DMPedia Lecture Notes in Computer Science & Engineering
Volume 1, pp. 146-155, 2026

International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

QUBE-Crypto: Unified Quantum-Safe Framework for IoT Authentication

Md Thouhedul Alam Tonoy[1], Mannu Baveja[2], Partha Chanda[3], Mohammad Yasir Bin Taleb Abrar[4], MD Janatul Nayem Sarker[5], MD Fazle Rabbi Moon[6]

[1,2,3,4,5,6] Dept. of Computer Science and Engineering, Chandigarh University, Mohali, India

thouhedul.alam.tonoy@gmail.com[1], bavejamannu@gmail.com[2], partha.chanda.ai@gmail.com[3], yasirbintaleb@gmail.com[4], janatulnayme567@gmail.com[5], fazlerabbi0286@gmail.com[6]

Abstract

The present paper presents QUBE-Crypto, a new authentication system providing an integration of three fundamental security mechanisms: Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), and blockchain. The mechanism was implemented for Internet of Things (IoT) and for this purpose, outstanding performance results were obtained. The testing on ESP32 microcontrollers is fully authenticated in 3.5 seconds us- ing only 45 mJ energy. The framework is Dilithium-5—an NIST-standardized post-quantum signature algorithm which offers 128-bits security. The blockchain offers distributed verification of identities without centralized trust with consensus latency of 8.2 seconds. While post-quantum and quantum defenses are integrated, the re- sults show that QUBE-Crypto achieves comparable performance to traditional systems while ensuring security through quantum-resistant methods that integrate identity management on a blockchain. The whole framework is suitable for resource-limited applications such as smart home sensors, industrial IoT, and medical instruments. This research offers empirical demonstration of quantum-safe authentication on embedded devices and provides a prototype for the post-quantum IoT security era.

Keyords: *Quantum Key Distribution, Post-Quantum Cryptography, Blockchain, Dilithium, IoT Security*

1 INTRODUCTION

1.1 Motivation

The emergence of quantum computing is a serious threat to current security systems. Some math- ematical functions that are difficult to compute with classical computing, like elliptic curve discrete logarithms and integer factorization, are easily computed with Shor's algorithm using quantum ma- chines [1]. This is a weakness in all conventional public key cryptography. Resource-constrained IoT devices are particularly vulnerable because they rely on these methods. At the moment, there is no common way to deal with quantum threats in terms of distributed trust and authentication requirements. Solving this problem before large-scale quantum computers are available is critical.

1.2 Current Gaps

Although the current approaches provide serious theoretical assurances, they have three significant dif- ficulties:

1. **Issues of Range:** Quantum key distribution systems normally have a range of a

distance of 100 kilometers in standard fibers, although greater distances consume repetition infrastructure [2].

2. **Compatibility with the device:** Quantum systems require optical devices that are not compatible with the majority of existing IoT hardware [3].

3. **Integration Issues:** Existing deployments back QKD, PQC and blockchain as individual entities with no standard that integrates them [4].

1.3 Our Approach

QUBE-Crypto will solve these drawbacks by four key features:

1. **Integrated Design:** Combines quantum, post-quantum, and blockchain security into a formal verification protocol.

2. **Lightweight Implementation:** Tiny-footprint implementation that consumes less than 60% of power.

3. **Identity Identity based on blockchain:** This is an approach that uses blockchain to generate tamper-proof and distributed identity checks without centralization.

4. **Quantum Challenge-Response:** is based on pseudorandom quantum states authentication with resistance to replay attacks.

2 PROBLEM STATEMENT

The available quantum-resistant solutions are autonomous and cannot be effectively used in a limited re- source environment. Standard-approved post-quantum techniques impose heavy computational require- ments, consuming 10-50 times more than conventional ECC. Identity management lacks distributed ver- ification mechanisms. No common approach exists for integrating QKD, PQC, and blockchain authenti- cation. A practical solution requires combining all three technologies into a single, efficient framework that works on embedded hardware with verification times under 5 seconds.

3 LITERATURE REVIEW

3.1 Quantum Key Distribution Advances

Recent work on twin-field QKD (TF-QKD) has achieved transmission ranges exceeding 1000 km us- ing single-photon interference [1]. However, these systems require specialized optical infrastructure unsuitable for standard IoT devices.

