ABSTRACT

Design of Quantum-safe Blockchain-enabled Cryptographic Security Schemes for IoT-Powered Smart Grid Networks

Hema Shekhawat
(21CS0002)

Degree for which submitted to

Doctor of Philosophy

Under the Supervision of

Dr. Kalka Dubey, Assistant Professor, RGIPT

Dr. Daya Sagar Gupta, Assistant Professor, IIT Mandi

Department of Computer Science & Engineering

Rajiv Gandhi Institute of Petroleum Technology, Jais

2024

Design of Quantum-safe Blockchain-enabled Cryptographic Security Schemes for IoT-Powered Smart Grid Networks

Abstract

The proliferation of Internet of Things (IoT) technology has led to the widespread interconnection of smart devices and sensors in modern times. However, security issues regarding authentication, data integrity, and confidentiality arise on the IoT environment because of the open architecture of the wireless technologies utilized by IoT devices. Researcher-proposed cryptographic security solutions abound to address the IoT's security challenges. We therefore intended our study to address these cryptographic issues in Smart-grid Networks (SGNs) driven by IoT.

"The second quantum revolution" is occurring in the current context, and it has made it possible to create ground-breaking new quantum instruments. The goal of quantum computing is to develop more advanced computing standards that may be able to tackle intricate structures. Because of the advancements in quantum computing, a new area of cryptography known as post-quantum cryptography (PQC) has surfaced that is resistant to quantum assaults. One of the most promising PQC methods for addressing quantum-based threats is the lattice-based cryptosystem, or LB-cryptosystem, which guarantees quantum security. The established security algorithms, such Diffie-Hellman (DH) and RSA, are resilient enough to withstand current security risks. On the other hand, most conventional algorithms' security, which is reliant on prime factorization and DH-type hard problems, has been projected to be broken by quantum technologies. Therefore, in order to safeguard various applications, the data of businesses, and information infrastructure in the quantum age, research is presently concentrated on resolving security and privacy issues by deploying LB-cryptosystems. Our work aims to explore recent developments in LB-cryptosystems that could enable the creation of safe models for SGNs that can withstand current and upcoming quantum attacks. Electricity generation, transmission, allocation, and use have all been studied in relation to SGNs as a bi-directional integration of communication. We present a thorough analysis of LB-cryptosystems and their possible uses in protecting SGNs in our work. In conclusion, we examine several PQC primitives, algorithms chosen by NIST, open-source tools and their packages, and different PQC industrial projects. Additionally, we contrast conventional cryptographic schemes with alternative PQC.

In this PhD research, we contributed to four quantum-secure schemes which is explained as follows:

I. **Quantum-safe Lattice-based Mutual Authentication and Key Agreement Protocol for the Smart Grid**
   In this work, a secure quantum-safe mutual authentication and key agreement mechanism is proposed for SGNs, that make use of the hard assumptions of small integer solution and inhomogeneous small integer solution problems of lattice. The proposed protocol is intended to offer confidentiality, anonymity, and hashed-based mutual authentication with a key exchange agreement. Similarly, this scheme allows creation and validation of the mutual trust among the smart-meters (SMs) and neighbourhood-area network gateway over an insecure wireless channel.

II. **Quantum-resistance blockchain-assisted certificateless data authentication and key exchange scheme for the smart grid metering infrastructure**

This work presents a lattice-based blockchain-assisted certificateless data authentication and key exchange strategy, and it methodically tackles the intrinsic research issues related to SGMI. Establishing quantum resistance, conditional anonymity, dynamic participation, and the ability to update and revoke keys are the main goals of this scheme. These are all necessary elements for the reliable execution of mutual authentication in SGMI.

III. **Quantum-resilience Blockchain-based Certificate-less Aggregate Signatures for Fog-assisted Smart Grid**

To mitigate issues such as a single point of failure and latency, this work integrates fog computing and blockchain (BC) technologies into the SGME, leveraging DCs as BC peers, thus proposing a decentralized SGME. Furthermore, in tackling security and privacy concerns, traditional signature schemes encounter challenges like elevated computational overhead, certificate management, and key escrow. Hence, this article adopts a lattice-based certificate-less approach and introduces a BC-based certificate-less scheme for aggregate signatures aimed at furnishing authentication, integrity, and privacy within the envisioned fog-based SGME.

IV. **Quantum-secure Deep learning-assisted blockchain-enabled certificate-less aggregate signcryption scheme for the Smart-grid**

The dynamic nature of SGNs introduces complexities in ensuring mutual authentication and secure key establishment between communicating entities. This work offers robust security mechanisms capable of detecting and thwarting quantum attack while ensuring efficient key generation and management to accommodate the scale and heterogeneity of SGNs deployments. Existing signcryption schemes are designed for the centralized architecture, in which computation and storage tasks are delegated to a single trusted authority. We aim to develop a blockchain-based deep learning-assisted signcryption scheme utilizing Deep Residual Networks (DRNs) to enhance security and efficiency for SGNs utilizing lattices. We endeavour to pave the way for a more resilient and scalable approach to securing SGNs, ensuring the integrity and privacy of data transmitted across diverse SGNs ecosystems.

Key Words: Lattice-based cryptography (LBC), certificate-less, aggregate signature scheme (ASS), Smart-grid networks, Blockchain (BC), Fog-based server, mutual authentication, and key exchange.