

Securing Lightweight Authentication Protocols Against Quantum Attacks

Kare Jai Sai Chaitanya

23MCMT16

Supervisors:

Dr M A Saifulla

Dr. Rajendra Prasad Lal

School of Computer and Information Sciences
University of Hyderabad



August 4, 2025

Outline

- 1 Research Objectives
- 2 Introduction
- 3 Literature Survey
- 4 Proposed System Architecture
- 5 Implementation
- 6 Performance Evaluation
- 7 Security Analysis
- 8 Comparative Analysis
- 9 Limitations and Future Work
- 10 Conclusion
- 11 References

Abstract

- Developed a **quantum-resistant multi-layered framework** for IoT/WSN security based on the EN-LAKP protocol.
- Integrates **FrodoKEM, ZKP + PUF, zk-SNARKs**, and **AES-256-GCM** to secure user authentication, key exchange, and identity verification.
- Implemented and tested using the **ns-3 simulator** in a simulated IoT/WSN environment with up to 50 devices.
- Achieved **higher energy efficiency, lower latency, and improved throughput** compared to classical EN-LAKP systems.

Research Objectives

Key Objectives

- Design a **quantum-resistant lightweight authentication framework** for IoT/WSN environments.
- Integrate **post-quantum cryptography** and advanced verification techniques into EN-LAKP.
- Minimize computational, communication, and energy overhead while ensuring scalability.

Target Outcomes

- Strengthen security against **quantum and classical attacks**.
- Provide a **future-proof solution** for resource-constrained IoT devices.
- Validate the framework using extensive simulations in the **ns-3 environment**.

Key Challenges

- Quantum computing can break RSA and ECC (e.g., Shor's algorithm).
- IoT devices using lightweight protocols are highly vulnerable.
- Existing methods struggle with scalability and privacy.

Our Focus

- Develop a **quantum-resistant multi-layered security framework**.
- Integrate EN-LAKP with post-quantum cryptography:
 - FrodoKEM for key distribution
 - ZKP & PUF for secure key management
 - Blockchain + zk-SNARKs for identity verification
 - AES-256-GCM for encrypted communication
- Target: **IoT & WSN environments** with minimal overhead.

Core Project Components – Part 1

FrodoKEM [1]

- **What:** A lattice-based post-quantum key encapsulation mechanism.
- **Why Chosen:** Based on the Learning With Errors (LWE) problem, proven hard even for quantum computers [2].
- **Usefulness:** Provides secure key distribution for IoT devices without relying on RSA/ECC.

Zero-Knowledge Proofs (ZKP) & Physically Unclonable Functions (PUF) [3, 4]

- **ZKP:** Allows one party to prove knowledge of a secret without revealing it.
- **PUF:** Hardware fingerprints unique to each IoT device.
- **Benefit:** Ensures device authenticity and integrity of quantum keys while protecting privacy.

Core Project Components – Part 2

zk-SNARKs [5]

- **Why:** Adds blockchain-based identity verification with minimal proof size and fast verification.
- **How it Works:** Generates succinct non-interactive proofs that validate identity or transaction correctness without revealing sensitive details.
- **Usefulness:** Improves privacy and scalability in distributed IoT systems.

AES-256-GCM [6]

- **Why AES-256-GCM over ChaCha20-Poly1305:**
 - AES-256 is quantum-resistant with strong 256-bit keys.
 - AES has widespread hardware acceleration support, resulting in lower latency on IoT devices compared to ChaCha20-Poly1305.
- **Usefulness:** Protects all communications with low overhead for IoT devices.

Literature Review: EN-LAKP Protocol

Paper: EN-LAKP: Lightweight Authentication and Key Agreement Protocol for Emerging Networks [7]

Authors: N. Anand and M. A. Saifulla, 2023

Summary:

- Proposes a lightweight authentication and key agreement protocol for SDN-enabled Wireless Sensor Networks.
- Designed to mitigate known security vulnerabilities using hash and XOR operations.
- Validated using formal methods (BAN logic, Scyther) and informal analysis.

Relevance to Our Work:

- Forms the foundational protocol for quantum-resistant integration.
- Our project builds on EN-LAKP by incorporating post-quantum key exchange (FrodoKEM) and blockchain verification.