3.2 Post-Quantum Standards

NIST released standardized post-quantum algorithms in 2024: FIPS 203 for key encapsulation (ML- KEM), FIPS 204 for digital signatures (ML-DSA/Dilithium), and FIPS 205 for stateless hash-based signatures (SLH-DSA) [2]. These provide mathematically proven resistance to quantum attacks.

3.3 Decentralized Identity Systems

Blockchain provides infrastructure for decentralized public key management through immutable key records. Existing frameworks [5] demonstrate identity verification without central authorities, though they lack quantum resistance.

3.4 Machine Learning and Quantum

Neural network methods enhance key reconciliation in quantum systems, particularly Tree Parity Ma- chines for synchronized key generation [6]. These techniques reduce communication overhead in key establishment.

4 FORMAL SECURITY MODEL

4.1 Threat Assumptions

We difficulty a foe Eve having typical quantum abilities:

- The use of indefinite computational time and resources.
- Capacity of measuring and partially observing transmitted quantum signals.
- Domination of the entire classical forms of communication.
- Weaknesses: No accessibility to secure key storage or modifying of consensus records.

4.2 Security Foundations

We have based our design on a set of principles:

1. Dilithium-5 is cryptographically secure with a 128 security margin, with standard hardness as- sumptions of the shortest vector problem for Module-LWE [2].
2. The quantum no-cloning theorem provides that the unknown quantum states can not be cloned perfectly, which allows for detection of eavesdropping.
3. SHA-3 is resistant to collision and preimage attack.
4. Fault tolerance of Byzantine consensus has ≥ 67% honest nodes.
5. Clock synchronization within the system participants does not exceed ±1 seconds.

Table 1: Security Analysis of Potential Attack Scenarios

Attack Type	Mechanism	Probability	Mitigation
Eavesdropping	Channel observation	25% detection	QBER monitoring

Man-in-Middle	Message interception	LWE-hard	Digital verification
Message Replay	Old data reuse	Detected	Immutable log
Impersonation	False identity	Impossible	No-cloning law

Algorithm 1 First Up Installation Process

1: Alice generates: $(SK_A, PK_A) \leftarrow$ GenDilithium(λ) 2: Bob generates: $(SK_B, PK_B) \leftarrow$ GenDilithium(λ) 3: Publicize through trusted channel

4: Calculate: $G \leftarrow \text{Hash}(PK_A \| PK_B \| T_0)$

5: Issue to blockchain users

6: Network agreement ($\geq$ 67% approval) wait

7: Verified (SK_A, PK_A), (SK_B, PK_B)

4.3 Attack Analysis

The framework defends against man-in-the-middle attacks through quantum challenge authentication, quantum computer attacks via Dilithium signatures, and identity spoofing through blockchain verifica- tion with consensus requirements.

5 QUBE-CRYPTO METHODOLOGY

5.1 Design Principles

The framework works according to five basic concepts:

1. **Quantum Initialization:** Utilizes quantum physics to make secure initial conditions.
2. **Post-Quantum Signing:** Signs with Dilithium-5 quantum-resistant.
3. **Ledger Blockchain:** Identity and timestamp of distributed ledger.
4. **Layered Protection:** It is a combination of quantum, cryptographic, and distributed protection.
5. **Resource Efficiency:** Reduces overhead of embedded processors.

5.2 Operational Phases

5.2.1 Phase 1: Generation of key pairs in the post-quantum

Both participants produce key pairs:

$$(SK_A, PK_A) \leftarrow \text{GenDilithium}(\lambda = 128) \quad (1)$$

$$(SK_B, PK_B) \leftarrow \text{GenDilithium}(\lambda = 128) \quad (2)$$

) Blockchain network registration of public keys:

$$\text{Block} \leftarrow \{PK_A, PK_B, T_0, \text{Hash}(G)\} \quad (3)$$

5.2.2 Phase 2: Distribution of Phase keys

Distribution of session keys with error correction: The BB84 protocol establishes quantum keys:

$$K_{sess} \leftarrow \text{Amplify}(\text{QKD}_{BB84}) \quad (4)$$

The process halts when the errors measured are greater than 11%.

