Issue Brief

September 2025
No : 464

Quantum Communication: The Future of Secure Information Transmission

Lt Col Pradeep Singh

Quantum Communication: The Future of Secure Information Transmission

Lt Col Pradeep Singh

Abstract

Quantum communication marks a significant advancement in secure information transfer. By harnessing the principles of quantum mechanics, it provides unprecedented levels of data protection, most notably through quantum key distribution (QKD). This article explores the core concepts of quantum communication, reviews key technological developments, and examines its diverse applications in sectors such as defense, finance, and healthcare. It also addresses the major challenges that limit large-scale adoption. The discussion concludes by emphasizing the transformative potential of quantum networks, particularly when integrated with emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT).

Keywords: quantum communication, quantum load distribution, secure information transfer, cyber security, quantum network

Introduction

Throughout history, the development of communication systems has been critical for technological progress. From the telegraph to the Internet, innovations have transformed how people exchange information. However, as the dependence on digital systems is growing, it has become an important challenge to ensure secure data transfer. Traditional encryption techniques, although effective to some extent, are increasingly vulnerable to the emergence of quantum computation (Mosca, 2018). Quantum communication, which uses principles of quantum mechanics, promises unique security levels in communication by offering almost unbreakable encryption strategies (Gisin & Thew, 2007). This article examines the basis of quantum communication, its leading principles, technological progress, applications, and the challenges it faces.

What is Quantum Communication?

Quantum communication is an emerging field that applies the laws of quantum mechanics to enable highly secure transmission of information. Unlike conventional communication, which sends data as classical bits (0s and 1s), it relies on quantum bits, or qubits, which can exist in multiple states simultaneously through a property called superposition. Another key feature is entanglement, where pairs of particles share a connected state such that changes to one instantly affect the other, even across long distances. The most practical application today is **quantum key distribution (QKD)**, which allows two parties to generate encryption keys with the guarantee that any interception attempt will disturb the quantum state and reveal the presence of an eavesdropper. While still in early stages, quantum communication is being tested for secure government, military, and financial networks, and it is expected to form the backbone of a future “quantum internet” that integrates with emerging technologies like quantum computing, artificial intelligence, and the Internet of Things (Giles, 2019).

Key Principles of Quantum Communication

Quantum call depends on a few basic ideas of quantum mechanics that set it apart from classical communication, the most (Shor & Preskill, 2000) (Schneider & Smalley, 2025)

1. **Superposition**: Qubits (quantum bits) can exist simultaneously in multiple states until they are measured. In quantum communication, this allows information to be encoded in many possible ways in a single qubit. When someone measures (or tries to intercept) a qubit in superposition, its state collapses into one of the possible outcomes this disturbance can be detected.

2. **Entanglement:** Two or more qubits can be entangled, meaning their states are strongly correlated even when separated by large distances. If one qubit of an entangled pair is affected or measured, the other qubit instantaneously reflects this change. In communication, entanglement can be used to establish secure links and to detect eavesdropping.

3. **Interference**: Since qubits in superposition can be thought of as combining multiple “paths” or “possibilities,” interference refers to the way these possibilities can reinforce or cancel each other. In quantum communication, interference helps to distinguish correct signals/information from “wrong” ones: the desirable outcomes are amplified, the undesirable ones are cancelled. This is a foundation for algorithms and protocols that aim for secure, reliable transmission.

4. **Decoherence**: Quantum states are fragile. Decoherence is when a quantum system loses its coherence i.e. when the qubit loses its quantum behaviour (superposition/entanglement) due to interaction with the environment or measurement. For quantum communication, decoherence is a big challenge, because it can degrade or destroy the quantum signals used for secure transmission. Minimizing or correcting for decoherence is essential.

5. **No-Cloning Theorem**: It is impossible to make an exact copy of an unknown quantity, which prevents undiscovered cutting.

6. **Heisenberg Principle of Uncertainty**: Measurement of certain quantum properties interferes with the system and ensures that eavesdropping experiments are demonstrable.

Quantum Key Distribution (QKD)

With the rise of quantum computing, the security of traditional cryptographic methods faces increasing uncertainty. Researchers have explored quantum-based approaches such as Quantum Key Distribution (QKD) and Quantum Cryptography (QC) as possible solutions. While these methods show theoretical promise, particularly through protocols like BB84 and E91, their practicality and long-term viability remain under debate.

