Engineering 5 (2019) 353–354

Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

News & Highlights

Quantum Cryptography via Satellite

Mitch Leslie

Senior Technology Writer

As it circled the Earth one night in 2017, the Chinese satellite Mozi, also called Micius, aimed a laser at a ground station in northeastern China (Fig. 1). Then, as it traveled toward Europe and into range, it directed a beam at a different receiver in Austria. These transmissions, delivered to sites 7600 km apart, were noteworthy because they marked the first time a satellite had relayed secret quantum keys for decrypting and viewing messages. With the keys, scientists in China and Austria were able to exchange and decipher encrypted images. And on 29 September 2017, the researchers used the system to set up an encrypted 75-minute video conference between members of the Chinese Academy of Sciences in Beijing and their counterparts at the Austrian Academy of Sciences in Vienna [1].

Mozi's performance of quantum key distribution (QKD) revealed that satellites can dramatically extend the range of the next-generation quantum communications networks that many countries and companies are building to ensure future digital security. The project's success demonstrated that satellite-based quantum cryptography, or encryption based on quantum principles, could allow users around the globe to use the technology to securely exchange data over long distances [2]. "This is definitely a breakthrough in quantum communication," said Eleni Diamanti, a quantum physicist at the Sorbonne University.

Quantum cryptography is becoming necessary because another nascent technology, quantum computers, threatens the encryption that now safeguards online financial transactions, cellphone calls and texts, and many other types of communications [3]. To deter snoopers, the public key encryption procedure that currently protects many of these transmissions requires two keys. Although anyone can access the public key, hackers cannot decipher communications they intercept because they lack the private key [4].

Breaking keys is extremely difficult since it involves factoring enormous numbers into prime numbers or solving other complex mathematical problems. However, conventional computers have compromised some widespread encryption keys, including an early standard for e-commerce [5]. Because they would be many times faster than today's machines, quantum computers would make cracking these keys much easier. Security experts predict that a speedy quantum computer could break 1024-bit Rivest–Shamir–Adleman (RSA) encryption, one of today's standards, in less than a day [6]. No quantum computer prototype currently has that capability, but their power is doubling about every six months, said Jonathan Dowling, a theoretical physicist at Louisiana State University.

Fig. 1. Image of the actual Mozi satellite under construction/testing. Credit: Cai Yang/Xinhua via ZUMA Wire.

Communication networks that rely on quantum cryptography would have improved security since they encode the keys necessary to decrypt messages in streams of photons. The advantage is that, because of the rules of quantum behavior, these keys have a built-in alarm. If an eavesdropper intercepts the key and passes on a copy, the key changes, alerting legitimate users that their key has been stolen [7]. If the sender and recipient can confirm that the quantum key has arrived safely, however, they can then securely exchange encrypted messages over conventional channels, said Dowling. "A message can be sent over cell phone, the Internet, or smoke signals, and it's secure."

Although some land-based quantum networks are already operating, satellites may overcome their biggest limitation: transmissions that fade within the distance of several hundred kilometers [1]. The world's longest terrestrial quantum network began operating in 2017 and stretches more than 2000 km from Shanghai to Beijing. The network tackles the distance problem with 32 so-called trusted nodes that share quantum keys with adjacent nodes, a mechanism that still poses some security risks [8,9]. In contrast,

https://doi.org/10.1016/j.eng.2019.04.006

satellite signals move mostly through space and weaken more slowly, so they can transmit quantum keys farther [2].

Physicist Jian-Wei Pan of the University of Science and Technology of China worked with his former PhD adviser Anton Zeilinger, a quantum physicist of the University of Vienna and a senior scientist at the Austrian Academy of Sciences (hence the China–Austria connection), and other researchers to develop the QKD technology and show that Mozi, which was launched in 2016, could send quantum keys from up to 1200 km away to the ground stations [1]. After relaying the keys, the satellite had done its job; the encrypted images and video shared between Austria and China traveled over conventional networks. This work was "a great technical achievement," said Charles Clark, a co-director of the Joint Quantum Institute at the University of Maryland.

Pan and his colleagues plan to launch more satellites that will improve on Mozi's performance [1]. In addition, other countries and organizations have launched or intend to launch QKD-capable satellites [10]. Still, "there's a long way to go until this compares with ground-based communication," said Clark. For example, Mozi could only transmit at night, and its low-Earth orbit meant that it was out of range of the ground stations much of the time [2].

Diamanti and Dowling suggested that the next development in quantum communications could be flotillas of nanosatellites. Cheap to produce and launch in large numbers, each smartphone-sized device would transmit data with the equivalent of a laser pointer, Dowling said. Such nanosatellite-based networks could efficiently perform the necessary QKD to enable highly secure long-distance communications on a global scale.

References

[1] Liao SK, Cai WQ, Handsteiner J, Liu B, Yin J, Zhang L, et al. Satellite-relayed intercontinental quantum network. Phys Rev Lett 2018;120(3):030501.
[2] Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, et al. Satellite-to-ground quantum key distribution. Nature 2017;549:43–7.
[3] Metz C, Zhong R. The race is on to protect data from the next leap in computers. And China has the lead [Internet]. New York: The New York Times; 2018 Dec 3 [cited 2019 Feb 28]. Available from: https://www.nytimes.com/2018/12/03/technology/quantum-encryption.html.
[4] Mann CC. A primer on public-key encryption. The Atl [Internet] 2002 Sep [cited 2019 Feb 28]:[about 1 p.]. Available from: https://www.theatlantic.com/magazine/archive/2002/09/a-primer-on-public-key-encryption/302574/.
[5] Cavallar S, Dodson B, Lenstra AK, Lioen W, Montgomery PL, Murphy B, et al. Factorization of a 512-bit RSA modulus. In: Preneel B, editor. Advances in cryptology—EUROCRYPT 2000. Berlin: Springer; 2000. p. 1–18.
[6] National Academies of Sciences, Engineering, and Medicine, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Intelligence Community Studies Board, Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing. Quantum computing: progress and prospects. Grumbling E, Horowitz M, editors. Washington, DC: The National Academies Press; 2018.
[7] Chen S. Why this intercontinental quantum-encrypted video hangout is a big deal [Internet]. San Francisco: Wired; 2018 Jan 20 [cited 2019 Feb 28]. Available from: https://www.wired.com/story/why-this-intercontinental-quantum-encrypted-video-hangout-is-a-big-deal/.
[8] Giles M. The man turning China into a quantum superpower. MIT Technol Rev [Internet] 2019;(1) [cited 2019 Feb 28]:[about 2 p.]. Available from: https://www.technologyreview.com/s/612596/the-man-turning-china-into-a-quantum-superpower/.
[9] Courtland R. China's 2000-km quantum link is almost complete. IEEE Spectr 2016;53(11):11–2.
[10] Khan I, Heim B, Neuzner A, Marquardt C. Satellite-based QKD. Opt Photonics News 2018;29(2):26–33.