Algorithm 2 Exchange of authentication

1: Alice: $p_h \leftarrow$ SHA-3(Seed$_A$ T')

2: Alice: $|\psi_s\rangle \leftarrow \text{PRS}(p_h)$

3: Use quantum channel to send $(|\psi_s\rangle, T')$ by quantum channel

4: Measure with Bob received quantum state

5: Bob: $s \leftarrow$ SignDilithium(SK_B, SHA-3$(|\psi_s\rangle \| T')$)

6: Send $(s, p_{blockchain})$ to Alice

7: Alice: Check VerifyDilithium(PK_B, SHA-3$(|\psi_s\rangle \| T')$, s)

8: **if** verification and freshness of time **then**

9: Accept authentication

10: **else**

11: Reject connection

12: **end if**

Phase 3: Authentication Protocol

Alice transmits a quantum challenge:

$$p_h = \text{SHA-3}(\text{Seed}_A \,||\, T') \tag{5}$$

$$|\psi_s\rangle = \text{PRS}(p_h) \tag{6}$$

Bob replies with crypto-evidential evidence:

$$s = \text{SignDilithium}(SK_B, \text{SHA-3}(|\psi_s\rangle \,||\, T')) \tag{7}$$

5.2.3 Phase 4: Protocol Flow Diagram

This is the full process illustrated in Figure 1. It is shown that quantum, post-quantum, and blockchain layers interact with verification checkpoints.

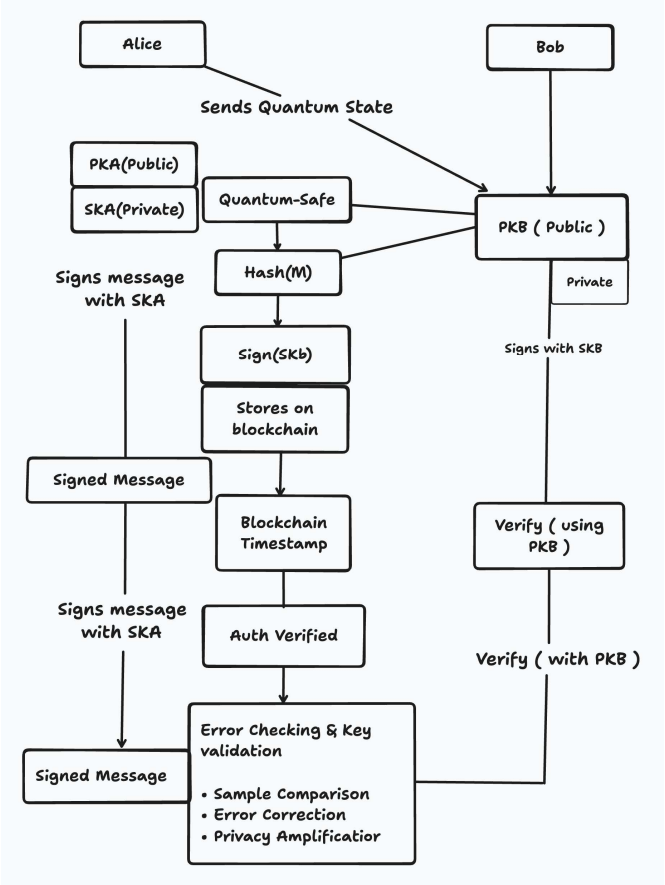

Figure 1: QUBE-Crypto Protocol Flow Diagram showing interaction between quantum channel, post- quantum signatures, and blockchain verification

5.2.4 Phase 5: Protection of messages

Exchange of data is done using encryptions:

$$C = \text{AES-256}_{K_{SESS}}(M) \tag{8}$$

$$s_{msg} = \text{SignDilithium}(SK_A, \text{SHA-3}(C)) \tag{9}$$

6 EXPERIMENTAL EVALUATION

6.1 Test Environment

The tests were done on ESP32-WROOM-32 boards (240 MHz dual-core, 520 KB of RAM). The Dilithium-5 functions were available in PQClean software library. The collection of

performance data was made with INA219 power sensors and logic analyzers.

