The Scientific Temper (2023) Vol. 14 (3): 1008-1013
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.69
https://scientifictemper.com/

REVIEW ARTICLE

Quantum key distribution-based techniques in IoT

Neeraj, Anita Singhrova

Abstract

Quantum key distribution (QKD) is a cryptographic technique that creates a secure channel of communication between two parties by applying the ideas of quantum physics. QKD ensures the confidentiality and integrity of data transmission by providing a unique key that the intended recipient can only access. Secure communication has become paramount with the proliferation of IoT (Internet of Things) devices. IoT devices have confined computational power and storage, making them vulnerable to attacks. QKD provides a safe and efficient solution for securing communication between IoT devices. This paper examines how QKD can be utilized in IoT, discussing its benefits and limitations, followed by the discussion on various QKD protocols suitable for IoT devices. In addition, the paper demonstrates that QKD is a promising solution for securing IoT communication, and its adoption significantly enhances the security and reliability of IoT networks.

Keywords: Authentication,Cryptography, Internet of Things, Quantum Computing, Quantum Key Distribution.

Introduction

Cryptography is the practice of protecting communication from third parties, it turns the original message into an unreadable version that can only be interpreted by someone with access to the key or code used to encrypt it. People have used cryptography to safeguard sensitive data, and it is now an essential component of digital communication and cybersecurity. Digital signatures, hashing, encryption, and decryption are a few examples of cryptographic methods (Singh *et al*. 2023).

The expansion of IoT devices has increased the amount of sensitive data transmitted across networks. As a result, the need for secure communication has become more critical than ever. Quantum key distribution (QKD) is a capable solution for securing communication in IoT networks. QKD uses quantum mechanics to create a communication channel between different parties. It provides a unique key that can only be accessed by the intended recipient, ensuring the confidentiality and integrity of data transmission.

As IoT devices have inadequate storage and limited computational power, traditional cryptographic techniques may not be suitable for securing communication in IoT networks. QKD offers a secure and efficient solution that can be implemented in IoT devices, providing an extent of security that is better than conventional cryptography.

Quantum Key Distribution

- QKD is an encryption method of distributing encrypted keys between parties (Kute *et al*., 2017). By employing quantum physics concepts to ensure security, it distributes cryptographic keys in a verifiable manner. Using QKD, two parties can create and share a key to protect and retrieve data. Public key ciphers, which make use of intricate mathematical computations and are excessively difficult to break, are used for key distribution on a broad scale. Public-key cipher viability, however, faces several difficulties, including persistent use of innovative attack techniques, inefficient random number generators, and overall developments in computation.
- **Need for QKD in communication:** The confidentiality of the information being communicated or stored primarily relies on encryptions in the present communication technologies and data security. Information security

Computer Science and Engineering, Deenbandhu Chhotu Ram University of Science and Technology, Sonepat, India.

***Corresponding Author:** Neeraj, Computer Science and Engineering, Deenbandhu Chhotu Ram University of Science and Technology, Sonepat, India, E-Mail: neeraj.schcse@dcrustm.org

How to cite this article: Neeraj, Singhrova, A. (2023). Quantum key distribution-based techniques in IoT. The Scientific Temper, **14**(3):1008-1013.

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.69

Source of support: Nil

Conflict of interest: None.

Received: 15/07/2023 **Accepted:** 10/08/2023 **Published** : 25/09/2023

in any cryptographic algorithm is solely dependent on key privacy. Modern public-key infrastructure (PKI), primarily used to secure the internet globally, is built on technically challenging algorithms. Security relies on the idea that doing specific computational tasks, like prime factorization of a vast number, in a reasonable amount of time is unattainable, even for a highly advanced classical computer.A key exchange technique named QKD entirely eliminates the possibility of eavesdropping. The basic principles of quantum physics assure that any instance of eavesdropping permanently alters the system, and attempts to eavesdrop are instantly recognized. The secure communication channel is illustrated in Figure 1.

