Applications of quantum cryptography for Internet of Things (IoT) security

Nuriddin Jabbarov [a)], Tukhtajon Kozokova, Lola Davronova, Iskandar Olimov

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

[a)] *Corresponding author: nuriddinjabbarov2606@gmail.com*

Abstract. The Internet of Things (IoT) has brought many benefits to modern society, but it also poses significant security challenges due to the large amount of data generated by IoT devices. One potential solution to these security challenges is quantum cryptography, which uses the principles of quantum mechanics to ensure secure communication. This paper analyzes the application of quantum cryptography in IoT systems, including system problems and solutions, discussions and results, and proposes quantum random number generation (QRNG) and quantum secure direct communication (QSDC) methods as solutions.

INTRODUCTION

The Internet of Things (IoT) encompasses a cluster of technologies that require various protocols, infrastructures, data storage mechanisms, and information technology (IT) communication methods. With the development of the Internet of Things (IoT) and the increase in sensitive and confidential information transmitted over these networks, security in this network has become a major concern [1]. One emerging technology that can effectively secure these networks is quantum cryptography. Quantum cryptography is a field of research that employs the principles of quantum mechanics to develop secure communication protocols. In this article, we discuss the use of quantum cryptography in IoT systems, the challenges it presents, and the solutions being developed to address these challenges.

Security issues in IoT systems

A. Data breach- IoT applications collect a significant amount of sensitive data from users to function properly and efficiently. Furthermore, most of this data consists of the user's personal information, which must be protected through encryption.

B. Data authentication- Even if the data is successfully encrypted, there is still a possibility of the device itself being compromised. Security is only recognized when the authenticity of data to and from an IoT device cannot be determined by any means.

C. Adjacent channel attacks- These are attacks based on information and data from the system implementation rather than weaknesses in the attack implementation algorithm. Power consumption, electromagnetic leakage, or noise may be sufficient to compromise the system.

D. Lack of updates- There are many IoT devices in the world now, and the number is increasing every year. When developing devices, developers often do not pay much attention to future updates of the device, and therefore a device that was considered secure at the time of manufacture may become insecure within a few years.

E. Malware and ransomware- An example of malware is the Mirai Botnet, which infects IoT devices running Argonaut Reduced Instruction Set Computer Core (ARC) processors. If the default username and password combination for the device is not changed, it is very easy for Mirai to infect the device. Ransomware is a type of malware that tends to lock users out of their devices and threatens to leak users' personal information if a ransom is not paid [2].

We need stronger cryptographic and security algorithms to prevent the abovementioned threats.

Quantum cryptography-Cryptography is the process of encrypting and protecting data so that only a person with a specific secret key can access the data. Quantum cryptography differs from traditional cryptographic systems in that it relies on physics rather than mathematics as the main aspect of its security model. Quantum cryptography does not

compromise the message without the knowledge of the senders or receivers and provides complete protection. In other words, information encoded in the quantum state cannot be copied or viewed without notifying the sender or receiver [3].

Quantum cryptography uses individual particles of light, or photons, to transmit data over optical fiber. Photons represent binary bits. The security of the system relies on quantum mechanics. These secure features include:

- Particles can exist in multiple places or states simultaneously.
- A quantum property cannot be observed without changing or disturbing it.
- The particles that make up the universe are indeterminate and can exist in multiple places or states of existence simultaneously.
- You can clone some quantum properties of a particle, but not the entire particle.

These properties make it impossible to measure the quantum state of any system without destroying that system.

Quantum key distribution. One of the main techniques used in quantum cryptography is quantum key distribution (QKD). QKD involves the transmission of a series of photons (light particles) in a state of random polarization. The sender and receiver each measure the polarization of the photons using a device known as a polarizer. Since the polarization of each photon is randomly generated, any attempt to capture or measure the photons necessarily distorts the state of polarization. As a result, an attempt to eavesdrop on the communication is detected immediately [2].

