












Research Paper

Leveraging Quantum Key Distribution for Data Security in Distributed Energy Resources

Asnal Effendi^{1,*} , Muntadher A. Hussein² , Nada Q. Mohammed³ , Hussam A. Abdulridui⁴ ,
Baydaa Sh.Z. Abood⁵ , Saoud C. Mashkoor⁶ , Zahraa Y. Shaker⁷ , Kadhum Al-Majdi⁸ ,
Khamdamov O. Nematullaevich⁹ , Dahlan Abdullah¹⁰ , and Yerkin Yerzhigitov¹¹ 

¹Department of Electrical Installation Engineering Technology, Institut Teknologi Padang, Indonesia.

²Department of Medical Laboratory Technics, Al-Manara College For Medical Sciences, Maysan, Iraq.

³Department of Medical Laboratories Technology, AL-Nisour University College, Baghdad, Iraq.

⁴Department of Medical Laboratory Technics, Al-Hadi University College, Baghdad, Iraq.

⁵College of Health and Medical Technology, National University of Science and Technology, Dhi Qar, Iraq.

⁶Department of Medical Laboratory Technics, Mazaya University College, Iraq.

⁷Department of Medical Laboratory Technics, Al-Zahrawi University College, Karbala, Iraq.

⁸Department of Biomedical Engineering, Ashur University College, Baghdad, Iraq.

⁹Tashkent State University of Economics, Islam Karimov Street, 49, Tashkent, 100066, Uzbekistan.

¹⁰Department of Informatics, Universitas Malikussaleh, Aceh, Indonesia.

¹¹Kazakh National Agrarian Research University, Abai 8, Almaty, Kazakhstan.

Abstract— The rapid proliferation of Distributed Energy Resources (DERs) introduces substantial challenges in securing the vast volumes of data exchanged within these decentralized networks. While traditional cryptographic methods remain effective, they are increasingly susceptible to the threats posed by quantum computing, particularly in the realm of key distribution. This paper proposes Quantum Key Distribution (QKD) as an advanced solution, harnessing the principles of quantum mechanics to deliver unparalleled security for cryptographic key establishment. We explore the application of QKD within DER systems, addressing specific constraints such as limited bandwidth, resource-constrained devices, and dynamic network topologies. We assess the feasibility of incorporating QKD into existing communication frameworks by evaluating the BB84 QKD protocol and its integration with DER infrastructures. Our study also considers practical aspects such as scalability, interoperability, and cost-effectiveness. The findings reveal that QKD achieves a practical key efficiency of approximately 50%, underscoring its suitability for DER applications. Moreover, QKD provides robust security features, including minimal error rates in noiseless environments, manageable error rates in noisy conditions, and strong resilience against eavesdropping. These capabilities ensure the integrity and confidentiality of data within DER networks, marking a significant advancement in secure communication technologies.

Keywords—Distributed energy resources, data security, quantum key distribution, BB84 protocol.

NOMENCLATURE

Abbreviations

BB84 BB84 protocol
CPES Cyber-physical Energy systems
CPS Cyber-physical systems
DER Distributed energy resources

DSO Distribution system operator
IDS Intrusion detection system
IoE Internet of everything
ISO/IEC 27001 International organization for standardization/international electrotechnical commission 27001
MFA Multi-factor authentication
NERC CIP North american electric reliability corporation critical infrastructure protection
PKI Public key infrastructure
QKD Quantum key distribution
SIEM Security information and event management
SSL Secure sockets layer
TLS Transport layer security
VPN Virtual private network
VPP Virtual power plant

Received: 02 Jul. 2023

Revised: 21 Aug. 2024

Accepted: 26 Aug. 2024

*Corresponding author:

E-mail: effendi.asnal@yahoo.com (A. Effendi)

DOI: [10.22098/joape.2024.15383.2177](https://doi.org/10.22098/joape.2024.15383.2177)

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

Copyright © 2025 University of Mohaghegh Ardabili.