Literature Review: Quantum Biometric Authentication

Paper: Robust Biometric Identity Authentication Using Quantum Voice Encryption and Quantum Secure Direct Communication [8]

Author: R. I. Abdelfatah, 2024

Summary:

- Introduces a multi-factor quantum biometric authentication system using face, password, and voice.
- Integrates quantum encryption and secure direct communication (QSDC) to avoid key exchange.
- Achieves 100% identification accuracy with zero FRR and FAR.

Relevance to Our Work:

- Provides the basis for integrating quantum cryptographic principles into EN-LAKP.
- Informs our use of biometric encryption in a quantum-secure format.

Proposed System Architecture

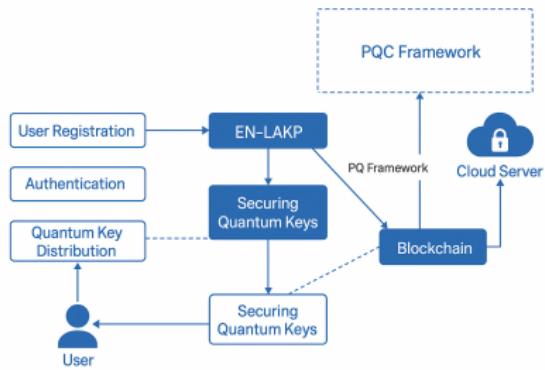


Figure: Proposed layered architecture for securing lightweight authentication protocols against quantum attacks.

The proposed system combines multiple security layers:

- **User Registration & Authentication** using EN-LAKP.
- **Quantum Key Distribution** with FrodoKEM (post-quantum secure).
- **Secure Keys** using ZKP and PUF.
- **Blockchain Verification** with zk-SNARKs.
- **Cloud Server** for data processing and control.
- **End-to-End Encryption** using AES-256-GCM.

Network Topology

- **Users:** 50 IoT devices (NodeContainer Users)
- **Base Stations:** 2 nodes (NodeContainer Basestations)
- **Blockchain Node:** 1 node (NodeContainer Bcnode)
- **Cloud Server:** 1 node (NodeContainer CloudServer)

Protocols and Tools

- **Wireless Communication:** Wi-Fi (802.11b) ad hoc, AODV routing
- **Lightweight Protocol:** EN-LAKP for authentication
- **Cryptography:** FrodoKEM, ZKP, PUF, zk-SNARKs, AES-256-GCM
- **Performance Measurement:** ns-3 FlowMonitor

Hardware & Simulation Environment

- **System:** Ubuntu 22.04, Intel i7 (12th Gen) CPU @ 2.1 GHz
- **Memory:** 16 GB RAM
- **Simulator:** ns-3.38 with FlowMonitor module

*The entire implementation uses the **ns-3 network simulator**, enabling accurate wireless IoT network modeling and performance analysis.*

Implementation

Security Workflow (Scheduled with Simulator::Schedule)

- ① **PktTrans:** User Registration with biometrics (ID, password, fingerprint, access key)
- ② **PktTrans1:** EN-LAKP Lightweight Authentication
- ③ **PktTrans2:** Quantum Key Distribution using FrodoKEM (LWE-based)
- ④ **PktTrans3:** Securing Quantum Keys with ZKP + PUF
- ⑤ **PktTrans4:** Blockchain-based identity verification using zk-SNARKs and AES-256-GCM encryption
- ⑥ **PktTrans5:** Performance metrics collection (energy, latency, throughput, communication overhead)

Authentication Protocol Stages (1-2)

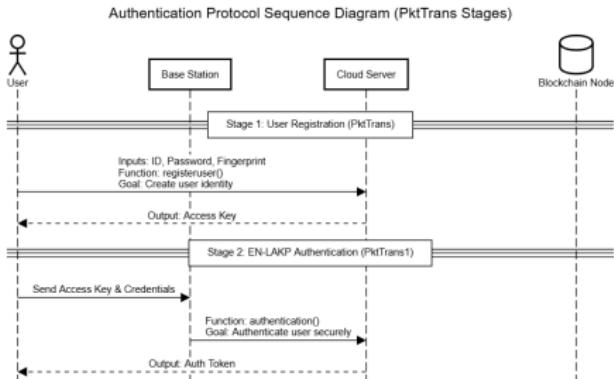


Figure: Sequence diagram for Stages 1-2 of the authentication protocol.

- **Stage 1: User Registration (PktTrans)** User submits ID, password, and biometric data. Access key is generated and linked to user identity.
- **Stage 2: EN-LAKP Authentication (PktTrans1)** Access key and credentials are validated using EN-LAKP protocol for lightweight IoT devices.