Imagine there are two people named Alice and Bob who want to send each other a secret message. With QKD, Alice sends a series of polarized photons to Bob through a fiber optic cable. This cable does not need to be shielded because the photons have a random quantum state. Alice initiates the message by sending a key to Bob. The key is a stream of photons moving in one direction. Each photon represents one bit of data - 0 or 1. However, in addition to linear movement, these photons oscillate in a certain way (Fig. 1).

Thus, before the sender Alice initiates the message, the photons travel through the polarizer. A polarizer is a filter that allows some photons to pass with the same vibration and others with a different vibrational state. Polarized states can be vertical (1 bit), horizontal (0 bit), 45 degrees right (1 bit), or 45 degrees left (0 bits). A transmission has one of two polarizations, representing a single bit, 0 or 1, in the circuit it uses.

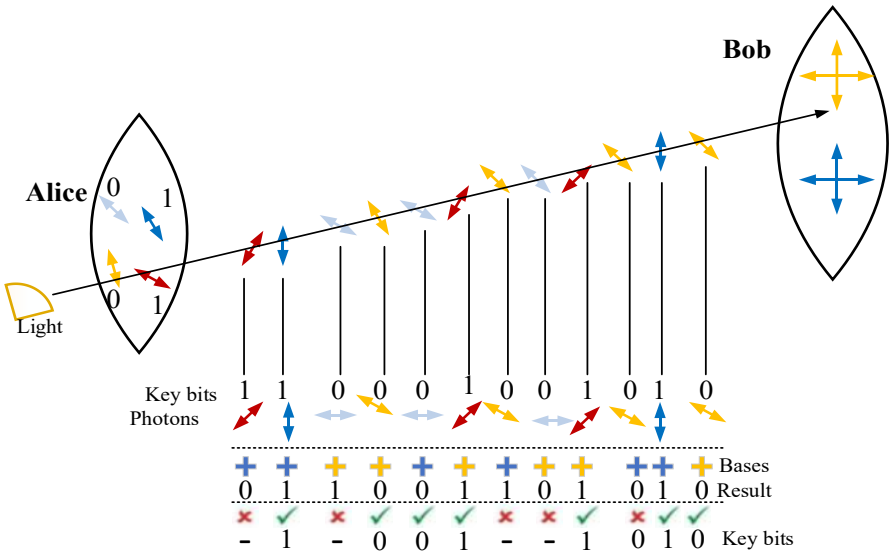

FIGURE 1. Implementation of quantum encryption via quantum key distribution (QKD)

The photons now travel along the optical fiber from the polarizer to the receiver, Bob. This process uses a beam splitter that reads the polarization of each photon. When receiving the photon switch, Bob does not know the correct polarization of the photons, so one polarization is chosen at random. Alice now compares what Bob used to polarize the switch and then lets Bob know which polarizer to send each photon from. Bob then confirms that he used the correct polarizer. Photons read with the wrong separator are then discarded, and the rest of the sequence is keyed [4].

If a third party tries to eavesdrop on the conversation, they have to read each photon to access the message. Then, they have to give this photon to Bob. By reading the photon, the third party changes the photon's quantum state, which introduces errors in the quantum key. This alerts Alice and Bob that someone is listening and that the key has been

compromised, so they discard the key. Alice needs to send Bob a new uncorrupted key, and then Bob can read the message from that key.

EXPERIMENTAL RESEARCH

In recent years, several studies have been conducted on quantum cryptography. In 2018, Wang et al. proposed a secure communication scheme based on chaotic maps and quantum key distribution. The scheme used chaotic maps to generate a secret key, which was then used in conjunction with QKD to establish a secure communication channel. In 2019, Zhang et al. proposed a quantum cryptography protocol based on quantum chaotic systems. The protocol used chaotic systems to generate a public secret key, which was then used to encrypt and decrypt messages. In 2020, Liu et al. proposed a new QKD protocol based on entangled photon pairs. The protocol used two entangled photon pairs to establish a secret key, which was then used for secure communication. Table 1 below provides an analysis of the scientists who have conducted research using this method to date and their work:

Table 1. analysis of research work and results in this field

Authors	Approach	Method	Main result
Wang et al. (2018)	Chaotic maps and QKD	Generate a secret key using chaotic maps and establish a secure communication channel using QKD	Secure communication is achieved using the proposed scheme
Zhang et al. (2019)	Quantum chaotic systems	Generate a public secret key using chaotic systems and use it to encrypt and decrypt messages	A new quantum cryptography protocol based on chaotic systems has been proposed
Lee et al. (2019)	QKD-based authentication	Improved security compared to traditional methods	A more effective authentication method than traditional methods
Liu et al. (2020)	Conjoined photon pairs	Generate a secret key using two entangled photon pairs and use it for secure communication	A new QKD protocol based on entangled photon pairs has been proposed
Zhou et al. (2021)	Data encryption based on QKD	Improved security and low latency compared to traditional methods	A low-latency encryption method

As the table shows, these studies found that using quantum cryptography in IoT systems can enhance security and reduce communication overhead and latency.

The impact of quantum computing on the Internet of Things. Quantum computing has various important features that classical computers do not possess, making the security of IoT more vulnerable than before. Although the IoT has encountered numerous threats to date, these security risks may escalate to an unprecedented level if quantum computing is implemented. Organizations relying on real-time IoT applications are coming to realize that quantum computing will become a formidable threat [5].

A. Key features of post-quantum cryptography

Post-quantum cryptography is a subfield of cryptography that deals with the design, implementation, and analysis of cryptographic algorithms. More broadly, researchers are striving to enhance information security infrastructure by implementing quantum-resistant primitives known as quantum-safe cryptography. Quantum cryptography is much more efficient than traditional methods due to the following properties:

1. Photon polarization. Used to describe the exact direction of polarization of light or photon particles, counting time plays an important role because these polarized light particles or photons can only be measured at a specific time to determine the correct state of polarization. If no specific photon filter is selected, the photon particle is lost [6].
2. Uncertainty Principle: The German physicist Heisenberg introduced the concept of uncertainty principle related to quantum information, formally known as the Heisenberg Uncertainty Principle [7], which states that it is difficult to measure the state of a particle without perturbing the particle because it has different states with varying probabilities. available in different situations.
3. Non-Clone Theory: In general, cloning refers to the creation of an identical state in another system, i.e., cloning quantum information is the art of producing an identical state in another system [8]. Cloneless quantum theory states that an unknown quantum state cannot be destroyed or cloned because there is currently no machine capable of doing so.

4. Teleportation: Quantum information has its hidden properties because, to measure the classical formation, the sender must calculate the original quantum state that was opened by the sender itself during classical communication, and the remaining information is quantum information. The continuous flow of quantum information, combined with the Heisenberg Uncertainty Principle and photon polarization properties, makes quantum cryptography an ideal choice for ensuring data security and privacy. With these fundamental properties, quantum cryptography enables IoT systems to confront the post-quantum IoT world.

B. Implementing quantum cryptography for IoT security

IoT devices have numerous vulnerabilities in terms of user or network security. Additionally, sometimes when there is an attack, where only one device in the entire IoT network may become infected with a virus, other devices trust the infected device and continue to communicate until the infection is detected. A threat may not be detected in time, and during this period, a significant amount of data can be transmitted to any malicious entity [9].

Some viruses can affect systems in such a way that they can only be removed by rebooting the systems, and industrial and corporate systems are not rebooted for extended periods. Thus, there are various points of vulnerability, and IoT systems are highly susceptible to attacks. Here, we explore a potential solution to IoT security through quantum cryptography [10].

A key aspect of quantum cryptography is the quantum key distribution discussed above [11]. The most significant feature of quantum key distribution is the channel's ability to detect the presence of any eavesdropper in the system architecture. This is fundamentally different from classical cryptography algorithms. In general, the two channels required to establish secure communication in QKD include a quantum channel and a non-quantum (conventional) channel. In the QKD process, messages are not sent directly over the quantum channel. Instead, an initial exchange of random bits containing irrelevant information is performed between two users. The primary purpose of this step is to detect any eavesdropping on the connection. If an eavesdropper is active, they may attempt to intercept the message. Monitoring the conventional channel provides the probability that the connection was tampered with or intercepted during transit. If any tampering is suspected, the connection is reset from the beginning. In another scenario, if the channel is deemed secure, the parties jointly agree to establish the next communication using the quantum bits as a one-time pad.