1. INTRODUCTION

The global energy sector is experiencing a profound shift driven by the integration of Distributed Energy Resources (DERs). These resources include a variety of technologies such as solar panels, wind turbines, battery storage systems, and electric vehicles, all of which are located closer to end-users compared to traditional centralized power plants [1]. This shift towards decentralization offers numerous benefits, including improved grid resilience, reduced transmission losses, and enhanced energy efficiency and sustainability. However, it also brings significant challenges, especially regarding data security. The proliferation of DERs generates vast amounts of data, essential for monitoring, controlling, and optimizing energy production and consumption [2]. Ensuring the security of this data is crucial to maintain the reliability, efficiency, and integrity of energy systems. Data breaches, cyber-attacks, and unauthorized access pose substantial risks, potentially leading to operational disruptions, financial losses, and physical damage to critical infrastructure. Data security in DERs involves protecting data at all stages [3]: generation, transmission, storage, and utilization. Key security objectives include maintaining the confidentiality, integrity, and availability of data. Confidentiality ensures that sensitive information is accessible only to authorized individuals. Integrity guarantees that data is accurate and has not been tampered with. Availability ensures that data is accessible when needed. Achieving these objectives is complex due to the distributed and dynamic nature of DERs, which involve numerous interconnected devices spread across wide areas. Ensuring data security in DERs involves addressing several key challenges through a variety of solutions. For secure communication networks, strong encryption protocols like TLS and SSL, Virtual Private Networks (VPNs), and the deployment of firewalls and Intrusion Detection Systems (IDS) are essential to prevent cyber-attacks such as eavesdropping and data interception. Robust authentication and authorization mechanisms, including Multi-Factor Authentication (MFA), Public Key Infrastructure (PKI), and Role-Based Access Control (RBAC), are crucial to verify identities and manage access permissions [1]. Secure data storage is achieved through data encryption, the use of distributed storage systems, and regular backups to protect against unauthorized access and ensure data integrity [4]. Effective data management involves data anonymization, strict access controls, and data integrity checks using checksums and hash functions. Advanced threat detection and response are facilitated by machine learning and AI to analyze data patterns, as well as Security Information and Event Management (SIEM) systems for real-time threat detection. Lastly, adherence to regulatory compliance and standards, such as ISO/IEC 27001 and NERC CIP, along with regular security audits, ensures that DER systems meet established security benchmarks and are continually monitored for vulnerabilities [4]. This paper contributes in the following ways:

- **Introduction and Application of QKD:** The paper presents Quantum Key Distribution (QKD) as a novel approach to enhancing data security within Distributed Energy Resources (DER) systems, specifically examining the practical application of the BB84 protocol in decentralized energy networks.
- **Evaluation of Practical Effectiveness:** It evaluates the key efficiency of QKD, demonstrating a practical effectiveness of around 50% through detailed simulations under various conditions, including ideal, noisy, and eavesdropped channels.
- **Identification of Implementation Challenges and Future Research:** The paper identifies key challenges related to implementing QKD in DER systems, such as scalability and cost-effectiveness, and highlights the need for further research to address these challenges and optimize quantum security solutions for decentralized energy environments.

The rest of the paper is structured as follows: Section 2 reviews methodologies for enhancing data security in DERs,

focusing on three main areas: QKD and cryptographic solutions, security architecture and integration, and analytical approaches. Section 3 details the integration of QKD with central monitoring units in DERs, showing that QKD can significantly enhance data security through real-time monitoring and anomaly detection. Section 4 demonstrates QKD's practical key efficiency of around 50% across various channel conditions, including noiseless, noisy, and eavesdropped scenarios. Finally, Section 5 concludes by highlighting the effectiveness of QKD in securing DERs while addressing challenges related to scalability and cost.

2. LITERATURE REVIEW

The investigated papers address diverse methodologies aimed at enhancing data security within energy systems and can be grouped into three main categories. The first group focuses on QKD and cryptographic solutions. Ref. [1] surveys recent work on blockchain-based energy data security, proposing a novel integrated security architecture that combines on-chain and off-chain methods for multi-blockchain environments. Ref. [5] suggests a cryptographic solution for fog computing security, blending AES-GMAC with information dispersal techniques to ensure data confidentiality, integrity, availability, and authentication, with improved security through encrypted data spread across fog nodes. Ref. [6] introduces a novel approach to enhance security in Energy Harvesting (EH) systems for the Internet of Everything (IoE), proposing a joint protection framework using incentive federated learning to detect malicious users and preserve privacy.

