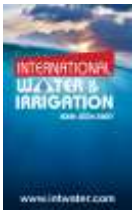


International Water and Irrigation
Volume 44 Issue 2 (2025)
ISSN: 0334-5807
Pages 314 - 321

Enhancing the Information Security of Distribution Automation System in Low Voltage Area Using Quantum Cryptography

Tian Erwei[1*], Zhang Jianbin[1], Zhao Tianjian[1]
[1]Shaoxing Power Supply Company of State Grid Zhejiang Electric Power Co.Ltd,Shaoxing Zhejiang, China
[1*]Corresponding author Email: tewhappy@163.com

Abstract: Power transmission and utilization systems are an integral part of the electrical grid's link to the end user. Ensuring the safe and sound transfer of data across all systems is closely tied to safeguarding personal information. This work presents a quantum cryptography solution that can improve the data safety of distribution automation systems in the low-voltage unit region. All three levels of the system—base station, access, and terminal—were considered throughout its design. The information that was delivered across the quantum key distribution (QKD) system was encrypted using a quantum key that was created by the key production modules on both ends of the transmission. This study accomplished the goal of facilitating the flexible and cost-effective transfer of the terminal-end quantum key in the context of QKD.

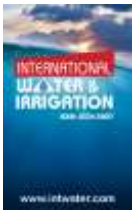
Keywords: Data security, quantum cryptography, QKD, distribution system, low voltage applications

I. Introduction

The regular supply of power is depended upon electronic communication, and the stability of that communication depends on its safe, steady functioning and the electricity grid consistency. In a timely manner, abnormalities, hidden dangers, and power communication defects can be found with precise and timely communication work in conjunction with an evaluation of power communication technology has garnered interest from a diverse range of individuals and has undergone verification testing across several domains, presenting a novel approach to guarantee safe information transfer [1]. Keys that are anti-theft and tamper proof are realized by utilizing the physical properties of photons to solve the issue of online safe key distribution. Information security in the domains of banking, energy, electricity, national defense, and government affairs can be significantly enhanced by QKD technology [2]. The swift advancement of quantum computing in the field of cybersecurity has generated both enthusiasm and apprehension in recent times. Quantum computing presents a serious difficulty to the security framework supporting our digital world even while it promises an unattainable computational power and the capacity to tackle intricate issues [3]. To perform parallel computation and information processing on some particular challenges, quantum algorithms can make use of features like quantum superposition and quantum entanglement. This allows for exponential acceleration of algorithmic speed [4]. The concept of a quantum Turing system with the help of transition matrices, quantum Turing computers is connected to both conventional and probabilistic Turing machines is further developed, and the possibility of a quantum physics-based universal quantum computer is postulated. This computer could potentially be far more powerful than classical ones in terms of computation that could handle massive amounts of data for complex quantum system simulations by utilizing features of quantum mechanics like entanglement and superposition. The primary issue is the need for a fresh key for every correspondence and the key exchange issue [5]. The application of quantum cryptography, as demonstrated in this work, can improve the data security of the distribution automation system in the low-voltage unit region.

II. Related work

This study offered an extensive analysis of the threats posed by quantum computing assaults, possible countermeasures, and unresolved issues for distributed energy resources (DER) [6] networks. The next provided



International Water and Irrigation
Volume 44 Issue 2 (2025)
ISSN: 0334-5807
Pages 314 - 321

a quantum-secure architecture that specifically targets sustainable mobile networks using QKD [7] and Post Quantum Cryptography (PQC). Using many use cases, focused the architecture usefulness and highlight the necessity for cutting-edge security measures in this new era. They examined the technological transition from traditional cryptographic methods [8] to quantum-enabled approaches to attain comprehensive security. This paper examined the latest breakthroughs in-field applications of QKD networks and discussed the progress made in QKD [9] standardization. That limited temperature variations enable the quantum bit error rate (QBER), which the interferometers determination use, to sustain phase and create bipartite key exchange for every feasible participant combination at the same time [10]. The suggested technique was implemented as a software package prototype for supervisory control and data acquisition (SCADA) [11] to maintain and use cryptographic keys for machine-to-machine authentication. This work initiated the investigation of location-driven, unconditionally-quantum-resistant cryptography utilizing the Lattice issue for pre- and post-quantum Internet of Things (IoT) [12] situations. The development and evaluation of QKD systems with relay-assisted satellite free-space optics (FSO) for secure vehicle networks were examined in this research. As relay stations, optical amplify-and-forward node-equipped high-altitude platforms (HAPs) were employed [13]. This lesson provided an overview of fundamental QKD and practical QKD technologies. This paper aimed to broaden the audience of researchers and practitioners interested in the topic of quantum communication, which was an extremely multidisciplinary one, with the ultimate objective of accelerating its development and widespread implementation [14]. This work investigated QKD on networks that were beyond 5G to solve the issue of IoT security [15]. A proposed method attempted to detect an unauthorized person between a transmitter and a receiver but inadvertently halts the QKD procedure while attempting to identify the intruder. The created device was a viable resource for designing quantum optical payloads for upcoming satellite missions and a cost-effective alternative for portable free-space transmitters [16]. The process was demonstrated a type of under realistic operational scenarios, the designed QKD system was capable of safely and efficiently distributing cryptographic keys [17]. Moreover, using quantum cryptography, were able to demonstrate unconditionally secure image transmission and reception between Alice and Bob linked across an unprotected public channel.

