Enhancing Smart Grid Security with Quantum Cryptography: A BB84-Based Framework

Shail garg
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22254@bl.students.amrita.edu

Yerukola Gayatri
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22267@bl.students.amrita.edu

A. Surya Kausthub
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22287@bl.students.amrita.edu

Shinu M Rajagopal
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
mr_shinu@blr.amrita.edu

***Abstract*—The study investigates how quantum cryptography can be employed to improve security in smart grid communication networks. Attempting to use the BB84 QKD protocol, it allows secure creation and management of those cryptographic keys that cannot be broken with the help of quantum and traditional hacking techniques. It depends on symmetric encryption mechanisms like AES to provide high data confidentiality during transmission. Regarding the key management, the system provides a key management server that distributes keys to the grid nodes and performs key updating to ensure control with the managing authority. It also presents reliability under practical conditions through performance analogs such as Quantum Bit Error Rates (QBER), and system latency. This approach shows that quantum cryptography can provide a highly secure and efficient communication network for the next-generation smart grid.**

***Index Terms*—Quantum Cryptography, Smart Grids, BB84 Protocol, Quantum Key Distribution (QKD), Symmetric Encryption, AES, Quantum Bit Error Rate (QBER), Secure Communication, Key Management, Cybersecurity in Energy Systems.**

I. Introduction

Security in today's smart grid systems is crucial because they play a vital role in the present and future distribution of energy in the world's complex and combined networks. These grid which incorporates sophisticated monitor, communication, and control technologies are the fundamental skeletal structures of critical infrastructure systems. Yet due to their reliance on digital operations, they are vulnerable to cyber risks which may result in system disruptions. Quantum computing is a new trend in the technology world, while classical cryptography can become ineffective when applying this trend, so researchers should look for quantum-secure approaches. The problem of key distribution and subsequent secure communication has become an area of immense focus with the introduction of quantum cryptography –The groundbreaking potential of quantum cryptography, which uses concepts from quantum mechanics, such as the Heisenberg Uncertainty Principle, to improve security, is examined by various researches. BB84 and other more recent Quantum Key Distribution (QKD) protocols are the main focus, and real-world issues such device flaws and assaults are addressed. By contrasting quantum and classical cryptography,focused is on applications in data security and secure communication. It ends with a consideration of potential advancements, including scalability and quantum digital signatures, establishing quantum cryptography as a promising technique for safe networks[1]. A revolutionary field based purely on the principles of quantum mechanics. This research domain has attracted a lot of attention especially because of the importance that this technology holds not only as an innovation but as a solution to some of the weaknesses in society and infrastructure.

As a firm starting point, it is necessary to address some basic issues related to the forthcoming research problem. Awareness concerning the principles of quantum cryptography and its superiority in opposition to conventional approaches introduce the reader to basic notions that contribute to its appreciation of its revolutionary characteristics. The BB84 Quantum Key Distribution (QKD) protocol reveals that QKD is important in solution to the problem of key exchange. Equally importantly, the communications and security issues in smart grids inflict practical imperatives for the incorporation of quantum cryptography solutions. These topics collectively lay down the preliminary platform on which one can locate the shortcomings of current methods and put forward the case for novel developments.

Although a lot of progress has been made in the domain of quantum cryptography and its theory[8], little effort has been paid to its implementation within the infrastructure of the smart grid. Many previous works have focused on individual QKD systems or have not considered the factors and parameters important when implementing the method in practice. Further, now available solutions are known to lack the ability to integrate quantum key distribution with strong classical encryption, thus leaving it full of voids in terms of viability and productivity. To overcome these limitations the present study suggests a new framework which is the BB84 protocol combined with symmetric encryption techniques like AES with the help of KMS. This approach is more effective not only in terms of quantum security resilience but also about the usability of the solution in Smart Grid environments.

This paper's objectives are to expand and assess a combined BB84 and symmetric encryption-based quantum and classical cryptographic approach for smart grids' communication systems against future adversities.

