Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 11
TPCEE 2025

The Comparison Between Quantum Communication and Traditional Encryption

Yixuan Xu

Beijing 21st Century International School, Beijing, 100020, China

xuyixuan20071220@outlook.com

Abstract. In recent years, as computational power increases, the traditional encryption methods are becoming increasingly vulnerable to attacks and thus have some safety issues. Therefore, the application of quantum communication has become increasingly widespread, and more technologies related to quantum communication have been invented. This article provides an overview of the differences between quantum communication and traditional encryption in terms of their advantages, disadvantages, security, and the challenges they face in applications. Indeed, the unique characteristics of quantum communication, like quantum superposition and quantum entanglement, provide quantum communication with good security. Furthermore, quantum communication has several advantages, like quantum key distribution, which ensures secure communication, high capacity, high speed, resistance to eavesdropping, and error correction. However, the traditional encryption is still widely used. The traditional encryption, which relies on mathematical algorithms and offers mature encryption methods like Advanced Encryption Standard and Rivest-Shamir-Adleman, must have advantages over quantum communication. Therefore, a comprehensive comparison between traditional encryption and quantum communication is essential to understand their respective roles in the future of secure information exchange.

Keywords: Quantum communication; traditional encryption; quantum physics.

1. Introduction

Quantum communication is an increasingly important method for communication because of its higher ability to be robust against noise and advantages in communication complexity problems [1]. Sensitive information can now be protected in previously unattainable ways thanks to this technology. It offers a degree of security that traditional encryption techniques cannot match by leveraging quantum physics. However, its application in reality has still faced some challenges.

Since quantum communication depends on an entirely different configuration, it is practically impossible to replace the current communication system. Thus, both the difficulties and potential for the future are included in the integration with the conventional network. Potential future developments include the ability to seamlessly integrate with traditional communication, utilizing the advantages of both [2]. Moreover, the quantum repeaters for long-distance communication also limit the spread of quantum communication since enhancing transmission across boundaries presents a considerable challenge; however, successful teleportation of quantum states has been accomplished over distances of several kilometers utilizing optical fibers. Given that information is encoded in orientation, maintaining entanglement over extensive distances proves to be quite arduous. Specifically, entanglement is vulnerable to losses during transmission through optical channels, which constrains the effective range of quantum communication [2].

In contrast, numerous methods of encryption have been created over the years since encryption was developed. These days, the two primary data encryption techniques are symmetric and asymmetric encryption [3]. Knotty mathematical " conundrum" that would take a traditional computer thousands of years to solve are the foundation of classical cryptography. Mathematical issues such as huge number factorization and discrete logarithms could serve as the foundation for these "puzzles." No matter how strong they are, traditional computing machines are impossible to solve these issues and decrypt encrypted database in a suitable period of time. Thus, the data should be secure unless hackers

Content from this work may be used under the terms of CC BY-NC 4.0 licence (https://creativecommons.org/licenses/by-nc/4.0/).
Published by Warwick Evans Publishing.

manage to obtain the encryption keys [4]. The safety of traditional cryptography depends on the confidentiality of the key. If the keys are kept out of the reach of prying eyes, it is almost difficult for the data to be compromised [4]. Furthermore, since there have been years after the application of the traditional encryption, the infrastructure of the traditional encryption has been well-developed. However, quantum communication needs advanced and sophisticated devices like transmitters or photonic chips for quantum communication and the internet. Also, the encryption method of quantum communication is not as mature as traditional encryption. Therefore, the widespread use of quantum communication has to wait for the improvement in both infrastructure and methods.

This article presents what limits the application of quantum communication and describes what causes the continuation of the application of traditional encryption.

2. Quantum Communication

The plural version of quantum is quanta. The definition of a quantum in physics is an energy packet. Entangle photons are a special kind of particle that share quantum states. The transfer of quantum information contained in a quantum state from one location to another is known as quantum communication. Data is not sent in bits using this communication technique. Instead, quantum bits (qubits) are used to transfer data. The entire information and communication technology (ICT) system is encrypted from beginning to end.