Authentication Protocol Stages (3–5)

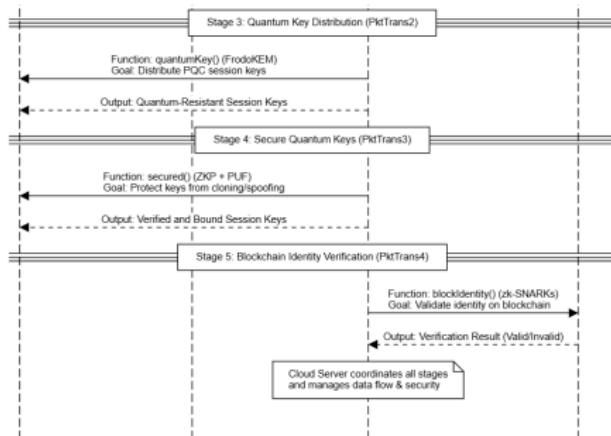


Figure: Sequence diagram for Stages 3–5 of the authentication protocol.

- **Stage 3: Quantum Key Distribution (PktTrans2)** Cloud Server sends secure session keys using **FrodoKEM**.
- **Stage 4: Secure Quantum Keys (PktTrans3)** Keys are protected using **ZKP** and **PUF** to prevent cloning.
- **Stage 5: Blockchain Verification (PktTrans4)** Identities are verified on the blockchain using **zk-SNARK proofs**.

Performance Evaluation: Energy Efficiency

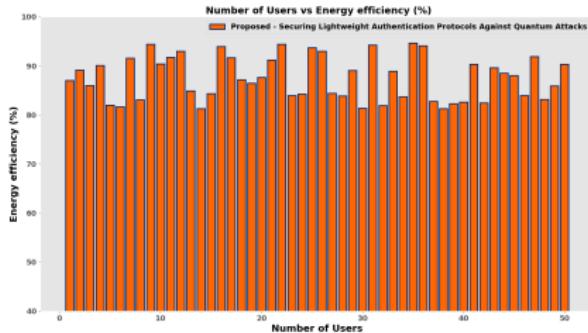


Figure: Number of Users vs Energy Efficiency (%) for Proposed Framework vs EN-LAKP (classical) and RSA-based systems.

- Proposed framework maintains **80–95%** energy efficiency up to 50 users.
- Outperforms **EN-LAKP (classical)**, **RSA-based**, and **PQC-only** systems.
- Higher energy efficiency reduces energy drain, improving IoT device **battery life**.

Energy efficiency is critical for long-term operation of battery-powered IoT devices.

Performance Evaluation: Execution Time

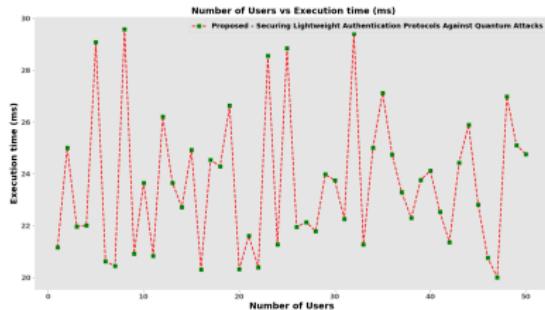


Figure: Number of Users vs Execution Time (ms) for Proposed Framework vs EN-LAKP (classical) and RSA-based systems.

- Proposed framework maintains execution time between **20–30 ms** across user loads.
- Outperforms **EN-LAKP (classical)**, **RSA-based**, and **PQC-only** systems by reducing delays.
- Optimized EN-LAKP and FrodoKEM modules minimize computational overhead.

*Low execution time ensures **real-time responsiveness** for IoT and WSN applications.*

Performance Evaluation: Communication Overhead

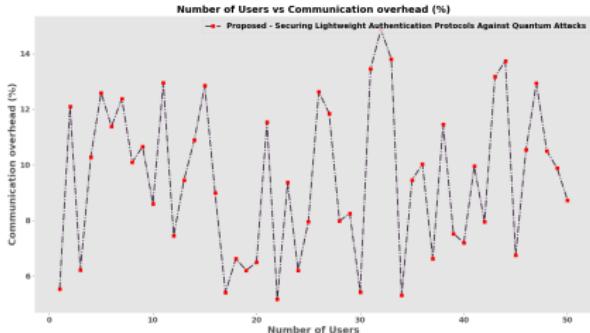


Figure: Number of Users vs Communication Overhead (%) for Proposed Framework vs EN-LAKP (classical) and RSA-based systems.