III. Structure design

The three layers that comprise the base station layer, access layer, and terminal layer are the three layers that make up the transmission network for electric distribution. The access layer in conventional terms refers to an access layer of medium voltage, while the phrase terminal layer refers to the low voltage access layer. The two layers that comprise this communication network access layer expansion and medium voltage foundation of access level are provided by the medium voltage, which covers the spectrum of remote terminal equipment. The transmission network among the substation and the main station makes up the convergence layer. The network of communication connecting each user's meter of the distributing transformer is called the access layer with low voltage. The remote observation of low-voltage infrastructure, such as charging heaps and user meters in residential areas, is accomplished through the use of an electricity distribution communication network. A potential application for this kind of technology is the examination of equipment and medium-voltage lines, including branch boxes and opening and shutting stations, distributed transformers, network cabinets in a circle, and column switches.

The system is configured as a main station with a business terminal that has an Enterprise Services Application Module (ESAM) module and an encryption machine, respectively. Additionally, data encryption and bidirectional identity and authentication between the terminal and main station are realized through the employment of symmetric key encryption technique. The structural design of a power distribution secure transmission system is determined in the present study using quantum encryption technology based on the original system, as shown in Figure 1. A quantum technology-based device was installed on the original encryption and authentication device other primary station side for corporate data encryption and decryption. The quantum key is located either built into or external to the terminal device, were used to both encrypt and decode the distribution with terminal's service information. The quantum key took every place of the previously utilized symmetric key.

International Water and Irrigation
Volume 44 Issue 2 (2025)
ISSN: 0334-5807
Pages 314 - 321

The system supported both offline and online quantum key distribution methods. The quantum key is utilized as a session key and substituted for the original symmetric key in the encryption module of the terminal or the cipher machine of the master station.

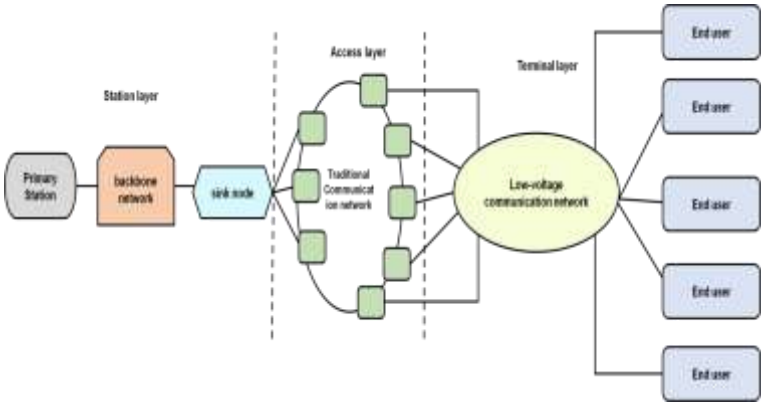


Figure 1: Architecture of electric quantum encryption system (EQES)

IV. Quantum key distribution (QKD) system

The main method of protecting data in today's vital infrastructure is encryption. Two methods of information security are provided by classical cryptography: private and public key encryption. Nevertheless, there are issues with each of these methods. A safe key distribution procedure is necessary for private key encryption. The foundation of public encryption is computational difficulty, which can be overcome with growing processing power and the development of quantum computing. A more recent type of encryption is not based on mathematical functions but rather on the fundamental ideas of quantum physics. A physical layer security system called QKD takes advantage of quantum physics. It ensures proven security even in the face of a quantum computer-initiated attack since it's confirmed without assuming the computing capacity or tactics of the eavesdropper.