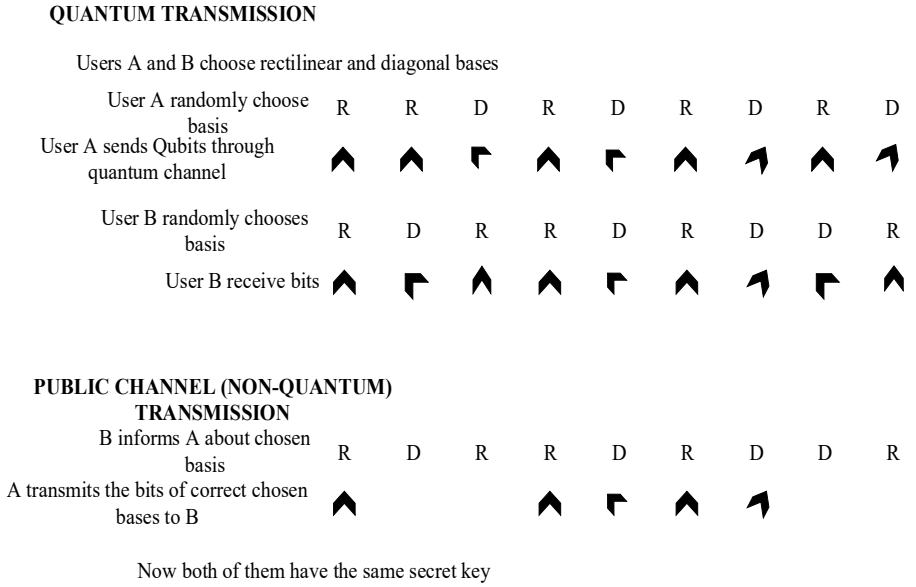

FIGURE 2. Illustration of QKD of BB84 protocol

The most widely used protocol for secure key agreement is the Bennett and Brassard (BB84) QKD protocol developed by Charles H. Bennett and Gilles Brassard, as discussed below [12]. Initially, both entities (e.g., users "A" and "B") define the polarization basis, namely Diagonal and Rectilinear. This step is crucial for communication because the agreed-upon basis in this step is used for further communication. Then, one of the two (e.g., user A) randomly selects a basis from which to identify qubits. The selected qubits are then transferred to the other entity through a

quantum channel. Next, user A informs user B about the chosen basis over a non-quantum channel, and if the communication is considered secure, they proceed.

Finally, user A transmits the qubits chosen by user B to a specific polarization basis, and ultimately, both entities have the same key by applying the BB84 protocol. Figure 2 illustrates the example discussed above using the BB84 protocol. By utilizing quantum state storage and two unitary operations, this protocol modifies the BB84 protocol and ensures that no party can determine the key, but both participating parties can determine the key between themselves [5].

RESEARCH RESULTS

Implicit security is achieved through the use of quantum secure direct communication (QSDC) [13] as a form of quantum communication that utilizes the methods and tools studied above to ensure secure communication between IoT devices. It provides a unique method for direct data transfer and secure communication implementation using quantum random number generation (QRNG), which creates a noise source with a high level of randomness, as we will.

A. Quantum random number generation (QRNG)

The main issue in the BB84 quantum cryptographic protocol is the maximum distance that photons can travel. Photons are essentially light particles that can easily be damaged by the environment or natural disasters. In cases where IoT networks span large distances, covering many cities or countries, photons have to travel very long distances. This is where quantum computing falls short. Additionally, quantum devices are bulky and expensive, making them unaffordable for many organizations. The existing quantum key distribution protocol is designed to work with only two devices, which is almost impossible to implement in real IoT systems that integrate hundreds of devices for communication [14].

