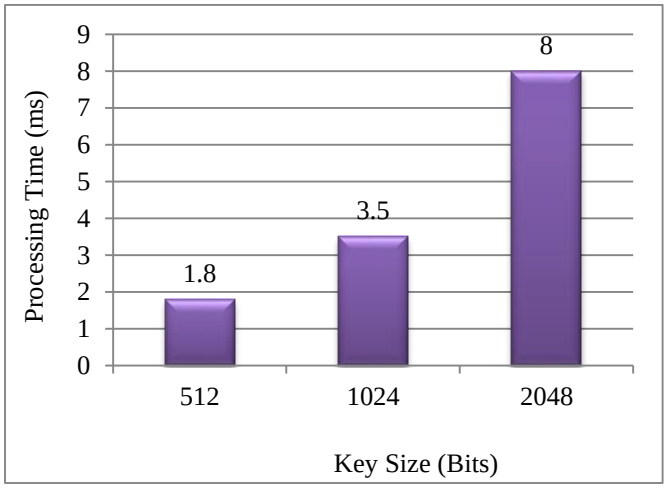

Fig. 3 RLWE - Secret key size and processing time comparison

7.2. MLWE

Figure 4 illustrates the variation of secret key size and processing time for MLWE (Crystal-Kyber) schemes. This scheme offers improved security margins and greater parameter flexibility relative to RLWE constructions; larger key sizes and higher processing overhead demand additional storage requirements. This graph acts as a benchmark for calculating the efficiency of the proposed MRMA-TDL methods.

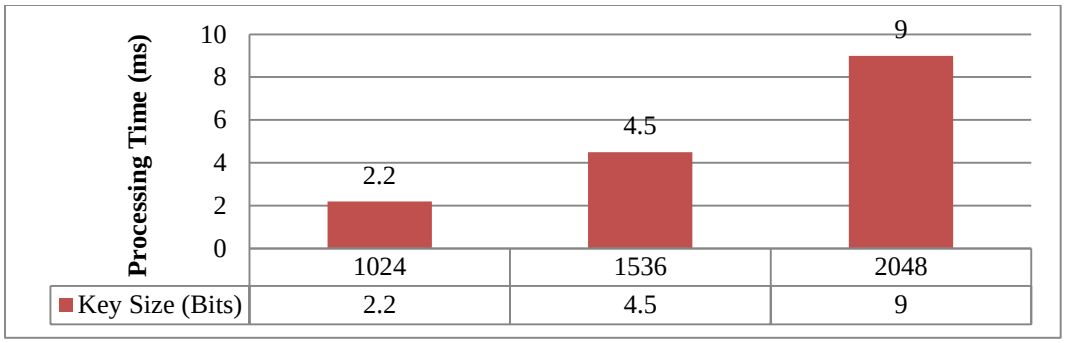

Fig. 4 MLWE secret key size and processing time comparison

7.3. Key Size Comparison

Figures 5 and 6 compare the secret key size and decryption accuracy of RLWE-NewHope, MLWE-Kyber (Bos et al. 2018), Proposed MRMA, and Proposed MRMA-TDL schemes for different polynomial degrees.

The figure shows that the proposed MRMA-TDL scheme has a negligible increase in key size compared to the basic MRMA scheme. Thus, it maintains lightweight storage requirements for IoT healthcare environments.

