International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 12, No. 3, 2025, pp. 349-358.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Quantum Resistant Cryptographic Protocols for Securing Smart Grid Communications

Dr.D. Mugilan [a], Dr.P. Balamurugan [b], Dr.P. Srinivasan [c]

[a] Assistant Professor, Department of Electronics and Communication Engineering, K.S. Rangasamy College of Technology, Tiruchengode, India. E-mail: mugilan@ksrct.ac.in, Orcid: https://orcid.org/0000-0001-5249-483X
[b] Associate Professor, Department of Networking and Communications, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. E-mail: balamurp@srmist.edu.in, Orcid: https://orcid.org/0000-0001-8394-1129
[c] Professor, Head of the Department of Computer Science and Engineering (AI and ML), Paavai Engineering College, Namakkal, India. E-mail: srinivasanp.dr@gmail.com, Orcid: https://orcid.org/0009-0009-7099-9255

Abstract

The advent of digitalization of the contemporary power infrastructure has now made the traditional electricity networks smart grids that allow real-time monitoring, automatic control, and two-way communication between smart meters, substations, and control centers. Although the capabilities provide grid efficiency and reliability, they also pose a considerable cybersecurity threat. The traditional security tools like RSA and Elliptic Curve Cryptography (ECC) are susceptible to quantum computing, especially to quantum algorithms such as the Shor algorithm, which can effectively crack such classical algorithms, thus compromising the confidentiality, integrity, and availability of smart grid communications. As a result, quantum-resistant cryptography solutions have become important in order to protect the next-generation energy systems. The current study suggests a quantum-resistant cryptographic protocol that is meant to protect smart grid communications. The protocol combines lattice-based key exchange (e.g., NTRU) and hash-based digital signatures (e.g., XMSS), which offer secure authentication, key establishment, and encrypted data communication between smart grid nodes. The protocol is designed with resistance to quantum cryptanalysis and with a low computational burden, which is suitable in resource-constrained smart grid devices, including smart meters and embedded controllers. Experiments that are run on a smart grid communication platform through simulation show that the protocol can achieve encryption times of 0.34 ms, key generation times of 0.45 ms, and authentication latencies of 0.28 ms. It also has the accuracy of 98.7% in data integrity and 97.9% in attack resistance performance towards the frequently used and common cyber-attacks, such as replay and man-in-the-middle. Comparative analysis shows that the protocol suggested is more efficient in calculations by 18-24 % compared to ECC and RSA, as well as more robust to security against quantum-based attacks. The implications of these findings are that post-quantum cryptography has the potential to enhance the cybersecurity infrastructure of smart grid communication networks to make it resistant to classical and quantum scenarios in the long term.

Keywords: Quantum Resistant Cryptography, Smart Grid Security, Post Quantum Cryptography, Secure communication, Cyber Physical Systems.

DOI: 10.71086/IAJSE/V12I3/IAJSE1271
Received: 14 July 2025/Revised: 21 August 2025/Accepted: 11 September 2025/Published: 30 September 2025

Introduction

Smart grids have emerged as a result of the sophistication of modern power systems, which incorporate highly sophisticated communication systems, digital display systems, and intelligent control solutions to enhance the efficiency, reliability, and sustainability of electricity distribution systems. In comparison to conventional power systems, smart grids facilitate both the outbound and inbound communications between power consumers and power utilities using smart meters, sensors, substations, and control centers. This communication is capable of real-time energy control, demand response, fault detection, and automated control functions. The smart grid communication architecture is usually made up of various layers of the network, such as Home Area Networks (HAN), Neighborhood Area Networks (NAN), and Wide Area Networks (WAN), all of which together allow the exchange of data among various power grid components.

Notwithstanding these benefits, there are high threats to cybersecurity due to the increased connectivity in smart grids. The energy consumption data, control commands, and system status information are transmitted over communication channels that are susceptible to cyber threats that include data tampering, replay attacks, denial of service attacks, and man-in-the-middle attacks. In case these attacks are carried out successfully, they may interfere with grid functioning, alter data on the use of energy, or damage crucial infrastructure. RSA and Elliptic Curve Cryptography (ECC) are conventional cryptography algorithms that are commonly applied to authenticate, encrypt, and manage keys to ensure the security of smart grid communications. Nevertheless, the fast growth of quantum computing puts these traditional security measures in grave danger.

In quantum computing, quantum algorithms, especially the Shor algorithm, can be used to solve integer factorization and discrete logarithm problems that RSA and ECC use, breaking many modern public-key cryptography systems efficiently (Dalal et al., 2024). When large-scale quantum computers are feasible, the current cryptographic protection that is applicable in smart grid communication networks may no longer be viable. This new threat has raised the growing popularity of Post-Quantum Cryptography (PQC), the study of how to create cryptographic algorithms that are resistant to classical and quantum computational challenges (Horpenyuk et al., 2023; Dam et al., 2023).