- **Quantum cryptography:** Using the inherent qualities of quantum physics, such as uncertainty and probability, quantum cryptography is a technique of encryption and data transmission that secures data indestructibly. Additionally, it enables accomplishing numerous cryptographic tasks that are not attainable with just conventional communication. The most well-known instance is QKD, which offers a data-theoretically secure approach to the key distribution problem (Kute *et al*., 2017). The science of quantum cryptography encrypts and transmits data using the quantum physics principles. The important modules of quantum cryptography are as follows.
- **One-Time Pad:** A randomly selected key, which is of the equivalent length as the plaintext, is XORed with the plaintext to form the ciphertext, and is known as a one-time pad (OTP) cipher (Upadhyay & Nene, 2016). All plaintexts of the specified size are equally likely to have produced the ciphertext if the key is randomly chosen.
- **Polarized photons:** In quantum cryptography, Alice sends photons via a transmission line to Bob, the recipient. Alice randomly selects a polarization for each photon from the several directions in which the photons are polarized (Brequet *et al*, 1994). Likewise, Bob selects a polarization at random to be used in the photon measurements. Any attempt to intrude on the communication channel will disrupt the photons and will be discovered by Alice and Bob due to the uncertainty principle of quantum physics. Because of the eavesdropping, any intercepted information will be useless to an attacker (Lardier *et al*., 2020).

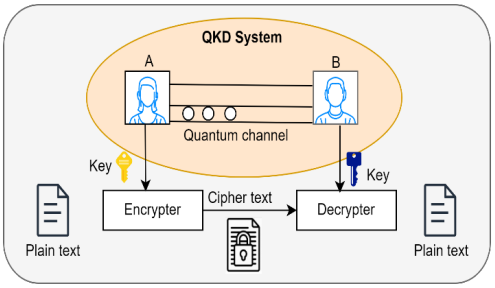

Figure 1 : Quantum channel in communication

Characteristics of QKD

QKD is a cryptographic mechanism that creates a secret key that can be exchanged between two parties (Lardier *et al*., 2019). The main characteristics of QKD are:

- **Security:** QKD offers an absolute security guarantee depending on the vital laws of quantum mechanics. QKD is based on the fact that any attempt to interrupt or measure the current state of quantum used in the protocol will be detectable, as it will inevitably disturb the state and introduce errors in communication.
- **Key Distribution:** QKD allows two parties to create a secret key between them, which can be used to decrypt and encrypt messages. The key distribution process is built on exchanging photons carrying quantum information.
- **Key Size:** QKD can produce keys of arbitrary length, limited only by the rate at which photons are transmitted between the parties.
- **Interoperability:** QKD can be combined with classical cryptography to provide a hybrid solution that offers both the security of QKD and the practicality of classical cryptography
- **Resilience:** QKD is inherently resilient to some types of attacks, for example man-in-the-middle attacks, because any attempt to intercept the quantum states used in the protocol will be detectable.
- **Complexity:** QKD can be more complex to implement than classical cryptography, particularly regarding the hardware and infrastructure required. However, advances in technology are making QKD systems more practical and accessible (Lardier *et al*., 2019)..

Quantum cryptographic algorithms

Taxonomy of Quantum cryptographic QKD protocols is illustrated in Figue 2. Broadly, QKD protocols are categorized into three types which are Quantum state, device-independent state, and based on architecture.

Based on Quantum state

Quantum state-based QKD protocols further divide into two major categories: continuous and discrete variables.

- **Continuous variable:** Compared to conventional one-way Gaussian protocols, a continuous-variable QKD system based on compressed states and heterodyne identification achieves more excellent secret key rates over a noisy line. This improved resilience to channel noise can be explained by adding noise to the signal that is transformed into the private key on purpose. Protocols come under this type, namely Gaussian-modulated coherent states (GMCS), Coherent one-way (COW), Reverse coherent, Coherent two-way, and entangled-based protocol (Huang *et al*, 2016).