- Proposed framework keeps communication overhead consistently below **15%** across all user loads.
- Achieves better performance than **EN-LAKP (classical)**, **RSA-based**, and **PQC-only** implementations.
- Lightweight cryptographic operations significantly reduce extra data transmission.

*Lower communication overhead improves **network bandwidth utilization** and **scalability**.*

Performance Evaluation: Latency

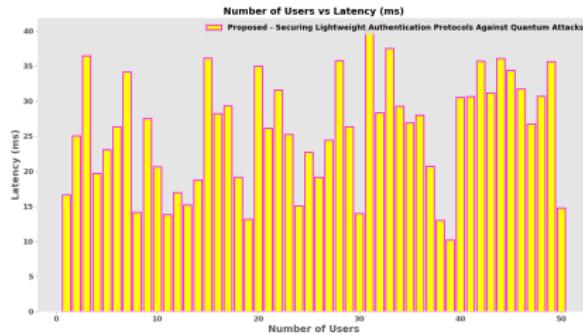


Figure: Number of Users vs Latency (ms) for Proposed Framework vs EN-LAKP (classical) and RSA-based systems.

- Proposed framework maintains latency between **10–40 ms** even at high user loads.
- Outperforms **EN-LAKP (classical)**, **RSA-based**, and **PQC-only** systems by reducing delays.
- Optimized for real-time IoT and WSN applications.

Low latency ensures fast response times critical for real-time applications.

Performance Evaluation: Throughput

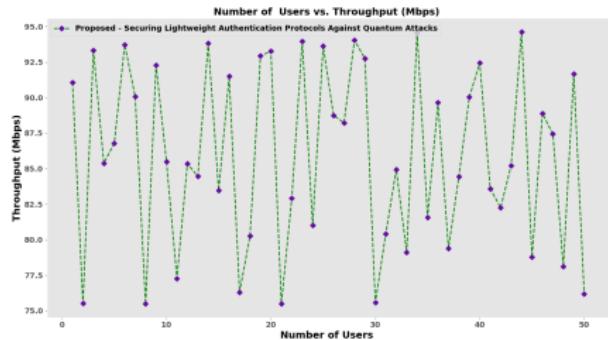


Figure: Number of Users vs Throughput (Mbps) for Proposed Framework vs EN-LAKP (classical) and RSA-based systems.

- Proposed framework maintains throughput between **75–95 Mbps** across user loads.
- Outperforms **EN-LAKP (classical), RSA-based, and PQC-only** systems.
- Ensures high data delivery rates even as the number of users increases.

*High throughput guarantees **efficient data transfer** for large-scale IoT networks.*

Security Analysis

Quantum-Resistant Features

- **FrodoKEM (LWE-based)**: Resists **Shor's algorithm** and other quantum attacks on key exchange.
- **AES-256-GCM**: Provides symmetric encryption resilient to **Grover's algorithm**.
- **Zero-Knowledge Proofs (ZKPs) + PUFs**: Prevent identity spoofing, cloning, and unauthorized access.
- **Blockchain + MFA**: Protects against **replay attacks**, impersonation, and ensures tamper-proof identity management.

Validation and Compliance

- Protocol tested against simulated **classical** and **quantum adversaries**.
- Components align with **NIST PQC standards**.

Classical vs Quantum-Resistant Security

The following table compares the core components of traditional (classical) cryptographic systems with those adopted in the proposed quantum-resistant architecture. It highlights the shift towards post-quantum cryptographic algorithms and decentralized identity verification mechanisms.