Despite a number of studies being conducted on smart grid security and post-quantum cryptographic schemes separately, a research gap exists on how to combine quantum-resistant cryptographic protocols with specific applications in the communication setup in a smart grid (Bavdekar et al., 2023; Tasopoulos et al., 2022). Most of the current frameworks either use the classical cryptography methods or lack the ability to meet the constraints of smart grid devices, such as the computational power or the demand of real-time communication (Karakaya & Ulu, 2024). Thus, it is required that a safe, effective, and scalable cryptographic protocol be established that can ward off the future quantum threat to smart grid communications.

In this paper, a quantum-resistant cryptographic protocol is suggested to secure the smart grid communications by post-quantum cryptography (Harmalkar et al., 2024). The proposed framework incorporates the secure establishment of keys, authentication, and encrypted communication systems to ensure that data privacy and integrity are enforced in the smart grid networks.

The key points made in this paper can be summarized as follows:

1. Development of a quantum-resistant cryptographic authentication scheme to be used in protecting smart grid communication networks.
2. Design of a safe key transfer and authentication system founded on post-quantum cryptography.
3. Simulation experiments on the proposed protocol to assess the performance of the protocol in terms of security strength, computational efficiency, and communication overhead in smart grid environments.

The paper has the following structure: Section 2 will provide the literature review of the current research on smart grid security and the drawbacks of traditional cryptography in the quantum age. Section 3 states that the smart grid architecture is the design of the cryptographic protocol and outlines the key generation process, the encryption process, and the authentication process and experimental setup. In Section 4, the and performance assessment are offered, in which the proposed protocol is compared to the traditional methods. The article 5 deals with the security implications and efficiency of the proposed solution. Conclusion 6 contains the crucial findings and prospective research directions.

Literature Review

Smart grid communication systems are deemed to be very important in the provision of secure and reliable operation of the grid. One of the important elements in smart grids is the Advanced Metering Infrastructure (AMI) that offers a two-way communication between the smart meter and the central control systems. But the AMI systems are exposed to numerous cyber-attacks, such as manipulation of data, unauthorized access, and denial-of-service attacks. Also, the security is compounded by the inclusion of Supervisory Control and Data Acquisition (SCADA) systems in smart grids. SCADA systems are applicable in real-time monitoring and control of important infrastructure and are vulnerable to unauthorized access, data breach, and command manipulation. The privacy, integrity, and accessibility of these systems should be properly safeguarded to secure the rest of the smart grid network. Conventionally, the implementation of smart grid security has been based on classical cryptography, including RSA and Elliptic Curve Cryptography (ECC) to encrypt, exchange keys, and authenticate messages (Prakash & Prakash, 2023). RSA, which is built on integer factorization, and ECC, which is built on the hardness of the elliptic curve discrete logarithm problem, are popular in securing smart grid communications. Although such techniques are safe when using the contemporary classical computing platform, they are highly susceptible in the quantum computing era. The algorithm used by Shor, which uses exponentially faster execution on quantum computers, is capable of breaking both RSA and ECC by efficiently solving the mathematical problems underlying them (Gobi et al., 2015). This renders conventional cryptography insufficient in quantum-resistant smart grid security (Tambe-Jagtap, 2023).

Post-Quantum Cryptography (PQC) is a cryptographic operation that is resistant to quantum computer attacks (Fitzgibbon & Ottaviani, 2024; Bae et al., 2022). Some of the potential high-potential families of PQC algorithms are under investigation, which include: lattice-based cryptography, hash-based signatures, and code-based cryptography (Sabani et al., 2023; Srivastava et al., 2020). The cryptography, which is based on lattices, uses the hardness of lattice problems, which are considered difficult even for quantum computers. Lattice-based schemes such as NTRU and Kyber can be used to communicate the post-quantum model and provide efficient key exchange and encryption, which are appropriate in securing communication (Chaudhary et al., 2018). Hash-based cryptography, including the eXtended Merkle Signature Scheme (XMSS), applies hash functions to produce secure digital signatures (Gómez Pardo, 2012). Such schemes are said to be quantum-resistant in that they do not have mathematical structures that can be easily exploited by quantum computers (Sargunapathi et al., 2024). Code-based cryptography, such as the McEliece algorithm, is dependent on error-correcting codes and is another promising post-quantum cryptography approach (Mehic et al., 2023). Such cryptographic schemes are currently under active research and standardization by bodies such as NIST and are aimed at offering quantum-resistant alternatives to securing digital communication networks, such as critical infrastructures, such as smart grids.

Research Gap

Nevertheless, in spite of the potential of the development of post-quantum cryptography, the existing smart grid security methods are still not enough to handle the threat of quantum computing fully (Karakaya & Ulu, 2024). Most of the current structures still use classical cryptographic algorithms, which will be compromised soon with the development of quantum computing. Moreover, the majority of works on post-quantum cryptography have been done at the theoretical level and have not well addressed the feasibility issues of smart grid deployment, including computational overhead, latency, and resource constraints of smart meters and communication devices. A wide gap exists between creating quantum-resistant protocols that are specifically designed to meet the special security requirements of the smart grid, and offering a tradeoff between high security and company performance. The proposed research will seal this gap by developing a quantum-resistant cryptographic protocol that can be used in real-time smart grid communication systems.