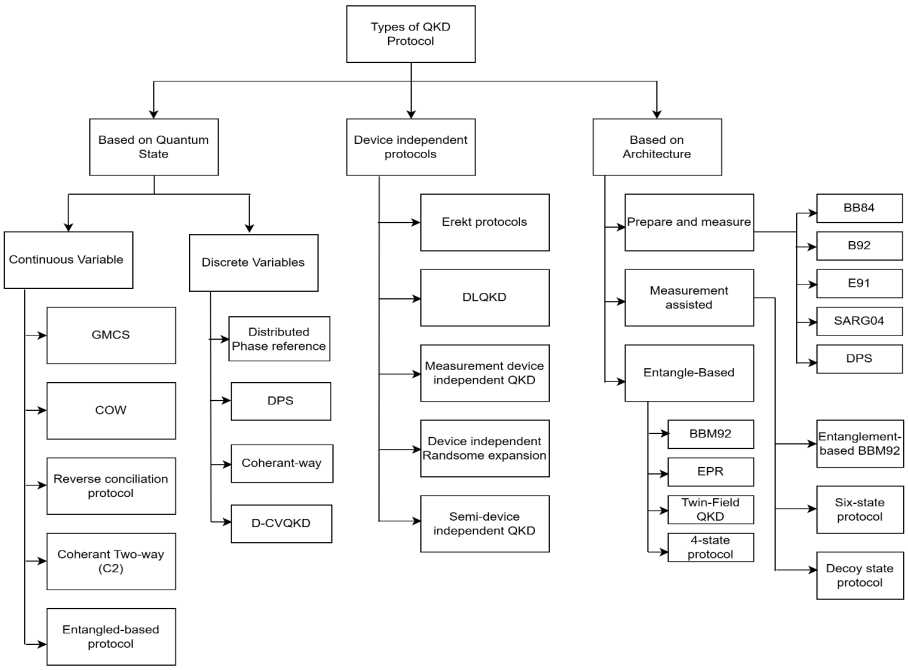

Figure 2: Types of QKD protocols

- **Discrete variable:** In Discrete-Variable QKD (DV-QKD), the source (Alice) prepares to transmit quantum signals to its recipient (Bob), which are made up of incredibly weak single photons with random data encoded in them. Bob uses a single-photon indicator to determine the condition of the incoming photons and gathers data that is somewhat connected to Alice's encoded data (Trizna & Ozols., 2018). Bob and Alice will use this info to apply digital signal processing to extract a key. Examples of DV-QKD protocols are differential phase shift (DPS) (Inoue, 2015), Coherent-way, and D-CVQKD.

Device independent protocols

Device-Independent QKD (DI-QKD) addresses the issue that consider the ideal circumstances of the theoretical protocol and neglect the problems that may occur when deploying a protocol, for instance, the photon-number-splitting attack. Alice and Bob must instead confirm that the input-output data of the devices violate a Bell inequality to demonstrate the protocol's security. Various types of DI-QKD protocols are measurement device-independent QKD, Erekt protocol, device-independent randsome expansion, and semi-device independent.

Based on Architecture

The network architecture, consisting of various nodes (trusted/non-trusted) connecting these lawful users, might be significant to protocol design. Due to security concerns, a secure method for distributing cryptographic keys is used for authentication (Alshowkan, 2022). One-way point-to-point communication is not ideal for long-distance communication. With the current QKD algorithms, low-distance group communications can be established where users can authenticate one another through a single trusted server. This category of QKD protocol is further divided into three categories: prepare and measured, measurement assisted and entabgle-based.

