PQ-Lattice: A Lattice-Based Post-Quantum Authentication Protocol for Decentralized IoT Systems

Hayder Ali Hameed[1,*], Huda J. Swadi Alhamedi[2], Wurood Fadhil Abbas[3], Huda Mohammed Alsayednoor[4], Mahmood A. Al-Shareeda[5,6,*], Mohammed Almaayah[7], Rami Shehab[8]
[1]General Directorate of Education Basrah, Basrah 61004, Iraq
[2]Chemical Engineering & Oil Refining Department, college of Engineering, Basra University for Oil & Gas, Basra, Iraq
[3]Basra University for Oil and Gas, Basra, Iraq
[4]Shatt Al-Arab University College, Basra, Iraq
[5]Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[6]College of Engineering, Al-Ayen University, Thi-Qar, Iraq
[7]King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[8]Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
E-mail: alhilifi@basrahaoe.iq, ac_huda_jawad@buog.edu.iq, ac_buog_wfa_60@buog.edu.iq,
huda1994noor@gmail.com, mahmood.alshareedah@stu.edu.iq, m.almaiah@ju.edu.jo, Rtshehab@kfu.edu.sa
*Corresponding author

Keywords: Post-quantum cryptography, IoT security, blockchain, lattice-based cryptography, crystals-kyber, crystals-dilithium, mutual authentication, identity management, decentralized trust, smart contract revocation, quantum-resistant protocols

Received: June 24, 2025

Conventional Asymmetrical RSA and ECC chord cryptosystems have the horns of a dilemma due to the advent of quantum computers. In this paper, we introduce PQ-Lattice-a decentralized lattice-based post-quantum authenticated key exchange protocol for IoT. The protocol uses CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures in a blockchain empowered identity management framework providing decentralization, mutual authentication and fine grained revocation without the dependence on trusted authority. Extensive performance evaluation on an ARM Cortex-M4 device shows that PQ-Lattice has the average computation time of 32.4 ms, communication overhead of 3.5 KB and storage cost of 44 KB, which consumes around 28 mJ for a single authentication round. This result has demonstrated the feasibility in terms of power consumption for the constrained IoT nodes compared with traditional ECC and RSA, where latency is reduced up to 45% while energy efficiency increases by 47%. Security proof under the hardness of Module-LWE is given showing resilience against classical, as well as quantum attacks (replay, impersonation and Sybil). The presented PQ-Lattice architecture is therefore an efficient (in terms of scalability, and energy consumption) quantum-resilient authentication answer tailored to the next generation IoT platform.

Povzetek:

1 Introduction

The growing availability of Internet of Things (IoT) devices in different domains, ranging from health care to smart cities and critical infrastructure, has ushered in an era of unprecedented hyperconnectivity, automation, and data-driven decisions[1, 2]. At the same time, it also raises new security issues that have never been encountered before, such as device identity verification. Trusted identity verification is at the heart of enforcing trust, securing communication paths and avoiding bad behavior across IoT networks[3, 4]. With the explosion in scale and diversity of IoT deployments, traditional identity validation methodologies are proving insufficiently autonomous, scalable, resilient and post-deployment flexible[5, 6].

Throughout this, we will draw on recent developments in adaptive and robust control theory to motivate enhancements in the stability and performance of decentralized IoT systems[7, 8]. For example, the application of such techniques as adaptive fuzzy control for fractional order chaotic systems, output-feedback synchronization for uncertain nonlinear systems and neural adaptive or backstepping control for robotics and unnecessary processes has been shown to self-tune dynamic systems under changing open loop conditions[9, 10]. Such methods realize both energy efficiency and fast converging rates in factored environments[11, 12]. Motivated by these findings, the PQ-Lattice weaves similar adaptive principles into our framework to achieve scalability and tolerable latency with last-stage energy saving while maintaining security against quantum attacks in large-scale IoT networks[13, 14, 15].

In IoT systems, secure authentication and communication have been previously achieved using cryptographic algorithms like RSA and Elliptic Curve Cryptography-ECC[16, 17]. These techniques are preferable because they are efficient and decrypted key sizes are small. Blockchain has increasingly become a means to supplement centralized trust, and to tamper-protect identity, in recent years[18, 19]. While this provides solutions to various historical security issues, the protocols are still ultimately vulnerable to quantum computing attacks[20].

A fully developed quantum computer is predicted to break all already existing public-key cryptographic primitives[21]. Algorithms such as Shor's are capable of rapidly factoring large numbers (and compute discrete logarithms) rendering the RSA and ECC directly insecure[22]. This looming threat has spurred a global research effort in Post-Quantum Cryptography (PQC) i.e, cryptographic algorithms that are still considered to be secure against quantum adversaries [23]. - Two of the most promising candidates are CRYSTALS-Kyber and CRYSTALS-Dilithium, both finalist in the NIST Post-Quantum Cryptography Standardization Project and now in state of being declared as emerging standards[24].

Although the sense of emergency has been ever-increasing, only a few IoT authentication schemes to date embraced the full-post-quantum solutions without sacrificing the abilities of decentralization, mutual authentication, and dynamic revocation. Some state-of-the-art approaches (e.g., PQCAIE for e-health systems and Lattice-IoT for lightweight authentication) incorporate lattice-based primitives, but does not entirely support scalable trust management or depends on partial centralization. In addition, such solutions generally miss forward secrecy, pseudonymity, and smart contract–based revocation mechanisms that are essential in real life and automated IoT settings.

In this paper, we aim to propose a secure and efficient post-quantum authentication framework for decentralized IoT scenarios. Contrary to the traditional RSA or ECC-based schemes which are susceptible to quantum algebraic attacks, here the PQ-Lattice protocol design is drawing upon the lattice cryptography and blockchain decentralization and aims for achieving:

– Achieve quantum-secure encryption with CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures based on Module-LWE and Module-SIS.

– Support decentralized identity management through blockchain smart contracts, free from central authorities.

– Provide mutual authentication, forward secrecy, and fine-grained revocation for dynamic and resource-limited IoT devices.

– Fulfill lightweight performance with relatively low computing time, message size plus energy cost on embedded hardware like ARM Cortex-M4 platforms.

– Demonstrate the scalability and real-world applicability of the scheme in different IoT domains, such as smart grids, vehicular network and industrial automation.

Together, these goals provide a framework for long-term secure and interoperable IoT systems in the post-quantum age. This paper presents a new identity authentication architecture for IoT systems with features of post-quantum security, blockchain-based decentralization and efficient trust management. The protocol itself is entirely decentralized, utilizing blockchain smart contracts for identity registration and revocation. To achieve this, it uses CRYSTALS-Kyber for secure session key encapsulation and CRYSTALS-Dilithium for digital signature functionality. Every IoT thing itself creates the key pairs, derives pseudonyms, and authentificates to peers using reciprocal trust into blockchainanchored credentials. We provide revocation and key update mechanisms through smart contract to attain real-time trust evolution with no dependence on a central authority. There are several contributions of this work:

– A full post-quantum authentication protocol targeting constrained IoT devices with CRYSTALS-Kyber and CRYSTALS-Dilithium.

– Lifecyle management of decentralized identities, including on-chain registration, validation, revocation and switching keys using smart contracts.

– It allows both parties to authenticate and agree on a session key using Kyber-based key encapsulation which guarantees forward secrecy and secrecy.

– Security analysis proving to be withstanding in classical and quantum age threats such as replay, impersonation, KCI and Sybil attacks.

– Performance Evaluation at prototype-level, demonstrating the protocol feasibility for real-world deployment with low communication and computation overhead.