The second group centers on system integration and security architecture. Ref. [3] introduces a new approach for secure data exchange in DERs using a Distribution System Operator (DSO), featuring a cybersecurity mesh with a distributed ledger and a private blockchain for managing data flows, transactions, and access control within microgrids. Ref. [2] discusses the transition of DERs to prototypes for the energy Internet, advocating for integrated systems to optimize energy usage, reduce waste, and ensure stable operations. Ref. [7] presents a comprehensive security framework for smart grid systems, integrating a layered defense model within the National Renewable Energy Laboratory's Security and Resilience Testbed, with recommendations for improving cybersecurity in utilities. Ref. [8] examines the integration of renewable energy systems like microgrids and Virtual Power Plants (VPPs) into existing grids, focusing on cybersecurity issues in Australian DERs and outlining security scenarios and standards development based on real-world DER installations. Ref. [9] explores the development of the energy Internet for integrating clean energy and managing power systems, proposing a system architecture and analyzing security measures for protecting distributed energy stations. Ref. [10] proposes a framework to protect DERs and critical power grid infrastructure from cyberattacks, ensuring secure DER integration while maintaining grid reliability, and includes resilience analysis methods and attack prevention measures for future smart grid integration.

The third group introduces analytical and modeling approaches. Ref. [4] proposes a framework to protect DERs and the power grid from cyber-attacks, introducing a resilience analysis methodology with metrics and design principles and recommending preventive, detective, and responsive measures for smart grids. Ref. [11] introduces a new methodology for assessing security in distribution systems with DERs, addressing challenges such as system intermittence from technologies like solar, and proving effective for both tutorial and real-world systems. Ref. [12] reviews security risks in DERs on the smart grid, particularly for solar and wind sources, identifying vulnerabilities, attacks, and potential solutions at the protocol level. Ref. [13] presents a design method for sizing DERs in stand-alone microgrids to meet critical load demands during outages, combining photovoltaics with energy storage systems and emphasizing compliance with IEEE standards and resilience considerations. Ref. [14] examines

evolving interconnection standards for DERs, highlighting the need for improved communications and interoperability to enhance grid flexibility, and includes cybersecurity assessments of PV inverters and grid-monitoring gateways, leading to recommendations for improving DER device security. Ref. [15] provides a comprehensive overview of Cyber-Physical Systems (CPS) security, focusing on Cyber-Physical Energy Systems (CPES), introducing a threat modeling methodology to identify vulnerabilities, and suggesting a CPS framework for simulating system behavior and assessing performance under adverse conditions. Ref. [16] focuses on securing DERs in power systems, emphasizing the importance of addressing cybersecurity challenges due to the interconnected nature of DERs.

Additionally, Ref. [17] serves as a disclaimer for work sponsored by a US Government agency, noting that the views expressed do not necessarily represent those of the US Government. It highlights challenges in integrating Quantum Key Distribution (QKD) into microgrid contexts due to the lack of a standardized system model. Although QKD offers robust security through quantum principles, adapting it to microgrid environments requires a tailored framework for decentralized energy networks.

The current deficiency in a unified model restricts broad adoption and the development of comprehensive security strategies specific to microgrid applications. Addressing these challenges requires focused research efforts aimed at devising efficient deployment strategies that align with the operational requirements of distributed energy resources within microgrid infrastructures.

3. PROPOSED METHOD

To effectively integrate QKD and a central monitoring unit into Resources DERs, a structured workflow is presented in Fig. 1. This workflow begins with the modeling of DER systems in MATLAB to identify secrecy key requirements, which are crucial for ensuring secure communication within the network. Following this, QKD is implemented in Python, employing the BB84 protocol to enhance the security of data transmission. A detailed flowchart has been developed to visually represent this integration process, illustrating the steps from real-time monitoring and data aggregation to the deployment of QKD for robust encryption. The subsequent sections of this paper will explore this workflow in depth, emphasizing how it contributes to the security and operational efficiency of DER systems.

Incorporating a central monitoring unit to oversee security in DERs significantly enhances the robustness and efficiency of the system (Fig. 2). This central unit provides real-time monitoring, data aggregation, and advanced analysis using machine learning to detect anomalies and potential security threats across the network. It ensures coordinated and swift responses to incidents, thereby minimizing damage and downtime.