To address these challenges, a proposed solution combines classical and quantum approaches. The first suggested solution retains current semiconductor chips but uses quantum techniques to generate long and unique cryptographic keys for each device. This can be achieved using QRNG, which creates a noise source with a high degree of randomness. Quantum computing is capable of efficiently and rapidly generating such large numbers. As a result, the keys will be extremely difficult to guess, and each device will have a unique key. The only way to obtain the key is to access the physical device configuration, a task that is very challenging to accomplish without anyone noticing. Therefore, it can be assumed that the key is well-protected, ensuring secure communication [15].

B. Quantum secure direct communication (QSDC)

It is also possible to use device-independent quantum cryptography to ensure trust in manufactured devices. QSDC, considered a form of quantum communication, provides security during direct transmission. QSDC was first proposed in 2000 to implement direct data transmission without key distribution. Later in 2003, Deng and Long presented all aspects of QSDC and proposed a two-stage QSDC [16]. Recently, QSDC has developed rapidly. In addition, secure direct communication based on continuous variables was presented [17]. Zhang et al. [18] demonstrated QSDC using a two-step QSDC protocol over an optical fiber with a critical distance of 500 m. Later, Qi et al. [19] addressed several key issues and provided a comprehensive security analysis of QSDC for practical application.

Zhou et al. [20] proposed a gauge-independent QSDC that eliminates gauge-related security gaps. Meanwhile, Zhou et al. [21] developed a device-independent QSDC, which represents a relaxation of security assumptions made in conventional protocols and improves communication security. In particular, using modern technologies, a quantum memory-free QSDC protocol has been developed, in which the quantum memory is lost, which solves one of the biggest obstacles to the practical application of QSDC.

A key requirement of QSDC using Wyner's listening channel model is to allow the communication system to operate at a power lower than the privacy capacity of the channel. An efficient quantum coding method using a combination of low-density parity-check (LDPC) codes was presented in the research work (Figure 3). The proposed method can operate in high-loss and high-error modes, which is unique for quantum communication. In this case, the communication distance is about 1.5 km, and the achieved secure data transfer rate is 50 bps, sufficient for text messages and images. Recently, a group at Tsinghua University further extended this practical prototype to a distance of 12.04 km with a communication speed of more than 4 kbps using classical optical fibers. These studies have provided a solid foundation for the practical application of QSDC.

In the coding and decoding layers shown in Figure 3, universal hashing families (UHF) perform the function of secure coding, aimed at ensuring information-theoretic security [22]. In this encoding method, the sender, Alice, first generates a locally random bit sequence of a certain length. Then, it uses reverse UHF (UHF^{-1}) to process the message together with local random numbers and general random numbers, achieving randomization of the secret message and

generating a new vector. This vector is encoded with an LDPC code and then mapped to the transmitted codeword. After receiving the codeword, Bob can extract the secret message through the appropriate stages of de-mapping, ECC decoding, and UHF. Eve cannot decipher a secret message if it is a partially stolen transmitted codeword. This secure coding scheme does not require changing the traditional coding structure. Arbitrary error correction codes and anti-loss codes can be used to enhance reliable communication capability.