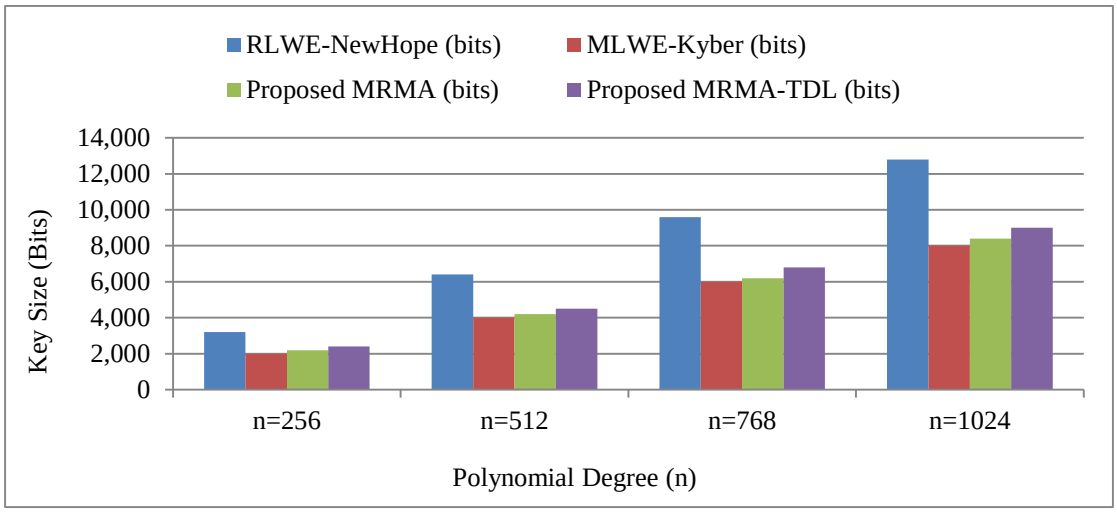

Fig. 5 Key size comparison across polynomial degrees

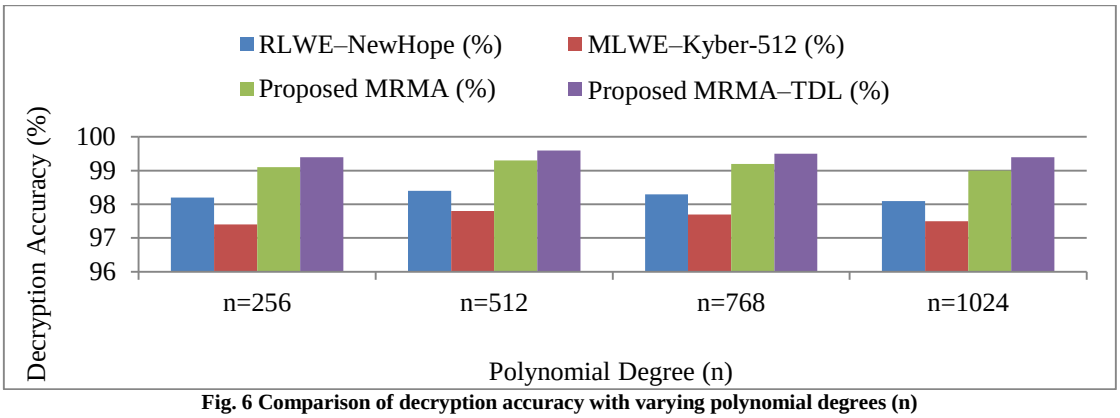

Fig. 6 Comparison of decryption accuracy with varying polynomial degrees (n)

All schemes are evaluated in identical simulation settings equivalent to NIST Level I security assumptions, with identical hardware/software configurations and the same measurement techniques for fair comparison. The effectiveness of the proposed MRMA-TDL framework under equivalent security settings is shown and discussed. The proposed MRMA scheme has the lowest authentication latency of 6.5 ms and the highest throughput of 900 operations per second, making this scheme practical for lightweight RLWE-based design. Combining Traffic Digital Lock with the proposed MRMA increases latency to 6.9 ms, and throughput is reduced to 890 operations per second. The key contribution of this additional layer is to improve the Authentication Acceptance Rate from 99.2% to 99.8%, and the clone detection rate is improved significantly from 88% to 97%. The proposed MRMA-TDL achieves the highest authentication accuracy and behavioral attack detection than RLWE-NewHope and MLWE-Kyber-512 (Bos et al. 2018), and has low computational overhead, making it suitable for resource-constrained healthcare IoT environments.