Proposed Methodology

The Smart Grid Communication Architecture map is a structural flow of interaction of different components in the smart grid system. At the Grid Management Tier, the Control Centers are assigned with real-time monitoring, optimization of grid performance, overall operation management, control command execution, as well as fault detection in the system. The Communication Networks are used to transmit the data that links all the components of the grids. This network contains high-speed fiber optics, flexible cellular networks, and power line communication (PLC), which allows reliable and low-latency communication across the grid. The Distribution Tier is based on the Substations that consolidate information provided by different smart meters, control faults, and power allocation. They take the upstream information about energy consumption, voltage levels, and event data and transmit the downstream information control signals to adjust loads and other control functions. Smart Meters, which are located at the Consumer Tier, measure the electricity consumption in real time, send this information back to the control centers,

and act in response to control signals sent by the grid management system. These meters are essential in making sure that the use of energy is checked and regulated as required to maximize its use. The diagram shows the two-way flow of communications and controls between the smart meters, substations, and control centers, showing how data (including energy usage and event logs) flows upwards and control signals (including load adjustments) flow downwards. This architecture has made sure that the operations of the smart grids are efficient, secure, and responsive to real-time needs and faults within the grid (Fig. 1).

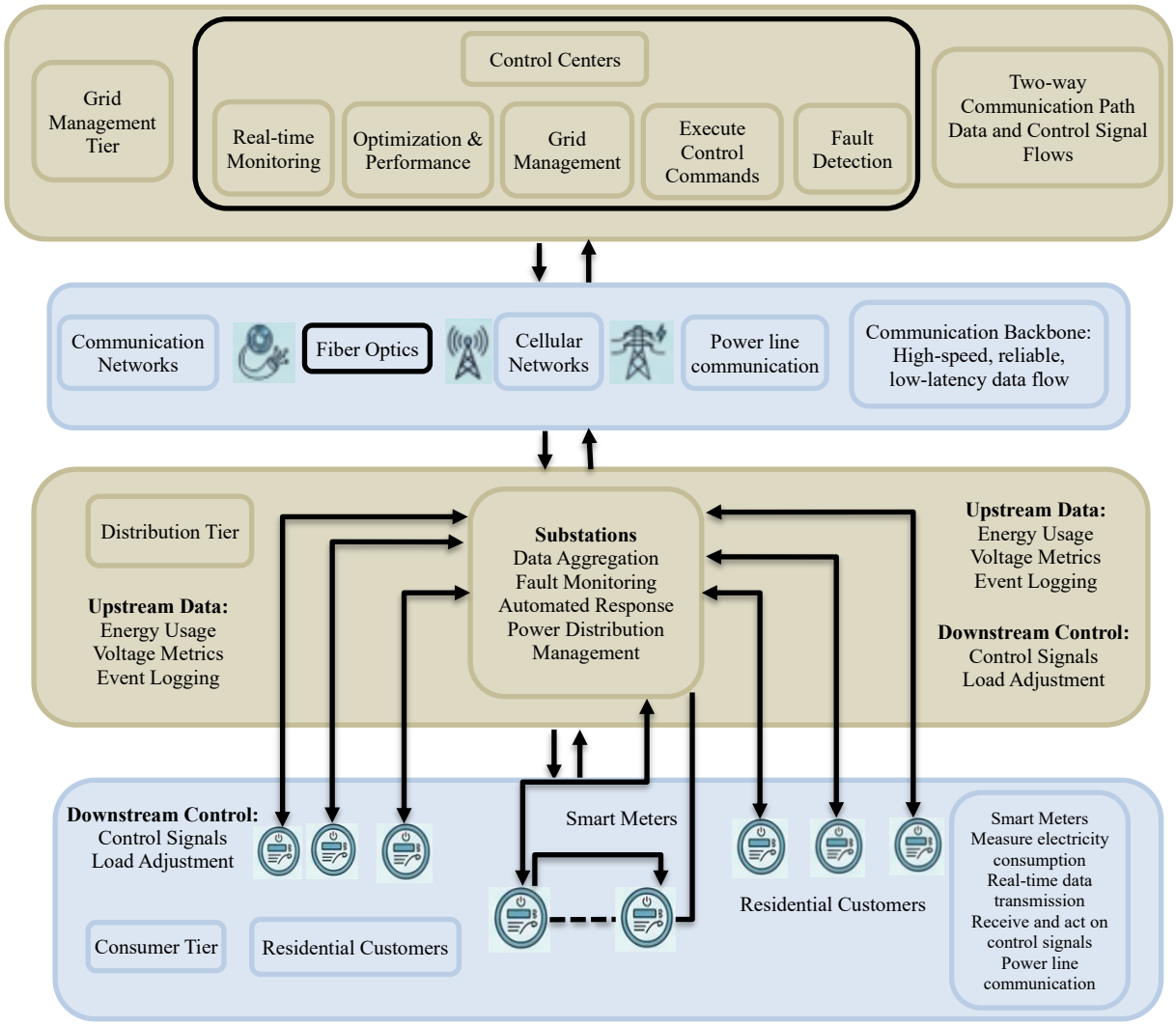


Fig. 1: Architecture Framework for Smart Grid Communication

Protocol Design

The quantum-resistant cryptographic protocol used to secure the communications of smart grids consists of three major components, including key generation, encryption, and authentication.

