Gartner®

Innovation Insight for Quantum Communication in China

Published 23 June 2021 - ID G00746959 - 7 min read

By Analyst(s): Arnold Gao, Daniel Sun, Owen Chen

Initiatives: Technology Innovation

China has included quantum technologies in its 14th Five-Year Plan, and leads in quantum communication research. Enterprise architecture and technology innovation leaders must understand the potential of this emerging technology to capture the innovation opportunities for their organizations.

Additional Perspectives

- Summary Translation + Localization: Innovation Insight for Quantum Communication in China
(22 July 2021)

Overview

Key Findings

- Quantum communication refers to the novel communication technologies that apply laws of quantum physics — including quantum superposition and quantum entanglement to protect data during transportation.

- In the quantum communication domain, quantum key distribution (QKD) has received more attention, as it can provide tamper evident remote secure key distribution to deal with the challenges driven by the emergence of quantum computing to the existing security architecture.

- QKD is not yet commercially viable before it can realize long-distance and secure quantum communication under realistic conditions.

- Quantum safe cryptography (QSC), which refers to encryption algorithms designed to be safe against quantum computers, also challenges the necessity of QKD.

Recommendations

Enterprise architecture and technology innovation leaders must:

- Evaluate the immediate and future business impact of quantum key distribution to their industry and organization by understanding the potential use cases described in this research.
- Discuss the postquantum security with business stakeholders to evaluate the timetable of adopting quantum key distribution by assessing the technology feasibility, organizational readiness and employee skills.
- Work with security and risk management leaders to proactively monitor the development progress, and the risks of QKD and QSC to determine the most commercially viable solution.

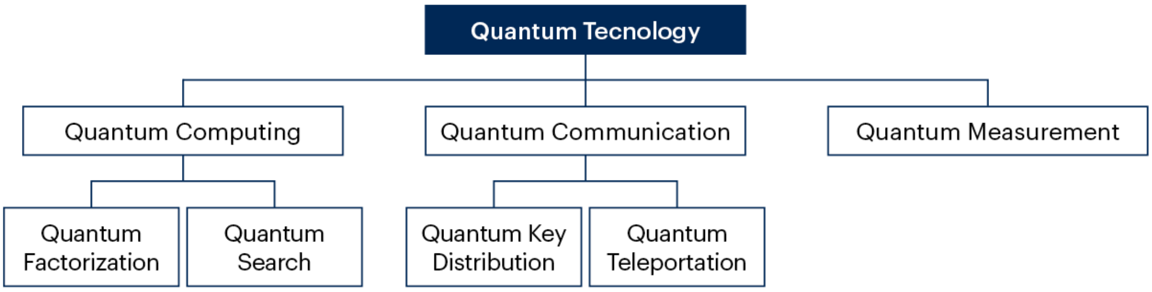
Introduction

Quantum technologies offer disruptive potential for communication, although they are not yet fully commercially viable. Quantum computing, quantum communication and quantum measurement are examples of quantum technologies. Many people have certain knowledge about quantum computing, but few are aware of quantum communication and its disruptive potential. Around the globe, China is a leading player in quantum communication research and has demonstrated the potential business values through certain use cases that cannot be ignored by digital leaders.

This research aims to introduce the definition and latest development progress of quantum communication, its business impacts and risks for future adoption (see Figure 1).

Figure 1: Quantum Technologies

Quantum Technologies



Source: Gartner
746959_C

Description

Quantum communication applies laws of quantum physics — including quantum superposition and quantum entanglement to protect data during transportation. The security of quantum communication is guaranteed by basic principles of quantum mechanics, such as the quantum unclonability theorem. At the current stage, quantum key distribution (QKD) and quantum teleportation are the most common techniques of quantum communication.

In the quantum communication domain, QKD has received more attention as it can provide tamper evident remote secure key distribution, guaranteed by the laws of quantum mechanics. Technically, QKD is a technology that uses quantum physics to secure the distribution of symmetric encryption keys. After the first QKD protocol BB841 was proposed by Bennett and Brassard in 1984, it attracted great attention with various schemes and applications.

China is a leading player in quantum communication and in particular in QKD research and application. In 2016, it launched the world's first quantum communication satellite (Micius) and achieved QKD by beaming photons between the satellite and two ground stations with a distance of 1,200 km.

In 2017, researchers of the University of Science and Technology of China have led the efforts to complete an over 2,000 km long optical fiber network for QKD between Beijing and Shanghai, with 32 trusted nodes through Jinan, Hefei and other cities.

In 2021, the Chinese research team established the world's first integrated space-to-ground quantum communication network. It combines over 700 fiber QKD links and two high-speed satellite-to-ground free-space QKD links to achieve quantum key distribution over a total distance of 4,600 km for users across the country.