7.4. Authentication Latency

Figure 7 depicts the comparison of the authentication latency of RLWE-NewHope, MLWE-Kyber-512, MRMA and MRMA-TDL. The latency of RLWE-NewHope and MLWE-Kyber-512 is 12 ms and 15 ms, respectively, and the proposed MRMA shows the lowest latency of 6.5 ms. The presence of the TDL layer results in a small increase in latency to 6.9 ms, which corresponds to an extra processing overhead of only 0.4 ms (6.15%). This is a marginal increase, but MRMA-TDL is still 42.5% faster than RLWE-NewHope and 54.0% faster than MLWE-Kyber-512, demonstrating that behavioral verification can be integrated with little effect on real-time authentication performance.

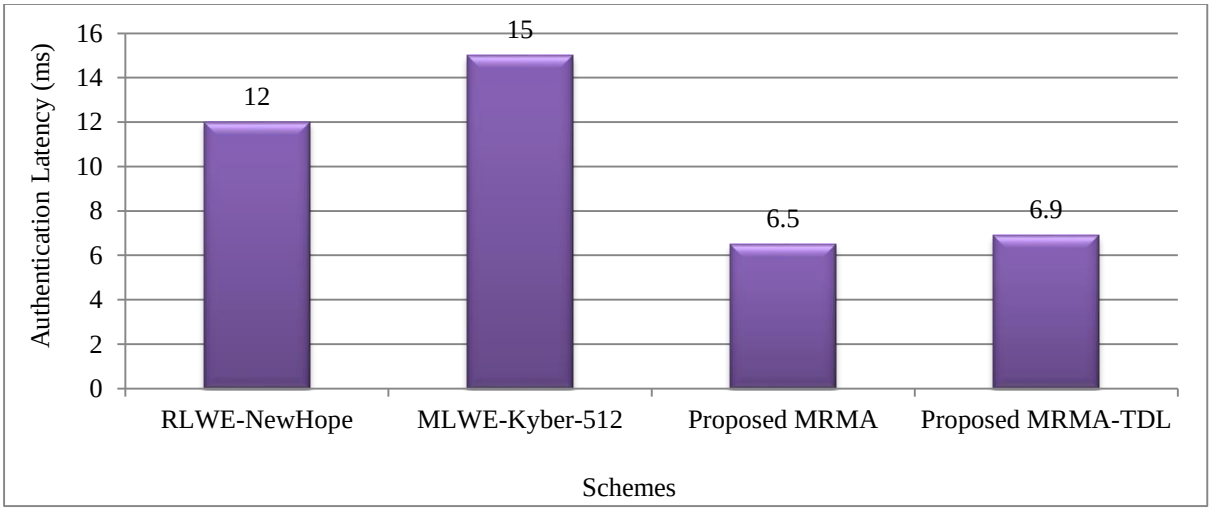

Fig. 7 Comparison of proposed scheme in terms of authentication latency

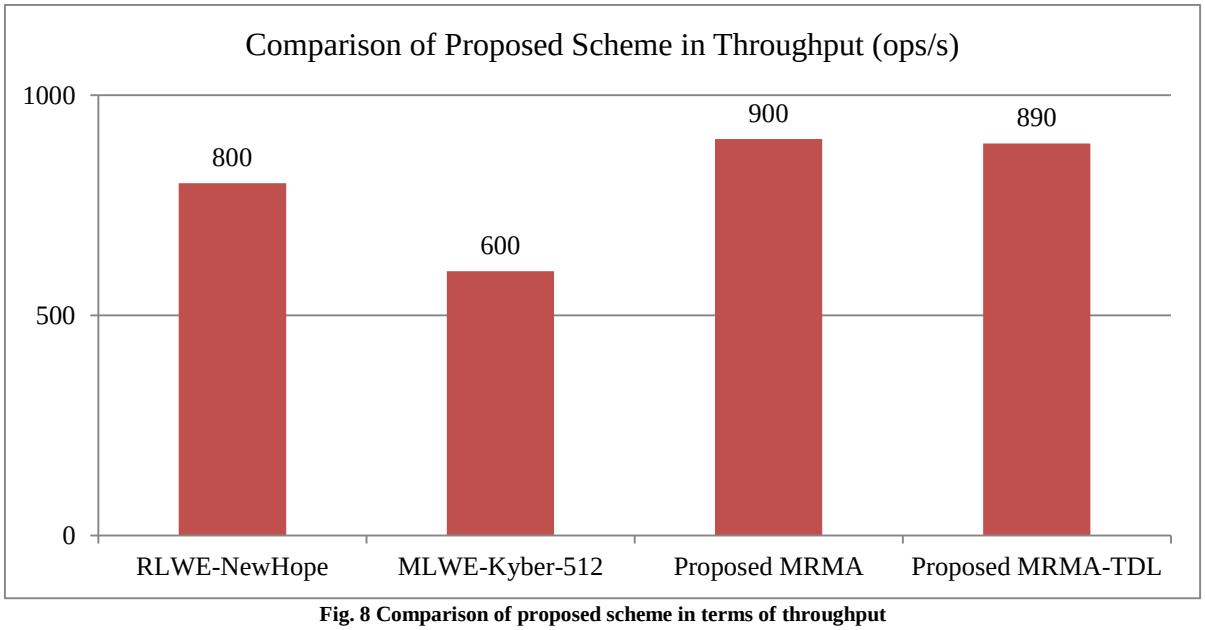

Fig. 8 Comparison of proposed scheme in terms of throughput

7.5. Throughput Comparison

In Figure 8, the authentication throughput for different schemes is shown. The proposed MRMA achieves the highest throughput of 900 authentications/s. The introduction of TDL reduces the throughput slightly to 890 authentications/s, which is only a reduction of 1.11%. However, MRMA-TDL still outperforms RLWE-NewHope (800 authentications/s) and MLWE-Kyber-512 (600 authentications/s) by 11.25% and 48.33%, respectively. The small reduction is because of the extra behavioral verification happening after a successful cryptographic authentication.

7.6. Authentication Acceptance Rate (AAR) Comparison

The Authentication Acceptance Rate (AAR) is the percentage of valid authentication requests that are accepted by the framework successfully. Figure 9 shows that the AARs of RLWE-NewHope, MLWE-Kyber-512, MRMA, and MRMA-TDL are 98.5%, 97.8%, 99.2%, and 99.8%, respectively. The addition of TDL enhances the AAR by 0.6 percent, indicating that the behavioral verification augments the authentication reliability without adversely impacting the legitimate devices.