By standardizing security protocols and optimizing resource allocation, the central unit improves overall system performance and scalability. However, challenges such as data privacy, network reliability, and initial setup costs must be addressed to fully realize these benefits. Attacks on control data acquisition systems in DERs pose serious risks to the integrity and reliability of energy networks by targeting the collection and transmission of critical data. These attacks, including man-in-the-middle (MitM), spoofing, denial of service (DoS), data tampering, and malware infections, can lead to data manipulation, system malfunctions, and widespread disruptions [1]. To mitigate these threats, implementing strong encryption, robust authentication mechanisms, intrusion detection and prevention systems (IDPS), regular security audits, and redundancy in data acquisition paths is essential. These measures ensure the integrity, confidentiality, and availability of control data, enabling the central monitoring unit to effectively manage and secure the DER network.

QKD offers a revolutionary solution for securing data in DERs by utilizing the principles of quantum mechanics to

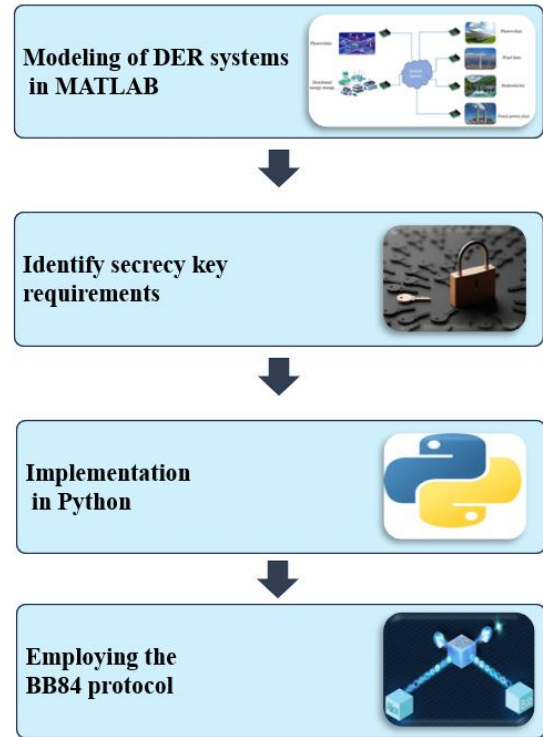


Fig. 1. Workflow for integrating QKD and central monitoring in DER.

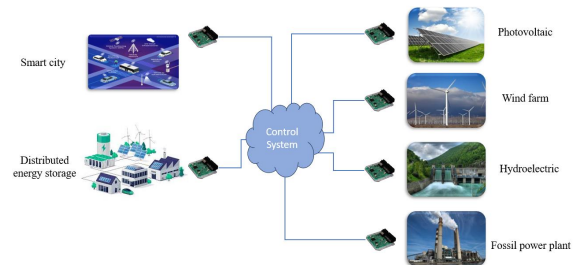


Fig. 2. System model of controlling distributed energy resources.

provide theoretically unbreakable encryption. QKD ensures that any attempt at eavesdropping is detected, as it alters the quantum state of the keys, allowing for immediate countermeasures. This technology provides future-proof security against emerging threats, including quantum computing, by relying on quantum physics rather than computational complexity. Implementing QKD involves establishing quantum communication channels, deploying QKD devices, and integrating quantum keys with classical encryption methods, ensuring robust protection for data transmission within DER networks and enhancing the overall security of critical energy infrastructure.

Fig. 3 illustrates the proposed secure data framework for a microgrid using QKD. In this setup, QKD devices generate and distribute cryptographic keys to the control system and various microgrid components, ensuring secure key exchange via yellow lines. These keys encrypt control data exchanged over blue lines, maintaining confidentiality and integrity. By utilizing quantum mechanics, QKD provides robust security, alerting the system to any eavesdropping attempts, thereby safeguarding the microgrid's operational communications from unauthorized access and tampering.

Table 1. Simulation results for the noiseless channel.

Qubit error-rate calculated by Alice	Key efficiency obtained	Bob's full key	Alice's full key	number of quantum bits
0.0%	50.0%	000000000000110001000 1000000010000110000010	0000000000000110001000 1000000010000110000010	100
0.0%	52.0%	0010011000001000000000 0000000000100010000011 1000000100000101100000 10000000001	0010011000001000000000 0000000000100010000011 1000000100000101100000 10000000001	150
0.0%	51.0%	0100000000111000110101 0000010011100000000000 0011011100000010100011 0111001000101000100010 0001000000100	0100000000111000110101 0000010011100000000000 0011011100000010100011 0111001000101000100010 0001000000100	200

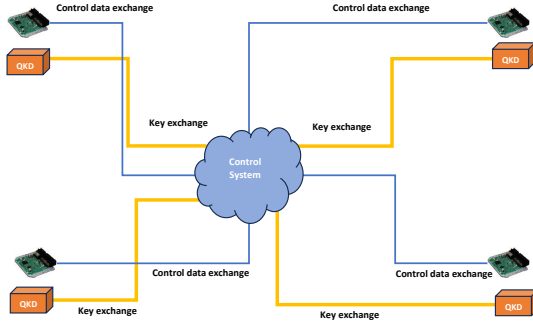


Fig. 3. The framework for securing control data exchange using QKD.

