量子密码通信研究进展

鲁韦昌

（重庆通信学院计算机科学与技术教研室　　重庆 400035）

摘要：本文通过阐述量子密码学产生，在通信领域中的开发与研制，到实际应用的过程，揭示量子密码在保密通信中发生着深刻变化，展示未来保密通信领域中快捷、可靠、安全的发展前景。

关键词：量子信息技术　量子密码通信　　量子密码学

量子密码通信是近二十多年来发展起来的通信技术，它利用量子物理特性以得到通信的保密性。它的发展在军事通信、商业通信、电子银行都有很好的发展前景。

一、量子密码学

经典密码体制有两种运用很广泛的体制，一是非对称密码体制，另一种是对称密码体制[1]。

非对称密码体制又称为公开密钥体制，接受消息者（通常称为 Bob）先选一组只有他自己知道的私人密码，由此私人密码推算出相应的公开密码，并将此公开传给准备发送消息的所有人，发送消息者（通常称为 Alice）利用公开的密钥将消息加密发给接受者 Bob。对于所有的人，包括窃听者（通常称为 Eve）很难从密文反推原来的消息，只有 Bob 既知道公开密钥又知道私人密码，才能将密文解密而还原成原文。这种传输消息体制中的 Alice 和 Bob 拥有不同的密钥故称为非对称密码体制，此体制的安全依赖于解密计算的复杂性。例如最常用的 RSA 密码算法，就是应用大数分解质因子的原理。在 Alice 与 Bob 之间传递的密文，是以公钥加密，而这个公钥是一个很大的数，例如 408508091（实际上用的数会远大于此）。密文只能以 Bob 握有的私钥解开，这把私钥是公钥的两个因数，而在这个例子里就是 18313 与 22307。通常含有的质因子愈大愈难将它们分解出来，因此至今密钥的安全性仍旧很高。按照现有的理论计算，分解一个 400 位数的质因子，用目前最先进的巨型计算机也需要用 10 亿年的时间，而人类的历史才不过几百万年。然而量子计算机概念的出世，严重动摇了 RSA 公鈅密码体制的安全性。1994 年，美国的 P.W.Shor 利用量子计算机理论证明，一个 N 位大数的质因子分解只需用 N 的多项式的时间而不是以前所认为的 N 的指数次的时间。利用量子计算机分解一个 400 位大数仅仅需要不到一年的时间！Shor 的工作引起了科学家们巨大的热情和兴趣。1995 年，美国 Grover 证明在搜索问题上量子计算机比经典计算机优越。因此当量子计算机的研究有了突破性的进展，因子分解的难度将会显著下降[2]。

对称密码体制又称专用密码体制，Alice 和 Bob 拥有相同的密码，Alice 用此密码加密，Bob 用同一密码解密，已经证明这种密码体制仅用一次才能保证完全安全，再次使用安全性将大打折扣。因此这样的密码体制尽管有安全保障，但效率太低，在实践中 Alice 和 Bob 的密码只能依靠两人会面或者有专门的信使传递，成本很高且存在新的安全隐患。为了提高密码的利用率，发展了 DES,AES 及 IDEA 等对称密码体制[1]主要靠计算复杂度的增加来实现密码的重复使用。然而，它同样面临量子计算机的发展变得岌岌可危。

从数学上讲只要掌握了恰当的方法任何密码都可破译。此外，由于密码在被窃听、破解时不会留下任何痕迹，用户无法察觉，就会继续使用同地址、密码来存储传输重要信息，从而造成更大损失。然而量子密码不是依赖于计算的复杂度，而是基于量子力学原理，利用量子的物理特性来保护信息。其原理是“海森堡测不准原理（Heisenberg uncertainty principle）”中所包含的一个特性，即当有人对量子系统进行偷窥时，同时也会破坏这个系统。在量子物理学中“海森堡测不准”原理表明,如果人们开始准确了解到基本粒子动量的变化，那么也就开始丧失对该粒子位置变化的认识。所以如果使用光去观察基本粒子,照亮粒子的光(即便仅一个光子)的行为都会使之改变路线,从而无法发现该粒子的实际位置。从这个原理也可知，对光子来讲只有对光子实施干扰才能“看见”光子。因此对传输光子线路的窃听会破坏原通讯线路之间的相互关系,通讯会被中断。另外,还有“单量子不可复制”定理。它是上述原理的推论,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必须先做测量,而测量必然会改变量子状态。根据这两个原理,即使量子密码不幸被 Eve 获取,也会因测量过程中对量子状态的改变使得 Eve 只能得到一些几乎无意义的信息。