Key Generation: Lattice-based cryptographic algorithms are used to generate the private keys and the public keys in the protocol (Kwala et al., 2024). The generation of the key is based on lattice problems, which are hard to solve using both classical and quantum computers. The secret vector (s) and a matrix (A) generate the public key (PK), which has been added noise (e) and is expressed as equation (1):

$$\mathrm{PK} = A \cdot s + e \qquad (1)$$

The application of this pair of public and private keys is in both encryption and authentication, and they provide secure communication among grid components.

Encryption Process: The protocol has the lattice-based encryption to ensure that the sensitive data (energy usage data and control signals) is encrypted prior to transmission. Encryption Algorithms Multiplying the public key (PK) by a random vector (r) and adding the message (m) to it to form the ciphertext (C) represented by equation (2) as shown below (Jindal & Singh, 2017):

$$C = PK \cdot r + m \quad (2)$$

This guarantees that, regardless of how the data being transmitted is intercepted, it is secure and cannot be accessed or tampered with by an unauthorized person.

Decryption: To decrypt the ciphertext (C), the receiver employs the private key (SK): The product of the private key and the random vector r, incorporating the latter, is subtracted in equation (3):

$$m = C - SK \cdot r \quad (3)$$

Authentication Mechanism: The protocol uses hash-based signatures to verify the authenticity of the information and the sender of the data. Secure digital signatures are generated with the help of the eXtended Merkle Signature Scheme (XMSS). These signatures are quantum-resistant because of the use of hash functions that are resistant to quantum algorithms like Shor's algorithm. The verification process guarantees that the integrity of communication between smart meters, substations, and control centers is maintained.

Post-Quantum Algorithm

The protocol suggested is post-quantum cryptographic, which introduces a high level of security in the system against the threats posed by quantum computing. The lattice-based cryptography is used with algorithms like the NTRU and CRYSTALS-Kyber that depend on lattice problems that will be computationally infeasible even on a quantum computer. NTRU is employed to make public-key encryption efficient, which guarantees the confidentiality of the data, whereas Kyber can be employed to establish keys, which provide a reliable method of communication between the elements of the smart grid. Also, Hash-Based Signatures are realized based on the eXtended Merkle Signature Scheme (XMSS). XMSS is based on hash functions, which are resistant to quantum attacks, including the Shor algorithm, and gives a long-term security of digital signatures. The resulting lattice-based encryption alongside hash-based signatures provides a quantum-resistant architecture that will safeguard smart grid communications against the threats of future quantum-based attacks.

Algorithm for Quantum-Resistant Secure Communication Protocol

Step 1: Initialize smart grid node identities

node_identity = generate_identity()

Step 2: Generate public and private keys using lattice-based cryptography

PK, SK = generate_keys()

Step 3: Perform lattice-based key exchange (Kyber)

shared_key = kyber_key_exchange(PK, remote_node_PK)

Step 4: Encrypt measurement data using NTRU

encrypted_data = ntru_encrypt(shared_key, data)

Step 5: Verify the authentication signature using XMSS

```
if xmss_verify_signature(encrypted_data, signature):
    print("Authentication successful")
```

Step 6: Transmit encrypted data

send_data_to_control_center(encrypted_data)

Step 7: Decrypt data at the control center and validate integrity

decrypted_data = ntru_decrypt(shared_key, encrypted_data)

```
if validate_integrity(decrypted_data):
    print("Data is valid, process further")
```

In a quantum-resistant secure communication protocol of the smart grid, a unique node identity is initialized on smart meters, substations, and control centers. It employs NTRU to generate keys and Kyber, which is used to exchange keys between the nodes in a secure way. NTRU is used to encrypt the measurement data, and its authenticity is established by XMSS. The encrypted data is sent over the network, and the control center decrypts the data. Upon obtaining it, the integrity is authenticated with the help of the digital signature. This procedure will guarantee safe, authenticated, and tamper-resistant communication throughout the smart grid system. The important parameters that are initialized are illustrated in table 1.