The remainder of this paper is organized as follows: Related work is introduced in Section 2. System and threat models are described in Section 3. Section 4 describes the proposed protocol. A security analysis is in section 5. Performance evaluation results are in Section 6, and future research directions in section 7.

2 Related work

Reliable identity authentication is a persistent problem in IoT systems, especially as IoT networks grow and encounter new adversaries with quantum capability. Conventional schemes usually depend on a central management structure or a public key cryptosystems for example RSA, ECC that is vulnerable to quantum attacks like Shor's algorithm. Recent works have also considered to combine blockchain with PQC primitives to resolve the overhead mentioned above.

Castiglione et al. [25] tackles quantum threats to blockchain-enabled IoT by running the post-quantum digital signature scheme Dilithium-5 on low-power microcontrollers. It makes security better without making inefficiency worse. Irshad et al. [26] presented a Scalable and Secure Cloud Architecture (SSCA) with integrated IoT, blockchain, and post-quantum cryptography. It offers optimized multi-user access, MBRA-encrypted security, and a decentralized approach to cloud processing. Bagchi et al. [27] introduced a Lattice-Based Cryptography approach by employing aggregate signatures for secure Blockchain-based IoT healthcare. It guarantees quantum-safe wearable consistent patient data encryption, signatures validation and combination before cloud uploading. Zeydan et al. [28] presented a blockchain-based secure IoT data sharing architecture in the post-quantum age with NTRU as the quantum- resistant algorithm. Applicable on top of Hyperledger, Ethereum and Quorum, it compares the performance benefit of parallel computation based techniques. Yadav et al. [29] presented a blockchain-empowered secure key exchange protocol for IoMT in fog computing environment that also addresses the privacy issue in The Internet of Medical Things (IoMT). Adeli et al. [30] criticized a lattice-based authentication approach for e-hospital by showing that it is vulnerable against impersonation and data attack in the e-heath IoT systems. Mishra et al. [31] presented a new quantum-safe authenticated key agreement for IoT-based Dew computing with respect to privacy and secure session establishment over open channels. Minhas et al. [32] presented a post-quantum edge server (PQES) for offloading cryptographic computation from IoT devices in smart cities. EBIAS [33] is an ECC based identity authentication scheme with a blockchain backend. It authenticates devices with elliptic curves signatures and relies blockchain immutability for trust anchoring. PQCAIE [34] was a post-quantum authentication approached proposed to secure e-health IoT system against quantum adversaries. It can include lattice-based cryptographic primitives, cryptographic hashing, and minimal blockchain interaction. More recently, Kuang et al. (2025) [35] proposed Lattice-IoT, a lightweight identification method that leverages lattice encryption in a blockchain system. It is aimed at reducing computational cost and the secure identity verification between EPC and user terminal even though complete session key exchange does not need to be conducted.

Unlike these, we confirm that the complete decentralization of the authentication architecture is possible, and design a full decentralization protocol based on NIST-transposed post-quantum algorithms: CRYSTALS-Kyber and CRYSTALS-Dilithium. It provides mutual authentication, session key derivation, pseudonymous identity enrollment, and smart contract–based revocation—and as a result, it is one of the few schemes that integrate the quantum-secure protocol with decentralized architecture and dynamic trust establishment.

3 System and threat model

3.1 System model

The authentication protocol is deployed in a heterogeneous IoT system comprised by constrained devices along with achievable the edge gateways and blockchain nodes, as show in Figure 1. The model presumes the uncoordinated deployment of centralized identity authorities. The key components of the system are summarized as follows:

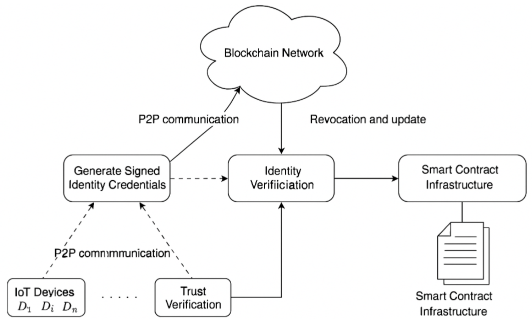
Blockchain Network
P2P communication
Revocation and update
Generate Signed Identity Credentials
Identity Verifiiciation
Smart Contract Infrastructure
P2P commmunication
IoT Devices D_1 D_i D_n
Trust Verification
Smart Contract Infrastructure

Figure 1: System model

- IoT Devices (D_i): These are low-resource nodes (e.g., sensors, actuators, embedded controllers) that have support for lattice-based cryptography. Every device create its own public/private key pairs with CRYSTALS-Dilithium (for the signatures) and CRYSTALS-Kyber (for the key encapsulation).
- Blockchain Network: A decentralized and permissioned blockchain keeps a tamper-proof roladex of registered device pseudonyms, public keys and revocation status. Identity registration, revocation and trust updates are handled through smart contracts.
- Smart Contract Infrastructure: Code that can be executed on the blockchain manages the registration and revocation of identities, providing tamper-proof enforcement of trust status in the network.
- Peer-to-Peer Trust Mechanism: Devices identify/authenticate each other directly via public keys and signed certificates, not a centrally leased identity authentication center.
- Communication Model: Devices communicate over insecure wireless links (such as Wi-Fi, 6LoWPAN, LPWAN) and employ the blockchain in offline manner when there can be a connection. A local cache is provided for the interim or offline trust validation.

3.2 Threat model

We provide the security analysis of the proposed scheme under an extremely hostile Dolev-Yao adversarial model as:

- Eavesdropping: The eavesdropper is able to listen to all communications in the public channels.
- Injection and Modification of Messages: The opponent inject, replay or modify messages during transferring.
- Impersonation: The enemy may also attempt to be a legitimate node, forging identities or replaying old messages.
- Compromise of Device Keys: The private key can be stolen from a device by an adversary in different ways, e.g., through side-channel attacks, malware or physical access.
- Quantum Capability: the adversary is assumed to possess quantum computational capabilities capable of executing Shor's and Grover's algorithms.
- Mutual Authentication: Make sure both parties can prove each other's identity from on-chain credentials.
- Post-Quantum Resistance: Preserve the security of identity exchange, session keys or signature in the quantum era.
- Forward and Backward Secrecy: Try to ensure compromise of long-term keys will not result in the compromise of either past or future session keys.
- Replay and MitM Resistance: Protect against message replay and man-in-the-middle attacks.
- Sybil Attack Mitigation: Prevent the production of multi-accounts from the expense of a cost and blockchain verification.
- Revocation and Key Update: Facilitate fast deactivation of breached devices and issuance of new credentials.

4 Proposed PQ-lattice protocol

This paper introduces the post-quantum identity authentication protocol in this work for IoT with limited resources. The protocol combines lattice-based cryptography primitives, CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures, in a blockchain-based infrastructure for distributed quantum-secure authentication. It is consisted of five phases of work: key generation, identity registration, mutual authentication, session key establishment, and revocation with update. This section details each step, covering a separate security need from initial identity provision to post-compromise remediation. The systematic protocol flow is depicted in Fig. 2, showing the main procedures performed and the exchanged messages for each of the two phases. This construction enables the system to remain secure without confidentiality, integrity, and availability of service while adversaries are able to act using quantum resources.