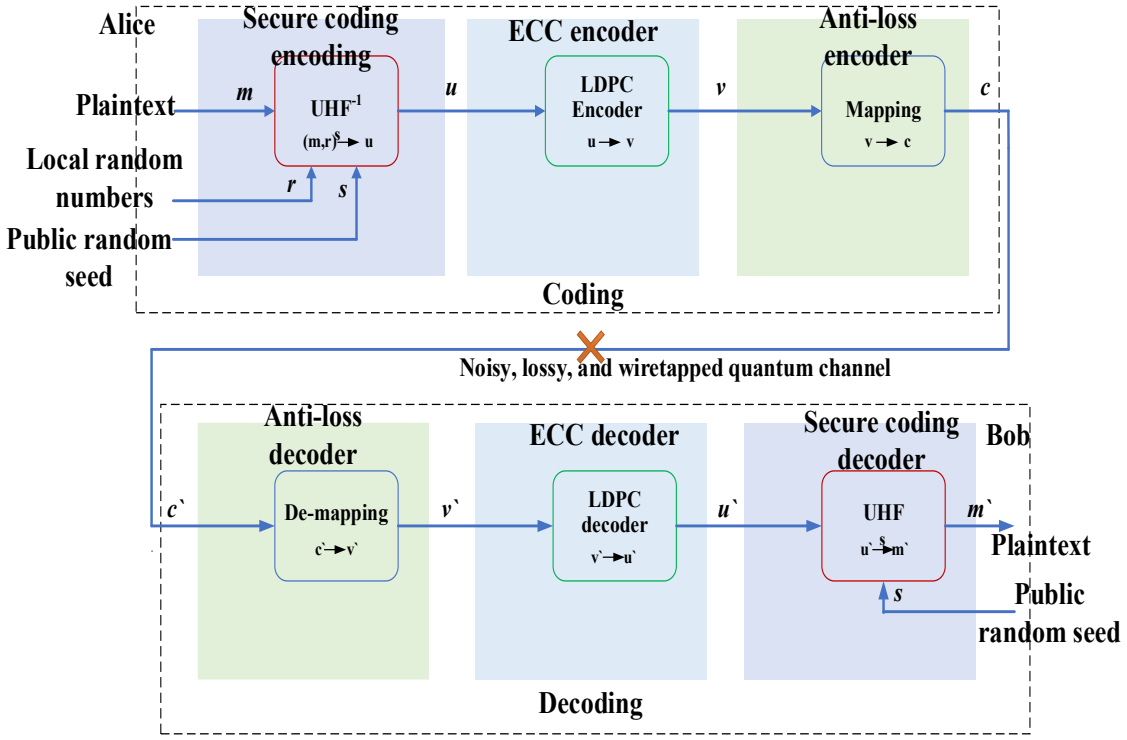

FIGURE 3. Encoding and decoding scheme for the QSDC experiment

The single photon source is provided by a strongly attenuated 1550 nm laser with a systematic pulse repetition frequency of 1 MHz. Both communication sides are controlled using field-programmable gate arrays (FPGAs). As discussed, recent advances in QSDC have accelerated for practical applications. Additionally, as Elsa Kania and John Costello pointed out in their 2018 CNAS report, QSDC enhances communication security, which is typically the value proposition of quantum communication. Furthermore, its direct transmission nature makes it a natural fit with post-quantum cryptography, which finds several important applications in the growing field of quantum networks. It should be noted that, on one hand, QSDC can be used independently for the direct transmission of small amounts of data in the most secure manner. On the other hand, its use can be similar to quantum key distribution, which means it can also be used to distribute a small number of secret keys and then combine them with a standard symmetric cryptography protocol, such as the Advanced Encryption Standard (AES). With the development of classical coding theory and the improvement of quantum devices, the prospects of quantum secure direct communication will be broad and bright.

CONCLUSIONS

The advent of IoT has enabled us to communicate with each other using the Internet in our daily lives. However, various problems have arisen following the use of these technologies. Various cryptographic primitives have been developed to address these problems. However, with the emergence of the idea of quantum computing, it became evident that this cryptography was not secure enough. It can be seen that the development of cryptographic solutions that provide the expected level of security in post-quantum IoT networks is required. In this article, we have discussed in detail the IoT-related issues and available countermeasures. In the following sections, a comprehensive description of the concept of quantum cryptography is provided. During this research work, QKD, one of the main methods used in quantum cryptography, and the BB84 protocol used within it, were employed to address the existing problems in the

IoT system and ensure secure communication between devices. We utilized the QSDC method to ensure secure communication, and as a result, the encoding and decoding schemes were demonstrated.