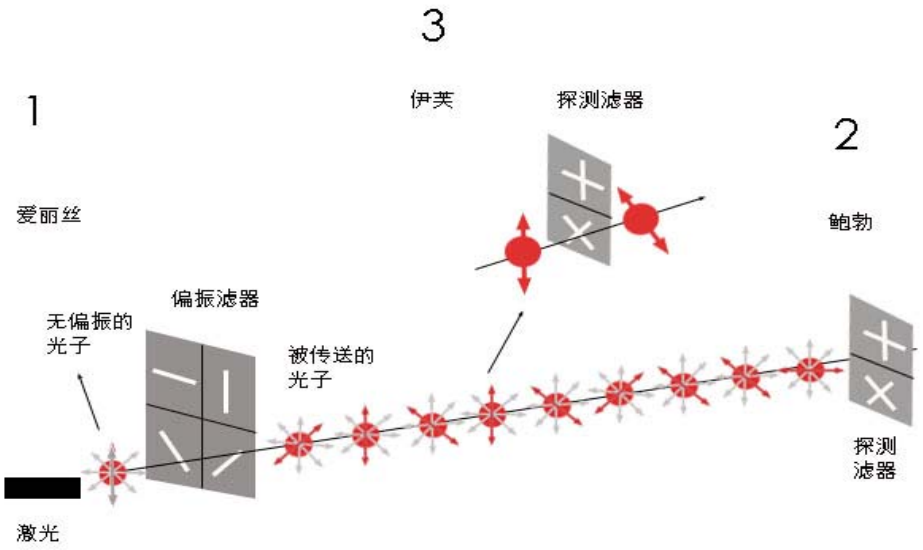
量子密码就是利用量子存在状态作为信息加密、解密的密钥，其原理就是被爱因斯坦称为“神秘远距离活动”的量子纠缠态(entangled state)。它是一种量子力学现象，指不论两个粒子间距离有多远，一个粒子的变化都会影响另一个粒子。因此当使用一个非线性晶体（如碘酸锂〔lithium iodate〕，硼酸钡〔barium borate〕）将一个光子“分裂”成一对纠缠的光子后，即使相距遥远它们也是相互纠结的。只要测量出其中一个被纠缠光子的属性，就容易推断出其他光子的属性。而且由这些光子产生的数据只有通过特定发送器、接受器才能解读。同时由于这些光子间的“神秘远距离活动”独一无二，只要有人要非法拦截这些数据，就会不可避免地扰乱光子的性质。而且异动的光子会像警铃一样显示出入侵者的踪迹，再高明的 Eve 对这种加密技术也将一筹莫展。这实际上就是一种不同于传统需要加密解密的加密技术，其实质在传递过程中规避 Eve 的窃听或者篡改。

二、量子密码通信

量子通信系统由量子态发生器、量子通道和量子接收设备组成。它是光纤通信技术的一种，只不过其量子通道利用光的量子物理特性，让一个个光子传输 0 和 1 的信息，量子通信技术所传输的信息是分为经典还是量子两类，前者主要用于量子密钥的传输，开发无法破译的密码；后者则是量子瞬间传送，一种令人难以置信但在量子世界里确实可行的瞬间远距离“实物”传输技术。

实现单光子密码通信，可以试想成 Alice 向 Bob 逐个地、随机地发出互不正交的两种量子状态水平偏振单光子及 45^0 偏振单光子，并规定水平偏振码值为 0，45^0 偏振码值为 1。Eve 要获取信息，必须截取并测量 Alice 和 Bob 的通信。Eve 有 50%的机会猜对 Alice 发送的是哪一种偏振光子，此时 Eve 能正确测出码值。Eve 还有 50%机会猜错码值，即使在猜错时仍由 50%机会得到正确码值，这样合起来 Eve 测得正确的码值机会有 75%。Eve 测得后，从 Alice 向 Bob 发送的量子态遭到破坏，Eve 为了掩饰窃听，需要伪装 Alice 向 Bob 发出的量子态，由于 Eve 只有 75%的正确码值，因而 Eve 向 Bob 发送的单光子状态将有 25%的机会错误，如此高的误码率(QBER)将容易被 Alice 及 Bob 发现。他们会舍弃这次通信，以维护通信安全。

实现通信协议的密码通信，以 BB84 协议为



（图 1：量子密码传输示意图）

例。协议采用四个非正交态作为量子信息态[图 1]，且这四个态分属于两组共轭基，每组基内的两个态

是相互正交的。两组基互为共轭是指一组基中的任一基矢在另一组基中的任何基矢上的投影都相等。因此，对于某一基的基矢量子态，以另一组共轭基对其进行测量会消除它测量前具有的全部信息而使结果完全随机，也就是说测量一组基中的量将会对另一组基中的量产生干扰。光子的线偏振量和圆偏振量就是互为共轭的量。不论是用左旋圆还是右旋圆偏振基测量线偏振光子，都是各以一半的几率得到左旋或右旋圆偏振态。反之亦然。