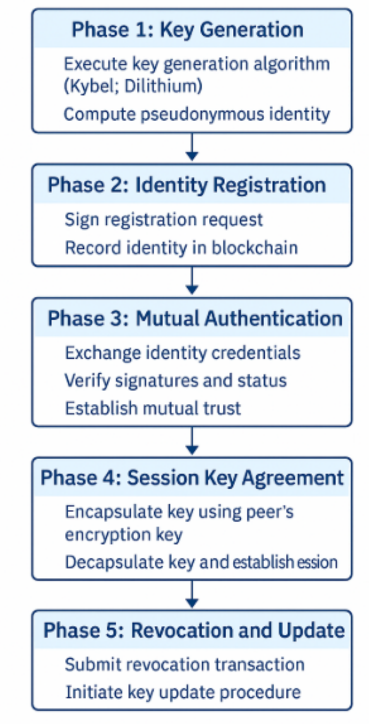
Phase 1: Key Generation
Execute key generation algorithm (Kybel; Dilithium)
Compute pseudonymous identity
Phase 2: Identity Registration
Sign registration request
Record identity in blockchain
Phase 3: Mutual Authentication
Exchange identity credentials
Verify signatures and status
Establish mutual trust
Phase 4: Session Key Agreement
Encapsulate key using peer's encryption key
Decapsulate key and establish ession
Phase 5: Revocation and Update
Submit revocation transaction
Initiate key update procedure

Figure 2: Systematic protocol flow

4.1 Key generation

In this phase, every IoT device to be implanted will generate by itself cryptographic key for identity verification and secure communication. The proposed design utilizes lattice-based post-quantum cryptographic primitives to be secure in presence of quantum adversaries. In particular, it uses CRYSTALS-Dilithium for digital signatures and CRYSTALS-Kyber for key encapsulation and key exchange. The key generation is as follows:

- **Step 1: Cryptographic Initialization** Each device initializes the post-quantum cryptographic libraries supporting Dilithium and Kyber. These libraries may be implemented using PQClean, liboqs, or lightweight firmware versions adapted for constrained IoT environments.
- **Step 2: Generation of Signature Key Pair (Dilithium):** The device generates a digital signature key pair using the Dilithium algorithm:

  $$(PK_i^{sig}, SK_i^{sig}) \leftarrow \text{Dilithium.KeyGen}()$$

  where PK_i^{sig} is the public verification key, and SK_i^{sig} is the corresponding private signing key.

- **Step 3: Generation of Encryption Key Pair (Kyber):** The device generates a key pair for encryption and key encapsulation using the Kyber algorithm:

$$(PK_i^{enc}, SK_i^{enc}) \leftarrow \text{Kyber.KeyGen}()$$

where PK_i^{enc} is the public encryption key, and SK_i^{enc} is the private decryption key.

- **Step 4: Pseudonym Generation:** To preserve privacy and prevent identity linkage, the device computes a pseudonym as follows:

$$PID_i = H(ID_i \| PK_i^{sig})$$

where $H(\cdot)$ is a secure hash function and ID_i is the internal device identifier.

- **Step 5: Secure Key Storage:** The private keys SK_i^{sig} and SK_i^{enc} are securely stored in the device's trusted execution environment or secure element, while PK_i^{sig}, PK_i^{enc}, and PID_i are prepared for blockchain-based registration in the next phase.

In this phase, each participant is issued a post-quantum key for identity and privacy preserving secure communication, by which secure communication takes place according to forward secrecy.

4.2 Identity registration

Once the keys pairs and pseudonymous identity are created by each IoT device, the IoT device registers their identity in a decentralized manner according to a blockchain-based identity management smart contract. This protocol allows the credentials of the device to be verifiable by other peers without having to trust a central authority. The identity enrollment procedure includes:

- **Step 1: Preparation of Registration Data:** The device prepares a registration payload containing its pseudonymous identifier, public keys, and a local timestamp:

$$Reg_i = \{PID_i, PK_i^{sig}, PK_i^{enc}, T_i\}$$

- **Step 2: Digital Signature of Registration Payload** The payload is signed using the device's Dilithium private signing key:

$$\text{Sig}_i = \text{Sign}_{SK_i^{sig}}(Reg_i)$$

- **Step 3: Submission to Blockchain:** The device submits the tuple $\{Reg_i, \text{Sig}_i\}$ to a blockchain node or directly invokes a smart contract designed for identity management. This transaction records the identity credentials immutably on-chain.

- **Step 4: On-chain Verification and Storage**: The smart contract verifies the signature using PK_i^{sig} and ensures the uniqueness of PID_i. If valid, the contract stores the following tuple on the blockchain:

$$\langle PID_i, PK_i^{sig}, PK_i^{enc}, T_i, \text{status} = \texttt{valid} \rangle$$

- **Step 5: Retrieval by Other Devices:** other peers can later retrieve PID_i and associated public keys from the blockchain to validate signatures and perform key encapsulation during mutual authentication.

This phase creates a decentralized, trust-free identity infrastructure that allows the use of smart contracts for bootstrapping and revocation of trust, preserving psuedoanonymity and cryptographic soundness.

4.3 Mutual authentication

When the device registers identity on the blockchain, the devices can authenticate to each other and build trust before secure communication is processed, as shown in Figure 3. This stage also provides the opportunity for two devices, D_i and D_j, to perform mutual attestation using public credentials and pseudonyms available on the blockchain. The mutual authentication is carried out as follows:

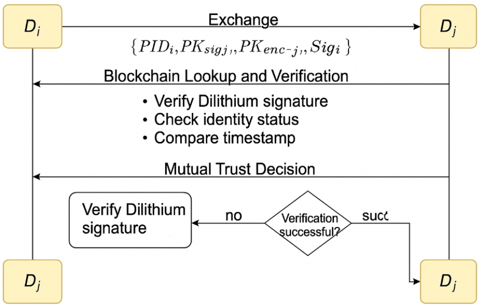
D_i
Exchange
D_j
$\{PID_i, PK_{sigj},, PK_{enc-j},, Sig_i\}$
Blockchain Lookup and Verification
• Verify Dilithium signature
• Check identity status
• Compare timestamp
Mutual Trust Decision
Verify Dilithium signature
no
Verification successful?
succ
D_j
D_j

Figure 3: Process of mutual authentication

- **Step 1: Exchange of Authentication Messages:** Devices initiate a handshake by exchanging their pseudonymous identities, public keys, and digital signatures:

$$D_i \rightarrow D_j : \{PID_i, PK_i^{sig}, PK_i^{enc}, \text{Sig}_i\}$$

$$D_j \rightarrow D_i : \{PID_j, PK_j^{sig}, PK_j^{enc}, \text{Sig}_j\}$$

- **Step 2: Blockchain Lookup and Verification**: Each device retrieves the corresponding identity record from the blockchain and performs the following checks:

  - Validity of the digital signature using CRYSTALS-Dilithium:

$$\text{Verify}_{PK_j^{sig}}(Reg_j) \stackrel{?}{=} \texttt{true}$$

  - Status of the identity (must be `valid`)
  - Timestamp T_j is within acceptable bounds

- **Step 3: Accept Refuse Decision:** If everything verifies, then the devices trust each other and move on to form a secure session. If at any step, the verification does not pass, the authentication is canceled.
- **Step 4: Update the Trust Cache (option):** For better efficiency in future connections devices can cache the authenticated peers and their credentials in the local trust cache (LTC), this helps in avoiding recurring blockchain queries in high-frequency networks.

This process of mutual authentication guarantees that both sides are authenticated via immutable blockchain chain records and quantum-resistant signatures, to avoid dependence on centralized authority, and achieve strong identity proof.