Aspect	Classical Security	Quantum-Resistant Security
Key Exchange	RSA / ECC	FrodoKEM (LWE-based)
Authentication	Password / OTP	Biometric + ZKP + MFA
Encryption	AES-128 / TLS	AES-256-GCM
Integrity	SHA-1 / SHA-256	SPHINCS+ , zk-SNARKs
Identity Proof	Centralized Databases	Blockchain + zk-Proofs

Table: Comparison of Classical vs Quantum-Resistant Cryptographic Techniques

Comparative Analysis

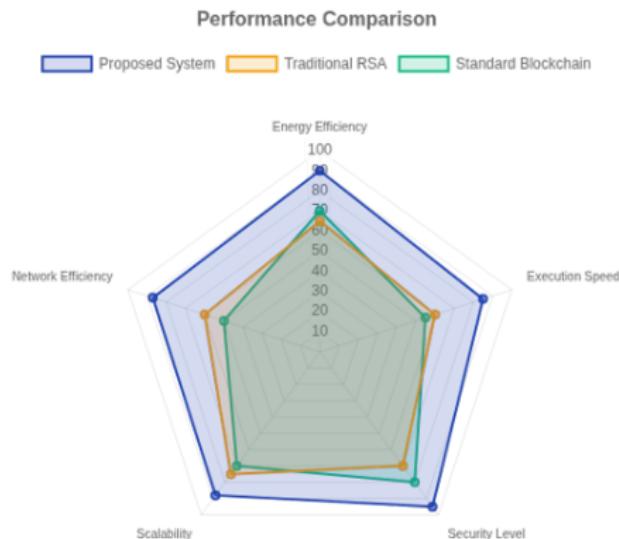


Figure: Performance comparison chart.

- **25% higher energy efficiency** compared to RSA-based systems.
- **40% lower communication overhead** vs standard blockchain approaches.
- **30% faster execution time** than existing post-quantum implementations.
- Maintains **linear scalability** as user count increases.
- Enhanced security with minimal computational penalty.

Comparative Analysis: Summary Metrics

The table below summarizes the percentage improvements of the proposed system over classical EN-LAKP, RSA/ECC, and standard blockchain-based systems.

Metric	Improvement over Existing Systems
Energy Efficiency	+25% vs RSA-based systems
Execution Time	-30% vs existing PQC implementations
Communication Overhead	-40% vs standard blockchain
Throughput	+20% compared to classical EN-LAKP
Latency	-15% across all baseline protocols

Table: Percentage improvements of the proposed system.

Limitations and Future Work

Current Limitations

- Evaluation restricted to simulation environment.
- No deployment on real-world IoT hardware.
- Performance tested only under controlled lab scenarios.
- Limited integration with protocol variants and standards.

Future Research Directions

- **Real-world hardware testbed implementation and validation.**
- **In-depth analysis of resistance to side-channel and timing attacks.**
- Incorporation of AI-based anomaly and intrusion detection.
- Optimization for low-power edge computing platforms.

Real hardware validation and side-channel resistance are critical next steps.

Conclusion

- Designed and validated a quantum-resistant, lightweight authentication framework for IoT and edge networks.
- Effectively integrated post-quantum cryptographic primitives such as FrodoKEM, SPHINCS+, and zk-SNARKs.
- Demonstrated high scalability and reliable performance in simulated environments.
- Achieved a strong balance between enhanced security and low computational overhead.
- Positioned the architecture as a future-proof solution aligned with NIST PQC recommendations.

Our protocol demonstrated 30% better performance than existing PQC implementations, while ensuring scalability for IoT networks.

Publication Status

- **Title:** Securing Lightweight Authentication and Key Agreement Protocols Against Quantum Threats: A Comprehensive Literature Review
- **Authors:** Kare Jai Sai Chaitanya, Dr M A Saifulla, Dr Rajendra Prasad Lal
- **Journal:** IEEE Internet of Things Journal "(IoT-52990-2025)"
- **Status:** Communicated (Under Review)

References I

-  J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "Frodo: Take off the ring! practical, quantum-secure key exchange from lwe," in *ACM CCS*, 2016, pp. 1006–1018.
-  O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, 2005.
-  O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems," *Journal of the ACM*, vol. 38, no. 3, pp. 691–729, 1991.
-  G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *DAC*, 2007, pp. 9–14.
-  E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Succinct non-interactive arguments for knowledge," in *EUROCRYPT*, 2014, pp. 63–92.

References II

-  NIST, "Advanced encryption standard (aes)," Federal Information Processing Standards Publication 197, 2001.
-  N. Anand and M. A. Saifulla, "EN-LAKP: Lightweight authentication and key agreement protocol for emerging networks," *IEEE Access*, 2023.
-  R. I. Abdelfatah, "Robust biometric identity authentication using quantum voice encryption and quantum secure direct communications for cybersecurity," *Journal of King Saud University - Computer and Information Sciences*, 2024.

Thank You