From Quantum Computing to Quantum Communications

As Published: https://doi.org/10.1145/3571450

Publisher: ACM|Communications of the ACM

Persistent URL: https://hdl.handle.net/1721.1/147698

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

DOI:10.1145/3571450

Michael A. Cusumano

Technology Strategy and Management

From Quantum Computing to Quantum Communications

Attempting to disentangle mechanical principles.

QUANTUM COMPUTING HAS been slowly progressing both as a technology and potential new platform business (see my previous column, "The Business of Quantum Computing," *Communications*, Oct. 2018). But another application of quantum mechanics that has attracted increasing attention is quantum communications.[12] In fact, the 2022 Nobel Prize in Physics was awarded last October to three scientists for their experiments proving the reality of quantum entanglement, which is fundamental to quantum cryptography and secure communications.[11] How did we get from quantum computing to quantum communications, and what is the business potential?

The same two physical phenomena that inspired quantum computing motivate quantum communications. The first is *superposition*. A quantum bit or "qubit" can behave as a wave as well as a discrete particle and exist in "superpositions" of states. That turns out to be the equivalent of 0, 1, or both simultaneously, rather than just 0 or 1, as in a digital computer. This characteristic as well as *quantum interference* (similar to how waves can amplify or "interfere" with each other) are fundamental to how quantum computers can potentially achieve exponential increases in computing power. The second is *entanglement*. This is the ability of two quantum particles (such as one photon split into two) to become connected and form a "system." The system pair can retain the specific correlations of the individual particles (such as a positive or negative spin in their energy states, which can translate into 0 or 1), even when physically separated.

Here is a simple model of how quantum communications works, using a basic quantum key distribution (QKD) method: Party A generates a "one-time pad"—a random cryptographic key used only once for each message transmitted—by measuring pairs of entangled photons. Party A uses the key to encrypt the information using conventional techniques and then sends the key bit-by-bit using entangled photons via a fiber-optic cable to Party B. Party B measures some of the entangled photons to determine if they have the correct key. If anyone or anything has interfered with the key generation or transmission, then the correlation of the entangled photons will have changed (such as from positive to negative) and the key will become invalid. The communication is secure because sender and receiver each randomly choose their measurement bases, and only when they choose the same measurement base will the results be valid for the key, which they use only once. There could still be errors in the transmission, but it is possible to calculate the expected error rate and to estimate if there has been an attempt at hacking. The sender and receiver also can repeat the transmission of the encryption keys multiple times until they are sure transmission of the key has been secure.[8,9]