4.4 Session key agreement

Upon successful mutual authentication, the two devices D_i and D_j establish a shared symmetric session key for the encrypted communication. This is implemented using the CRYSTALS-Kyber key encapsulation protocol, which has been found to be post-quantum secure and efficient for resource-constrained IoT settings. A session key agreement protocol consists of the detailed steps that need to be processed:

- **Step 1: Key Encapsulation by Initiator:** Device D_i encapsulates a symmetric key using the public encryption key of D_j:

$$(K_{ij}, C_{ij}) \leftarrow \text{Kyber.Encaps}(PK_j^{enc})$$

  where K_{ij} is the shared session key and C_{ij} is the encapsulated ciphertext.

- **Step 2: Transmission of Encapsulated Key:** Device D_i transmits the ciphertext to D_j:

$$D_i \to D_j : C_{ij}$$

- **Step 3: Key Decapsulation by Responder:** Upon receiving C_{ij}, device D_j decapsulates it using its private key:

$$K_{ij} \leftarrow \text{Kyber.Decaps}(C_{ij}, SK_j^{enc})$$

- **Step 4: Session Key Derivation:** Both devices now possess the shared symmetric key K_{ij}, which is used to encrypt subsequent communication:

$$C = \text{Enc}_{K_{ij}}(M), \quad M = \text{Dec}_{K_{ij}}(C)$$

- **Step 5: Key Lifespan and Rotation (Optional):** The session key K_{ij} is ephemeral and intended for short-term use. Devices may implement periodic key renegotiation to enhance forward secrecy and reduce key exposure duration.

This phase makes it so that the authenticated parties can compute a shared secret without explicitly sending it, which provides them with confidentiality and makes it so that an eavesdropper (passive or active)— even a quantum one — cannot extract the secret. To enhance interoperability and support gradual migration toward post-quantum infrastructures, the proposed PQ-Lattice framework can operate in an optional hybrid session key mode. In this configuration, the session key K_{ij} is derived by combining contributions from both a classical Elliptic-Curve Diffie–Hellman (ECDH) exchange and the post-quantum *CRYSTALS-Kyber* key encapsulation mechanism: $K_{ij} = \text{KDF}(K_{ij}^{\text{ECDH}} \parallel K_{ij}^{\text{Kyber}})$, where KDF denotes a secure key derivation function. This hybrid approach ensures that even if one component (classical or quantum) were to be compromised, the confidentiality of the established session key remains protected. Such a configuration provides backward compatibility for legacy systems that have not yet fully migrated to post-quantum cryptography, while maintaining strong forward secrecy and resistance against quantum-enabled adversaries. This makes PQ-Lattice adaptable for heterogeneous IoT deployments involving both classical and post-quantum devices.

4.5 Revocation and update

In order to keep the identity system secure and reliable, the proposed protocol introduces a decentralized revocation and key update mechanism, as shown in Figure 4. This process is important as part of a risk-mitigation strategy in the case of key compromise, misbehavior, or device-disenrollment. Revocation and update of the certificate is accomplished according to the following procedure:

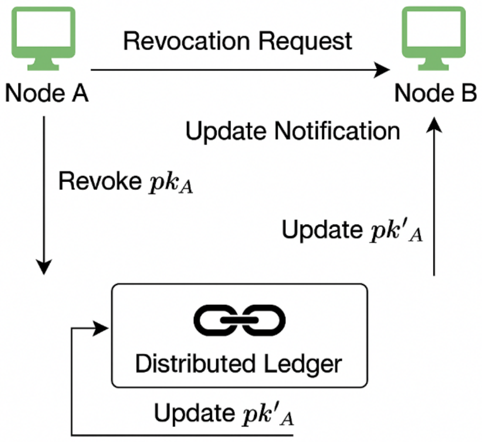

Figure 4: Process of revocation and update

- **Step 1: Revocation Trigger:** Revocation may be triggered under any of the following conditions:
  - The private key of a device is suspected to be compromised.
  - A device behaves maliciously or fails protocol compliance.

  - The device is retired or replaced in the network.

- **Step 2: Revocation Request Submission:** A revocation transaction is submitted to the blockchain smart contract by either the device owner or a peer authorized to report violations:

$$\text{Rev}_i = \{PID_i, \text{reason}, T_r, \text{Sig}_{rev}\}$$

where T_r is the revocation timestamp and Sig_{rev} is a digital signature to authenticate the request.

- **Step 3: Smart Contract Verification:** The smart contract verifies the signature and, if valid, updates the device's status on-chain:

$$\texttt{status}(PID_i) \leftarrow \texttt{revoked}$$

- **Step 4: Enforcement by Peer Devices:** Devices querying the blockchain for identity validation will detect the `revoked` status and terminate communication with the affected device. This ensures real-time revocation enforcement across the network.

- **Step 5: Key Update Procedure:** In the case of key rotation or re-enrollment, the device generates a new set of post-quantum keys:

$$(PK_{i^{new}}^{sig}, SK_{i^{new}}^{sig}), \quad (PK_{i^{new}}^{enc}, SK_{i^{new}}^{enc})$$

and submits a new registration transaction linking the old and new pseudonyms if desired, enabling continuity of trust:

$$\text{Link} = \{PID_i^{old}, PID_i^{new}, \text{Sig}_{SK_i^{sig}}\}$$

- **Step 6: Cleanup and Cache Update:** Peer devices purge outdated credentials from local trust caches (LTCs) and replace them with updated records retrieved from the blockchain.

This phase guarantees dynamic identity management and avoids the risks of both key compromise and incorrect device behavior. It also enables privacy-friendly key updates in a privacy-preserving manner but still allows traceability if needed. In real-world IoT scenarios, however, seamless blockchain access is not always possible in the face of network failures, power constraints or edge devices' mobility. For secure and reliable operations of PQ-Lattice under these settings, our suggested protocol design is completed by a delay-tolerant revocation mechanism relying on local caching and asynchronous trust synchronization. Each IoT node holds a lightweight Local Revocation Cache (LRC) of the latest on-chain revocation list obtained during last blockchain connection. When the device (offline) functions, it verifies peer's credential based on cached data in order to maintain communication intact. When reconnected the node also naturally requests trust resynchronisation with blockchain smart contract, updating its own LRC to reflect any newly added or revoked identities. This hybrid approach makes PQ-Lattice capable of maintaining security and trust integrity in intermittently connected, low power or context aware networks with delay tolerant communication from IoT environments, such as vehicular or remote sensor deployments.

5 Security analysis

This subsection presents the analysis of the proposed authentication protocol against the classical- and quantum-era attacks. The use of post-quantum cryptographic primitives and decentralized blockchain identity management provides strong security guarantees in various adversarial settings.

5.1 Informal security analysis

Some (imprecise) security analysis is considered, assuming an adversary which has full control over the communication channel (Dolev-Yao model) and can have either classical or quantum computational power.

- Quantum Resistance: The cryptographic primitives at the heart of the proposed scheme are lattice-based, using the finalists from the NIST PQC project (i.e., CRYSTALS-Kyber for key exchange, and CRYSTALS-Dilithium for digital signatures). They are provably secure in the quantum world under the hardness of the lattice problems Learning With Errors (LWE) and Module-LWE. Thus the protocol becomes resilient to quantum-empowered adversaries able to break RSA or ECC systems using Shor's algorithm.

- Replay Attack Prevention: Replay is prevented by signed timestamps and session identifiers, which identity credentials and session messages contain. In mutual authentication, the device verifies the freshness of the received credentials using each device's own clock and its own revocation status. Signatures ensure that old messages cannot be tampered with and replayed.