The introduction of the first-ever QKD protocol took place. Qubits are represented in this approach as solitary photons in a channel, which can be either open space or an optical fiber. A quantum and a classical channel are needed for QKD to be implemented successfully. Important information is sent by single photons over the quantum path.

The Quantum Error Bit Rate (QBER) assessment indicates the presence of an adversary trying to intercept and compromise the connection. The two most frequent errors that are introduced into a QKD communication method are Intercept Resend attacks and channel noise from depolarization. In both free space and optical fiber, depolarization takes place in channels, which is represented by the depolarizing parameter p. The percentage of pulses or photons that the eavesdropper decides to intercept and transmit is known as the attack level. If the attacker decides to intercept every sent pulse, then$\varepsilon = 1$, this corresponds to ¼ of the sorted key having mistakes. The definition of QBER is Equation (1):

$$QBER = q_e(1 - q_{ch}) + (1 - q_e)_{qch} = \frac{\varepsilon}{4} + \frac{2p}{3}(2 - \varepsilon) \quad (1)$$

Where qch and q_e stand for the attack mistakes and the channel, respectively.

A secure communication technique called QKD is used to exchange encryption keys that are only known to two parties at a time. It exchanges cryptographic keys in a proven manner that ensures security by using characteristics inherent in quantum physics. A key that is needed to encrypt and decode messages may be created and shared by two parties inrecognition to the QKD. The process of sharing the key between parties is known as QKD for online distribution network and offline network architecture.

A. Online distributed network structure

International Water and Irrigation
Volume 44 Issue 2 (2025)
ISSN: 0334-5807
Pages 314 - 321

The fiber optic network was utilized to create the QKD network, and the generation control devices and administrative devices were supplied by the quantum key server. The device for managing quantum keys included features for controlling their distribution, managing them, storing keys, producing keys, and further information.

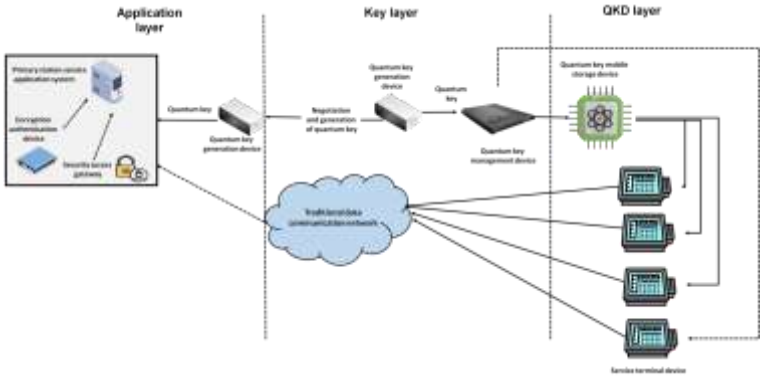


Figure 2: System architecture for QKD networks

Figure 2 shows the integration of quantum cryptography network with the power data network. Integrated into the main station the aggregation sides of the key management system were equipped with quantum key management devices. The distributions along with the storage of keys were made possible by connecting the quantum key administration device QKD layer to the distributed quantum key network. To enable key insertion and operation, the QKD device is connected to thehighest level of quantum key encryption and decryption system.To achieve long-distance transmission in a quantum QKD network, methods such as quantum relay and trusted relay must be used. Networks are made more flexible by utilizing devices like quantum switches and others to adjust to the demands of complex systems.

B. Offline distribution network architecture

Quantum key equipment is limited by volume, cost, and other variables, making it impossible to directly connect to a multitude of service terminals over the internet for the deployment of service equipment across a wide range of sites. Hardware for mobile storage with quantum keys distributed offline has improved.

The pre-application mode is used for the master computer layer equipment to achieve quantum key injection. To match symmetric keys in the quantum keys injected into a company terminal, the master station layer equipment might be equipped with a particular amount of quantum keys that the QKD terminal injected. Every layer of access to theQKD device was configured to output a quantum key from the system download interface to a third-party secure storage media in the notification reading mode. The distribution terminal received the quantum key from the third-party security reserve media by connecting to each physical interface port one at a time. There were several quantum keys at each distribution terminal, and each terminal acquired a unique set of quantum keys. These pre-stored quantum keys are utilized to perform encrypted communication with the main platform business system throughout the ensuing business encryption communication procedure, negating the need for a quantum key distribution network. To create a quantum key pool for use in encrypted enterprise information transmission, a certain number of quantum codes would be kept in the main station business system and transportation terminals under the offline distribution technique.