- **Prepare and measure:** Quantum communication and cryptography's fundamental building blocks are P&M networks. Non-orthogonal quantum encodings are required to spread quantum connections in the network. P&M allows for higher communication rates and data-theoretic integrity. Various protocols have already been proposed under this category; some examples are BB84, B92, E91, SARG04, and Differential-phase-shift (DPS) (Huang, 2008).
- **Measurement assisted:** It is essential to guarantee a secure key rate & the distribution range in QKD. This entanglement-based approach based on 2-Bell states extends the transmission range. By merging the concept of small state advance, the protocol can double communication distance, deprive of any security vulnerabilities connected to the measurement device and manage key generation rates via untrusted third parties compatible with the BBM92 protocol. There are various protocols under this category, including entanglement-based BBM92, Six-state protocol, and decoy state protocol.
- **Entangle-based:** Due to its repeater-like rate-loss scaling, twin-field (TF), this QKD has quickly emerged as the most practical option for long-distance secure fiber communication. however, its implementation difficulty, could delay or even block its advancement in

the actual world if this issue is not addressed. All current configurations effectively adopted a massive, asset-inefficient optical structure that lacks the scalability that matures QKD systems given with simplex quantum connections to fulfil its requirement for twin-field coherence. BBM92, EPR, twin-field QKD, and 4-state protocol falls under this category.

QKD in IoT authentication

In QKD, polarized photons are used for communication. Quantum indeterminacy is a special characteristic of quantum physics. Any measurement of the photons will alter their state. Therefore, it is nearly impossible to break a quantum key. The benefit of QKD is that an Eve(interceptor) in the network may be easily recognized. The two qualities of sending the private Key are quantum superposition and entanglement. Quantum superposition represents the product of two waves as one or the opposite.

QKD is a technique that practices quantum mechanics to securely distribute cryptographic secret keys between two parties, ensuring that any attempt to intercept or eavesdrop on the transmission is detectable.

In IoT, authentication is critical to ensure that devices communicate with authorized parties and prevent unauthorized access to sensitive information.

QKD can be used in authentication in IoT by generating a unique key pair for each device, which can be used to authenticate the device and the messages it sends. QKD guarantees that only authorized nodes can access the network, preventing potential attacks, and unauthorized access. Another way QKD can be used in authentication is by generating a collective secret key is used to validate the device and encode data transmission between the and server/gateway, ensuring that data cannot be intercepted or tampered with during transmission. Various QKD- inspired authentication techniques in IoT are illustrated in Table 1. This section accomplishes a literature comparison made by researchers in direction of strong authentication using quantum computing, communication, and support safe IoT (Beniwal & Singhrova, 2022).

Benefits of QKD in IoT Environment

The use of QKD in authentication in the Internet of Things (IoT) (Bansal & Singhrova, 2023) has several advantages (Bhatt & Sharma, 2019):

- **Enhanced security:** QKD offers enhanced security as it uses quantum mechanics to securely distribute cryptographic keys, making it is not possible for an attacker to interrupt or eavesdrop on the communication without being noticed.
- **More robust authentication:** QKD allows for generating unique key pairs for each device, making it possible to achieve stronger authentication between devices and prevent unauthorized access to the network.
- **Protection against replay attacks:** QKD generates a unique key pair for each device, making it difficult for attackers to replay messages, as the keys used to encrypt the message would not be the same as those used in the original transmission.
- **Increased efficiency:** QKD is also more efficient than traditional key-distribution methods as it allows for faster key exchange via secure channels.
- Future-proofing: QKD is also considered a future-proof technology as it is not susceptible to attacks from quantum processors, which may threaten traditional cryptographic methods.
- **Reduced risk of data breaches:** QKD minimizes the risk of data breaches. It provides a secure method for key distribution, making it almost impossible for attackers to gain unauthorized access to the network.
- **Enhanced security:** QKD offers enhanced security as it uses quantum mechanics to securely distribute cryptographic keys, making it is not possible for an attacker to interrupt or eavesdrop on the communication without being noticed.
- **More robust authentication:** QKD allows for generating unique key pairs for each device, making it possible to achieve stronger authentication between devices and prevent unauthorized access to the network.
- **Protection against replay attacks:** QKD generates a unique key pair for each device, making it difficult for attackers to replay messages, as the keys used to encrypt the message would not be the same as those used in the original transmission.
- **Increased efficiency:** QKD is also more efficient than traditional key-distribution methods as it allows for faster key exchange via secure channels.
- **Future-proofing:** QKD is also considered a future-proof technology as it is not susceptible to attacks from quantum processors, which may threaten traditional cryptographic methods.
- **Reduced risk of data breaches:** QKD minimizes the risk of data breaches. It provides a secure method for key distribution, making it almost impossible for attackers to gain unauthorized access to the network.
- **Improved regulatory compliance:** In industries such as healthcare, financial services, and government, there are strict regulatory requirements around data privacy and security. QKD can help organizations meet these requirements by providing a more secure key distribution and authentication method.
- **Lower operational costs:** QKD can reduce the operating costs of managing and securing IoT networks. It eliminates the need for manual key management.
- **Increased trust and confidence:** QKD can increase the trust and confidence of end-users and customers, providing higher security and protection for their data and improving customer satisfaction and loyalty.