4. SIMULATION RESULTS

In this section, we have investigated the performance of employing quantum encryption to secure transmission information within a microgrid. The study focuses on the application of QKD protocols to enhance the security of data communications among various components of the microgrid. We simulated a range of scenarios, including both ideal and realistic conditions, to evaluate the robustness of quantum encryption against potential eavesdropping and noise. The developed program simulates the security of data transmission within a microgrid using a structured approach with various classes representing the microgrid components and communication channels. The basic experiment is conducted in an ideal, noiseless environment, but the flexible design of the base classes allows for easy customization to introduce noise models or potential interference scenarios. The program includes a feature to validate the transmitted data by comparing segments for errors, ensuring data integrity. Data measurement and transmission outcomes are implemented using Python, providing a robust and efficient simulation of real-world conditions. Additionally, the program generates detailed transcripts summarizing the results of each simulation, offering clear insights into the effectiveness and reliability of data security measures within the microgrid.

4.1. Noiseless channel

A quantum noiseless channel refers to an idealized communication pathway in quantum information theory where transmitted quantum states remain undisturbed throughout their journey from sender to receiver. In the context of microgrid communications, a noiseless quantum channel would theoretically provide an ideal medium for exchanging sensitive data among microgrid components. The following results show the outcome of simulations conducted for key exchange between the PV controller and the control central unit.

The simulations focused on evaluating the performance of quantum encryption protocols in securing data transmissions within the microgrid context. These results highlight the effectiveness

of QKD in establishing secure communication channels between distributed energy resources (DERs) like PV controllers and the central control unit.

4.2. Noisy channel

A noisy quantum channel with Hadamard gate errors refers to a communication pathway in quantum information theory where transmitted quantum states may be affected by noise and disturbances, particularly errors associated with the Hadamard gate. The Hadamard gate is a fundamental gate in quantum computing that creates superposition states, and errors in this gate can lead to incorrect outcomes in quantum operations. In the context of microgrid communications, a noisy quantum channel with Hadamard gate errors can pose challenges for the exchange of sensitive data among different microgrid components. The following results show the outcome of simulations conducted for key exchange between the PV controller and the control central unit.

4.3. Eavesdropped channel

An eavesdropped channel in the BB84 QKD protocol refers to a communication pathway where an unauthorized third party, called Eve, intercepts and measures the quantum states transmitted between Alice and Bob. Eve randomly chooses a measurement basis (standard or Hadamard), which can disturb the original states and introduce errors if her basis does not match Alice's preparation basis. These disturbances are detected by Alice and Bob by comparing a subset of their key bits. A higher-than-expected error rate indicates eavesdropping, leading them to discard the compromised key and repeat the protocol to ensure security. The provided code simulates this scenario, illustrating how Eve's interference impacts the integrity of the transmitted quantum states.

The error rate calculated by Alice is higher in the presence of an eavesdropper (Eve) because Eve intercepts and measures the qubits intended for Bob, which disturbs their quantum states. This interception and measurement process by Eve introduce additional errors into the qubits that Alice sends, leading to a higher observed error rate when Bob receives and measures them.

In our simulation study, we investigated the performance of QKD protocols for securing data transmission within a microgrid. We explored various scenarios, including ideal, noisy, and eavesdropped channels, to assess the robustness of quantum encryption against different conditions. In the noiseless channel scenario, quantum states are transmitted without any disturbances, representing the optimal conditions for QKD. The simulations showed a perfect qubit error rate of 0.0%, indicating no transmission errors. The key efficiency ranged between 50% and 52%, demonstrating effective key generation and distribution. The length of the quantum keys varied from 100 to 200 bits. These results confirm that QKD performs exceptionally well in ideal conditions, providing high security and reliability for microgrid communications. In contrast, the noisy channel scenario involved the presence of noise and errors, particularly those associated with the Hadamard gate,

Table 2. Simulation results for the noisy channel.

