“黑科技”量子通信如何保证信息安全

量子通信是当前世界上最为先进的保密通信技术，以量子通信为基础，可以构筑天地一体化、高速灵活、安全稳定的通信网络基础设施。

中国电子科技集团公司电子科学研究院 | 袁苏文

2017年以来，在代表通信技术前沿阵地的量子通信领域，我国可谓是捷报频传：首先是今年3月量子通信京沪干线开始最后阶段的贯通测试，其次是量子纠缠分发实现千公里量级的传输，再次是近日我国成功实现水下量子通信实验。一个个里程碑进展的获得，代表我国不断攻克量子通信的关键技术难题，将量子通信研究带入了新时代。

业界普遍认为，量子通信是当前世界上最为先进的保密通信技术，以量子通信为基础，可以构筑天地一体化、高速灵活、安全稳定的通信网络基础设施。这样的网络基础设施不仅可以应用于国防、军事等国家级保密领域，还可以应用在数据中心、金融、区块链、物联网等国民经济领域。

那么，以高安全著称的量子通信出现的必要性何在？量子通信又如何确保通信信息的安全性？本文对上述问题进行分析和说明。

传统加密算法防护能力趋弱

近年来“斯诺登事件”的爆发给我国敲响了信息通信安全的警钟，而“WannaCry”、“Petya”等勒索病毒的出现，则表明在互联网前沿领域还存在很多不安全的地带。因此，加强网络与信息通信安全保护、构筑信息安全防护的长城，是我国信息通信领域的当务之急。

正所谓“道高一尺魔高一丈”，安全威胁和防控措施从来都是“矛和盾”的关系，因此安全防护不可能一劳永逸，而是需要根据新的形势不断自我提升，这就是量子通信出现的必要性。

目前业界使用最为广泛的公钥加密算法，为1977年由美国3位科学家提出的RSA129算法。该算法的原理是，将两位质数相乘获得一个129位的数字，其中的两个乘数就是隐藏在公钥加密算法中的关键信息。这一加密算法的原理是：两个质数的乘积计算非常简单，但是要把乘积进行因式分解难度就特别大，而且数字越大，越难以破解。按照1977年的计算能力，破解129位的数字大约需要4亿亿年。

但是时隔17年后，破解加密算法的时间就缩减到了8个月左右。而现在量子计算出现后，计算速度和能力大大提升，使得破解RSA129加密算法的时间进一步缩减到了几十秒。

其根本原因在于，传统的通信加密一般在加密数据和传输介质上做文章，而这种加密方法只能增加破译的难度，无论采用先进算法破译，还是采用超级计算机暴力破译，破解传统通信加密数据都只是时间长短的问题。随着计算能力的提升，破解时间变得越来越短，甚至达到秒级。

因此，采用全新信息安全技术提升安全防护能力已经迫在眉睫。与量子计算如影随形的另一项技术——量子通信进入了人们视野。

量子力学三大原理确保信息传输安全可靠

在探讨量子通信之前，首先看看量子是什么。量子是能表现出物理特性的最小单元，是能量的最基本携带者；一个物理量如果存在不可分割的最小基本单位，那么这个物理量是量子化的。而量子通信则是结合量子物理学和密码学，利用量子态的物理性质提供绝对安全保障的通信方式。

量子通信之所以安全有保证，主要是因为量子力学具有三大基本原理：测不准原理、不可克隆原理、纠缠态原理。

测不准原理，即海森堡不确定性原理。与粒子的位置和动量可以同时取确定值所不同的是，受粒子波动性的影响，两个非对易的量子不可能同时被精确测量。测不准原理，使得对任何量子传输进行监听、监测的目的都会落空。

不可克隆原理，是指量子态不同于

经典状态，它非常脆弱，任何测量都会改变量子态本身，传输过程中如果有第三方克隆某个量子态，那么该量子态就会被毁灭，因此一个未知的量子态是无法被精确克隆的。不可克隆原理，有效杜绝了非法分子通过克隆复制信息的可能。

量子的纠缠态原理相对来说较为复杂，它是指在微观世界里，不论两个量子间距离多远，都会产生“心电感应”，一个量子的变化都会影响另一个量子。例如，两个量子A和B有“0”和“1”两个状态，如果A处于“0”的状况，那么就可以判定B处于“1”的状况。这种跨越空间能够瞬间影响双方的量子纠缠，曾经被爱因斯坦称为“诡异的互动性”，它是量子力量最为神秘的特点之一。