Both quantum computing and quantum communications have attracted

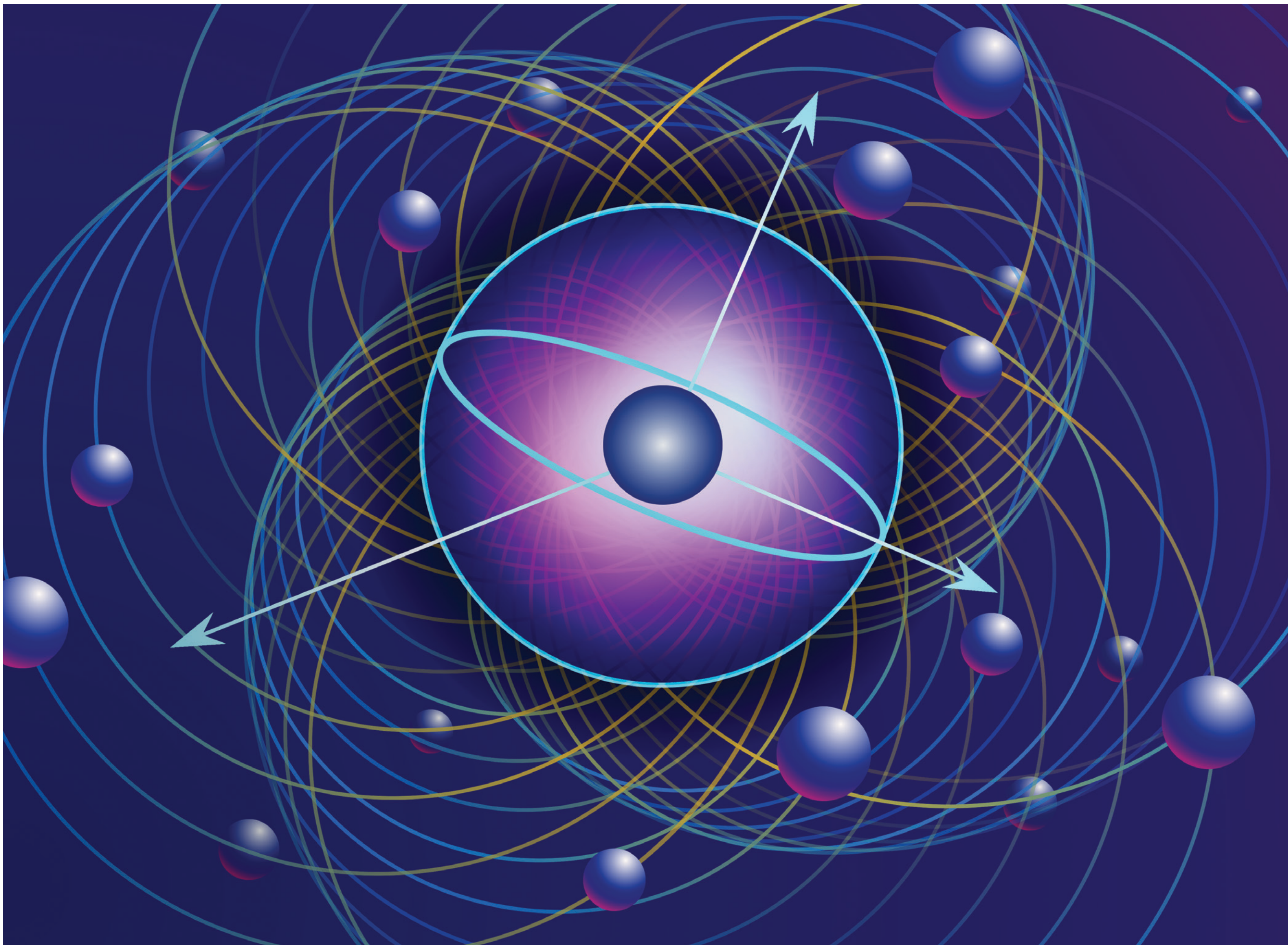

IMAGE BY ANATOLII STOIKO

skepticism because they rely on the strange properties described by quantum mechanics. In particular, Albert Einstein and his co-authors, in a 1935 paper, called entanglement "spooky action at a distance."[7] How one entangled particle knows what the other is doing *seems* to transfer information instantly—faster than the speed of light, which would contradict Einstein's Theory of Special Relativity. The concept remained controversial until John Bell in 1964 showed how to determine if entanglement was real or not.[3] Multiple experiments over 50 or so years, led by the winners of the 2022 Nobel Prize in Physics, have proven entanglement and every other prediction of quantum mechanics *are* real.[6,14]

Scientists also have concluded there is no paradox or conflict with the speed of light because entanglement involves no transmission of information. Entangled particles apparently share a more fundamental physical correlation than we can describe with our classical concepts of space and time. The distance between entangled particles functioning as a system is theoretically irrelevant; they share random properties and exhibit them in tandem, instantly. Quantum communication exploits these phenomena, though it also requires conventional communication. Sender and receiver still need to compare and confirm their measurements of the entangled photons after the transmission, and this exchange of information cannot occur faster than the speed of light.

Both quantum computing and quantum communications have attracted skepticism because they rely on the strange properties described by quantum mechanics.