The rest of the paper is structured in the following manner: In Section II, a detailed literature review on the topics of quantum cryptography and security aspects of smart grid systems is presented. In Section III, the proposed methodology is explained in detail, along with its components and implementation strategy. In Section IV, the results, including performance measures such as quantum bit error rate (QBER) and system delay, are shown. In Section V, the main conclusions drawn from the analyzed data are expressed and their relevance is indicated. Finally, in Section VI, the proposed framework's future scope is explained and advancements and applications are suggested.

II. Literature survey

Quantum cryptography has surfaced as a viable method to address the vulnerabilities introduced by quantum computing, especially through protocols for Quantum Key Distribution (QKD) like BB84. Previous research has investigated QKD applications in secure communication, the Internet of Things (IoT), and smart grid systems, tackling practical issues such as noise interference, key synchronization, and the detection of eavesdropping. While some studies aim to combine QKD with traditional encryption techniques, others emphasize the importance of post-quantum cryptography to protect against quantum-related threats, with only a few exploring the connection between practical application and scalability.

Pljonkin, A.With an emphasis on fiber-optic phase coding for secure communication and synchronization for precise key generation, the paper examines commercial quantum key distribution (QKD) systems. It displays a 500 bits per second key rate, auto-compensation features, and an experimental setup showing a 24 km QKD network. Additionally covered are developments and trends in quantum cryptography.[2]

Sharma, N. Quantum Key Distribution (QKD), a secure cryptographic technique that uses quantum physics to facilitate unconditionally secure key exchange, is examined in this work. It examines fundamental ideas, important protocols such as BB84, E91, and SARG04, and both discrete and continuous-variable experimental implementations of these protocols. Secure communication and improved cryptographic systems are examples of practical uses; scalability, speed, and range are the main areas of active study. The conclusion establishes QKD as a fundamental component of quantum information science by highlighting its revolutionary potential in secure communication[3].

Banerjee, S.The paper reviews commercial Quantum Key Distribution Systems (QKDS), detailing their principles, protocols like BB84, and practical implementations using fiber optics. It highlights key generation at 500 bits per second over 24 km, synchronization challenges, and vulnerabilities. Real-world applications in secure communications are discussed, with emphasis on advancements in quantum technology. The study underscores QKDS's significance as classical cryptography faces quantum computing threats[4].

Sajimon, P.C.In order to protect IoT devices from the threat of quantum computing, which makes conventional cryptographic techniques susceptible, the study assesses Post-Quantum Cryptography (PQC) solutions. Using a Raspberry Pi 4, it evaluates NIST's third-round PQC finalists and finds that LightSaber-KEM and Dilithium2 are the best options for resource-constrained IoT devices because of their effectiveness and low power needs. The report urges the incorporation of quantum-safe cryptography into IoT systems and draws attention to the present dependence on antiquated protocols such as TLS 1.2. Quantum-resistant TLS/DTLS implementations for improved IoT security are the main focus of future research[5].

Giroti, I.The paper addresses the risks associated with quantum computing by analyzing how quantum mechanics can improve cryptographic security. It focuses on Quantum Key Distribution (QKD), particularly the BB84 system, which leverages quantum concepts like entanglement and superposition to detect eavesdropping. In order to demonstrate how quantum technologies have the potential to revolutionize secure communication, the study also presents post-quantum cryptography, focusing on algorithms made to withstand quantum attacks[6].

Jasoliya, H.The paper looks at how secure communication could be revolutionized by quantum cryptography. It highlights the application of quantum concepts like entanglement and no-cloning to stop data breaches by contrasting traditional encryption techniques with quantum-based alternatives. Quantum Key Distribution (QKD) protocols, their function in protecting IoT systems, and implementation issues such as cost, distance, and technical limitations are all covered in the paper. The authors point out that quantum cryptography is a promising development in the fight against new cybersecurity threats since it can detect eavesdropping[7].