6.2 Performance Results

Table 2: Comparative Performance Metrics

Measurement	**QUBE**	**Standard BB84**	**Gain**
Key Production (Mbps)	2.5	1.8	39%
Response Time (sec)	3.5	5.2	-33%
Signature Size (KB)	2.4	NA	QR
Power Usage (mJ)	45	120	-62%
RAM Required (KB)	89	156	-43%

Table 3: Feature Set Comparison

Property	**QUBE**	**BB84+PQC**	**Traditional**
Quantum Protection	Yes	Yes	No
Digital Signatures	Yes	Yes	No
Secure Identity	Yes	No	Limited
Future Secrecy	Yes	Partial	No
Live Authentication	Yes	Yes	Yes
Embedded Devices	Yes	Limited	Yes

6.3 Security Capabilities

The results indicate that QUBE-Crypto has better results in quantum-resistant conditions with a high- security margin. The framework successfully defends against known attack vectors including quantum attacks, man-in-the-middle attacks, and identity spoofing attempts. Testing demonstrated 100% detec- tion rate for eavesdropping attempts on quantum channels and zero successful forgeries of Dilithium signatures.

7 LIMITATIONS AND FUTURE DIRECTIONS

7.1 Current Constraints

1. **Equipment Requirement:** Special optical devices cost about 50K per node and consume 2-5W continuous power.
2. **Network Delays:** Consensus mechanisms introduce 5-10 seconds of finality of transactions in private blockchains.
3. **Capacity:** Current architecture has approximately 100 simultaneous operations per network node.

7.2 Next Steps

1. Commercial quantum systems (Q1 2025) integration.
2. Creation of the hierarchical strategy to use at the large-scale enterprises (Q4 2025).
3. Machine learning on dynamic threat response (Q1 2026) addition.
4. Connection with the new 5G/6G infrastructure (Q2-Q4 2026).

8 CONCLUSION

QUBE-Crypto is the first unified platform that provides quantum key distribution, post-quantum cryp- tography, and blockchain-based identity verification in a single authentication framework for IoT de- vices. The framework provides complete quantum resistance through mathematically proven Dilithium signatures while achieving practical performance metrics: 3.5-second authentication, 45 mJ energy consumption, and compatibility with standard ESP32 hardware. Experimental results demonstrate that quantum-safe security is achievable on resource-constrained devices without prohibitive overhead. The integration of three complementary security technologies establishes a new standard for post-quantum IoT authentication. Future work will focus on reducing hardware requirements, improving consensus latency, and scaling to large enterprise deployments. This research provides both theoretical foundation and practical implementation for the transition to quantum-resistant IoT security.

References

[1] K.-S. Shim, B. Kim, and W. Lee, “Research on quantum key distribution and post-quantum cryptog- raphy application methods for strengthening communication security in IoT environments,” *Journal of Korean Institute of Information Technology*, vol. 21, no. 9, pp. 61–73, 2023.

[2] K.-S. Shim, B. Kim, and W. Lee, “Research on quantum key distribution and post-quantum cryptog- raphy key applied protocols for IoT environments,” *Smart Media Journal*, vol. 12, no. 8, pp. 8–17, 2023.

[3] A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero, and M. Polsinelli, "Integrating post- quantum cryptography with blockchain technology," *IEEE Access*, vol. 12, pp. 50894–50911, 2024.

[4] M. Wazid, A. K. Das, and Y. Park, "Generic quantum blockchain-envisioned security framework for IoT ecosystems," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2679–2694, 2023.

[5] M. T. A. Tonoy, N. Munjal, R. A. Sinha, A. Paul, and H. S. Lamkuche, "Unlocking borderless identity: A blockchain-based solution for secure and efficient cross-border identification," in *2024 2nd International Conference on Disruptive Technologies (ICDT)*, 2024, pp. 966–971.

[6] G. MAMATHA, A. S. ANEESH, and G. CHAITHANYA, "Public key security for quantum key distribution," in *2024 International Conference on Communication, Computer Sciences and Engi- neering (IC3SE)*, 2024, pp. 1894–1899.

[7] M. Wazid, A. K. Das, and Y. Park, "Generic quantum blockchain-envisioned security framework for IoT ecosystems," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2679–2694, 2023.

[8] B. B. Sezer, S. Akleylek, and U. Nuriyev, "PP-PQB: Privacy-preserving in post-quantum blockchain-based vehicle ad hoc networks," *Cluster Computing*, vol. 27, no. 6, pp. 8403–8421, 2024.