Table 1: Various QKD based authentication techniques in IoT

Year	*Technique*	*Implementation/ Methodology*	*QKD protocol*	*Observations*
2022 (Alshowkan)	Authentication in smart grid applications using QKD	Used secret keys to verify the connection between PV and Intel agents.	MQTT	Achieved information-theoretic authentication in smart grid communications.
2022 (Shabir)	Multi-level authentication using fuzzy logic.	Used Fuzzy logic based QKD	QRNG, irregular BB84	Proposed CMMLA scheme and executed the algorithm on QKD online simulator
2021 (Zheng)	Quantum key distribution with two-way authentication	QKD used to implement secure key distribution and identity authentication.	Pseudo random functions	Proposed a scheme by using quantum state and quantum encoding base.
2021 (Abdulkader)	Secure IoT system using QKD with block cipher	Used QBER to decrease the error rate.	RC6, BB84	Proposed an authentication protocol for IoT based applications.
2021 (Roy)	Quantum-Safe User Authentication Protocol for the IoT.	Used public key encryption and post quantum cryptography.	OTP	Five phase algorithm Used lattice-based cryptography. It also registered the gateway nodes for two-way authentication.
2021 (Wang)	Experimental authentication of QKD with post-quantum cryptography	Demonstrated using two well connected relay networks.	PQC	Verified stability, feasibility, and efficiency of QKD algorithm.
2019 (Bhatt)	Quantum Cryptography for IoT Security	Implemented and analysed Quantum cryptography in context of IoT security.	NA	Identified the security threats in IoT
2018 (Lohachab)	Secure communication and authentication scheme using QKD and ECC in IoT.	AVISPA tool used to simulate the proposed algorithm.	ECC, BB84	Artificial intelligence used along with post quantum cryptography.
2008 (Huang)	Implementation of QKD in Wireless network Wi-Fi (IEEE 802. 11).	Used C++ language on the Linux Platform	B92, BB84	Identified the usage of QKD in authentication and encryption for the IEEE802.11 network.

Issues and Challenges

Despite the many advantages of Quantum Key Distribution (QKD), there are also some limitations worth mentioning here (Aleksic *et al*., 2015):

- **Distance limitations:** QKD is limited by distance, as the transmission of quantum signals through fiber optic cables can only reach a limited range before the signal strength is lost. This limits the scope of QKD networks, which may require additional infrastructure or repeaters to extend the range.
- **Hardware limitations:** QKD requires specialized hardware and infrastructure, which is costly and complex to deploy and maintain. Implementation of QKD at a large scale became a problem.
- **Vulnerability to side-channel attacks:** QKD is vulnerable to side-channel attacks, where attackers can obtain information about the key by monitoring the hardware used in the QKD process.
- **Key management:** The keys generated through QKD require careful management to ensure they are secure and not compromised. Thus, additional resources and processes must be in place to manage and monitor the keys.
- **Limited compatibility:** QKD is incompatible with some communication protocols and systems such as TCP/IP, and UDP. This may limit its use in specific applications.
- **Interoperability:** There needs to be more standardization and interoperability among QKD technologies, which may limit the ability to integrate QKD into existing communication networks.