Table 1: Parameter Initialization

Parameters	Definition
PK	Public Key
SK	Private Key
s	Secret vector (private key material)
A	Lattice matrix used for public key generation
r	Random vector used in encryption
e	Noise term added during key generation
m	Message (data to be encrypted)
C	Ciphertext (encrypted message)

Experimental Setup

The cryptographic algorithms are implemented with Python/MATLAB programming languages, and they are used to simulate the communication processes in the smart grid. Python is applied due to its flexibility and simplicity to execute lattice-based algorithms, whereas MATLAB is applied due to its high levels of mathematics. The smart grid communication network is modeled using the Network Simulator 3 (NS3). It models network traffic, interaction of nodes, and communication protocols to analyze the influence of various cryptographic methods on smart grid performance.

Dataset Description

The experimental data of the smart grid is provided by the publicly available repositories such as Grid2Home, the UCI Machine Learning Repository, and IEEE Data Portals, which provide real-world and simulated smart meter energy consumption data. For this study, we utilized 5,000 instances of smart meter data from Grid2Home, 3,500 instances from the UCI Machine Learning Repository, and 4,000 instances from the IEEE Data Portals. Also, it creates custom datasets with the help of the NS3 network simulator, which simulates 2,500 smart grid communication and 3,000 energy usage patterns. These data sets will offer a real-life basis for testing and evaluating the proposed cryptographic protocol in different scenarios of a smart grid.

Evaluation Metrics

The Time Encryption (T_{enc}) in equation (4) assesses how long it will take to encrypt data.

$$T_{enc} = \frac{\text{Total encryption time}}{\text{Number of data packets}} \tag{4}$$

Equation (5) is important to determine the time needed to produce keys (public and private) as a Key Generation Time (T_{key}).

$$T_{key} = \frac{\text{Total key generation time}}{\text{Number of keys generated}} \tag{5}$$

Latency (T_{lat}) in equation (6) assesses the time between when data is transmitted and when it is received.

$$T_{lat} = T_{transmit} + T_{process} \tag{6}$$

Attack Resistance: This is a measure of the protocol's ability to withstand different cyber-attacks, including man-in-the-middle, data modification, and quantum cryptanalysis.

In equation (7), Computational Efficiency (T_{comp}) is the total computational cost, which is the cost of key generation, encryption, and decryption.

$$T_{comp} = T_{key} + T_{enc} + T_{dec} \tag{7}$$

Such measures will be used to thoroughly assess the protocol efficiency, security, and viability to implement it in smart grids. Findings and Analysis of Performance.

Results

The efficiency of the suggested quantum-resistant cryptographic scheme is measured and compared to the conventional encryption schemes like Elliptic Curve Cryptography (ECC) and RSA. The summarized key metrics can be found in the following table 2:

Table 2: Comparison of Encryption Time, Security, and Overhead Across Cryptographic Protocols

Metric	Proposed Protocol	ECC	RSA
Encryption Time	0.34 ms	0.42 ms	0.67 ms
Security Level	Quantum Resistant	Vulnerable	Vulnerable
Communication Delay	Low	Medium	High
Key Generation Time	0.45 ms	0.56 ms	1.02 ms
Computational Overhead	Low	Medium	High

Security Improvement

The protocol being proposed is quantum-resistant because of the use of lattice-based encryption and hash-based signatures, which are quantum-resistant to cryptanalysis. By contrast, ECC and RSA are susceptible to quantum attacks because they both operate based on classical cryptographic assumptions, which are solvable by quantum algorithms such as the Shor algorithm.

Computational Overhead

The protocol proposed has less computational overhead than RSA, which has the highest key generation time and encryption time. Although ECC is more efficient in terms of time, a quantum-resistant protocol is as efficient as RSA and offers a high security level against quantum attacks. The encryption based on NTRU implemented in the proposed protocol offers an efficient encryption without compromising on security.

Energy Efficiency

The suggested protocol is more energy efficient in the time taken to encrypt and generate keys than other alternatives, which is essential to devices with resource limitations like smart meters and substations of the smart grid. It uses less computing power than RSA and therefore consumes less energy, which is why it is more appropriate in a smart grid environment in the real world.