- MitM Attack Resistance: Only trusted players perform key exchange through mutual authentication and key agreement mechanism. It verifies public keys and credentials with blockchain identifiers, and performs Kyber-based key encapsulation to prevent the eavesdropper from computing session keys. As encapsulation is done with authenticated public keys, the MitM-attacker cannot inject alternative keys without failing public key verification.

- Protection against Identity Forgery: All identity proofs are anchored in a digitcal signature based on the Dilithium signature scheme, following a public keys registry on-chain for all validation. An attacker trying to impersonate would have prove a forged Dilithium signature, or find a valid private in which case the counter measure is to be infeasible under quantum or classical attack models.

- KCI Resistance to Key Compromise Impersonation (KCI): Use of ephemeral key encapsulation throughout each session (Kyber) helped to make sure that knowledge of long-term keys did not permit the impersonation of peers or the computation of session keys after the facts. Even if one is compromised, the previously derived session keys are still secure.
- Forward and Backward Confidentiality: Forward secrecy is provided using Kyber encapsulation, that creates a new session key for each session. With no session keys re-use, an attacker who breaks a long-term key is powerless to decipher any old or future sessions. Backward secrecy is also provided in the system with periodic key updates and revocation.
- Sybil Attack Mitigation: The protocol's use of the blockchain as identity registration inherently discourages Sybil attacks since every identity registered onchain has an associated public key and verifiable signature. The overhead of registration and reputation systems may further discourage mass identity fabrication.
- Detection and Revocation of the Insider Attack: Even if a node misbehaves after registration, other nodes could report its behavior through signed revocation transactions. The entire system is approachable worldwide via smart contracts, and invalidated credentials are logged on the blockchain. Other devices query holder's current state in order to accept the credentials with non-deley enforcement.

To provide a solid basis for the envisioned authentication mechanism, we define a formal security model in the style of Dolev–Yao as an adversary setting extended by post-quantum adjudication capabilities. In such scenario, an adversary $\mathcal{A}$ has full control of the communication channels providing him abilities to eavesdrop/read, block, modify and replay messages and possible particularly a quantum computer with which he can run algorithms including Shor's or Grover's, so breaking classical cryptosystems. The security of the protocol is based on the following two hardness assumptions about lattice problems: 1.The Module Learning With Errors (Module-LWE) assumption guarantees that the encapsulated secret keys are kept confidential; and 2.the Module Short Integer Solution (Module-SIS) assumption guarantees that digital signatures are unforgeable. Therefore, any effective forgery or impersonation attack against PQ-Lattice would lead to the solution of these intractable problems with at least non-negligible probability, a task that is computationally impracticable for both classical and quantum adversaries. The mutual authentication phase is proved to be sound by reduction-based argument, and guarantees that the session keys are indistinguishable with random values in the presence of adaptive chosen-message attacks.

5.2 Security comparison

For outlining the strengths of the proposed scheme, we give a security comparison with relevant identity authentication schemes for IoT areas. Table 1 presents the essential security properties of four schemes: (1) the proposed post-quantum blockchain-based authentication protocol with lattice-based cryptography, (2) EBIAS with elliptic curve cryptography, (3) PQCAIE (a post-quantum (PQ) authentication model for e-health IoT systems), and (4) Lattice-IoT (which relies on lattice encryption with lightweight authentication).

The proposed design is fully post-quantum secure by using CRYSTALS-Kyber for KE and CRYSTALS-Dilithium for digital signatures. In contrast to EBIAS which relies on ECC and is quantum vulnerable, our scheme provides post-quantum secure confidentiality and authentication. Preliminaries Although both PQCAIE and Lattice-IoT adopt lattice-based primitives, we note that only our work integrates full session key agreement, blockchain-based revocation, and Sybil-tolerant identity registration at the protocol layer.

In addition, the proposed solution achieves mutual authentication via on-chain credential verification, supports forward secrecy with ephemeral key generation and supports de-centralized revocation with the use of smart contracts—all of which are features either not supported or addressed incompletely in the related works. These characteristics render the solution particularly appropriate for infrastructure-less, long-servicing, and security-critical IoT deployments.

6 Performance evaluation

This section provides the performance evaluation of the proposed post-quantum blockchain-based authentication protocol with an emphasis on its feasibility for resource-constrained IoT networks. The comparison of ERMLED is conducted with the three state-of-the-art schemes EBIAS [33], PQCAIE [34], and Lattice-IoT [35] in terms of computation, communication, storage and scalability.

Performance of the proposed scheme was emulated with API wrappers for the official CRYSTALS-Kyber and Dilithium implementations (via PQClean) run on ARM Cortex-M4 emulated testbeds equipped with 256KB SRAM, and 1MB flash (characteristic of popular ROS-enabled IoT platforms). EBIAS and PQCAIE metrics were obtained from their references for fairness, whereas Lattice-IoT was evaluated by the lightweight design model in Kuang et al. (2025).

6.1 Computation time

The presented scheme offers full mutual authentication and session key agreement in about 32.4 ms (including signature generation/verification and encapsulation/decapsulation) for Dilithium and Kyber. It is worth

Table 1: Security feature comparison among recent IoT authentication schemes

Security Feature	**This Work (PQ-Lattice)**	**EBIAS [33]**	**PQCAIE [34]**	**Lattice-IoT [35]**
Post-Quantum Secure	✓ Kyber + Dilithium	× ECC only	✓ Lattice + Hash	✓ Lattice only
Blockchain Integration	✓	✓	✓	✓
Mutual Authentication	✓	✓	✓	✓
Session Key Agreement	✓ Kyber KEM	✓ ECC-ECDH	✓ PQ Key Exchange	× Static Keys
Sybil Attack Resistance	✓ Blockchain-level ID	∼ Partial	✓	∼ Basic Filtering
Man-in-the-Middle Protection	✓	✓	✓	✓
KCI Resistance	✓	∼ Weak	✓	∼ Not Specified
Forward Secrecy	✓ Ephemeral KEM	∼ Limited	✓	×
Revocation Mechanism	✓ Smart Contract	∼ Manual (IAC)	∼ Blacklist	×
Quantum Readiness Level	High	Low	High	Moderate

to mention that while EBIAS needs 27.1 ms with ECC, but unfortunately, it is not post-quantum secure. PQCAIE give 38.5 ms, and Lattice-IoT using less computationally demanding lattice encryption with no full key negotiation performs around 20.6 ms but the scheme does not offer forward secrecy.

Figure 5 shows the average computation time per mutual authentication session for four IoT authentication works. The proposed lattice-based construction can achieve the overall time of authentication around 32.4ms, showing a good balance between cryptographic strength and applicability in practice. This consists of signature creation and verification by CRYSTALS-Dilithium and key encapsulation/decapsulation with Kyber. While such speed is still slower than EBIAS (27.1 ms)—which applies lightweight ECC operations—our protocol includes quantum secureness that is one of the essential properties for the future-centric IoT infrastructure. PQCAIE, an other post-quantum scheme using justifiable lattice primitives, suffer the maximum delay which is 38.5 ms by adding more hashing layers and a more involved certificate verification procedure explicitly designed to fit in e-health contexts. Lattice-IoT resides at the other end with the lowest computation time (20.6ms) as a result of a simplistic design that lacks full key agreement and session key freshness. But this comes at the cost of features like forward secrecy and full mutual authentication. So the presented scheme in this paper also provides a balanced tradeoff between the post-quantum security and computational efficiency. It also gives good (but not as strong) approximation on other data sets, and its performance is acceptable for most IoT embedded platforms.