In a now-famous 2017 experiment, researchers at the University of Science and Technology in China split photons into entangled pairs and then retained the entanglement across 300 miles of an optical fiber network connecting ground stations as well as 1,200 miles between ground stations and a satellite.[5,16] The Chinese also used the satellite to facilitate a QKD-encrypted videoconference between Beijing and Vienna. The network used 32 special repeaters to decrypt the quantum keys into conventional code and then re-encrypt them each time into entangled quantum states.[9] The Chinese effort demonstrated the concept; commercial quantum cryptography must overcome several hurdles.

First, fiber-optic cables, which are

Venture capital-funded quantum communications and networking startups.

Product Stage

- IDQ; https://www.idquantique.com/ (QKD and quantum random number generation)
- Quantum Xchange; https://quantumxc.com/ (QKD and data encryption)
- KETS; https://kets-quantum.com/ (QKD on a photonics chip)
- QRate; https://goqrate.com/ (QKD and quantum random number generation)
- Quibetekk; https://qubitekk.com/ (entangled photon with integrated laser)
- Single Quantum; https://singlequantum.com/ (superconducting nanowire single photon detector)
- QApp; https://en.qapp.tech/ (quantum-resistant algorithms for post-quantum cryptography)
- Quantum C-Tek; http://www.quantum-info.com/ (QKD networking equipment)

Prototype Stage

- NuQuantum; https://nu-quantum.com/ (single photon manipulation)
- Quside; https://quside.com/ (quantum random number generation)
- Qunnect; https://int.quconn.com/ (room-temperature quantum memory and photon networking)
- Cryptonext Security; https://cryptonext-security.com/ (post-quantum cryptography)
- Qunu Lab; https://www.qnulabs.com/ (QKD and quantum random number generation)
- Go-Quantum; https://goquantum.tech/ (post-quantum data transmission devices)

Source: Compiled from data in Lepskaya, M. "Will Quantum Computing Remain the Domain of the Specialist VC?" *TechCrunch* (Jan. 18, 2022), and company websites.

used for most QKD systems, absorb some photons over distance, generally limiting the range of one signal to a few tens of kilometers. This signal degradation occurs with conventional messages sent over fiber-optic cables as well. The solution for conventional messaging has been to install digital repeaters that copy, amplify, and then relay the signal. But quantum information—here, the state of the entangled quantum bits—is unknown and so there is nothing for a conventional digital repeater to copy or amplify. As the Chinese did, it is possible to translate the quantum key into digital bits and then repeat the quantum cryptography process and create new quantum crypto keys. The problem here, though, is that decrypted keys in each repeater can become targets for hackers. Researchers are developing quantum repeaters that maintain or reestablish the quantum state of the keys, though no one as of yet has a working system.[9]

Even though the key is quantum-encrypted and secure, the data is conventionally encrypted and, like decrypted keys, can become the target of hackers.

Second, current QKD systems transmit the main data over a conventional network such as the Internet. Even though the key is quantum-encrypted and secure, the data is conventionally encrypted and, like decrypted keys, can become the target of hackers.[9]

Third, conventional (digital) random number generators may not be truly random. This remains a problem for cryptography in general.[13] If they are used in a hybrid quantum and classical communications system, then security is potentially compromised. By contrast, quantum random numbers generated from, for example, the superposition of photons, appear to be truly random. This is why quantum cryptography must deploy quantum random number generators along with the one-time pad method in order to offer a truly secure communications platform.[4]

A broader solution is to create a "quantum Internet" where both the data transmitted and the encryption keys at all stages use quantum information.[10] There is progress here as well. For example, researchers at the University

A broader solution is to create a "quantum Internet" where both the data transmitted and the encryption keys at all stages use quantum information.

of Chicago have transmitted quantum-encrypted information directly through entangled particles, without fiber-optic cables, using photons as well as sound particles called phonons. Their experiment has worked across one meter, and potentially the distances could be much longer. However, the Chicago system must be kept at only a few degrees above absolute zero, limiting its practicality.[1]