Based on science, quantum cryptography utilizes the natures of quantum physics to protect database. Quantum cryptography enables the safety of communications by encrypting and decrypting messages using the quantum level unpredictability of matter. Quantum encryption makes use of qubits, whereas classical and post-quantum cryptography encode data in bits. In this sense, quantum computing and quantum cryptography are comparable [4]. Quantum key distribution (QKD) is now the most famous use of quantum computing cryptography. QKD enables safe, unbreakable, and eavesdropper-proof data exchange between two parties. In contrast to the other two tactics, QKD can assist the parties involved in the conversation in identifying eavesdropping efforts. However, no-cloning theorem and other features of quantum physics prevent hackers from directly measuring data transmitted over a QKD link. Additionally, they would immediately notify communication parties that their connection is insecure by introducing mistakes into the qubits if they attempted to do so [4]. Speaking about hardware, QKD needs photon emitters and specialized optical fiber connections to transmit and receive encrypted data. Establishing a QKD infrastructure at an enterprise scale can cost several million dollars. Standard QKD cannot be introduced into the infrastructure through software upgrades alone; QKD requires specific hardware channels [4]. Nonetheless, a few providers of quantum cybersecurity are developing digital substitutes for QKD. These substitutes are considerably simpler to implement while maintaining the advantageous characteristics of conventional QKD. The goal of QKD is to increase the security of traditional communication channels by strengthening their resistance to eavesdropping. To disperse the encryption keys, it usually uses polarized photons sent via optical cables or open space. The state of a qubit is thus represented by the polarization of each individual photon. Either a wired or wireless classical channel is used to send the encrypted data. Once a secure key has been distributed, the typical communication between Alice, the sender, and Bob, the recipient, is secured using symmetric encryption techniques like AES. More sophisticated procedures than QKD will be necessary in the long run. Imagine a time in the future when multi-location quantum processors work together to solve challenging issues that traditional computers are unable to tackle, or when a tiny quantum device safely transfers demanding computations to a potent quantum server without disclosing the sensitive information or the type of calculations being requested. These are just two examples of situations where quantum communication will be required and protocols already exist. Nevertheless, compared to QKD, the use cases and protocols for beyond-QKD applications are still far less developed. New uses and applications will unavoidably arise as other quantum technologies—like quantum computing, quantum sensing, and quantum memory—continue to advance.

Discrete optical devices are commonly used in conventional quantum communication systems. Optical glasses, such as fused quartz and silica, and optical crystals, such as calcite and beta barium borate, are frequently used to assemble these devices separately. They are then connected by optical fibers or free space. Even though it is beneficial to develop individual components to meet the strict requirements that are always high fidelity, high efficiency, fast speed, and ultra-low loss in quantum information applications, conventional discrete optical structures have always struggled with reliability and interconnect cost, especially when dealing with large-scale networks that connect hundreds of thousands of customers. For example, high mechanical and thermal stabilities are needed to reduce space and phase misalignment over time caused by temperature changes and external pressures. However, global stabilization in complicated discrete optical systems is challenging to accomplish. Chip-scale quantum communication systems provide many advantages over existing huge systems made of discrete optical components, which may not be able to satisfy the increasing requirements for larger volume transmission ability. One excellent platform for the next generation of quantum technology is quantum photonic circuits [5]. Stability and scalability are important benefits over discrete optical systems, in addition to shrinking. The chips are lithographically manufactured as a single unit rather than being built piece by piece, which enables scalability. Because the circuits constructed on a sturdy and small solid substrate can reduce fluctuations from vibrations or temperature changes, stability is attained. Achieving the degree of performance and integration needed for highly effective quantum communication and quantum information processing depends on these two benefits. Furthermore, there is a good chance that quantum photonic chips will be produced at a low cost. Although creating the necessary photomasks is expensive initially, mass production can significantly lower the average cost per chip.

3. Classical Encryption

The complexity of mathematics is the only aspect that influences the encryption methods employed in classical cryptography; specifically, the computational difficulty of factoring large numbers is what gives classical cryptography its encryption security. A more modern type of encryption called quantum cryptography enables two people to establish a secure communication that depends only on the immutable laws of quantum mechanics. Data is transmitted using these characteristics in a manner that is supposedly impenetrable by hackers. The two forms of cryptography take distinct approaches to and solutions for the key exchange problem, which asserts that exchanging keys or other information is necessary to establish a secure communication channel where no other party may access a copy of the key(s) or data. The standard encryption techniques used by almost all businesses and government organizations today to safeguard their data are referred to as classical cryptography. Think about encryption protocols like Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA). RSA is considered one of the most powerful classical cryptography algorithms. To remain computationally complex enough to withstand brute-force attacks while being streamlined enough to be quick after deployment, it completely relies on logarithmic functions. RSA eliminates the requirement for key exchange in situations where it is utilized by switching the order in which key sets are used for the encryption and decryption of general data. The recipient's public and private keys are used for encryption and decryption, respectively. The RSA encryption method is one of the most popular and frequently used Public-Key Encryption (PKE) algorithms. It was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. Because factoring large integers into their most important factors is difficult, this method provides security. Two keys are used: a public key that is freely shared by everyone and a private key that is kept hidden by the owner. The basis of classical cryptography is a complex mathematical "conundrum" that would take thousands of years to solve on a conventional computer. Mathematical issues such as discrete logarithms and huge number factorization can serve as the foundation for these "conundrum." Traditional computers, although it is powerful, could not resolve these problems and decrypt encrypted data in a reasonable length of time. Thus, the data should be secure unless hackers manage to obtain the encryption keys. Symmetric and asymmetric encryption are the two fundamental types. A system that uses the same encryption key and decryption key is known as symmetric key cryptography. When being utilized for