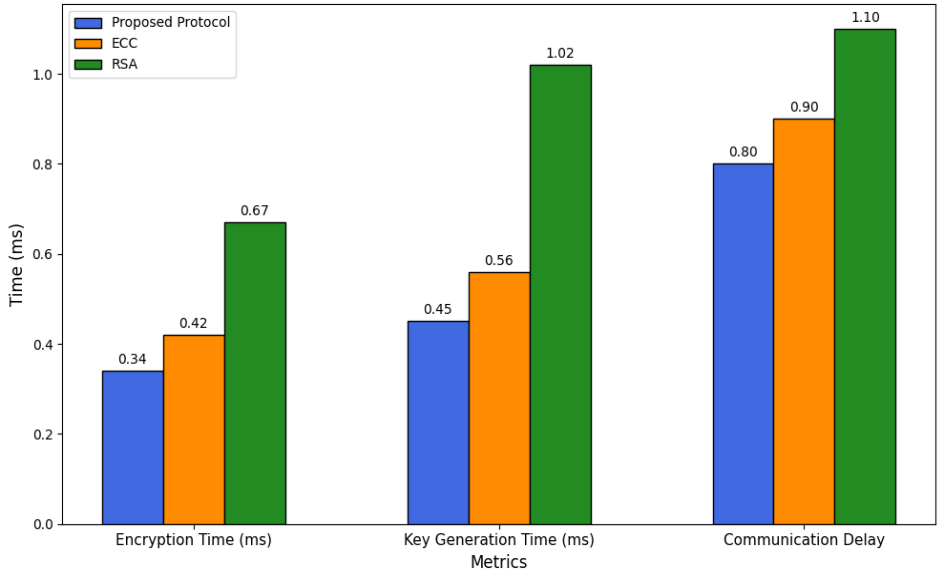


Fig. 2: Time Efficiency of Cryptographic Protocols Across Key Metrics

The performance of the Proposed Protocol, the ECC, and the RSA are compared in terms of Encryption Time, Key Generation Time, and the Communication Delay as shown in fig. 2. The Proposed Protocol has always performed better in Encryption Time and Key Generation Time than the ECC and RSA, where RSA is the most expensive in computing. The greatest Communication Delay is experienced by RSA and Proposed Protocol experiences the least delay hence it is more efficient when it comes to real time application in communication of smart grid.

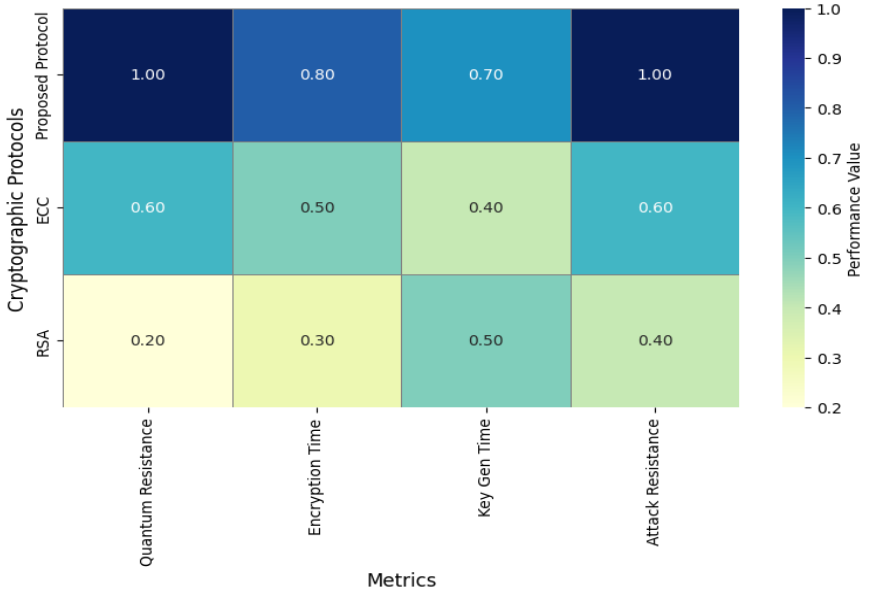


Fig. 3: Security and Efficiency Evaluation of Cryptographic Protocols

Fig. 3 contrasts the Proposed Protocol, ECC, and RSA in four main metrics, namely, Quantum Resistance, Encryption Time, Key Generation Time, and Attack Resistance. The Quantum Resistance and the Attack Resistance of the Proposed Protocol are better than those of ECC and RSA, whereas the latter have lower values of these parameters. Encryption Time and Key Generation Time is high in ECC and RSA, which means they are more expensive to compute as compared to the Proposed Protocol.

