Contents lists available at ScienceDirect

Engineering

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

News & Highlights

量子卫星密码技术

Mitch Leslie

Senior Technology Writer

2017年的一个晚上，当中国卫星墨子号（Mozi），又称Micius，在地球上空盘旋时，它将激光器瞄准了中国东北部的一个地面站（图1）。然后，当它前往欧洲并进入射程时，它将激光射束指向了奥地利的另一个接收器。这些发送到距离中国7600 km远的地方的传输信号是值得注意的，因为它们标志着一颗卫星第一次传递了用于解密和查看信息的秘密量子密钥。借助这些密钥，中国和奥地利的科学家能够交换和解密加密图像。2017年9月29日，中国科学院（Chinese Academy of Sciences）与奥地利科学院（Austrian Academy of Sciences）的研究人员通过该系统，举行了一个加密的75 min视频会议[1]。

Mozi的量子密钥分配（quantum key distribution，QKD）性能表明，卫星可以大大扩展下一代量子通信网络的范围，许多国家和公司正在建立这些网络，以确保未来的数字安全。该项目的成功表明，基于卫星的量子加密技术或基于量子原理的加密技术，能够让全球用户可以使用该技术远距离安全地交换数据[2]。“这绝对是量子通信的一大突破”，索邦大学（Sorbonne University）的量子物理学家Eleni Diamanti说。

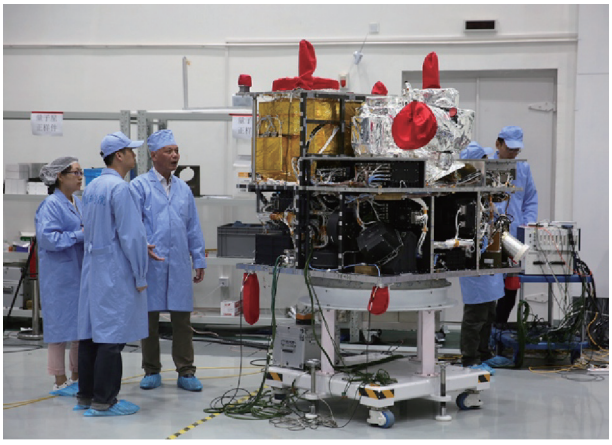

图1. 正在建造和测试的Mozi卫星的实际图像。图片来源：Cai Yang（新华社）。

量子密码学正变得必不可少，因为另一种新兴技术——量子计算机正威胁着通信加密技术，而通信加密技术目前正保护着在线金融交易、手机通话和短信，以及许多其他通信类型[3]。为了阻止窥探者，目前支持这些传输的公钥加密过程需要两个密钥。尽管任何人都可以访问公钥，但黑客无法破译他们拦截的通信，因为他们缺少私钥[4]。

破解密钥是非常困难的，因为它涉及将大量数字分解为素数或解决其他复杂的数学问题。然而，传统的计算机已经破解了一些被广泛使用的加密密钥，包括电子商务的早期标准[5]。因为量子计算机的速度比现在的机器快很多倍，所以破解这些密钥更加容易。安全专家预测，一台高速量子计算机可以在不到一天的时间内破解1024 bit的Rivest-Shamir-Adleman（RSA）加密（这是当今的标准之一）[6]。路易斯安那州立大学（Louisiana State University）的理论物理学家Jonathan Dowling说，目前还没有量子计算机原型具备这种能力，但它们的计算能力每六个月就会翻一番。

依赖于量子加密技术的通信网络将具有更高的安全性，因为它们编码了在光子流中解密消息所需的密钥。由于量子行为规则，这些密钥的优点是有一个内置的警报。如果窃听者截获了密钥并传递副本，密钥就会

英文原文: Engineering 2019, 5(3): 353–354
引用本文: Mitch Leslie. Quantum Cryptography via Satellite. *Engineering*, https://doi.org/10.1016/j.eng.2019.04.006

更改并提醒合法用户他们的密钥已被窃取[7]。Dowling说，如果发送者和接收者能够确认量子密钥已经安全到达，那么他们就可以通过传统的渠道安全地交换加密信息。“通过手机、互联网或烟雾信号发送信息是安全的。”

虽然一些陆基量子网络已经开始运行，但卫星可能会克服它们最大的局限性：传输信号会在几百公里的距离内消失[1]。世界上最长的地面量子网络于2017年开始运行，从上海至北京距离超过2000 km。该网络解决了32个所谓的可信节点的距离问题，这些节点与相邻节点共享量子密钥，但是这种机制仍然存在一些安全风险[8,9]。相比之下，卫星信号主要通过空间移动并且减弱得更慢，因此它们可以进一步传输量子密钥[2]。

中国科学技术大学（University of Science and Technology of China）的物理学家潘建伟与他的前博士导师、维也纳大学（University of Vienna）量子物理学家、奥地利科学院（Austrian Academy of Sciences）（因此与中国和奥地利联系）高级科学工作者Anton Zeilinger，以及其他的研究人员共同合作，开发了QKD技术，并且表明，在2016年发射的Mozi可以将距地面1200 km的密钥发送至地面站[1]。在转发密钥之后，卫星已经完成了它的工作；奥地利和中国之间就可通过传统网络共享加密图像和视频。这项工作是“一项伟大的技术成就”，美国马里兰州立大学联合量子研究所（Joint Quantum Institute at the University of Maryland）的联席主任Charles Clark说。

潘建伟和他的同事计划发射更多的卫星，以提高Mozi的性能[1]。此外，其他国家和组织已经或正计划发射具有QKD能力的卫星[10]。不过，“与地面通信相比，量子通信还有很长的路要走”，Clark说。例如，Mozi只能在夜间发射，而且它的低地球轨道意味着它大部分时间都在地面站的范围之外[2]。

Diamanti和Dowling认为，量子通信的下一步发展可能是纳米卫星舰队。Dowling表示，每台智能手机大小的设备都可以生产和发射大数据，并且可以用激光指示器的方式传输数据，生产成本低廉，数量庞大。这种基于纳米卫星的网络可以有效地执行必要的QKD，从而在全球范围内实现高度安全的远距离通信。

Reference

[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 City: 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 2p.]. 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.