Quantum Key Distribution (QKD) and Quantum Cryptography (QC) sound exciting on paper, but in practice, people approach them with caution. QKD uses the principles of quantum mechanics to create and share encryption keys, with the unique advantage of being able to spot if someone is trying to eavesdrop something traditional cryptography can't do on its own. Take the BB84 protocol from 1984, for example: it encodes keys in quantum states that change if intercepted, immediately alerting both parties. Another approach, the E91 protocol introduced in 1991, uses entangled photons and Bell's inequalities to secure key exchange.

These methods clearly show the scientific promise of QKD, but real-world use comes with significant hurdles. The technology requires highly specialized (and expensive) hardware, doesn't have built-in authentication, and even real systems have shown vulnerabilities. On top of that, QKD setups are rigid, costly to maintain, and hard to fit into today's communication networks. Post-quantum cryptography (PQC), on the other hand, is often seen as a more practical path forward. It's based on mathematical algorithms designed to withstand quantum attacks, and the best part is that it works on existing infrastructure. PQC can be updated or patched like regular software, and it scales easily across different systems. That flexibility and cost-effectiveness make it an attractive option for securing the future of digital communication.
(NSA, n.d.).

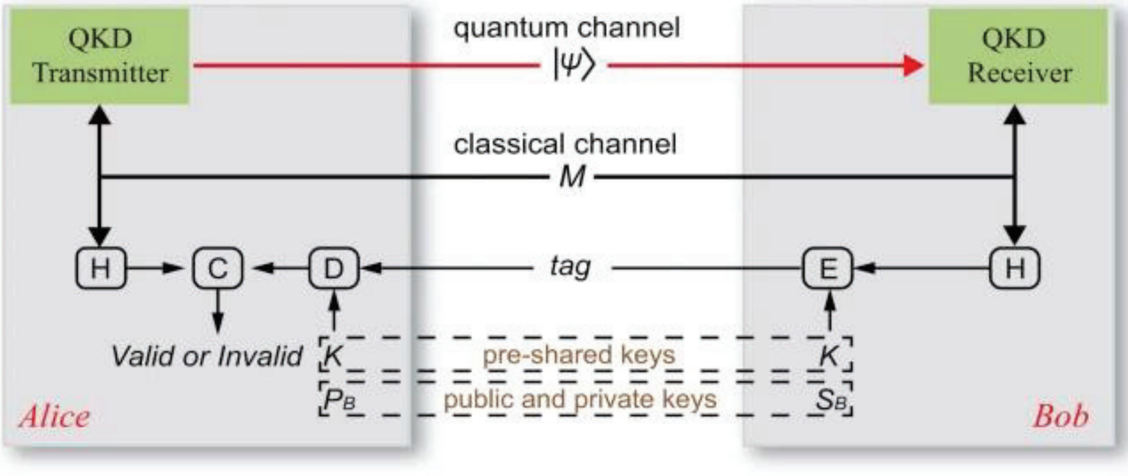

Figure 0.1 (L. J. Wang et al., 2021)
flow diagram of post-quantum cryptography authentication

Technological Advancements

In recent years, remarkable successes have been observed in quantum communication technology, paving the way for its widespread use:

Quantum Repeaters: These are essential devices designed to solve the biggest hurdle in long-distance quantum communication: signal loss. As photons (light particles) travel through optical fibers, many are absorbed or scattered, which limits secure communication to a few hundred kilometers. Unlike classical amplifiers that just boost a signal, quantum repeaters use a process called "entanglement swapping." They create a chain of shorter, entangled links that are then connected to form a single, long-distance entanglement channel. This allows a quantum signal to be faithfully extended over vast distances without being measured and destroyed, making inter-city or even cross-country fiber-optic quantum networks feasible (Briegel et al., 1998).

Satellite-based QKD (Quantum Key Distribution): While fiber optics are effective on the ground, achieving global quantum communication requires overcoming physical barriers like oceans. Satellite-based QKD is the solution. By transmitting quantum signals through the near vacuum of space, where photon loss is dramatically lower than in fiber, satellites can link ground stations thousands of kilometers apart. The groundbreaking Micius satellite, launched by China, served as a powerful proof-of-concept by successfully distributing a quantum key between continents (Yin et al., 2017). This demonstrated the viability of building a secure, global communication network protected by the laws of quantum physics (Liao et al., 2017).

Integrated Photonics: Early quantum communication experiments involved large, expensive, and delicate equipment spread across an entire optical table. Integrated photonics revolutionizes this by shrinking all the necessary components such as single-photon sources, beam splitters, and detectors onto a single, compact microchip. These "photonic integrated circuits" (PICs) are not only vastly smaller but also more stable, energy-efficient, and cheaper to produce. This miniaturization is a critical step for moving quantum communication from the laboratory to the real world, enabling its integration into everyday devices like servers, network cards, and eventually even personal electronics (J. Wang et al., 2020).