communications, the one key "must be shared between the sender and the receiver" via key exchange. The primary purpose of symmetric key cryptography is to safeguard confidentiality, not the accuracy or legitimacy of data. Note 50 Symmetric key algorithms are exemplified by AES, DES, Blowfish, RC4, and SEAL. In conventional cryptography, a "key," which is a secret string of random integers, is exchanged between the communicating parties. In symmetric encryption, the communicating parties use the same key to encrypt and decrypt data. Data is encrypted using the recipient's public key, which is publicly available, and decrypted using the recipient's private key in asymmetric (public-key) encryption. Classical cryptography's level of security is determined by the key's secrecy. If the keys are hidden from prying eyes, it is almost impossible for the data to be hacked until the development of powerful quantum computers. Asymmetric key cryptography is a more recent invention than symmetric key encryption, which has been in use for millennia. The encryption and decryption keys in a public-key cryptography system are separate, sometimes referred to as asymmetric key cryptography. With this approach, different parties may own the public encryption and private decryption keys, opening up a range of asymmetric communication options, such as key exchange and digital signatures. Asymmetric-key encryption has an advantage over symmetric-key encryption in that it does not have to deal with the problem of key exchange for two parties to connect or communicate because the public keys that will be used to encrypt the data are readily available. Data integrity, validity, and confidentiality can all be safeguarded by public key encryption. Asymmetric-key algorithms include the well-known ones, RSA, ElGamal, DSS, and PGP. However, now, quantum computing can easily crack these passwords.

4. Conclusion

Generally speaking, the goal of both conventional and quantum cryptography—also referred to as quantum security or quantum encryption—is to encrypt data while maintaining its validity, security, and integrity. Nonetheless, there are other areas in which the two approaches diverge. First, conventional encryption makes use of mathematical riddles that have been intractable for billions of years on a standard computer. Discrete logarithms and the factorization of huge numbers are two examples of these problems. In a conventional encryption-protected system, its intractable nature stops unauthorized users from listening in on encrypted messages. Nonetheless, quantum communication relies on the data security offered by quantum mechanics and is based on science. In traditional encryption, a "key," which is a secret string of random numbers, is exchanged between the parties. The approach is vulnerable to security issues since its security depends on the confidentiality of the key. By utilizing the unexpected nature of matter at the quantum level (qubits) to encrypt and decrypt communications, quantum encryption guarantees more secure communication. Public Key Cryptography and Data Encryption Standard are two popular techniques for advanced conventional encryption. In the former, the communication channel's security is determined by a key made up of a lengthy, randomly selected string of bits. In the latter method, each user has two keys, public and private, that can only partially decrypt and encrypt data. The astonishing numbers generated by the combination of the encoding and the key can add to the system's complexity and cost. Furthermore, traditional numerical keys can no longer offer genuinely secure communication due to exponential improvements in processing power and the creeping approach of quantum computing. All in all, quantum communication is a new way of encryption. Although it has advantages like Unbreakable Encryption, Enhanced Security, Resistance to Quantum Computing Attacks, and Faster Data Protection. It is limited by the infrastructure requirement, the high cost of the specialized equipment and devices, and scalability. Traditional encryption is an old technology that has well-developed communication systems and methods. The sophisticated form of traditional encryption is still hard to decipher. The system of traditional encryption is more mature than quantum communication. Therefore, it takes a long time to replace traditional encryption with quantum communication. However, unquestionably, quantum cryptography is revolutionizing the field of cybersecurity. Strong and secure encryption techniques will become ever more important as quantum computing develops. Quantum cryptography promises to encrypt communications and protect data in previously unthinkable ways by utilizing the power of quantum mechanics.

References

[1] Cozzolino D. High-dimensional quantum communication: benefits, progress, and future challenges. Advanced Quantum Technologies, 2019, 2 (12): 1900038.

[2] Singh R, Bodile R. A quick guide to quantum communication. 2024.

[3] Rossi V. Cybersecurity in the quantum era: a study of perceived risks in conventional cryptography and discussion on post quantum methods. Journal of Physics: Conference Series, 2021, 1964: 042002.

[4] Quantropi. Classical vs. quantum vs. post-quantum cryptography. 2020. Available at: https://www.quantropi.com/differences-between-classical-quantum-post-quantum-cryptography/.

[5] Luo W. Recent progress in quantum photonic chips for quantum communication and internet. Light: Science & Applications, 2023, 12 (1): 161.