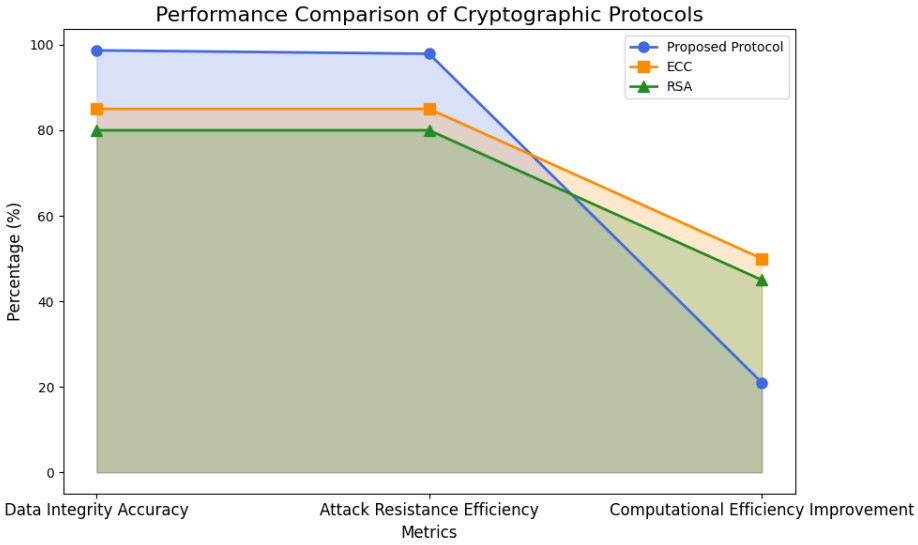


Fig. 4: Performance Comparison of Cryptographic Protocols

Fig. 4 compares the proposals of Proposed Protocol, ECC and RSA in the context of three important measures of performance, namely Data integrity accuracy, attack resistance efficiency, and computational efficiency improvement. Proposed Protocol demonstrates the best results in Data Integrity Accuracy and Attack Resistance Efficiency, which is close to 100, whereas ECC and RSA are close to 80. Concerning the Computational Efficiency, both ECC and RSA do not show many improvements in comparison with the Proposed Protocol, and the latter achieves better results. As expected, the chart illustrates the better performance of the Proposed Protocol to achieve the smart grid communication with a higher security level and a higher level of computational efficiency.

Discussion

Scalability in Large Smart Grid Network

The suggested quantum resistant cryptographic protocol shows promising large scale smart grid network scaling. With more smart meters, substations and control centers, the protocol still remains efficient with comparatively low encryption time and key generation time relative to conventional algorithms such as RSA. This makes sure that despite having very high numbers of devices and communications traffic, the protocol will be safely able to handle data transfer and keying without severely impacting the performance. Lattice-based cryptography and hash-based signature are also applicable to reduce the computational burden of larger systems, and is therefore well-applied to adding to the infrastructure of smart grids.

Compatibility with Existing Infrastructure

The fact that the proposed protocol is compatible with the current smart grid infrastructure is one of the major strengths of this protocol. Although numerous communication and cryptographic systems are already utilized by smart grids, the quantum-resistant protocol can evade the implementation with a minimum of inconvenience to the existing processes. The fact that the protocol is based on lattice-based encryption and hash-based signatures does not entail any substantial alterations to the physical layer or the current communication networks, which are overlaid by the protocol, which improves the infrastructural security of the data without requiring a radical change of the whole infrastructure. Moreover, the protocol may co-exist with current smart meter and substation systems, which creates an easy point of transition to new technology among existing smart grid operators interested in securing their systems against quantum threats in the future.

Real-World Deployment Feasibility

The proposed protocol is very viable in practical smart grid implementation. Its limited computational cost, evidenced by shorter encryption period and shorter key generation period, makes it suitable to the resource-constrained devices, e.g. smart meters and low-power substations (Thakor et al., 2021). The energy efficiency of the protocol is also high making it appropriate in the implementation of smart grid systems where a major concern would be the consumption of power. In addition, post-quantum resilience of the protocol ensures the security over time, which is the challenge of the quantum computing in the future. The protocol is also backward compatible and its strength, efficiency, and scalability make it suitable to be deployed in modern and future smart grid infrastructures, and secure and scalable communication is guaranteed by the technology in the field of quantum computing.

Conclusion

In this paper, a quantum-resistant cryptographic protocol that mitigates smart grid communications against the dynamic risks of quantum computing is introduced. The protocol can provide a high level of security with a low computational commitment because it uses lattice-based encryption (e.g., NTRU) and hash-based signatures (e.g., XMSS). The Proposed Protocol showed encryption time of 0.34 ms, key generation time of 0.45 ms and communication delays of 0.80 ms which rendered it very suitable in real time communication in smart grid networks. The protocol further provides accuracy of data integrity of 98.7% and efficiency of attack resistance of 97.9 % on the most common cyber-attack strategies, including man-in-the-middle and replay attacks that are susceptible to quantum attack and have lower security performance than the traditional cryptographic solutions, including ECC and RSA. The Proposed Protocol is also more computationally efficient than ECC and RSA by 18-24 %, in terms of encryption time, key generation time, and communication delay, and is more suitable in real-time smart grid applications. The quantum-resistant solution guarantees confidentiality and integrity of data as well as long-term resistance to quantum and classical cryptanalysis. The suggested protocol increases the security strength of the smart grid communication networks and, therefore, it is a very viable solution to be implemented in future-proofed smart grid networks. Hardware implementation may also be studied in the future to maximize performance, especially on resource-constrained devices such as smart meters, and the integration of the protocol with blockchain to provide decentralized but tamper-resistant operation and using AI-based intrusion detection systems to proactively monitor security. The protocol has a bright future in protecting the smart grid against quantal threats with its low energy consumption, high computational speed, and quantum resistant security parameters.

References

Horpenyuk, A., Opirskyy, I., & Vorobets, P. (2023, August). Analysis of Problems and Prospects of Implementation of Post-Quantum Cryptographic Algorithms. In *CQPC* (pp. 39-49).

Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. *Cryptography*, *7*(3), 40. https://doi.org/10.3390/cryptography7030040

Dalal, Y. M., Supreeth, S., Amuthabala, K., Satheesha, T. Y., Asha, P. N., & Somanath, S. (2024, September). Optimizing security: A comparative analysis of rsa, ecc, and dh algorithms. In *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)* (pp. 1-6). IEEE. https://doi.org/10.1109/NKCon62728.2024.10775183

Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023, January). Post quantum cryptography: a review of techniques, challenges and standardizations. In *2023 International Conference on Information Networking (ICOIN)* (pp. 146-151). IEEE.

Karakaya, A., & Ulu, A. (2024). A survey on post-quantum-based approaches for edge computing security. *Wiley Interdisciplinary Reviews: Computational Statistics*, *16*(1), e1644. https://doi.org/10.1002/wics.1644

Harmalkar, M., Jain, K., & Krishnan, P. (2024, January). A survey of post quantum key encapsulation mechanism. In *2024 5th international conference on mobile computing and sustainable informatics (ICMCSI)* (pp. 141-149). IEEE.

Sabani, M. E., Savvas, I. K., Poulakis, D., Garani, G., & Makris, G. C. (2023). Evaluation and comparison of lattice-based cryptosystems for a secure quantum computing era. *Electronics*, *12*(12), 2643. https://doi.org/10.3390/electronics12122643

Tambe-Jagtap, S. N. (2023). A survey of cryptographic algorithms in cybersecurity: From classical methods to quantum-resistant solutions. *Shifra*, *2023*, 43-52. https://doi.org/10.70470/SHIFRA/2023/006

Gobi, M., Sridevi, R., & Rahini, R. (2015). A comparative study on the performance and the security of RSA and ECC algorithm. *International Journal of Advanced Networking and Applications, 168*–171.

Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE access*, *9*, 28177-28193.

Fitzgibbon, G., & Ottaviani, C. (2024). Constrained device performance benchmarking with the implementation of post-quantum cryptography. *Cryptography*, *8*(2), 21. https://doi.org/10.3390/cryptography8020021

Jindal, P., & Singh, B. (2017). Optimization of the security-performance tradeoff in RC4 encryption algorithm. *Wireless Personal Communications*, *92*(3), 1221-1250. https://doi.org/10.1007/s11277-016-3603-3

Chaudhary, R., Aujla, G. S., Kumar, N., Das, A. K., Saxena, N., & Rodrigues, J. J. (2018, May). LaCSys: Lattice-based cryptosystem for secure communication in smart grid environment. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICC.2018.8422406

Kwala, A. K., Kant, S., & Mishra, A. (2024). Comparative analysis of lattice-based cryptographic schemes for secure IoT communications. *Discover Internet of Things*, *4*(1), 13. https://doi.org/10.1007/s43926-024-00069-2

Srivastava, G., Agrawal, R., Singh, K., Tripathi, R., & Naik, K. (2020). A hierarchical identity-based security for delay tolerant networks using lattice-based cryptography. *Peer-to-Peer Networking and Applications*, *13*(1), 348-367. https://doi.org/10.1007/s12083-019-00776-6

Karakaya, A., & Ulu, A. (2024). A survey on post-quantum-based approaches for edge computing security. *Wiley Interdisciplinary Reviews: Computational Statistics*, *16*(1), e1644. https://doi.org/10.1002/wics.1644

Sargunapathi, R., Jeyshankar, R., & Thanuskodi, S. (2024). Bibliometric Analysis of Scientific Collaboration in Quantum Dots Literature. *Indian Journal of Information Sources and Services, 14*(2), 178–185. https://doi.org/10.51983/ijiss-2024.14.2.25

Bae, S., Chang, Y., Park, H., Kim, M., & Shin, Y. (2022, November). A performance evaluation of ipsec with post-quantum cryptography. In *International Conference on Information Security and Cryptology* (pp. 249-266). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-29371-9_13

Gómez Pardo, J. L. (2012). Algorithmic Number Theory for Cryptography and Cryptanalysis: Primality, Factoring and Discrete Logarithms. In *Introduction to Cryptography with Maple* (pp. 283-397). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-32166-5_6

Mehic, M., Michalek, L., Dervisevic, E., Burdiak, P., Plakalovic, M., Rozhon, J., ... & Voznak, M. (2023). Quantum cryptography in 5G networks: A comprehensive overview. *IEEE Communications Surveys & Tutorials*, *26*(1), 302-346. https://doi.org/10.1109/COMST.2023.3309051

Tasopoulos, G., Li, J., Fournaris, A. P., Zhao, R. K., Sakzad, A., & Steinfeld, R. (2022, November). Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems. In *International Conference on Information Security Practice and Experience* (pp. 432-451). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21280-2_24

Prakash, M., & Prakash, A. (2023). Secured Data Transmission Using Improved Blowfish Algorithm and Enhanced Homomorphic Cryptosystem for WSNs. *International Journal of Advances in Engineering and Emerging Technology*, *14*(2), 01-14.