Qubit error-rate calculated by Alice	probability of Hadamard gate failure	Key efficiency obtained	Bob's full key	Alice's full key	The size or number of quantum bits
4.545454545454546%	0.05	44.5%	000000101000011100000011 000010110100011000101001 010100001000010100001010 0001000010110011	000000101000011100000011 000010110100011000101001 010100001000010100001010 0001000010110011	200
3.8461538461538463%	0.05	52.5%	000010110100110101100000 000101101000000100001001 100100100000011010010010 101000111100000010010001 000001001	000010110100110101100000 000101101000000100001001 100100100000011010010010 101000111100000010010001 000001001	400
	0.05	51.6%	000010000001101111110000 000000100001000000000001 00001100011100000000011 100100100110000000000001 000000000001000100111 011110010000100000001101 01000000000001	000010000001101111110000 000000100001000000000001 00001100011100000000011 100100100110000000000001 000000000001000100111 011110010000100000001101 01000000000001	600
16.3265306122449%	0.2	50%	00101000001000000000111 10000001100001000000000 010000000000000000101010 10010001000000001000010 0010100	00101000001000000000111 10000001100001000000000 010000000000000000101010 10010001000000001000010 0010100	200
8.181818181818182%	0.2	55.25%	00001000000110101000000 11001101000100011000001 01000000110000001101010 000010100111101100001000 00000001000000100	00001000000110101000000 11001101000100011000001 01000000110000001101010 000010100111101100001000 00000001000000100	400
8.783783783783784%	0.02	49.66%	10101000001001101000010 0000000100000000100000 00010000110001000000000 0011100000110000000000 010000001000010001011 1100010000100000110110 00010000000000010	10101000001001101000010 0000000100000000100000 00010000110001000000000 0011100000110000000000 010000001000010001011 1100010000100000110110 00010000000000010	600

Table 3. Simulation results for the channel in the presence of Eve.

Qubit error-rate calculated by Alice	Key efficiency obtained	Bob's full key	Alice's full key	number of quantum bits
0.0%	52.0%	0000000100001101000000110 0000100101100101001001001 00001000000000100100010001 100001001001001100010000010	0000000100001101000000110 0000100101100101001001001 00001000000000100100010001 100001001001001100010000010	200
0.0%	51.0%	000101010000000010000000 0100000011001000000110100 0000101010000100000110100 0000000000010001000100000 00000	000101010000000010000000 0100000011001000000110100 0000101010000100000110100 0000000000010001000100000 00000	400
0.02	49.66%	0110100001110000000010001 1100100000001100001000001 0000000011011111000000100 0011100010001011000010001 000001000010000000000000 1010010101010000110000001 00011000	0110100001110000000010001 1100100000001100001000001 0000000011011111000000100 0011100010001011000010001 000001000010000000000000 1010010101010000110000001 00011000	600

which creates superposition states. The qubit error rates ranged from 3.85% to 16.33%, reflecting the impact of noise on the transmission. Key efficiency varied between 44.5% and 55.25%, showing some degradation due to noise. Despite the noise, the system maintained relatively high key efficiency, indicating its resilience and robustness in practical, noisy environments.

The eavesdropped channel scenario simulated the interference of an unauthorized third party, Eve, who intercepts and measures the qubits. This interception introduced additional errors, resulting in higher qubit error rates, which ranged from 9.80% to 17.09%. Key efficiency was affected, ranging from 51.5% to 52.83%. The increased error rates highlight the impact of eavesdropping on the integrity of the transmitted quantum states and underscore the importance of effective measures to detect and mitigate unauthorized interceptions. Overall, the simulations demonstrate that QKD is highly effective for securing microgrid communications. While ideal conditions allow for optimal performance, the system remains robust in noisy environments and can detect eavesdropping attempts, though with some impact on key efficiency. These findings underscore the importance of quantum encryption in providing secure and reliable data transmission within microgrids.