Alvarez, D.The study examines the development and uses of quantum cryptography, a discipline that uses quantum physics to improve the security of encryption. Alongside cutting-edge uses including quantum coin flipping, secret sharing, and random number generation, it highlights quantum key distribution (QKD) as the most advanced field. There includes discussion of issues including noise, entanglement requirements, and device reliability, while advancements in device-independent protocols are highlighted. The study comes to the conclusion that although certain applications encounter theoretical and practical challenges, technological and protocol developments will continue to influence secure communication in the future[8].

Chaudhuri, K.The paper explores quantum cryptography as a means to secure network communication by leveraging quantum mechanical properties, particularly in quantum key distribution (QKD). It reviews classical and quantum cryptographic protocols, emphasizing innovations like the BB84 protocol and the proposed three-party model for secure key exchange. The paper highlights the challenges of interference and data loss, and introduces a methodology to enhance security using quantum entanglement and discreet key sharing. Future prospects in communication and information security through advancements in quantum technology are discussed, aiming to address current vulnerabilities and improve system reliability[9].

Aji, A.In order to overcome the issues that quantum computing presents to conventional cryptography, the research examines simulation platforms for quantum key distribution (QKD) networks. It draws attention to how advances in quantum computing have made traditional algorithms like RSA vulnerable, and it presents QKD as a safe substitute based on quantum mechanics. The study examines several QKD simulation frameworks, including QuCCs, qkdSim, and NetSquid, assessing their capacity to replicate defects in the real world, modularity, and protocol support. The results highlight the necessity of scalable, precise, and effective simulation tools to support the real-world creation of quantum-secure communication systems[10].

Abulizi, J.In order to improve the security of power grid communication networks, the integration of quantum cryptography into smart grids is examined in this research. It examines important technologies, such as quantum key distribution (QKD), which is used for long-distance transmission, fault analysis, and safe encryption. In order to address issues such signal interference, short transmission distances, and exorbitant costs, the study suggests alternatives such as quantum key cloud services and WDM technology for multiplexing. The results show promise for developing reliable quantum-secure communication systems and increasing the accuracy of fault location, opening the door for scalable and reasonably priced energy infrastructure applications[11].

Lardier, W.In order to integrate quantum key distribution (QKD) protocols into smart grid communications, the study presents Quantum-Sim, an open-source co-simulation platform. The platform, which is built on the MOSAIK framework, enables researchers to model and examine QKD-based protocols, gauge their effectiveness, and evaluate security against vulnerabilities such as man-in-the-middle (MITM) attacks. Numerous QKD protocols (such as BB84 and SARG04) and cryptosystems are supported, offering a flexible setting for testing quantum communication in authentic power grid situations. While addressing implementation and testing problems, the study highlights QKD's promise for safe and effective smart grid communication[12].

Bera, B.The study discusses how advances in quantum computing have made traditional encryption techniques vulnerable in smart grid applications. In order to protect post-quantum communication, it suggests a simple security protocol based on the Ring Learning With Errors (RLWE) lattice issue. For smart grid applications like smart metering and e-vehicle charging, this protocol guarantees data secrecy, authentication, and integrity while fending against assaults including denial-of-service, quantum, and man-in-the-middle attacks. The suggested approach exhibits improved security in post-quantum scenarios, scalability, and lower communication and computing costs through comparative analysis and real-time testing[13].

Bebrov, G.The use of Quantum Key Distribution (QKD) to improve information privacy in Smart Grid communication networks is examined in this research. It identifies flaws in conventional cryptography brought about by advances in quantum computing and assesses different QKD systems according to criteria such as key rates, operational distances, prices, and reliability. For best results, the study suggests a hybrid QKD network that combines Continuous Variable (CV) and Discrete Variable (DV) methods using Measurement-Device Independent (MDI) QKD. This method solves confidentiality issues in Smart Grid communications while ensuring safe key distribution, lowering expenses, and integrating easily with current optical communication infrastructure[14].