V. Application procedure for quantum keys

The network for quantum cryptography invented the technique of quantum bargaining. Using the quantum key for authentication or encryption, along with other issues, is discussed and resolved through its application. According to the requirements of application, the key is read from the quantum server by a quantum key server upon connection. The quantum key server made a request when it was received to make sure that it met all

International Water and Irrigation
Volume 44 Issue 2 (2025)
ISSN: 0334-5807
Pages 314 - 321

requirements, including the key distribution procedure right away. The QKD technique has five connections and nine stages, as shown in Figure 3.

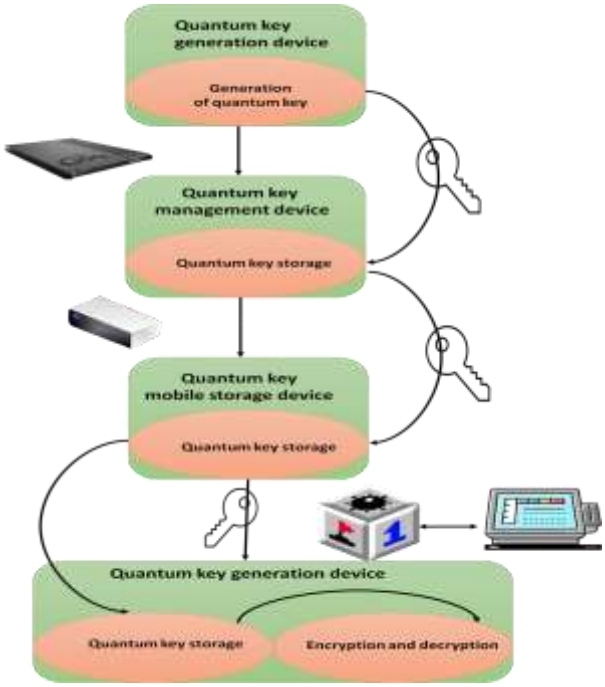


Figure 3: Quantum key application process

VI. User Authentication

This project used a distribution website that is governed by a substation as a demonstration application to confirm the system functionality in a real-world application setting. Distribution automation and information-collecting services related to power use were also included in the access services package. Figure 4 illustrates the particular deployment plan.

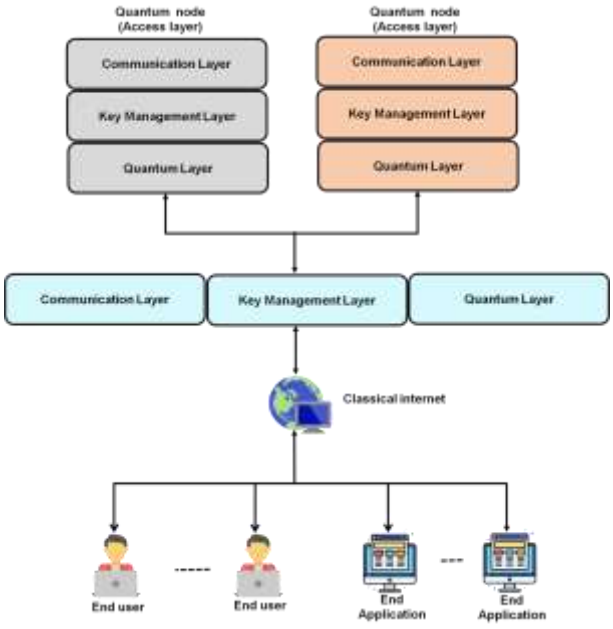


Figure 4: User authentication of quantum keys for power allocation and consumption

International Water and Irrigation
Volume 44 Issue 2 (2025)
ISSN: 0334-5807
Pages 314 - 321

In the case of the allocation of power information services, for instance, the maximum key capacity is $9Mbit$, the first offline key value is $4Mbit$, and every complete of online key distribution process was originally determined to be $12kbit/s$. A one-minute packet transmitting interval was established as the minimum unit$T$. Following the service, an encrypted communication performance of the system is tested using the one-time payment (OTP) encryption approach.

Figure 5 show the access latency, cipher text transmission rate, and packet loss rate for various user categories while assuming that the conditions were achieved. The network as a whole had a packet loss rate of less than 2%, and access latency fluctuations fell between 0.5 and 0.9, in compliance with technical rules for power system communication architecture.