5. CONCLUSION

This paper highlights the pivotal role of Quantum Key Distribution (QKD) in enhancing the security of Distributed Energy

Resource (DER) systems. Leveraging the principles of quantum mechanics, QKD provides a level of cryptographic security that surpasses traditional methods, particularly in addressing vulnerabilities introduced by the rise of quantum computing. Our research demonstrates that QKD can achieve a practical key efficiency of approximately 50%, making it a viable solution for securing DER networks. Through simulations across various channel scenarios, QKD has shown exceptional robustness, with minimal error rates in noiseless environments, manageable errors in noisy conditions, and strong resistance to eavesdropping. Furthermore, integrating QKD into DER frameworks not only strengthens security but also tackles key operational challenges such as scalability and cost-effectiveness. This integration ensures that DER networks can grow and incorporate more renewable energy sources without compromising security. The findings of this study lay the groundwork for the future implementation of QKD in real-world DER systems, offering a scalable, cost-efficient, and highly secure solution tailored to the dynamic and resource-constrained nature of these networks. In conclusion, QKD represents a significant advancement in secure communication technologies for DER systems. As the energy sector continues to evolve with the integration of renewable energy resources, the adoption of QKD will be crucial in ensuring the long-term security, integrity, and reliability of energy networks. Future research should focus on refining QKD protocols to further enhance their efficiency and exploring their application in broader smart grid and energy management contexts.

REFERENCES

- [1] Y. He, Z. Zhou, Y. Pan, F. Chong, B. Wu, K. Xiao, and H. Li, "Review of data security within energy blockchain: A comprehensive analysis of storage, management, and utilization," *High-Conf. Comput.*, p. 100233, 2024.
- [2] Z. Lv, W. Kong, X. Zhang, D. Jiang, H. Lv, and X. Lu, "Intelligent security planning for regional distributed energy internet," *IEEE Trans. Ind. Inf.*, vol. 16, no. 5, pp. 3540–3547, 2019.
- [3] M. Sheikholeslami, Z. Li, M. Shahidehpour, K. Gering, A. Sugiarto, A. Valderrama, N. Gurung, H. Zheng, and A. Vukojevic, "Data security in networked microgrids for transacting energy," in *2022 IEEE PES Transactive Energy Syst. Conf.*, pp. 1–5, IEEE, 2022.
- [4] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst.: Theor. Appl.*, vol. 1, no. 1, pp. 28–39, 2016.
- [5] H. Noura, O. Salman, A. Chehab, and R. Couturier, "Preserving data security in distributed fog computing," *Ad Hoc Networks*, vol. 94, p. 101937, 2019.
- [6] Q. Pan, J. Wu, A. K. Bashir, J. Li, W. Yang, and Y. D. Al-Otaibi, "Joint protection of energy security and information privacy for energy harvesting: An incentive federated learning approach," *IEEE Trans. Ind. Inf.*, vol. 18, no. 5, pp. 3473–3483, 2021.
- [7] D. Saleem, A. Sundararajan, A. Sanghvi, J. Rivera, A. I. Sarwat, and B. Kroposki, "A multidimensional holistic framework for the security of distributed energy and control systems," *IEEE Syst. J.*, vol. 14, no. 1, pp. 17–27, 2019.
- [8] R. S. Ravi, A. Jolfaei, D. Tripathy, and M. Ali, "Secured energy ecosystems under distributed energy resources penetration," *Internet Things Cyber-Phys. Syst.*, vol. 2, pp. 194–202, 2022.
- [9] J. Zhang, "Distributed network security framework of energy internet based on internet of things," *Sustainable Energy Technol. Assess.*, vol. 44, p. 101051, 2021.
- [10] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst.: Theor. Appl.*, vol. 1, no. 1, pp. 28–39, 2016.
- [11] O. F. Avila, J. A. Passos Filho, and W. Peres, "Steady-state security assessment in distribution systems with high penetration of distributed energy resources," *Electr. Power Syst. Res.*, vol. 201, p. 107500, 2021.
- [12] A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security," *Energies*, vol. 11, no. 9, p. 2360, 2018.
- [13] P. Siritoglou, G. Oriti, and D. L. Van Bossuyt, "Distributed energy-resource design method to improve energy security in critical facilities," *Energies*, vol. 14, no. 10, p. 2773, 2021.
- [14] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, "Cyber security assessment of distributed energy resources," in *2017 IEEE 44th Photovoltaic Specialist Conf.*, pp. 2135–2140, IEEE, 2017.
- [15] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021.
- [16] I. Zografopoulos, N. D. Hatziaargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Syst. J.*, 2023.
- [17] K. L. Stamber, A. Kelic, R. A. Taylor, J. M. Henry, and J. E. Stamp, "Distributed energy systems: Security implications of the grid of the future," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2017.