Conclusion

In the digital age, QKD is a potential method for secure communication. QKD-based authentication techniques can provide better safety against network attacks, including eavesdropping, Man-in-middle attacks (MIME), and replay attacks.

The literature review identified various QKD-based authentication techniques, including QKD-based authentication protocol, QKD-and ECC-based authentication protocol, and QKD and Fuzzy logic-based authentication protocol. Each method has pros and cons, which can be evaluated based on several parameters, such as technology, QKD protocols, and security. The decision to use a QKD-based authentication technique ultimately depends highly on the application-specific requirements and the compromises among privacy, computational complexity, and practicality. Future research scope in this domain can focus on emerging hybrid techniques that associate the strengths of different QKD-based authentication techniques to provide better security and suitability for real-world applications.

References

Kute, S. S., & Desai, C. G. (2017). Quantum cryptography: a review. *Indian Journal of Science and Technology*, *10*(3), 1-5.

Upadhyay, G., & Nene, M. J. (2016, May). One time pad generation using quantum superposition states. In *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 1882-1886). IEEE.

Breguet, J., Muller, A., & Gisin, N. (1994). Quantum cryptography with polarized photons in optical fibres: Experiment and practical limits. *Journal of Modern Optics*, *41*(12), 2405-2412.

Huang, D., Huang, P., Wang, T., Li, H., Zhou, Y., & Zeng, G. (2016). Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol. *Physical Review A*, *94*(3), 032305.

Trizna, A., & Ozols, A. (2018). An overview of quantum key distribution protocols. *Inf. Technol. Manage. Sci*, *21*.

Inoue, K. (2014). Differential phase-shift quantum key distribution systems. *IEEE Journal of Selected Topics in Quantum Electronics*, *21*(3), 109-115.

Lo, H. K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical review letters*, *108*(13), 130503.

Huang, X., Wijesekera, S., & Sharma, D. (2008, February). Implementation of quantum key distribution in Wi-Fi (IEEE 802.11) wireless networks. In *2008 10th International Conference on Advanced Communication Technology* (Vol. 2, pp. 865-870). IEEE.

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

Shabbir, M., Ahmad, F., Shabbir, A., & Alanazi, S. A. (2022). Cognitively managed multi-level authentication for security using Fuzzy Logic based Quantum Key Distribution. *Journal of King Saud University-Computer and Information Sciences*, *34*(4), 1468-1485.

Zheng, X., & Zhao, Z. (2021). Quantum key distribution with two-way authentication. *Optical and Quantum Electronics*, *53*(6), 304.

Abdulkader, Z. A. (2021). A secure iot system using quantum cryptography with block cipher. *Journal of Applied Science and Engineering*, *24*(5), 771-776.

Roy, K. S., & Kalita, H. K. (2019). A quantum safe user authentication protocol for the internet of things. *International Journal of Next-Generation Computing*, *10*(3).

Wang, L. J., Zhang, K. Y., Wang, J. Y., Cheng, J., Yang, Y. H., Tang, S. B., ... & Pan, J. W. (2021). Experimental authentication of quantum key distribution with post-quantum cryptography. *npj quantum information*, *7*(1), 67.

Bhatt, A. P., & Sharma, A. (2019). Quantum cryptography for internet of things security. *Journal of Electronic Science and Technology*, *17*(3), 213-220.

Lohachab, A. (2018, April). Using quantum key distribution and ECC for secure inter-device authentication and communication in IoT infrastructure. In *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)* (pp. 26-27).

Aleksic, S., Hipp, F., Winkler, D., Poppe, A., Schrenk, B., & Franzl, G. (2015). Perspectives and limitations of QKD integration in metropolitan area networks. *Optics express*, *23*(8), 10359-10373..

Lardier, W., Varo, Q., & 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.

Lardier, W., Varo, Q., & Yan, J. (2020, June). Dynamic reduced-round cryptography for energy-efficient wireless communication of smart IoT devices. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

Lardier, W., Varo, Q., & 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.