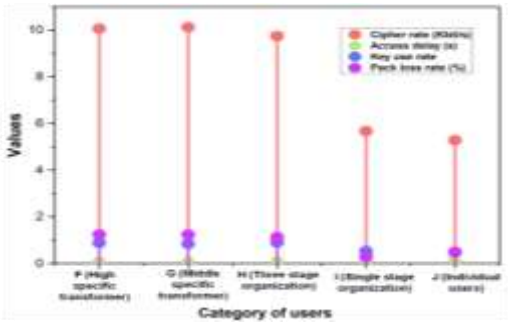


Figure 5: Comparison of different user

To satisfy the demands of a large number of users, because of the complexity of communication systems and the large number and dispersion of electrical enterprise terminal sites, need to expand system capacity, 10.7, 21.3, 39.5, 57.0, and 75.0 Kbit/s were the transmission rates that were set as standard. Table 1 shows the system capacity test results.

Table 1: Test of system capacity

Transmission rate class ($kbit/s$)	**Packet loss rate** (%)	**Access delay (s)**
10.7	**1.49**	**0.45**
21.3	**1.25**	**0.48**
39.5	**1.39**	**0.35**
57.0	**2.16**	**1**
75.0	**2.45**	**1**

The equipment of real measurement results was essential with the design of theoretical value. Under the assumption that the QOS index criteria are met, the mean uplink transmission speed recorded in a field might approach 64kbit/s, with room for future improvement. Simultaneously, the scheme's viability was confirmed, and the system's practicality was enhanced.

The value of a measure and supplied by a measuring tool or device is known as a measured value. It's stated as the product of a numerical value and a unit and is commonly standardized and expressed in percent. It finds application in metrology applications. A fitted value is the mean response value that a statistical model predicts based on the values of its components, factor levels, and predictors. A 5kW distributed quantum power plant with 800V low voltage operates in the same 9kM x 9kM grid. The quantum power plant of electrical information is collected once per hour and itis obtained by the inverter. Figure 6 shows the real-time power curve for the electric facility.

International Water and Irrigation
Volume 44 Issue 2 (2025)
ISSN: 0334-5807
Pages 314 - 321

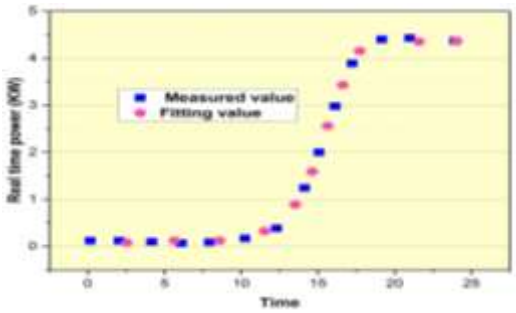


Figure 6: Power measurement for quantum power plant

The fixed length of 100 km optical fiber occurred for network design. The quantum transceiver node's number of received Smart Inverters (SI) determines the cost of setting up QKD and key distribution delay.

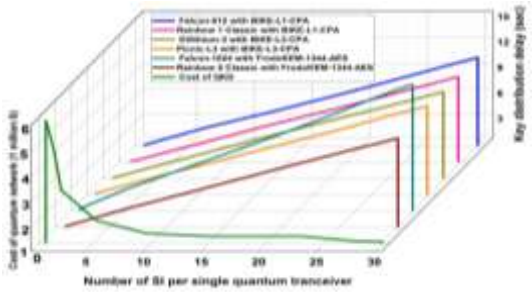


Figure 7: QKD network cost and key distribution latency

The study findings in Figure 7 show that cost reduces nonlinearly while key distribution latency grows linearly with the quantity of SI connected to one quantum transceiver node. Specifically, cost drops significantly when three to five SI are coupled to an individual quantum transceiver node. The cost remains relatively constant even with an increase in the amount of SI if there are seven and greater. With a key distribution latency of less than one second, distributed energy resources (DER) can be run steadily, and quantum channels can be connected to all SIs for an implementation cost of 5.5 million dollars. A key distribution delay occurs if a quantum transceiver node is linked DER is performed using up to five Sis of 2.6 to 4.5 s. Moreover, cost will decrease to less than $1 million with a $17-20\ SI$ connection for an optical transceiver node, which lowers the cost to $0.2\ to\ 0.3$1 million, when QKD latency above10 s, this leads to DER losing stability. To implement QKD, it's necessary to examine the right cost and network design in relation to the actual cost and key distribution delay.