Khan, B.The paper proposes a secure smart grid architecture using post-quantum blockchain technology to address privacy and security challenges posed by the advent of quantum computing. It leverages lattice-based cryptography, particularly the Ring Learning With Errors (R-LWE) problem, to enhance security against quantum attacks. The architecture integrates a post-quantum signature scheme for secure data communication and transaction validation among grid components, ensuring data confidentiality, integrity, and availability. The proposed system demonstrates improved scalability, reduced vulnerabilities, and compatibility with existing smart grid infrastructures, providing a robust solution for post-quantum era security requirements[15].

Our research introduces a BB84-based QKD framework specifically designed for smart grids, incorporating symmetric encryption (AES) along with centralized key management to facilitate secure and efficient communication. In contrast to earlier studies that analyze QKD and classical cryptographic methods in isolation, our method demonstrates resilience in noisy environments, confirmed by latency and Quantum Bit Error Rate (QBER) evaluations. The integration of error detection along with real-time key regeneration improves the reliability of the system, showcasing its scalability and practicality for essential infrastructures. This hybrid approach distinctively merges the advantages of both quantum and classical cryptography to bolster cybersecurity within energy systems.

III. Methodology

The proposed framework utilizes *Quantum Key Distribution (QKD)* techniques specifically the *BB84 protocol* for secure key generation and uses *AES encryption algorithms* to provide adequate communication in a smart grid environment. First, the BB84 protocol is set up and run where Alice assumes the role of an initiator generates some random bits, and then places these bits onto quantum states either using the Z-basis or X-basis. These quantum states are passed through a noisy quantum channel to Bob who measures the states using an independent basis which he chooses randomly and other states are kept for Alice's measurement bases. A common dagger is produced by keeping those bits for which Alice's and Bob's bases are the same and discarding them for which basest were different. Adding noise to the channel serves the purpose of obeying practical conditions and also aids the system in calculating the *Quantum Bit Error Rate (QBER)*, which is defined as the number of inconsistent bits. This calculation of QBER acts as a measure of the eavesdropping activity and the quality of the channel.

When the shared key is created, this key is transferred by a *Central Authority* to the smart grid nodes for secure exchanges. The key is also padded to comply with the size specifications of AES encryption algorithm. Using the key generated by Quantum Key Distribution, Node A prepares an AES-encrypted ciphertext of the text message: 'Energy load balanced at 70%' Node B receives the ciphertext from Node A and uses the same key to decrypt and check the message. A decision mechanism is included to ensure that the QBER remains within acceptable thresholds. In case the QBER goes beyond a certain level normally determined by practical considerations of noise or spying, normal conditions of the key generation process are returned so that the security of the system is not compromised.

To determine how well the system performs, the framework is applied, and brief findings are presented to the reader. With respect to the above, the framework is tested with varying key lengths of 16, 32, 64, and 128 bits. Then, each key length considers the time of key generation and encryption (latency) and the QBER values as well. These performance characteristics are used to study the scalability and robustness of the framework. The simulation also indicates how latency and QBER vary with key length in the system, showing us the effect of longer key and noisier channel on the system. This is the point at which tension is introduced into the frame to ensure the workings of the whole frame at high costs.

Figure 1 presents the flow of the proposed system providing a step-by-step process involving secure key generation and communication.

The research also includes the application of error correction mechanisms in subsequent versions to accommodate adverse QBER levels while enhancing key usability. To represent realistic quantum channel communication imperfections, noise levels are intentionally set to 10%. This is done to allow the system to work under varying levels of channel attenuation and secure data transmission. While AES encryption allows for the integration of easily existing communication networks, security is enhanced by using quantum keys enabling a mixed architecture to governmental infrastructures that are for instance smart network systems.