Quantum Networks: Recognizing the future threat posed by quantum computers to current encryption standards, nations and large corporations are investing heavily in building dedicated quantum communication infrastructures. These networks connect multiple quantum devices to create a web of unconditionally secure links. The primary goal is to safeguard critical sectors such as government, defense, finance, and energy grids from espionage. By establishing these secure backbones, authorities can ensure the long-term confidentiality of sensitive data and create a foundation for the future “quantum internet”(Wehner et al., 2018).

Applications for Quantum Communication

Quantum conversation holds excellent capacity throughout many sectors, a few of them are as below:

Secure Government and Military Communication: For government and military operations, maintaining absolute confidentiality is paramount. Given the rise of sophisticated cyberattacks, often from state-level adversaries, traditional encryption methods face future threats from advances in computing. Quantum communication offers a solution with security guaranteed by the laws of physics. By using techniques like Quantum Key Distribution (QKD), military and government agencies can create and share encryption keys in a way that makes eavesdropping impossible without being detected. This ensures that classified data, strategic communications, and

command-and-control signals are protected from interception and tampering, providing an unparalleled level of security for national secrets and defense operations (Naseer Alsarmi, 2025).
Financial Sector: The financial industry is built on trust and the secure handling of incredibly sensitive information. A single breach can lead to catastrophic losses and erode public confidence. Quantum communication can fortify this sector against even the most advanced hacking threats. By implementing quantum networks between data centers and branches, banks and financial institutions can secure transactions, client account information, and proprietary trading data with encryption that is provably unbreakable. This technology would render "harvest now, decrypt later" attacks useless, as data intercepted today would remain secure even against the quantum computers of the future, ensuring the long-term integrity and confidentiality of the global financial system (Jančiūtė, 2025).

Healthcare Services: Patient data is among the most personal and private information and protecting it is a legal and ethical obligation. The healthcare industry relies on the rapid exchange of this data between hospitals, clinics, labs, and insurers. Quantum communication can create ultra-secure channels for transmitting these sensitive medical records. This would drastically reduce the risk of unauthorized access, which can lead to identity theft, fraud, and violations of patient privacy. By ensuring that the transmission of electronic health records, imaging data, and genomic information is fundamentally secure, quantum networks can uphold patient confidentiality and build a more trustworthy digital health ecosystem (Ur Rasool et al., 2023).

Blockchain and Cryptocurrency: The security of most current blockchain and cryptocurrency networks relies on cryptographic algorithms that could one day be broken by a sufficiently powerful quantum computer. This "quantum threat" poses a significant risk to the long-term viability of digital assets and decentralized ledgers. Quantum communication offers a powerful defense. By integrating QKD to distribute keys or by creating new quantum-resistant cryptographic protocols, blockchain networks can be future-proofed. This would secure the process of validating transactions and maintaining the integrity of the distributed ledger, protecting digital assets and blockchain-based systems from being compromised by the arrival of quantum computing.

Challenges and Limitations

Technological Complexity and Infrastructure - A primary hurdle in the widespread deployment of quantum communication is its immense technological complexity. Building a robust quantum network requires more than just laying optical fiber; it necessitates sophisticated infrastructure, the most critical of which are quantum repeaters. Unlike classical amplifiers, these devices are at the cutting edge of physics and engineering, designed to extend quantum signals over long distances without destroying their fragile quantum states. Developing, manufacturing, and maintaining such advanced hardware demands not only massive financial investment but also a workforce with highly specialized expertise in quantum physics and precision engineering, creating a significant barrier to entry.

The Role of Integrated Photonics - Integrated photonics stands out as a key enabling technology that directly addresses the challenges of complexity, cost, and scale. Early quantum communication systems were bulky, expensive setups confined to laboratory environments. By shrinking the necessary optical components like photon sources, interferometers, and detectors onto a single microchip, photonic integrated circuits (PICs) create miniaturized, stable, and energy-efficient quantum systems. This transition from the lab bench to the chip is crucial for making quantum communication practical and commercially viable, paving the way for its integration into existing network hardware, data centers, and eventually, everyday electronic devices.