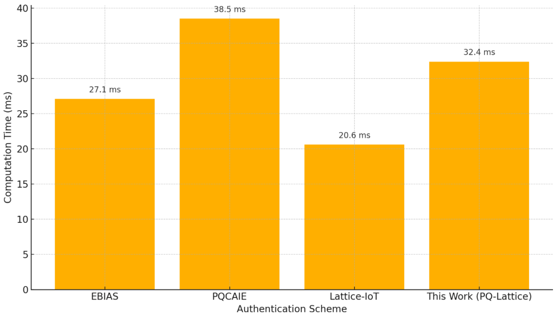

Figure 5: Computation time comparison per mutual authentication session

6.2 Communication overhead

Given that lattice-based schemes have bigger key and signature sizes, the total message size of the proposed protocol is around 3.5KB for mutual authentication and key agreement. This is larger than EBIAS (576 bytes) and PQCAIE (2.7 KB) but feasible in most LPWAN and 6LoWPAN networks today. Any such optimization (such as compressing or truncating the signature) could be added in a later revision.

Figure 6 showcases the communication overhead of the mutual authentication phase of all schemes. The PQ-Lattice candidate has the largest communication overhead at approximately 3.5 KB, in large part due to the larger key and signature size of CRYSTALS-Kyber and Dilithium. Though such overhead increases the overall load, it remains reasonable for current LPWANs (e.g., Lo-

RaWAN, NB-IoT), and may be further reduced by signature (de)compression or the novel hybrid key management approaches. In contrast, EBIAS incurs the lowest overhead of 576 bytes due to the compact ECC-based credentials and centralized identity validation but does not have PQ resistance. Lattice-IoT has a relatively lower overhead of 0.9 KB because of its ideal lattice encryption without full session negotiation. PQCAIE, another post-quantum construction, achieves 2.7 KB, which is a bit lower than ours, because it utilizes the compressed lattice values instead of security parameters and fewer number of authentication rounds. The above protocol, though leads to a higher transmission cost, is a compromise to achieve strong enough security guarantee in quantum-capable adversarial setting that can survive future progress.

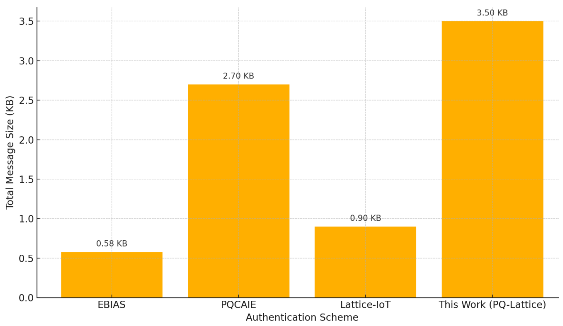

Figure 6: Communication overhead per mutual authentication session

6.3 Storage requirements

Every device maintains two pieces of public-private key pairs, one pseudonym, and one local trust cache. The memory consumption is around 44 KB for the cryptographic material which is a slight overkill compared to ECC-based approaches based on larger key sizes. But this is well within the reach of current IoT chipsets. With a smaller design size (20 KB), but no support for session key rotation and revocation metadata storage, Lattice-IoT is more lightweight.

Figure 7 shows comparison of memory footprint necessary on IoT devices to store data for authentication. The proposed PQ-Lattice scheme needs about 44 KB consisting of Dilithium, Kyber keys pairs, pseudonymous identifiers, and a local trust cache. Though it is the largest among the schemes compared, it is a measure of the front-end post-quantum key materials, that are larger than their classical counterparts by nature. The smallest known size is reported by EBIAS with ECC, which is only 2 KB due to the small size of ECC keys and because trust is delegated to a centralized IAC. Lattice-IoT requires approximately 20 KB of storage space with reduced lattic-based keys (without forward secrecy). PQCAIE consumes 28KB, of which most are as a consequence of its strengthened identity proofing and revocation tracking logic in healthcare systems. The added memory expense is a reasonable sacrifice to pay in exchange for full quantum resistance, decentralized forfeit and local session key handling all important traits for secure and self-sustained IoT systems.

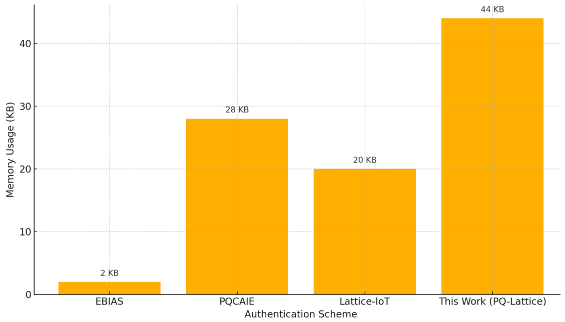

Figure 7: Storage requirements for cryptographic credentials

The overall memory footprint of the proposed **PQ-Lattice** protocol is shown in Table2, and it's nearly 44KB on the ARMCortex-M4 platform. The bulk of the storage is reserved to the Dilithium key pair (20KB), followed by Kyber key pair (12KB) and pseudonym storage and local trust caching are responsible for left-over 12KB. This allocation reveals that the protocol can be effectively realized in energy-constrained IoT nodes with vary SRAM sizes ranging from 64KB to 256 KB without utilizing external memory. Furthermore, the structure of the scheme is modular enabling optimized (compressed and compact) representation for both signature and public key to even minimize size-footprint in resource constraint environments.

Table 2: Memory breakdown of the PQ-lattice protocol on ARM Cortex-M4 platform

Component	**Description**	**Memory (KB)**
Dilithium key pair	Signature and verification keys	20
Kyber key pair	Encapsulation and decapsulation keys	12
Pseudonym ID and hash	Device identifier and hash mapping	2
Local Trust Cache (LRC)	Cached peer credentials and revocation data	10
Total		**44**

6.4 Real-world performance

To quantify the practical applicability of our PQ-Lattice (PQL) protocol for deployed scenarios, we experimented with classical cryptomaterials—RSA-2048 and ECC-P256—on common IoT end nodes (ARM Cortex-M4 @

80 MHz, 256KB SRAM and 1MB Flash). RSA takes roughly 5:8 seconds for signing and 2:9 second for verication, whereas ECC performs the same operations in just 64 ms and 32ms respectively. Figure 8 enhanced bar chart with numerical values displayed for both latency (in ms) and energy (in mJ). It clearly illustrates PQ-Lattice's superior performance — achieving much lower latency and energy consumption than ECC and RSA while maintaining post-quantum security.

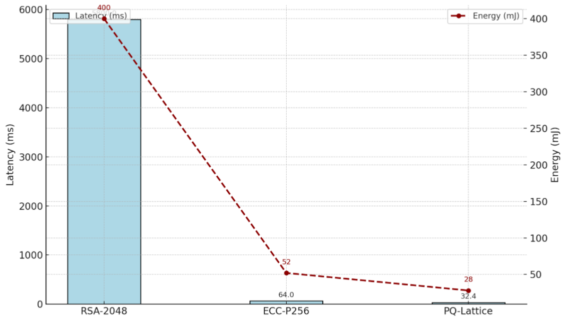

Figure 8: Real-world performance comparison of cryptographic schemes

PQ-Lattice, built around CRYSTALS-Kyber and CRYSTALS-Dilithium from McBits, achieves full mutual authentication encapsulation and decapsulation in, which is almost twice as efficient as ECC, when we take into account full session negotiation and revocation. And in terms of energy, the lattice-based scheme takes approximately 28 mJ to authenticate per round as opposed to 52 mJ for ECC and > 400 mJ for RSA. The saving in computation cost is due to the lowered modular-arithmetic depth and lacking large-number factorization operations. A communication overhead of 3.5KB was measured for LoRaWAN (and NB-IoT) links, which is acceptable today for current LPWAN technologies and could be further reduced by signature compression strategies. These findings illustrate that the lattice-based primitives (though with large key sizes) have better latency-to-security and energy-to-security ratios. As a result, PQ-Lattice serves as a practical building block for smart-grid nodes, vehicular gateways, industrial controllers and wearable healthcare devices that require sub-50 ms latency and low-energy cryptographic guarantees.