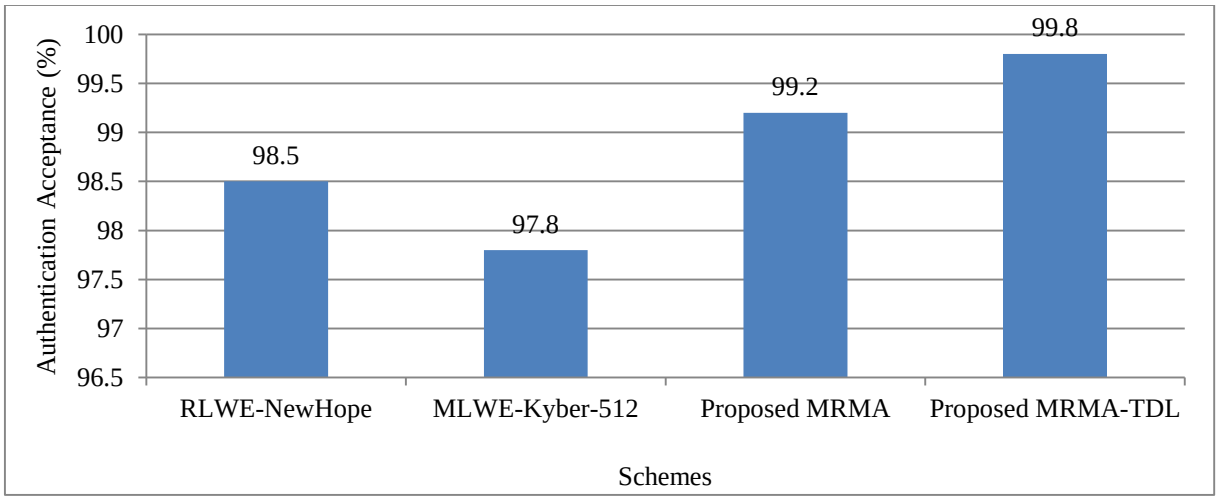

Fig. 9 Comparison of AAR

7.7. Clone Detection Rate Comparison

The clone-device detection ability of the evaluated schemes is shown in Figure 10. The conventional RLWE-NewHope and MLWE-Kyber-512 detect 72% and 81%, respectively, and MRMA enhances the detection capability to 88% by improving the cryptographic authentication. The behavioral verification improves the clone detection rate to 97% with the proposed MRMA-TDL. This is 9 percentage points better than MRMA, 25 percentage points better than RLWE-NewHope and 16 percentage points better than MLWE-Kyber-512. These results show that behavioral traffic profiling can substantially increase the resilience against cloned and spoofed IoT devices.

The analysis of the performance shows that the proposed MRMA-TDL framework has a smaller key size and lower authentication latency compared to the conventional RLWE-NewHope and MLWE-Kyber schemes.

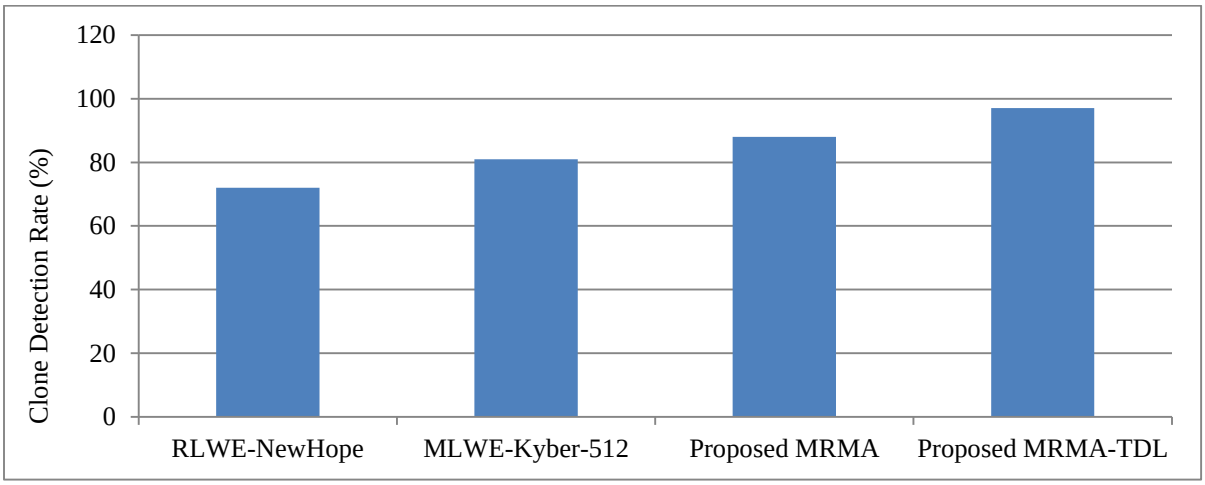

Fig. 10 Comparison of clone detection rate

7.8. Ablation Study

The effect of the Traffic Digital Lock was isolated by comparing MRMA with and without behavior verification. The authentication latency increases by 0.4 ms, and the throughput decreases by 10 authentications/s with TDL enabled. However, this small computational overhead greatly improves the reliability of authentication: AAR is improved from 99.2% to 99.8%, and clone detection rate is improved from 88% to 97%. As shown in Table 8, TDL provides a good trade-off between computational cost and behavioral security.

