量子密码技术开辟通信安全新时代

屈　平　　方　芳

2004 年 6 月 3 日, 世界上第一个量子密码通信网络在美国马萨诸塞州剑桥城正式投入运行。主持这套网络建设的是美国 BBN 技术公司。新的量子密码通信网络已成功地实现了该公司与哈佛大学之间的连接, 不久将延伸至波士顿大学。新的量子密码通信网络与现有因特网技术完全兼容, 网络传输距离约为 10 千米。这个由美国 BBN 技术公司研发的量子密码通信网络和现有的宽带网并没有太大的不同——采用普通光纤传输数据, 并且与普通网络完全兼容。与普通网络不同的是, 该网络中传输的数据采用了量子密码技术进行加密。目前, 网络有 6 个节点, 已经从 BBN 公司铺设到了哈佛大学, 预计今年年底将延伸至波士顿大学。量子密码通信是目前唯一被证明绝对安全的保密通信方法, 美国《商业周刊》把它列在了“改变人们未来生活的十大发明”的第三位。据美国权威机构估算, 量子保密通信系统一旦商用, 将形成多达 10 亿美元的市场。

量子密码通信技术新进展

2002 年 10 月, 德国慕尼黑大学和英国军方下属的研究机构合作, 在量子密码技术研究中取得重要进展。科学家们在德国和奥地利边境的楚格峰和卡尔文德尔峰之间用激光成功传输了光子密钥。这次传输的距离达到 23. 4 千米, 试验的成功使通过近地卫星安全传送密钥并建立全球密码发送网络成为可能。他们在这次试验中采用的密钥是偏振光。光子用不同偏振角代表二进制位的“0”和“1”, 而光子发射的顺序代表了二进制代码的排序。激光信号发射装置每次发送一个有效的光子, 而发射方和接收方通过电话核对每个光子的发射和接收时间、是否丢失、偏振角是否改变。一旦发生光子丢失或偏振角改变的情况, 发射方就可以从密钥序列中去掉这个光子, 从而组成一个新的密钥。科学家在试验中并没有使用复杂的仪器, 接收激光信号的是普通的 25 厘米望远镜。他们解释说, 之所以选择在两座山峰之间试验, 是因为在约 3000 米的高度上, 气流扰动对试验的影响比较小。

2003 年 8 月, 美国国家标准与技术研究所和波士顿大学的科研人员, 研制出一种能探测到单脉冲光的探测器, 它同时还能将误测或“漏测”率几乎减少到零。这一新成果的报告发表在《应用物理通讯》上, 它为开发安全量子通信和密码系统提供了关键技术。目前的大多数光子探测器只对可见光运行良好, 对单光子的探测就不太可靠, 而且由于随机的电子噪音, 其漏测率也很高。新的仪器采用光纤通信的近红外线光波, 它的漏测率已经可以忽略不计。研究所没有选择感光材料, 而是用了与光纤通信线相连接的钨丝。钨丝被冷却到适当温度。当光纤将一个光子传输到钨丝时, 温度会升高, 仪器就探测到它引起的电阻增强。

2003 年 11 月, 日本总务省量子信息通信研究推进会提出了以新一代量子信息通信技术为对象的长期研究战略, 计划在 2020~ 2030 年间, 建成绝对安全保密的高速量子信息通信网, 以实现通信技术质的飞跃。日本计划在 5 年内实现在 100 千米左右的中距离通信中, 使用量子加密技术, 到 2007 年将构筑起量子信息技术高速通信实验系统, 在 2020~2030 年间建成利用量子加密技术的安全高速的量子信息通信网。为了实现这一目标, 日本专家建议设置开放实验室, 以供不同领域的专家信息交流之用。

2003 年 5 月在奥地利维也纳大学从事合作研究的中国科技大学教授潘建伟博士及其同事, 在量子纠缠态纯化的实验研究中取得了突破性进展。英国《自然》杂志以封面文章的形式发表了题为《任意纠缠态纯化的实验研究》的论文, 潘建伟是第一作者。2001 年春, 潘建伟教授与其合作者曾意外发现了利用现有技术在实验上可行的量子纠缠态纯化的理论方案, 并于当年 4 月 28 日在《自然》杂志上发表。经过两年的艰苦努力, 潘建伟和他的同事们最近终于在实验上成功地实现了高精度的纠缠态纯化。这项研究成果不仅从根本上解决了目前在远距离量子通信中遇到的困难, 而且也将极大地推动可容错量子计算的研究。《自然》杂志审稿人称赞潘建伟等人的论文“构成了量子信息实验领域一个非常重要的进展”,“首次在实验上无可辩驳地证明了量子信息处理中任意未知的退相干效应是可以被克服的”。而 1999 年, 潘建伟关于量子态隐形传输实验实现的论文同伦琴发现 X 射线、爱因斯坦建立相对