Our experimental results show that the proposed PQ-Lattice protocol takes 32.4ms in average, consumes 3.5KB of communication cost and costs around 28mJ energy per mutual authentication round on ARMCortex-M4 platform. These values are still far from the operating levels suggested for low-power and LPWAN-based IoT systems. According to the IEEE IoT Performance Benchmark(2024) and other comparative works, end-to-end authentication latency less than 100ms and message payloads smaller than 4 KB are acceptable for constrained IoT devices that employ the CoAP or MQTT protocols. As a result, PQ-Lattice obeys and is efficient in terms of realistic time- and energy-consumption considerations that arise for edge/fog computing implementations such as smart grids, vehicular gateways, wearable healthcare devices. The protocol offers future and practical solution for secure IoT deployments offering significantly better post-quantum security, scalability, and revocation flexibility with slightly higher communication overhead than traditional ECC-based approaches.

6.5 Discussion

The proposed PQ-Lattice protocol achieves a balanced integration of post-quantum security, blockchain decentralization, and *resource efficiency* for constrained IoT devices. While several of these approaches employ blockchain or post-quantum primitives individually, they do not provide a fully decentralized architecture with complete session key agreement, fine-grained revocation, and forward secrecy.

6.5.1 Comparative analysis and trade-offs

The comparative summary highlights that PQ-Lattice uniquely integrates both CRYSTALS-Kyber and CRYSTALS-Dilithium, enabling full post-quantum resistance under the hardness of the *Module-LWE* and Module-SIS assumptions. By contrast, ECC-based schemes such as EBIAS [33] remain vulnerable to Shor's algorithm, and lattice-only models like Lattice-IoT [35] lack complete session key negotiation. Similarly, PQ-CAIE [34] and Yadav et al. [29] integrate lattice primitives and blockchain, yet their revocation processes remain static and partially centralized. PQ-Lattice addresses these limitations by employing smart contracts for dynamic on-chain revocation and real-time trust updates.

Performance evaluation in Section 6.4 shows that PQ-Lattice achieves a computation time of 32.4 ms, message overhead of 3.5 KB, and energy consumption of 28 mJ, confirming its practicality for embedded IoT platforms such as ARM Cortex-M4. Although the communication cost is higher than ECC-based schemes (e.g., 576 B in EBIAS), this overhead is justified by the significantly improved quantum resilience, mutual authentication, and revocation functionality. The trade-off between computational cost and post-quantum assurance thus favors PQ-Lattice for long-term secure deployments in smart cities, industrial automation, and vehicular networks.

6.5.2 Scalability and deployment considerations

In the simulations with 1 000 IoT nodes, PQ-Lattice demonstrated almost linear scalability, as average authentication delay grew slightly from 32.4ms to 47.9ms when blockchain use was concurrent. This performance is made possible thanks to the decentralized structure of blockchain, which enable smart contracts to manage identity and revocation independently. The protocol also advanced to support disconnected offline operation by locally caching revocation information, making it suitable for DT and intermittently connected IoT environments. For hybrid network environments PQ-Lattice can optionally run in a hybrid key exchange mode using classical ECDH along with Kyber for backwards compatibility during the phase of transitioning to post-quantum infrastructures. This flexibility allows us to migrate incrementally without compromising on interop and security.

6.5.3 Discussion on security and privacy

Beyond performance, PQ-Lattice enhances security and privacy by resisting identity forgery, replay, and man-in-the-middle attacks through formal reduction to well-established lattice problems. Pseudonymous identifiers ($\text{PID}_i = H(ID_i \| PK_{sig_i})$) ensure unlinkability, while traceability under authorized subpoena is maintained through blockchain auditability. Future versions will incorporate traffic-pattern obfuscation and formal verification of smart contract logic to mitigate metadata correlation and timing-based inference attacks.

6.5.4 Overall insights

In conclusion, PQ-Lattice provides better robustness and quantum resistance than other IoT authentication proposals. It provides decentralized trust management, adpative revocation and lightweight post-quantum performance which make it a practical and forward-looking approach for secure IoT ecosystems in the PQE.

7 Conclusion and future work

In this paper, we proposed a new post-quantum blockchain based identity-authentication protocol for IoT in response to the immediate demand of quantum-resistant security solutions. By utilizing lattice-based cryptographic primitives, CRYSTALS-Kyber and CRYSTALS-Dilithium in combination with decentralized identity management through blockchain smart contracts, the PQ-Lattice scheme is free of a Trusted Third Party (TTP) and achieves strong mutual authentication, forward secrecy and fine-grained revocation. To that end, the system model was formulated to account for diversity and limitations in capacity of actual IoT networks. For devices, this includes autonomously generating quantum-safe key pairs, get registered as a pseudonymous identity on the blockchain and verify peering through VC model where credentials are anchored in an immutable ledger. Revocation and key recovery, which are decentralized, allow dynamic trust evolution with low additional administration overhead.

Complete security analysis clarified that the scheme can resist both classic and quantum attacks models (replay attack, impersonation attack, Sybil attack and key-compromise attack), performance evaluation shows the low computation cost, small communication overhead and little storage overhead on resource-strip IoT device. In addition to its cryptographic structure, PQ-Lattice shows a behavior of adaptive robustness analogous with intelligent systems that behave according to the requirement at the present condition imitating once again control systems designed for stable operation in uncertain environments. In wide area IoT deployments, such variations of latency, power and link quality can be addressed by incorporating adaptive optimization techniques inspired from control theory. In this sense, PQ-Lattice works likewise as adaptive control techniques—that is for instance adaptive fuzzy control for real fixed-time synchronization of f ractional-order chaotic systems, output-feedback projective synchronization of uncertain nonlinear systems and robust neual adatpive control o f multivariable dynamical systems. These techniques indicate how the protocol may adjust its parameters (e.g., key update interval, signature compression or authenticator frequency), depending on environmental changes and variations in load.

For a 1000 node virtual network, involving synchronous interaction with parallel blockchains saw the average authentication delay only increase from 32.4 ms to 47.9 ms, which demonstrated near-linear scalability. This stability is due to smart-contract management decentralization and the isolation of node-to-node operations.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU254611).

References

[1] X. Mu and M. F. Antwi-Afari, “The applications of internet of things (iot) in industrial management: a science mapping review,” *International Journal of Production Research*, vol. 62, no. 5, pp. 1928–1952, 2024.

[2] K. Sharma and S. K. Shivandu, “Integrating artificial intelligence and internet of things (iot) for enhanced crop monitoring and management in precision agriculture,” *Sensors International*, vol. 5, p. 100292, 2024.

[3] Q. A. Al-Haija and A. Droos, “A comprehensive survey on deep learning-based intrusion detection systems in internet of things (iot),” *Expert Systems*, vol. 42, no. 2, p. e13726, 2025.

[4] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, “Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing,” *The Journal of Supercomputing*, vol. 80, no. 3, pp. 3738–3816, 2024.