Benefits and Uses

A security solution is only as strong as its weakest link, and in the existing cryptography of network communication, the weakest link is the secret symmetric key distribution based on public key infrastructure (PKI).

The emergence of quantum computing will become an increasing challenge to the PKI security architecture. Google's Craig Gidney and KTH's Martin Ekera have demonstrated that a quantum system could crack 2,048-bit RSA encryption with 20 million quantum bits (qubits) in only eight hours — rather than requiring 1 billion qubits as previously theorized. [1] Although a 20 million qubits quantum system seems very distant, as today's state-of-the-art quantum computers only have less than 100 qubits, we expect an exponential growth of qubits in the next few years. For example, IBM planned a 1,121-qubit quantum processor for 2023 [2], Google planned to build an error-corrected computer with 1 million physical qubits by 2029. [3] Therefore, enterprise architecture and technology innovation leaders must be prepared for the future when the existing cryptography can no longer ensure the security of communication and the protection of long-lived data.

QKD offers unconditional, future-proof communication to deal with the challenge. According to the basic principles of quantum mechanics, the cryptographic keys are transferred by transmitting photons that are impossible to copy and store. Once the QKD link has been established, it theoretically cannot be hacked. This is an important advantage over current PKI, as QKD eliminates the possibility of intercepting the public keys during communication and decrypting them at a future date by quantum computing or other advanced decryption algorithms — when they are commercially viable.

QKD is valuable for use cases that require data secrecy for many years. In the public sector, communications between government bodies or the military may need to be kept secret for 20 years. If the communication is encrypted by RSA, retrospective decryption can jeopardize national security. QKD is also suitable for financial institutions that need to store financial and customer data, or for agencies dealing with health records and/or human genome data in the life-science industry.

China has already conducted a number of experiments as proof of concept projects by applying QKD:

Industrial and Commercial Bank of China adopted quantum encrypted transmission of Beijing-Shanghai Internet Banking remote data via the quantum communication technology. It was the first application of the 1,000-km-level quantum communication technology in the banking industry, and also an important milestone for the industrial application of quantum communication technology in China.

Huishang Bank in China's Anhui Province uses QKD between its main data center and its backup center. The bank has also applied quantum encryption to transmit digital certificates between its branches and the China Financial Certification Authority (CFCA), ensuring the security of certificate issuance management.

Hainan province has set up a demonstration project, which adopts the quantum cryptography technology employed by the Micius satellite to secure transmissions between the government's data center, the Industrial and Commercial Administration Bureau's provincial science and technology unit, and the local Human Resources and Social Security Department.

Risks

From theory to practical application, there are still many challenges to realize long-distance and secure quantum communication under realistic conditions. Channel loss and detector noise restrict the scope of application of quantum key distribution. How to obtain a higher coding rate (i.e., key generation rate) and a longer key transmission distance remains a problem that must be solved urgently.

During the journey of realizing secure and practical quantum communication, various theoretical ideas and experimental schemes have been continuously proposed — from the earliest BB841 protocol to the recent measurement-device-independent QKD (MDI-QK) protocol and twin-field quantum key distribution (TF-QKD). However, the foundational research on quantum communication networks is still in the open exploration stage, while solutions and technical directions have not yet converged for large-scale commercial adoption.

In addition, quantum safe cryptography (QSC), which refers to communication algorithms designed to be safe against quantum computers, is challenging the necessity of QKD. The National Institute for Standards and Technology (NIST) has hosted several rounds of competitions to identify the most promising QSC protocol since 2016 and aims to establish new standards for quantum-safe communications. After reducing the initial pool of 69 candidate protocols, seven have become the third round finalists, with eight alternative candidates. It is expected that, in 2022, the standards of QSC algorithms will be finalized. Therefore, it is likely that QSC will first become the mainstream technology for future communication, which poses a significant challenge to the development of QKD.

Recommendations

Enterprise architecture and technology innovation leaders must:

- Evaluate the immediate and future business impact of quantum key distribution to their industry and organization by understanding the potential use cases described in this research.

- Discuss the postquantum security with business stakeholders to evaluate the timetable of adopting quantum key distribution by assessing the technology feasibility, organizational readiness and employee skills.

- Work with security and risk management leaders to proactively monitor the development progress and the risks of QKD and QSC to determine the most commercially viable solution.

Evidence

[1] How Quantum Computer Could Break 2,048-Bit RSA Encryption in 8 Hours, Communications of the ACM.

[2] IBM's Roadmap For Scaling Quantum Technology, IBM.

[3] Google Goal: Build an Error Corrected Computer With 1 Million Physical Qubits by the End of the Decade, Quantum Computing Report.

[4] Quantum Key Distribution: Advantages, Challenges and Policy, Cambridge University Science and Policy Exchange.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Venture Capital Growth Insights: Post-Quantum Cryptography

Predicts 2021: Disruptive Potential During the Next Decade of Quantum Computing