The Challenge of Global Scalability - For quantum communication to evolve from isolated national networks into a truly global "quantum internet," significant non-technical challenges must be overcome. Technology alone is not enough; international cooperation is essential. This requires the development and adoption of universal standards and protocols to ensure that hardware and software from different countries are interoperable. Furthermore, a framework of international regulations and agreements is necessary to govern the secure exchange of data across borders, establish trust between nations, and manage the shared operation of a global infrastructure. Without this worldwide consensus, the full potential of a secure, interconnected quantum network cannot be realized.

The Future of Quantum Communication

The future of quantum communication seems promising, with global efforts for the development of practical systems. As several countries invest in quantum techniques, quantum communication can be mainstream in one or two decades. Future global quantum data can revolutionize security and provide uninterrupted levels of uniform encryption for authorities, financial institutions, and private individuals. Combining quantum communication with other new technologies, such as artificial intelligence (AI) and Internet of Things (IoT), can lead to safer and reliable communications networks that provide improved opportunities for secure data transfer in industries.

Conclusion

Quantum communication represents an advance in the transmission of secure information. Although technological and infrastructure challenges persist, rapid QKD progress, integrated satellite and photonic-based systems are paving the way for a safe quantum internet. Governments, financial institutions, and defense organizations are already exploring their implementation, signaling a future change towards networks with quantum safety.

References

Briegel, H. J., Dür, W., Cirac, J. I., & Zoller, P. (1998). Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Physical Review Letters*, *81*(26), 5932. https://doi.org/10.1103/PhysRevLett.81.5932

Giles, M. (2019, February 14). *Explainer: What is quantum communication?* MIT Technology Review. https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/

Gisin, N., & Thew, R. (2007). Quantum communication. *Nature Photonics*, *1*(3), 165–171. https://doi.org/10.1038/NPHOTON.2007.22;KWRD

Jančiūtė, L. (2025). Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework. *International Cybersecurity Law Review 2025 6:2*, *6*(2), 145–154. https://doi.org/10.1365/S43439-025-00135-7

Liao, S. K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., Yin, J., Shen, Q., Cao, Y., Li, Z. P., Li, F. Z., Chen, X. W., Sun, L. H., Jia, J. J., Wu, J. C., Jiang, X. J., Wang, J. F., Huang, Y. M., Wang, Q., … Pan, J. W. (2017). Satellite-to-ground quantum key distribution. *Nature*, *549*(7670), 43–47. https://doi.org/10.1038/NATURE23655;TECHMETA

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security and Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

Naseer Alsarmi, H. S. (2025). Strategic Review of Quantum Capabilities in Military and National Cyber Defense. *Proceedings of the 2025 3rd International Conference on Inventive Computing and Informatics, ICICI 2025*, 1556–1562. https://doi.org/10.1109/ICICI65870.2025.11069595

NSA. (n.d.). *Quantum Key Distribution (QKD) and Quantum Cryptography QC*. National Security Agency. Retrieved September 15, 2025, from https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Schneider, J., & Smalley, I. (2025, June 10). *What Is Quantum Computing?* IBM. https://www.ibm.com/think/topics/quantum-computing

Shor, P. W., & Preskill, J. (2000). Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, *85*(2), 441. https://doi.org/10.1103/PhysRevLett.85.441

Ur Rasool, R., Ahmad, H. F., Rafique, W., Qayyum, A., Qadir, J., & Anwar, Z. (2023). Quantum Computing for Healthcare: A Review. *Future Internet 2023, Vol. 15, Page 94*, *15*(3), 94. https://doi.org/10.3390/FI15030094

Wang, J., Sciarrino, F., Laing, A., & Thompson, M. G. (2020). Integrated photonic quantum technologies. *Nature Photonics*, *14*(5), 273–284. https://doi.org/10.1038/S41566-019-0532-1;SUBJMETA

Wang, L. J., Zhang, K. Y., Wang, J. Y., Cheng, J., Yang, Y. H., Tang, S. B., Yan, D., Tang, Y. L., Liu, Z., Yu, Y., Zhang, Q., & Pan, J. W. (2021). Experimental authentication of quantum key distribution with post-quantum cryptography. *Npj Quantum Information 2021 7:1*, *7*(1), 1–7. https://doi.org/10.1038/S41534-021-00400-7

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, *362*(6412). https://doi.org/10.1126/SCIENCE.AAM9288

About the Author

Lt Col Pradeep Singh is an alumni of Indian military academy. Commissioned into Regt of Artillery. He has served various terrains of the country. He is an M.Sc (Tech) and has done Post graduate diploma in business management in Information technology and system management from NMIMS. He has done various courses in AI, ML and AR/VR from various online platforms. He has done instructor in school of artillery. He has had the opportunity to serve in UN in Democratic Republic of Congo..

The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.