AT&T, BT, Fujitsu, HP, Huawei, IBM, Mitsubishi, NEC, NTT, Toshiba, and Raytheon are the leaders among established firms researching quantum networks, usually in partnerships with other firms, universities, and governments. For example, BT has joined the University of Cambridge and several other academic institutions and firms, led by Toshiba Europe, to build a trial QKD network, with funding from the U.K. government.[a] Startups are also very active. *TechCrunch* recently listed nine venture-backed companies with products already on the market and six others with prototypes (see the accompanying table). The product functionality may be only in the proof-of-concept stage, but the overall approach seems promising: Create QKD appliances and networking equipment using photons and (if possible) operating at room temperature. Meanwhile, continue investing in quantum random number generators and other technology for quantum networks and data transmission.

The quantum cryptography market in 2021 already generated revenues of approximately $100 million and was estimated to reach $476 million by 2030.[15] McKinsey also estimates the total quantum communications market could generate as much as $8 billion in revenue by 2030.[2] This forecast may be wildly optimistic and will require researchers to overcome daunting technical hurdles within the next few years. Still, as with quantum computing, there seems to be no shortage of interest and investment.

We may still want to describe entanglement as "spooky action at a distance." However, as with other quantum phenomena and even gravity itself, scientists and engineers do not have to understand *why* a phenomenon exists. They can still identify mechanical principles and use their understanding of *how* the world works to run experiments and—eventually—build new products and services. C

a See https://bit.ly/3UBFW6Q

References

1. Ashford, E. New techniques improve quantum communications, entangle phonons. *University of Chicago News* (June 17, 2020).
2. Batra, G. et al. Shaping the long race in quantum communication and quantum sensing. *McKinsey.com* (Dec. 21, 2021).
3. Bell, J.S. On the Einstein Podolsky Rosen Paradox. *Physics 1*, 3 (1964), 195–200.
4. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature 556* (2018), 223–226.
5. Billings, L. China shatters 'spooky action at a distance' record, preps for quantum Internet. *Scientific American* (June 15, 2017).
6. Brubaker, B. How Bell's Theorem proved 'spooky action at a distance' is real. *Quanta Magazine* (July 20, 2021).
7. Einstein, A. et al. Can quantum-mechanical description of physical reality be considered complete? *Physics Review 47* (1935), 777–780.
8. Gillis, A. Quantum key distribution (QKD). *TechTarget.com* (Jan. 2020).
9. Giles, M. Explainer: What is quantum communication? *MIT Technology Review* (Feb. 14, 2019).
10. Gyongyosi, L. and Imre, S. Advances in the quantum Internet. *Commun. ACM 85*, 8 (Aug. 2022), 52–63.
11. Kwai, I. et al. Nobel prize in physics is awarded to 3 scientists for work exploring quantum weirdness. *The New York Times* (Oct. 5, 2022).
12. Lepskaya, M. Will quantum computing remain the domain of the specialist VC? *TechCrunch* (Jan. 18, 2022).
13. Mandich, D. 'Random' might not be as random as you think. Forbes.com (Sept. 29, 2021).
14. Popkin, G. Einstein's 'spooky action at a distance' spotted in objects almost big enough to see. *Science* (Apr. 25, 2018).
15. Verified Market Research. Quantum cryptography market size worth $476.83 million, globally, by 2030 at 18.67% CAGR. *Prnewswire.com* (Aug. 18, 2022).
16. Wapner, J. Cybersecurity attacks are a global threat. Chinese scientists have the answer: Quantum mechanics. *Newsweek* (June 15, 2017).

Michael A. Cusumano (cusumano@mit.edu) is a professor and Deputy Dean at the Massachusetts Institute of Technology Sloan School of Management, Cambridge, MA, USA, coauthor of *The Business of Platforms* (2019), and a member of the MIT Center for Quantum Engineering (https://cqe.mit.edu/).

The author thanks Will Oliver of MIT for his detailed explanations and help with the text. Ganesh Vaidyanathan also provided comments.