论等影响世界的重大研究成果一起被《自然》杂志评为“百年物理学 21 篇经典论文”。

2003 年 7 月，中国科学技术大学中科院量子信息重点实验室的科学家在该校成功铺设一条总长为 3. 2 千米的“特殊光缆”——一套基于量子密码的保密通信系统。2003 年 11 月，华东师范大学研制成功国内首台量子保密通信样机。目前他们已拥有十几项国内外发明专利，部分单元器件已达到国际领先水平。他们将努力争取参与量子保密通信系统标准的制定。

科学家希望，将来可以实现 1000 千米距离的量子密码传输。这样就可以利用卫星来传递信息，并在全球范围内建立起保密的信息交换体系。

量子密码通信技术的原理

量子密码学的理论基础是量子力学，而以往密码学的理论基础是数学。与传统密码学不同，量子密码学利用物理学原理保护信息。首先想到将量子物理用于密码技术的是美国科学家威斯纳。威斯纳在海森堡测不准原理和单量子不可复制定理的基础上，逐渐建立了量子密码的概念。海森堡测不准原理是量子力学的基本原理，指在同一时刻以相同精度测定量子的位置与动量是不可能的，只能精确测定两者之一。单量子不可复制定理是海森堡测不准原理的推论，它指在不知道量子状态的情况下复制单个量子是不可能的，因为要复制单个量子就只能先作测量，而测量必然改变量子的状态。

威斯纳于 1970 年提出，可利用单量子不可复制的原理制造不可伪造的电子钞票。由于这个设想的实现需要长时间保存单量子态，这是不太现实的，因此电子钞票的设想失败了。但是，单量子态虽然不好保存却可以用来传递信息，威斯纳的尝试为研究密码的科学家们提供了一种新的思路。

量子密码最基本的原理是量子纠缠——一个特殊的晶体将一个光子割裂成一对纠缠的光子。被爱因斯坦称为“神秘的远距离活动”的量子纠缠，是指粒子间即使相距遥远也是相互联结的。大多数量子密码通信利用的都是光子的偏振特性——这一对纠缠的光子一般有两个不同的偏振方向，就像计算机语言里的“0”和“1”。根据量子力学原理，光子对中的光子的偏振方向是不确定的，只有当其中一个光子被测量或受到干扰，它才有明确的偏振方向，它代表“0”和“1”完全是随机的，但一旦它的偏振方向被确定，另外一个光子就被确定为与之相关的偏振方向。当两端的检测器使用相同的设定参数时，发送者和接收者就可以收到相同的偏振信息，也就是相同的随机数字串。另外，量子力学认为粒子的基本属性存在于整个组合状态中，所以由纠缠光子产生的密码只有通过发送器和接收器才能阅读。窃听者很容易被检测到，因为他们在偷走其中一个光子时不可避免地要扰乱整个系统。

当前，量子密码研究的核心内容，是如何利用量子技术在量子通道上安全可靠地分配密钥。所谓密钥，在传统的密码术中就是指只有通信双方掌握的随机数字串。

量子密钥分配，其安全性由海森堡测不准原理及单量子不可复制定理保证。根据这两个原理，即使量子密码不幸被电脑黑客撷取，也因为测量过程中会改变量子状态，黑客得到的会是毫无意义的数据。

我们可以这样描绘科学家们关于“量子密码”的设想：由电磁能产生的量子（如光子）可以充当为密码解码的一次性使用的“钥匙”。每个量子代表 1 比特含量的信息，量子的极化方式（波的运动方向）代表数字化信息的数码。量子一般能以四种方式极化：水平的和垂直的，而且互为一组；两条对角线的，也是互为一组。这样，每发送出一串量子，就代表一组数字化信息。而每次只送出一个量子，就可以有效地排除黑客窃取更多的解密“钥匙”的可能性。

量子密码安全可靠

加密是保障信息安全的重要手段之一。在现有的各种密码中，没有哪种是解不开的。现在常用的标准加密方式是用一串随机数字对信息进行编码。比如，用数字串“5、1、19、20”来加密英文单词“east”（四个数字分别表示单词中四个字母在英文字母表中的位置）。这种加密方案有一个致命的缺陷——从数学上来讲，只要掌握了恰当的方法，任何密码都是可以被破译的。更糟糕的是，这种密码在被窃听破解时，不会留下任何痕迹，合法用户无法察觉，还会继续使用同一个地址储存重要信息，损失就会更大。

现在就是最安全的公钥密码系统，一旦遇上量子计算机，也形同虚设。须臾之间量子计算机便能破译这种密钥。要是用量子密钥来加密信息，那就连量子计算机也只能望“密”兴叹了。量子密码术是一种截然不同的加密方法，是密码编制人员追求的最高境界。主要是利用两种不同状态的快速光脉冲