REFERENCES

1. J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J*, vol. 1, no. 1, pp. 3–9, Feb. 2014, doi: 10.1109/JIOT.2014.2312291.
2. A. P. Bhatt and A. Sharma, "Quantum Cryptography for Internet of Things Security," *Journal of Electronic Science and Technology*, vol. 17, no. 3, pp. 213–220, Sep. 2019, doi: 10.11989/JEST.1674-862X.90523016.
3. R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, "Quantum cryptography," *http://dx.doi.org/10.1080/00107519508222149*, vol. 36, no. 3, pp. 149–163, 2006, doi: 10.1080/00107519508222149.
4. H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, "Quantum cryptography," *Appl Phys B*, vol. 67, no. 6, pp. 743–748, 1998, doi: 10.1007/S003400050574.
5. A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet of Things*, vol. 9, p. 100174, Mar. 2020, doi: 10.1016/J.IOT.2020.100174.
6. "Using Quantum Key Distribution and ECC for Secure Inter-Device Authentication and Communication in IoT Infrastructure by Ankur Lohachab, Karambir :: SSRN." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3166511 (accessed Aug. 21, 2023).
7. W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," *Original Scientific Papers Wissenschaftliche Originalarbeiten*, pp. 478–504, 1985, doi: 10.1007/978-3-642-61659-4_30.
8. "Quantum Theory: Concepts and Methods," *Quantum Theory: Concepts and Methods*, 2002, doi: 10.1007/0-306-47120-5.
9. L. Bishop, S. Bravyi, A. W. Cross, J. Gambetta, J. Smolin, and March, "Quantum Volume," 2017.
10. N. Jones, "Computing: The quantum company," *Nature*, vol. 498, no. 7454, pp. 286–288, 2013, doi: 10.1038/498286A.
11. "Future-proofing Security in a Post-Quantum Cryptography World - Security Boulevard." https://securityboulevard.com/2019/05/futureproofing-security-in-post-quantum-cryptography-world/ (accessed Aug. 21, 2023).
12. V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations.," *Phys Rev Lett*, vol. 92, no. 5, p. 4, 2002, doi: 10.1103/PHYSREVLETT.92.057901.
13. G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys Rev A*, vol. 65, no. 3, p. 3, Dec. 2002, doi: 10.1103/PHYSREVA.65.032302.
14. S. Gupta and C. Dutta, "Internet of Things Security Analysis of Networks using Quantum Key Distribution," *Indian J Sci Technol*, vol. 9, no. 48, Dec. 2016, doi: 10.17485/IJST/2016/V9I48/105551.
15. "IoT security algorithm accepted by NIST for quantum cryptograph..." https://www.eenewseurope.com/en/iot-security-algorithm-accepted-by-nist-for-quantum-cryptography-project/ (accessed Aug. 21, 2023).
16. F. G. Deng, G. L. Long, and X. S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys Rev A*, vol. 68, no. 4, p. 6, Aug. 2003, doi: 10.1103/PHYSREVA.68.042317.
17. S. Pirandola, S. L. Braunstein, S. Lloyd, and S. Mancini, "Confidential direct communications: A quantum approach using continuous variables," *IEEE Journal on Selected Topics in Quantum Electronics*, vol. 15, no. 6, pp. 1570–1580, Nov. 2009, doi: 10.1109/JSTQE.2009.2021147.
18. F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," *Sci Bull (Beijing)*, vol. 62, no. 22, pp. 1519–1524, Nov. 2017, doi: 10.1016/J.SCIB.2017.10.023.
19. R. Qi *et al.*, "Implementation and security analysis of practical quantum secure direct communication," *Light: Science & Applications 2019 8:1*, vol. 8, no. 1, pp. 1–8, Feb. 2019, doi: 10.1038/s41377-019-0132-3.
20. Z.-R. Zhou, Y.-B. Sheng, P.-H. Niu, L.-G. Yin, and G.-L. Long, "Measurement-Device-Independent Quantum Secure Direct Communication," May 2018, Accessed: Aug. 21, 2023. [Online]. Available: http://arxiv.org/abs/1805.07228
21. L. Zhou, Y. B. Sheng, and G. L. Long, "Device-independent quantum secure direct communication against collective attacks," *Sci Bull (Beijing)*, vol. 65, no. 1, pp. 12–20, Jan. 2020, doi: 10.1016/J.SCIB.2019.10.025.
22. D. Pan, X.-T. Song, and G.-L. Long, "Free-Space Quantum Secure Direct Communication: Basics, Progress, and Outlook," *Advanced Devices & Instrumentation*, vol. 4, Jan. 2023, doi: 10.34133/ADI.0004.