Abstract

Design of Some Identity- and Lattice-based Public Key Cryptosystem for Blockchain-Assisted IOT Applications

Abstract submitted to
Rajiv Gandhi Institute of Petroleum Technology, Jais, Amethi
for the award of the degree

of

Doctor of Philosophy

by

Pooja Verma
(Enrollment No. 21CS0004)

under the guidance of

Dr. Kalka Dubey
(Department of Computer Science & Engineering, RGIPT- Jais)

Dr. Daya Sagar Gupta
(Department of Mathematics, IIT - Patna)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
RAJIV GANDHI INSTITUTE OF PETROLEUM TECHNOLOGY
JAIS AMETHI
DECEMBER 2025

Abstract

The Internet of Things (IoT) makes it attainable for sensors and other intelligent equipment to be connected to each other without any problems. This leads to new ideas in fields like intelligent healthcare and intelligent transportation systems. IoT has a lot of benefits, but it also has big security problems because of the openness of wireless communication, the fact that devices are different, and the fact that they don't have enough computing power. This makes it easy for data to be intercepted, changed, or accessed without permission. Using cryptographic primitives like encryption, digital signatures, and key agreement protocols keeps data safe, private, and authentic. But conventional cryptographic schemes depend on central authorities, which can lead to single points of failure. By providing decentralization, immutability, and secure data sharing, integrating blockchain technology solves this problem. Blockchain helps keep patient records safe in intelligent healthcare and helps vehicles communicate and manage their identities safely in intelligent transportation. This makes IoT-based systems more reliable and resilient overall.

Formal proofs in both the conventional Random Oracle Model (ROM) and the Quantum Random Oracle Model (QROM) reveal that the suggested systems are quite secure and can stand up to both conventional and quantum-powered enemies. Also, security reductions are based on well-known difficulties that are hard to solve with computers, which adds to the claims of security guarantees. Hyperledger Fabric and the appropriate cryptography libraries are utilized to implement the plans and ensure they function effectively in distributed settings. Performance is measured by the costs of computing and communicating, as well as the blockchain's throughput and latency. This shows how well the system works as a whole.

When compared to alternative state-of-the-art structures, the proposed schemes demonstrate greater efficiency and feasibility, making them a suitable choice for real-world use in the IoT application areas for which they were designed.

We presented four secure techniques in this PhD project, which are outlined below:

I. **A Pairing-Free Data Authentication and Aggregation Mechanism for Intelligent Healthcare Systems.**
A secure mutual authentication protocol is suggested to create a reliable connection between a patient and the medical server, ensuring that both parties are thoroughly checked before sharing critical information. The framework is built to stop prevalent threats like man-in-the-middle, impersonation, and replay, which makes online medical care safer. Pairing-free identity-based cryptography is used to make key management easier and cut down on the amount

of computing power required. An aggregator node is used to reduce latency and make it possible to collect data on a large scale. An integrated key agreement phase makes sure that medical data stays private while it is being sent.

II.. **An Improved Certificateless Mutual Authentication and Key Agreement for Cloud-Assisted Wireless Body Area Network**
In the context of cloud-assisted Wireless Body Area Networks (WBANs), we identified critical flaws and limitations in Cheng et al.'s scheme. To address these, we propose an enhanced certificateless security protocol that eliminates key escrow and certificate management issues. Formal security analysis in the Random Oracle Model (ROM) confirms secure mutual authentication between patients and medical servers via session keys. The scheme resists man-in-the-middle, impersonation, forward secrecy violations, replay attacks, and others.

III. **Quantum-Safe UAV-Assisted Blockchain Authentication for Secure Vehicle Communications in ITS**
A quantum-safe, UAV-assisted, blockchain-enabled, authenticated key agreement protocol is proposed for Intelligent Transportation System (ITS) environments. It employs lattice-based cryptography to ensure resistance against both classical and quantum adversaries and uses blockchain for robust, privacy-preserving identity management. UAVs are integrated to reduce latency and deployment costs compared to purely RSU-based infrastructures. The protocol supports conditional privacy, allowing vehicles and UAVs to be authenticated without disclosing real identities while still enabling misbehavior traceability. It ensures message integrity, mutual authentication, and resistance to replay, impersonation, and data tampering attacks. A formal security analysis in the Quantum Random Oracle Model demonstrates strong security against quantum-capable adversaries, and experimental results confirm its scalability and higher efficiency than existing ECC- and lattice-based ITS schemes.

IV.. **Quantum-Defended Lightweight Blockchain Authentication Protocol for Smart Healthcare System.**
A quantum-resistant lightweight mutual authentication protocol is designed to secure communication between patients and the medical server in a smart healthcare environment. The protocol incorporates a blind signature mechanism so that collector points can be validated on the blockchain, enabling other nodes to verify that the received medical data is authentic while preserving confidentiality. The Quantum Random Oracle Model is used to analyze the authentication and key agreement phases, ensuring quantum-safe mutual authentication and secure session key establishment. Furthermore, the medical server is implemented over a blockchain-based architecture to enhance security, privacy, and transparency, while removing single-point-of-failure issues and achieving low computational and communication overhead.

Keywords: Internet of Things (IoT), Blockchain Technology, Identity-Based Cryptography, Certificateless Cryptography, Lattice-Based Cryptography, Authentication, Integrity & Confidentiality, Intelligent Healthcare & Transportation System.