[5] A. E. Adeniyi, R. G. Jimoh, and J. B. Awotunde, "A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security," *Computers and Electrical Engineering*, vol. 118, p. 109330, 2024.

[6] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, "Securing the internet of things in artificial intelligence era: A comprehensive survey," *IEEE access*, vol. 12, pp. 25 469–25 490, 2024.

[7] A. Boulkroune, F. Zouari, and A. Boubellouta, "Adaptive fuzzy control for practical fixed-time synchronization of fractional-order chaotic systems," *Journal of Vibration and Control*, p. 10775463251320258, 2025.

[8] A. Boulkroune, S. Hamel, F. Zouari, A. Boukabou, and A. Ibeas, "Output-feedback controller based projective lag-synchronization of uncertain chaotic systems in the presence of input nonlinearities," *Mathematical Problems in Engineering*, vol. 2017, no. 1, p. 8045803, 2017.

[9] F. Zouari, K. B. Saad, and M. Benrejeb, "Robust neural adaptive control for a class of uncertain nonlinear complex dynamical multivariable systems," *International Review on Modelling and Simulations*, vol. 5, no. 5, pp. 2075–2103, 2012.

[10] ——, "Adaptive backstepping control for a single-link flexible robot manipulator driven dc motor," in *2013 International Conference on Control, Decision and Information Technologies (CoDIT)*. IEEE, 2013, pp. 864–871.

[11] G. Rigatos, M. Abbaszadeh, B. Sari, P. Siano, G. Cuccurullo, and F. Zouari, "Nonlinear optimal control for a gas compressor driven by an induction motor," *Results in Control and Optimization*, vol. 11, p. 100226, 2023.

[12] F. Zouari, K. B. Saad, and M. Benrejeb, "Adaptive backstepping control for a class of uncertain single input single output nonlinear systems," in *10th International Multi-Conferences on Systems, Signals & Devices 2013 (SSD13)*. IEEE, 2013, pp. 1–6.

[13] D. Abu Laila, M. Aljawarneh, Q. Al-Na'amneh, and R. Bin Sulaiman, "Optimizing intrusion detection systems through benchmarking of ensemble classifiers on diverse network attacks," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, p. 71–84, 2025. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2025.1.4

[14] H. A. Ali, M. H. I. Khalaf, S. A. Fadek, H. M. Alsayednoor, A. J. Kaishesh, Z. M. Alzamili, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "A privacy-preserving framework for iot using behavior obfuscation and differential privacy in blockchain–cloud architectures," *Journal of Robotics and Control (JRC)*, vol. 6, no. 6, pp. 2613–2627, 2025.

[15] Q. Al-Na'amneh, M. Aljawarneh, A. S. Alhazaimeh, R. Hazaymih, and S. M. Shah, "Securing trust: Rule-based defense against on/off and collusion attacks in cloud environments," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, p. 85–114, 2025. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2025.1.5

[16] A. Yadav, P. Sharma, and Y. Gigras, "A comparative study of elliptic curve and hyperelliptic curve cryptography methods and an overview of their applications," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*. IEEE, 2024, pp. 01–06.

[17] A. Rachmayanti and W. Wirawan, "Elliptic curve cryptography (ecc) based authentication scheme on iot networks for health information systems," in *2024 International Seminar on Intelligent Technology and Its Applications (ISITIA)*. IEEE, 2024, pp. 125–130.

[18] D. Ressi, R. Romanello, C. Piazza, and S. Rossi, "Ai-enhanced blockchain technology: A review of advancements and opportunities," *Journal of Network and Computer Applications*, vol. 225, p. 103858, 2024.

[19] D. Bennet, L. Maria, Y. P. A. Sanjaya, and A. R. A. Zahra, "Blockchain technology: Revolutionizing transactions in the digital age," *ADI Journal on Recent Innovation*, vol. 5, no. 2, pp. 192–199, 2024.

[20] A. Alomari and S. A. Kumar, "Securing iot systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions," *Internet of Things*, vol. 25, p. 101132, 2024.

[21] E. Fathalla and M. Azab, "Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations," *IEEE Access*, 2024.

[22] M. A. R. Javaid, M. Ashraf, T. Rehman, and N. Tariq, "Impact of post quantum digital signatures on blockchain: Comparative analysis," *The Asian Bulletin of Big Data Management*, vol. 4, no. 1, pp. Science–4, 2024.

[23] M. A. Al-Shareeda, A. A. H. Ghadban, A. A. H. Glass, E. M. A. Hadi, and M. A. Almaiah, "Efficient implementation of post-quantum digital signatures on raspberry pi," *Discover Applied Sciences*, vol. 7, no. 6, p. 597, 2025.

[24] P. Mondal, S. Adhikary, S. Kundu, and A. Karmakar, "Zkfault: Fault attack analysis on zero-knowledge

based post-quantum digital signature schemes," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2024, pp. 132–167.

[25] A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero, and M. Polsinelli, "Integrating post-quantum cryptography and blockchain to secure low-cost iot devices," *IEEE Transactions on Industrial Informatics*, 2024.

[26] R. R. Irshad, S. Hussain, I. Hussain, J. A. Nasir, A. Zeb, K. M. Alalayah, A. A. Alattab, A. Yousif, and I. M. Alwayle, "Iot-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing," *IEEE Access*, vol. 11, pp. 105 479–105 498, 2023.

[27] P. Bagchi, B. Bera, A. K. Das, S. Shetty, P. Vijayakumar, and M. Karuppiah, "Post quantum lattice-based secure framework using aggregate signature for ambient intelligence assisted blockchain-based iot applications," *IEEE Internet of Things Magazine*, vol. 6, no. 1, pp. 52–58, 2023.

[28] E. Zeydan, Y. Turk, S. B. Ozturk, H. Mutlu, and A. A. Dundar, "Post-quantum blockchain-based data sharing for iot service providers," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 96–101, 2022.

[29] D. K. Yadav, D. Yadav, Y. Pal, D. Chaudhary, H. Sahu, and A. Manasa, "Post quantum blockchain assisted privacy preserving protocol for internet of medical things," in *2023 IEEE World Conference on Applied Intelligence and Computing (AIC)*. IEEE, 2023, pp. 965–970.

[30] M. Adeli, N. Bagheri, H. R. Maimani, S. Kumari, and J. J. Rodrigues, "A post-quantum compliant authentication scheme for iot healthcare systems," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 6111–6118, 2023.

[31] D. Mishra, K. Pursharthi, M. Singh, and A. Mishra, "Construction of post quantum secure authenticated key agreement protocol for dew-assisted iot systems," *International Journal of Information Security*, vol. 24, no. 1, p. 19, 2025.

[32] N. Minhas, "Post-quantum authentication scheme for iot security in smart cities," 2024.

[33] W. Wang, B. Yan, B. Chai, R. Shen, A. Dong, and J. Yu, "Ebias: Ecc-enabled blockchain-based identity authentication scheme for iot device," *High-Confidence Computing*, vol. 5, no. 1, p. 100240, 2025.

[34] K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, S. Mussiraliyeva, and A. Chehri, "Pqcaie: Post quantum cryptographic authentication scheme for iot-based e-health systems," *Internet of Things*, vol. 27, p. 101228, 2024.

[35] Y. Kuang, Q. Wu, R. Chen, and X. Liu, "Blockchain based lightweight authentication scheme for internet of things using lattice encryption algorithm," *Computer Standards & Interfaces*, p. 103981, 2025.