Finally, the system performance is presented in two advanced plots: Key Length vs Latency and Key Length vs QBER. These plots are produced to illustrate the effects of the key length on the computational load and the noise in the channel, respectively. The data from the BB84 protocol and the data from the AES encrypted video are compared to assess the scalability, quality, and strength of the proposed approach. This sequential analysis confirms the system's viability for real-world application particularly in the area of secure smart grid communications.

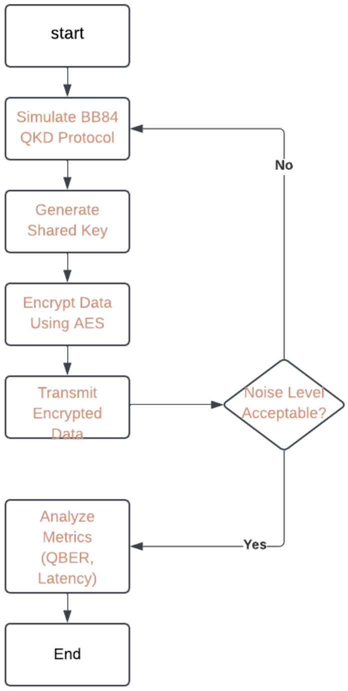


Fig. 1. Flow chart of the proposed methodology

IV. Results

A. Latency Analysis

The curve involving *Key Length vs Latency* has a positive slope. In the case of very short keys, for example, of 16 bits long, the delay experienced is insignificant ($\sim$ 2 seconds) while in the case of longer keys, for instance, of 128 bits long, the delay extends proportionately to $\sim$ 10 seconds. It jitters because there are more bits to process within the BB84 protocol. This increase also occurs because more time is required to prepare the quantum states, to make the measurements, and to carry out the reconciliation for longer keys. Such a growth indicates a steady and controlled increment in the amount of delay imposable, thus reassuring that the system is scalable and longer keys can be accommodated, would there be no performance choking. The findings support the pillars of the framework – its capacity for efficiency is retained even with the increase in key size making it suitable for deployment in practical and time-critical applications like smart grids as shown in Figure 2.

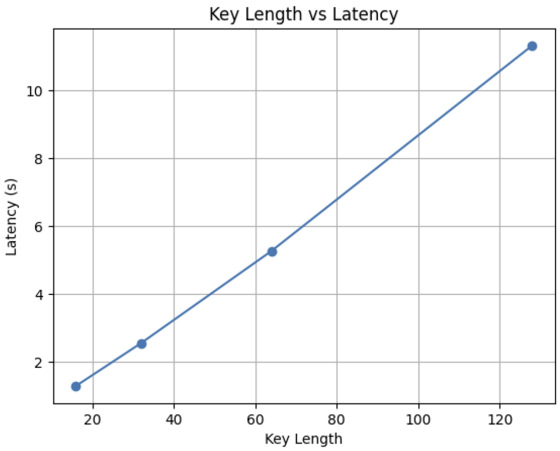


Fig. 2. Key Length with respective to Latency

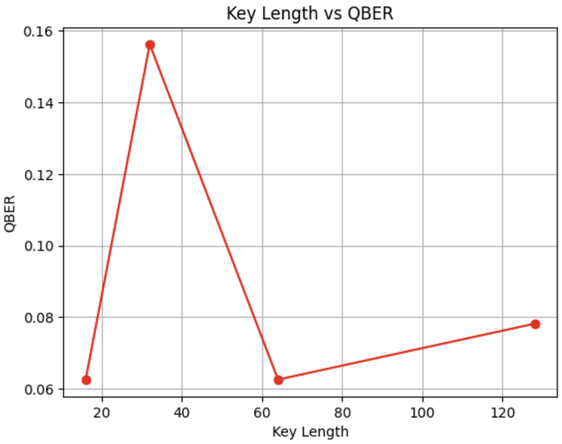
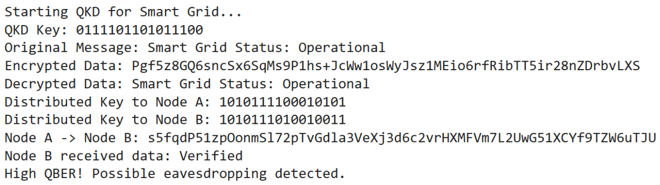