Table 8. Ablation study of the TDL layer

Configuration	Latency (ms)	Throughput (auth/s)	AAR (%)	Clone Detection (%)
MRMA	6.5	900	99.2	88
MRMA-TDL	6.9	890	99.8	97

8. Conclusion

This study investigated lightweight post-quantum mutual authentication for healthcare IoT by integrating RLWE-based cryptographic authentication, Traffic Digital Lock behavioral verification, and offline QAOA-assisted parameter selection. The contribution is at the protocol and system levels rather than modification of the RLWE hardness assumption. MRMA provides certificate-bound bidirectional authentication and session-bound key derivation, whereas TDL provides an independent behavioral verification layer based on packet size, transmission frequency and communication delay. Under the evaluated simulation environment, MRMA-TDL achieved an average authentication latency of 6.90 ms, throughput of 890 authentications/s, Authentication Acceptance Rate of 99.8%**,** and clone-detection rate of 97%**.** In comparison with MRMA without TDL, behavioral verification introduced additional 0.40 ms (6.15%) latency and reduced throughput by 10 authentications/s (1.11%)**,** while improving AAR from 99.2% to 99.8% and clone detection from 88% to 97%**.** The 100-run analysis also produced a 95% confidence interval of 6.84–6.96 ms for MRMA-TDL latency and 96.85–97.15% for clone detection. These findings demonstrate a favorable simulation-level trade-off between authentication efficiency and behavioral clone detection. The results must nevertheless be interpreted within the limitations of the present study. Evaluation was performed primarily using Python-based workstation simulation rather than an embedded medical-IoT platform. The post-quantum security argument remains conditional on the hardness and concrete security of the selected RLWE parameter set. TDL provides empirical behavioral detection and may be challenged by an adaptive adversary capable of accurately mimicking the legitimate traffic profile. Furthermore, the current construction does not claim perfect forward secrecy under compromise of long-term private keys. Future work will focus on implementation and benchmarking on ARM Cortex-M/ESP32-class platforms, byte-level communication and memory profiling, direct comparison of QAOA with classical parameter-optimization methods, evaluation against adaptive behavioral mimicry, and comprehensive TDL assessment using FAR, FRR, precision, recall, F1-score and ROC-AUC.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

Funding Statement

This research received no external funding.

Acknowledgments

The authors would like to thank the Department of Electronics and Communication Engineering, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India, for providing the research facilities and academic support required to carry out this work.

References

[1] Vadim Lyubashevsky, "Lattice Signatures without Trapdoors," *31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 738-755, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[2] Fengxia Liu et al., "A Survey on Lattice-based Digital Signature," *Cybersecurity*, vol. 7, no. 1, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Richard Lindner, and Chris Peikert, "Better Key Sizes (and Attacks) for LWE-based Encryption," *Lecture Notes in Computer Science*, pp. 319-339, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[4] Vadim Lyubashevsky, Chris Jason Peikert, and Oded Regev, "On Ideal Lattices and Learning with Errors Over Rings," *Journal of the ACM*, vol. 60, no. 6, pp. 1-35, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[5] Joppe Bos et al., "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM," *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, London, UK, pp. 353-367, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Erdem Alkim et al., "*Post-Quantum Key Exchange—A New Hope*," Radbound University, pp. 1-19, 2016. [Google Scholar] [Publisher Link]