复杂性科学的几大学派及其研究特点

柴立和　杨　战
(天津大学环境科学与工程学院　300072)

近几十年来, 国际学术界出现了一门新学科——复杂性科学, 它致力于复杂系统理论与现有传统学科交叉的研究, 目前已掀起了一股研究复杂性和非线性问题的热潮, 数学家、物理学家、经济学家、生物学家和计算学家等都在共同开展这一问题的研究, 复杂性科学将成为一个驾驭在 21 世纪生命科学、信息科学、材料科学等高新领域之间的一个横断学科, 被誉于"21 世纪的科学"。

本文从哲学角度分析了现代科学中还原论和简单性思维方式的起源以及复杂性科学诞生的背景, 研究了目前复杂性科学研究的几大学派的基本特征, 指出应汲取各大学派的优点, 结合我国的实际情况, 全面推进我国的复杂性科学研究。

人类面临的实际世界是复杂多变的, 存在涉及到多种因素和多方面相互作用的千姿百态的复杂现象。在古希腊和古代中国, 人们在对自然界复杂现象的认识过程中, 产生了朴素的唯物主义认识观, 它是人类智慧的结晶, 是人类文明长河中的宝贵财富。但由于当时科学技术水平的低下, 人们对客观世界复杂性的认识还只能说是停留在猜测和思辨的水平上, 还没能提出非常有科学依据的理论体系; 所以, 在西方近代科学产生之前, 特别是在中世纪, 人们对世界的看法基本上是混乱的, 总是需要这样或那样的神来主宰世界万物, 这时候的科学往往被披上神学的外衣, 科学的发展从而受制于社会政治和意识形态的干扰。400 年前, 随着近代西方自然科学的悄然兴起, 尤其是文艺复兴之后, 人们对世界的认识进入了一个崭新的境界。人们通过对自然现象的分析、综合和判断而诞生的牛顿力学和微积分学使人类悟出了一套大自然的规律, 从此机械决定论取代了神决定论, 人们开始试着用数学的语言和方法来了解周围的一切, 这深深影响了人类后 200 多年的信念、认知途径和思维方法。人们把世界和谐与有序的基础简单地理解为简单性, 认为世界最终是由

(光子) 来以无法破译的密码传输信息。任何想测算和破译密钥的人, 都会因改变量子状态而得到无意义的信息, 而信息合法接收者也可以从量子态的改变而知道密钥曾被截获过。单量子态有两个特殊的脾气, 使它能"守口如瓶": 一是根据量子不可克隆原理, 未知的量子态不能被精确复制, 所以人们不能像复制钥匙一样复制量子态; 二是由于量子不确定性原理, 任何试图对它"不轨"的举动, 都会毁坏套在信息上的量子密钥"信封", 使盗贼自曝形迹。从理论上来说, 用量子密码加密的通信不可能被窃听, 安全程度极高。

假设黑客入侵网络, 黑客必须用一个特殊的接收设施从一连串的量子中"吸"出一个来获取信息, 但这样一来, 发出量子密码的一方立即就会发现量子流中出现了空格。为了避免被发现, 一般黑客会再发射一个量子来填补这个空格。但是, 由于"量子密码"是采用量子的极化方式(波的运动方向) 来编排密码的, 而根据量子学原理, 要同时检测出量子的 4 种极化方式, 几乎毫无可能, 黑客填补进去的量子只能是根据自己的猜测随便发射的——这样, 这个"不合群"的量子很快就会被发现, 从而防止信息被窃取。

华东师大研制的量子保密通信样机由一对身高 1.2 米的"情侣"组成: 发送信息的叫"爱丽斯", 接收信息的叫"鲍勃"。且看这对"情侣"如何使用量子密钥互通"保密情书"。首先, 爱丽斯发出一串单光子的脉冲序列。通过长达 50 千米的光纤, 鲍勃接收到了这串"爱的信号"。然后, 根据量子们的完整情况, 鲍勃会判断是否有"第三者"想"插足"。如果一切正常, 这对"情侣"就同时获得一串密钥。现在, 爱丽斯用量子密钥把情书"上锁", 通过公共信道发送给鲍勃。量子密钥采用完全无章可循的真随机数, 而且密钥长度等于书信长度。这串密钥就像魔术师一样, 对情书施展障眼术, 使得它在旁人看来只是一群纷乱的麻点。当鲍勃用密钥打开"量子锁", 情书内容才真相大白——原来是爱丽斯的玉照! 在密钥的传输过程中, 任何对密钥的偷窥和复制都会被鲍勃识破。而且为确保安全, 这串密钥在新的情书传递中将不再被使用, 也就是说, 每封情书都有各自的密钥, 故而量子密钥也称为"一次性便笺"密钥。