Fig. 3. Key Length with respective to QBER

B. QBER Analysis

The plot illustrating the relationship between *Key Length and QBER* demonstrates a much less fixed association between the two. When dealing with shorter keys like 16 bits, the QBER parameter is relatively low ($\sim$ 6%), this is because there are hardly any mismatch errors resulting from noise in the quantum channel. However, if 32-bit keys are used, there is an increase in QBER to $\sim$ 16%, which is largely due to random noise effects. Whereas in the case of longer keys like 64 and 128 bits, the QBER remains constant at approximately $\sim 8\%$ indicating the system's ability to handle the noise. Figure 3 shows this relationship, QBER tolerable levels for secure communications are achieved even though occasional spikes in QBER highlight the noisiness in quantum communications. Its enhanced ability to raise the alarm on high QBER as in the warning message *"High QBER! Possible eavesdropping detected,"* ensures possible threats or too much noise overload from occurring resulting in proactive measures like regenerating keys.



```
Starting QKD for Smart Grid...
QKD Key: 0111101101011100
Original Message: Smart Grid Status: Operational
Encrypted Data: Pgf5z8GQ6sncSx6SqMs9P1hs+JcWw1osWyJsz1MEio6rfRibTT5ir28nZDrbvLXS
Decrypted Data: Smart Grid Status: Operational
Distributed Key to Node A: 1010111100010101
Distributed Key to Node B: 1010111010010011
Node A -> Node B: s5fqdP51zpOonmSl72pTvGdla3VeXj3d6c2vrHXMFVm7L2UwG51XCYf9TZW6uTJU
Node B received data: Verified
High QBER! Possible eavesdropping detected.
```

Fig. 4. quantum cryptography implementation results

C. Encrypted Communication Analysis

The system can encrypt and decrypt messages using keys that have been generated through QKD as shown in Figure 4. The plain text message which reads *"Smart Grid Status: Operational"* was encrypted into ciphertext before being decrypted back to its original form, confirming the functionality of both encryption and decryption processes. Moreover, Node A encrypted the plaintext message and sent it as a ciphertext to Node B. After that, Node B was able to successfully decrypt this message and confirmed that it was received accurately. This indicates the strength of the system in supporting secured communication among its nodes.

D. High QBER Detection

As shown in Figure 3 the system issued a *High QBER* notice during the simulated experiment which indicates its ability to detect abnormal conditions in the quantum channel. High QBER values may occur due to high noise levels or eavesdropping threats. The system's operation is designed in such a way that insecure communication under these circumstances is impossible due to the implemented mechanism that causes the key generation process to be initiated once again. This increases the overall performance of the framework thus making it appropriate for critical infrastructures where the security level is highly regarded.

E. Summary of Observations

The proposed framework has seamlessly combined quantum cryptography with AES encryption for the provision of secure, extended, and dependable communication in smart grids. From the Key Length vs Latency graphs, it was observed that an increase in latency was directly proportional to the key length which showed scalability as well as the extension of larger keys with minimal computational cost being incurred. Even with some intermittent increases in QBER caused by noise, the system was able to support secure communication with QBER values being within reasonable limits. The processes of data encryption and decryption were completed successfully on a consistent basis which verified the claims on communication security of the framework. Moreover, the occurrence of high QBER was an indication of the high tolerance of the system which allowed the system to cope with possible threats or excessive noise to the communications. Consequently, the findings support the position that the framework is a suitable and workable architecture to be used for the security of communications in a smart grid system.