量子通信的加密原理总结起来有如下两方面：一是不依赖于传统的计算复杂性，而是基于量子力学中的海森堡测不准原理和不可克隆定理等基本原理；二是利用光子的量子态作为密钥或者是信息本身的载体，收发双方可以通过量子测量的方法检测出这些光子在传输过程中是否遭到了窃听者的截获，一旦确认遭到窃听则丢弃所传输的密钥或信息，从而确保过程的安全。

量子通信出现两大应用分支

基于量子力学的三大原理，目前在量子通信方面出现了两大应用分支，一个是量子密钥分发，二是量子隐形传态。

量子密钥分发技术是把密钥编码在量子态上，利用量子力学原理通过量子信道传输于发送者和接收者之间，用于保密通信双方之间建立和传送密钥，而经密钥加密后的消息密文仍然通过传统信道传输。

目前量子密钥分发比较著名的理论方案有BB84方案、B92方案和E91方案。其中BB84方案采用4个量子态和两组正交的测量基，发送方随机选择量子态发送，接受方随机选择测量基测量。等发送和测量一组数据后，接收者告诉发送者每次他使用的是哪个测量基，由于发送者清楚地知道自己发送了哪些态，因此他也知道接收者选错了测量基还是选对了测量基，它通过

公开信道告诉接收者保留哪些选对了的测量基结果。

B92方案采用两个非正态实现量子密钥分发，简化了BB84方案的过程，B92方案中通信双方不用通过对比测量基就能知道保留哪些结果，简化了通信过程，但是传输效率下降了一半，有75%的结果都被抛弃，因此从实际应用的角度看BB84方案更为广泛。

E91方案将一对相互纠缠的粒子分别发送给收发双方，让他们分别对其测量，当两个人选取的测量基一致时，A端可以通过自己的测量结果推测出B端的测量结果，从而在二者之间建立起相同的密钥，这就是纠缠态能用于数据传递的原理。如果存在窃听者，根据测量坍缩原理，他的测量行为一定会破坏量子的纠缠，因此对安全性的检验就转化为了对纠缠的检验。与BB84和B92方案相比，E91方案能够提供更高的安全性，但是验证过程较为繁琐，传输效率低。

量子隐形传态则是一种利用量子安全特性进行直接通信的方式。与量子密钥分发的根本性区别在于，量子隐形传态过程中，通信双方不需要事先生成密钥，而是通过直接建立量子信道的方式进行通信，即直接完成秘密信息的安全传输，而无需进行使用密钥的加密和解密处理。量子隐形传态的安全性也是基于量子不可克隆原理、量子测不准原理，以及纠缠粒子的关联性和非定域等。总体而言，量子隐形传态还处于基础研究阶段。

我国位于研发应用前列

1982年，法国物理学家艾伦·爱斯派克特成功完成了一项实验，证实微观粒子“量子纠缠”的现象确实存在；1993年，美国科学家C.H.Bennett提出了量子通信的概念，同年6位来自不同国家的科学家，基于量子纠缠理论，提出了量子通信最初的基本方案，由此开启了量子通信从实验室走向产业应用的新阶段。

在产业化阶段中，中国走在了前列。从上世纪八十年代开始，中国科技大学的郭光灿院士已经开始系统地研究量子光学及其行业。1997年，在奥地利留学的中国青年学者潘建伟与荷兰学者波密斯特等人合作，首次实现了未知量子态的远程传输。这是国际上首次在实验室成功地将一个量子态从甲地的光子传送到乙地的光子上。实验中传输的只是表达量子信息的“状态”，作为信息载体的光子本身并不被传输。

2000年左右，中科大以郭光灿和以潘建伟为首的两个团队在量子通信研究上已经取得了很好的科研成果，但这些成果都处于前期的试用阶段。2009年国庆阅兵仪式上使用了量子通信加密设备，国家也开始给予重大支持，量子通信研究成果得到肯定。而2013年开始京沪干线的建设，则意味着量子通信在我国进入加速发展的状态。

量子通信在国内最具标志性的事件，是2016年8月16日凌晨我国发射人类历史上第一颗用于量子通信研究的“墨子号”，该卫星将配合多个地面站实施星地量子密钥分发、星地量子纠缠分发和地星量子远程传态等量子通信领域的实验。“墨子号”的成功研制并发射，使得中国进一步扩大了在量子通信领域的世界领先优势。

除了“墨子号”之外，我国已经建设了合肥城域网、芜湖量子通信网、山东量子通信网、京沪干线、沪杭干线、上海通信网等量子通信试验网，量子通信这一“黑科技”正从实验室走向规模应用，标志着我国已然走在了世界量子通信领域发展前列。

编辑 | 舒文琼 shuwenqiong@bjxintong.com.cn