VII. Conclusion

This research examines how utilizing quantum cryptography might improve the information protection of distribution automation systems in areas with low-voltage stations. To properly ensure the information security of the electrical sector, quantum communication was included in the national electric information system construction plan. Quantum secure communication devices are applied to the encryption of information, identification verification, and additional security protocols. Enhancing service data security and protection capabilities is crucial. The online and offline QKD patterns are based on quantum communication technology that the huge number and broad distribution features of electrical terminal. The system architecture and deployment achieved the large-scale, low-cost implementation of quantum secret communication technology in the electrical business while also meeting safety regulations. It can significantly improve the power system's resistance against high-performance computers' infiltration and destruction of communication. The distance between the actual device and the model is the main disadvantage of quantum cryptography because of the introduction about side channels that is used to monitor and contact information privacy. Future research must assess the suggested

International Water and Irrigation
Volume 44 Issue 2 (2025)
ISSN: 0334-5807
Pages 314 - 321

security models to see if we are appropriate for reducing the risks that are arising in the field of quantum cryptography.

Reference

[1] Wen, H., Xu, A. and Qi, H., Application of quantum key distribution in intelligent security operation and maintenance of power communication networks. Results in Physics, 2023, 54, p.107041.

[2] Hoque, S., Aydeger, A. and Zeydan, E., Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. 2024, arXiv preprint arXiv:2404.10602.

[3] Bi, L., Miao, M. and Di, X., A Dynamic-Routing Algorithm Based on a Virtual Quantum Key Distribution Network. Applied Sciences, 2023, 13(15), p.8690.

[4] Ullah, M.H., Eskandarpour, R., Zheng, H. and Khodaei, A., Quantum computing for smart grid applications. IET Generation, Transmission & Distribution, 2022, 16(21), pp.4239-4257.

[5] Yu, X., Liu, Y., Zou, X., Cao, Y., Zhao, Y., Nag, A. and Zhang, J., Secret-key provisioning with collaborative routing in partially-trusted-relay-based quantum-key-distribution-secured optical networks. Journal of Lightwave Technology, 2022, 40(12), pp.3530-3545.

[6] Ahn, J., Kwon, H.Y., Ahn, B., Park, K., Kim, T., Lee, M.K., Kim, J. and Chung, J., Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd). Energies, 2022., 15(3), p.714.

[7] Hoque, S., Aydeger, A. and Zeydan, E., Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. 2024, arXiv preprint arXiv:2404.10602.

[8] Chawla, D. and Mehra, P.S., A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. Internet of Things, 2023, p.100950.

[9] Stanley, M., Gui, Y., Unnikrishnan, D., Hall, S.R.G. and Fatadin, I., Recent progress in quantum key distribution network deployments and standards. In Journal of Physics: Conference Series (Vol. 2416, No. 1, p. 012001). 2022, December. IOP Publishing.

[10] Fitzke, E., Bialowons, L., Dolejsky, T., Tippmann, M., Nikiforov, O., Walther, T., Wissel, F. and Gunkel, M., Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding. PRX Quantum, 2022, 3(2), p.020341.

[11] Alshowkan, M., Evans, P.G., Starke, M., Earl, D. and Peters, N.A., Authentication of smart grid communications using quantum key distribution. Scientific Reports, 2022, 12(1), p.12731.

[12] Althobaiti, O.S. and Dohler, M., Quantum-resistant cryptography for the Internet of Things based on location-based lattices. IEEE Access, 2021, 9, pp.133185-133203.

[13] Vu, M.Q., Pham, T.V., Dang, N.T. and Pham, A.T., Design and performance of relay-assisted satellite free-space optical quantum key distribution systems. IEEE Access, 2020, 8, pp.122498-122510.

[14] Amer, O., Garg, V. and Krawec, W.O., An introduction to practical quantum key distribution. IEEE Aerospace and Electronic Systems Magazine, 2021, 36(3), pp.30-55.

[15] Al-Mohammed, H.A., Al-Ali, A., Yaacoub, E., Qidwai, U., Abualsaud, K., Rzewuski, S. and Flizikowski, A., Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios. IEEE Access, 2021, 9, pp.136994-137004.

[16] Avesani, M., Calderaro, L., Schiavon, M., Stanco, A., Agnesi, C., Santamato, A., Zahidy, M., Scriminich, A., Foletto, G., Contestabile, G. and Chiesa, M., Full daylight quantum key distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Information, 2021, 7(1), p.93.

[17] Jain, A., Khanna, A., Bhatt, J., Sakhiya, P.V., and Bahl, R.K., Experimental demonstration of free space quantum key distribution system based on the bb84 protocol. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). 2020, July. IEEE.