V. Conclusion

A novel and efficient framework that employs Quantum Key Distribution (QKD) and Advanced Encryption Standard (AES) for enhanced protection of smart grid communications. In addition, the framework exhibited a well-defined performance, with linear latency increase proportional to the key length while demonstrating tolerance to external interferences due to good acoustic QBER control. Its power to encrypt, decrypt, and authenticate the information while it is impossible to use any high QBER allows reliable and robust functioning. The framework is, therefore, viable in that it combines the advantages of quantum and classical encryption systems. These findings highlight its promise to deliver secure communication systems in the advanced age tailored to an environment characterized by high risk such as smart grids.Future scope could include real-time distribution of keys forms the core component of the proposed framework and hence there is potentiality for application in larger smart grid networks. It is proposed to incorporate such novel technologies as blockchain in the secure trading of energy and to validate the framework on the platform of real quantum computers. Further, the energy-optimized position and exploring one more hybrid crypto system model will be beneficial to implement its feasibility and reliability in the smart grid domain .

References

[1] Sehgal, S.K. and Gupta, R., 2021, December. Quantum Cryptography and Quantum Key. In 2021 International Conference on Industrial Electronics Research and Applications (ICIERA) (pp. 1-5). IEEE..

[2] Pljonkin, A. and Singh, P.K., 2018, December. The review of the commercial quantum key distribution system. In 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 795-799). IEEE.

[3] Sharma, N., Singh, P., Anand, A., Chawla, S., Jain, A.K. and Kukreja, V., 2023, June. A Review on Quantum Key Distribution Protocols, Challenges, and Its Applications. In International Conference on Recent Developments in Cyber Security (pp. 541-550). Singapore: Springer Nature Singapore.

[4] Banerjee, S., Nikhilesh, M., Sharma, A., Sreedevi, A.G., Rana, S. and Chaudhary, D., 2023, October. Quantum Safe Construction of Authentication and Key Exchange Based on Module Lattices. In 2023 4th IEEE Global Conference for Advancement in Technology (GCAT) (pp. 1-6). IEEE.

[5] Sajimon, P.C., Jain, K. and Krishnan, P., 2022, May. Analysis of post-quantum cryptography for internet of things. In 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 387-394). IEEE.

[6] Giroti, I. and Malhotra, M., 2022, December. Quantum Cryptography: A Pathway to Secure Communication. In 2022 6th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (pp. 1-6). IEEE.

[7] Jasoliya, H. and Shah, K., 2022, March. An exploration to the quantum cryptography technology. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 506-510). IEEE.

[8] Alvarez, D. and Kim, Y., 2021, January. Survey of the development of quantum cryptography and its applications. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1074-1080). IEEE.

[9] Chaudhuri, K. and Singh, T., 2015, September. Securing networks using Quantum Cryptography. In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-5). IEEE.

[10] Aji, A., Jain, K. and Krishnan, P., 2021, October. A Survey of Quantum Key Distribution (QKD) network simulation platforms. In 2021 2nd Global Conference for Advancement in Technology (GCAT) (pp. 1-8). IEEE.

[11] Abulizi, J., Qingsheng, H. and Wei, W., 2022, November. Quantum Cryptography Technology and Application in Smart Grid. In 2022 IEEE 22nd International Conference on Communication Technology (ICCT) (pp. 1213-1217). IEEE.

[12] Lardier, W., Varo, Q. and Yan, J., 2019, October. Quantum-sim: An open-source co-simulation platform for quantum key distribution-based smart grid communications. In 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (pp. 1-6). IEEE.

[13] Bera, B. and Sikdar, B., 2024, September. Securing Post-Quantum Communication for Smart Grid Applications. In 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (pp. 555-561). IEEE.

[14] Bebrov, G., Dimova, R. and Pencheva, E., 2017, May. Quantum approach to the information privacy in smart grid. In 2017 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP) (pp. 971-976). IEEE.

[15] Khan, B., Haq, I.U., Rana, S. and Rasheed, H.U., 2022, August. Secure smart grids: Based on post-quantum blockchain. In 2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST) (pp. 653-658). IEEE.