[7] Mihir Bellare, and Phillip Rogaway, "Entity Authentication and Key Distribution," *Advances in Cryptology*, pp. 232-249, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ali Shahidinejad, and Jemal Abawajy, "Decentralized Lattice-based Device-to-Device Authentication for the Edge-Enabled IoT," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6623-6633, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sadra Fathenojavan, Ali Moeini, and Hamid Haj Seyyed Javadi, "A Post-Quantum Lattice-based Lightweight Anonymous Authentication Scheme for IoT," *Journal of Cybersecurity*, vol. 11, no. 1, pp. 1-8, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Gagan Kumar et al., "Post-Quantum Secure Lattice-based Lightweight Authentication and Key Agreement Scheme for Multilayer IoT-Enabled Smart Grid System," *IEEE Internet of Things Journal*, vol. 13, no. 11, pp. 24604-24617, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[11] Yongfei Huang et al., "An Efficient RLWE-based Privacy-Preserving Authentication Scheme based on Edge Computing in Industrial Internet of Things," *IEEE Transactions on Services Computing*, vol. 17, no. 5, pp. 2012-2026, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Lingzhe Meng, Qilong Zhu, and Yuanyuan Zhang, "Privacy Protection for Patient-Family Binding E-health System Three-Factor Authentication Key Agreement," *2022 3rd International Conference on Electronics, Communications and Information Technology (CECIT)*, Sanya, China, pp. 402-411, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Arman Ahmad, and S. Jagatheswari, "Lattice-based Three Party Authenticated Key Agreement Scheme in Medical IoT for Post-Quantum Environment," *IEEE Access*, vol. 12, pp. 157247-157259, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] K.S. Riya et al., "Encryption with User Authentication Model for Internet of Medical Things Environment," *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 507-520, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Khizar Hameed et al., "A Context-Aware Information-Based Clone Node Attack Detection Scheme in Internet of Things," *Journal of Network and Computer Applications*, vol. 197, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Dhruti Upadhyaya, Neha J C, and Venugopal K, "Beyond Signature Validity: Behavioral Fingerprinting for Fake Device Detection in Post-Quantum IoT Networks," *2025 9th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, Bangalore, India, pp. 1-6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Azlina Ahmadi Julaihi, Md Asri Ngadi, and Raja Zahilah binti Raja Mohd Radzi, "A Comprehensive Authentication Taxonomy and Lightweight Considerations in the Internet-of-Medical-Things (IoMT)," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 8, pp. 1013-1025, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Saad N. Altamimi et al., "Interpretable AI-based Intrusion Detection with Hybrid Feature Optimization for Smart Infrastructures," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 50, pp. 3587-3607, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[19] Upendra Chaurasiya, Rakesh Tripathi, and Tirath Prasad Sahu, "Enhancing IoT Network Security: A Feature Selection and Explainable AI Approach for DDoS Attack Detection," *Iranian Journal of Science*, vol. 50, no. 2, pp. 617-634, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[20] Kostas Blekos et al., "A Review on Quantum Approximate Optimization Algorithm and its Variants," *Physics Reports*, vol. 1068, pp. 1-66, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Hafiz Muhammad Waseem, Gregory Epiphaniou, and Carsten Maple, "Quantum-Assisted Optimization and Security for Trustworthy AI-driven Healthcare," *IEEE Transactions on Quantum Engineering*, vol. 7, pp. 1-25, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[22] Dur-E-Shahwar Kundi et al., "AxRLWE: A Multilevel Approximate Ring-LWE Co-Processor for Lightweight IoT Applications," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10492-10501, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Zeeshan Siddiqui, Jiechao Gao, and Muhammad Khurram Khan, "An Improved Lightweight PUF–PKI Digital Certificate Authentication Scheme for the Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 19744-19756, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Kun Wang, "Secure Authentication of Identity Information for Quantum Resistant IoT Devices Based on R-LWE and QIBE," *Journal of Cyber Security Technology*, vol. 9, no. 2, pp. 151-168, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Attila Altay Yavuz, Saleh Darzi, and Saif Eddine Nouma, "LiteQSign: Lightweight and Quantum-Safe Signatures for Heterogeneous IoT Applications," *IEEE Access*, vol. 13, pp. 171442-171456, 2025. [CrossRef] [Google Scholar] [Publisher Link]