中国联合研发团队率先实现量子安全“双保险”

作者：writer 来源：爱科学

本文原地址：https://www.iikx.com/news/progress/13887.html

中国联合研发团队率先实现量子安全“双保险”。中国的科研界和产业界正携手应对量子计算带来的信息安全挑战。近日，来自中国科学技术大学、上海交通大学、云南大学与国盾量子、国科量子等公司的联合研发团队宣布，完成了国际上首次量子密钥分发（QKD）和后量子加密算法（PQC）的融合应用。相关论文5月6日发表在国际学术期刊《自然物理杂志—量子信息》上。

随着量子计算的发展，经典密码算法的安全性逐渐感受到威胁。而能抵御量子计算破解、实现量子安全的技术路线主要有两种：一是量子保密通信，其中发展成熟的主要是量子密钥分发（QKD），具有不依赖于数学假设的无条件安全性；二是后量子加密（PQC）算法，比如格密码，目前已知的量子计算算法无法有效破解。QKD、PQC两种技术路线之间是竞争还是合作，也一直是外界聚焦的问题。

中国团队的实验证明两种技术可实现优势互补，并非二选一的零和博弈。本次研究中，科研人员在QKD网络中使用PQC认证代替原来的QKD设备预制密钥认证，且验证了新方案在城域范围内QKD中继网络和全通网络中应用的可行性。利用PQC认证，可以将QKD网络中可信中继替换为光开关，每个用户只需要通过PKI申请1个数字证书，就可以实现任意两用户之间的直连；新用户也只需要获得1个数字证书，就可以立即与其他用户建立QKD连接，提高了QKD网络的操作性和效率。

研究结果显示，这种新型安全认证方案可以利用PQC简化QKD在复杂网络环境下的身份认证和密钥管理，同时QKD则提供了PQC等公钥体系无法确保的无条件安全性，两种技术结合，进一步保障量子保密通信网络系统安全性，也提高了量子保密通信网络的经济性、便利性，将极大促进量子保密通信的应用和推广前景。

值得注意的是，本实验也是跨领域、跨团队，科研和产业结合的探索。论文作者中，中国科技大学的研究人员包括中科院院士潘建伟及其同事张强等量子信息领域的学者；上海交通大学计算机系教授郁昱则常年从事密码学和后量子密码学研究。实验设备采用了国盾量子自主研制的QKD产品，国盾量子研发团队在实验中进行了相关QKD设备和PQC上位机通信的设计，搭建实验平台完成QKD+PQC的网络实验的数据采集、分析等工作。各方共同发挥自身的科研和产业优势，推动量子安全技术的融合发展。

QKD和PQC这两种抵御量子计算威胁的方案是两种完全不同的技术体制的技术，该研究工作首次将两种看似完全不同的技术进行融合，PQC解决了QKD预置密钥的关键问题，而QKD则弥补了PQC待验证的长期安全性问题，两者联合最终保证了网络系统安全性，展现了两种技术的优势互补，实现了量子安全双保险。（来源：中国科学报赵广立）

相关论文信息：https://doi.org/10.1038/s41534-021-00400-7

作者：潘建伟等 来源：《自然物理杂志—量子信息》