现在我们假定 Alice 与 Bob 约定用这两种偏振基中的四种偏振态来实现量子密钥分配，操作步骤如下：

（1）Alice 随机地选择右旋、左旋、水平或垂直四种中任一种偏振态的光子并发送给 Bob;（2）Bob 随机地独立选择线偏振基或圆偏振基测量该光子的偏振态；（3）Bob 实际所测到的偏振方向（只有 Bob 自己知道，其中一些态未被检测到）；（4）Bob 公布他检测到态时所采用的测量基（如，通过打电话告诉 Alice），但不公布测量到哪个偏振态，Alice 告诉 Bob 哪些测量基是正确的并保留下来，其余的丢弃掉；（5）Alice 和 Bob 仅保留相同基时的态，并按约定的规则转化为二进制序列（如左旋圆偏振态和水平线偏振态代表比特“0”，右旋圆偏振态和垂直线偏振态代表比特“1”）。（6）确定有没有致命的窃听（7）通过公开的信道进行纠错，即称为的数据协调。（8）进行密性放大，即指牺牲部分 Alice 和 Bob 共有的信息来将 Eve 可能以获取的信息变为无效，密性放大是通过公开的信道进行的。最后 Alice 和 Bob 共同拥有的码序列，就是所需的密码[3]。

三、量子密码通信的进展状况

如何让信息快速、方便、安全地传递是信息科学的主要课题，量子密码学产生正是基于此思想。在 1970 年美国哥伦比亚大学的科学家威斯纳（S.Wiesner）提出如何将量子特性用于密码科学，利用单量子态制造不可伪造的“电子钞票”，这个构想因量子态的寿命太短而无法实现。受此启发，确让 IBM 的贝内特(Bennett C H)博士和加拿大学者布拉萨德(Brassard G)想到单量子态虽然不好保存但可用于传输信息。在 1984 年提出了第一个量子密钥分配方案，称为 BB84 协议。1992 年 C.H.Bennett 又提出了一种更简便但效率减半的方案，即 B92 协议。

最早的量子密钥分配（QKD）网络实验是由英国的 P.D.Townsend 小组于 1998 年提出。他们利用光无源器件——分束器（splitter）实现了 Alice 与多个 Bob 之间的密钥分配。美国国防高级研究计划局(DARPA)与哈佛大学、波士顿大学和美国国家标准与技术研究所(NIST)等多家研究机构合作展开了量子保密通信与 IP 互联网结合的 5 年试验计划，并于 2003 年在 BBN 实验室进行了成功的实验运行。经过近 20 年的发展，量子密码通信目前已从单纯研究逐步走向实际应用。2002 年 7 月以日内瓦为基地的公司（id Quantique）已在长达 67Km 的光纤上实现单光子密码通信。2004 年 3 月日本 NEC 公司宣称创下了量子密码传输距离的新记录——150Km，这一距离为量子密码技术的实用化提供了可能。2004 年 6 月 3 日，6 节点的 QKD 网络在哈佛大学、波士顿大学和 BBN 公司之间利用标准电信光缆进行了通信。这套网络目前拥有 6 个节点，其中：由 4 个是可以互操作的弱相干量子密钥分发系统，它们的脉冲比率为 5MHz；另外两个是高速自由空间量子密钥分发系统。这套网络主要通过普通光纤来传输采用密码加密的数据，与现有互联网技术完全兼容，网络传输距离约为 10Km。到 2005 年 3 月，这套网络已增加到 10 个节点，并且增加了基于量子纠缠的量子密钥分发系统。2007 年 3 月，中国研究人员在北京网通的实际线路上利用量子路由器实现了分布 3 个不同地点的 4 用户长时间稳定 QKD 和视频保密通信。欧洲的英、法、德、意等国家建立了基于量子保密的安全通信网络，简称 Secoqc[4](Secure Communication Based on Quantumn Cryptography)，并于 2008 年在奥地利的维也纳实验证实了 5 个节点的 Secoqc QKD 网络。2009 年 10 月 9 日 id Quantique 公司网站发布，由日内瓦、瑞士西部的应用科学大学和大学的身份证 Quantique 公司，长期在一个网状网络环境长期的量子密码技术合作，建立 SwissQuantum 测试网络，运行超过 6 个月，并于最近通过了累计运行时间标记 12000 小时，这标志着这项技术成熟、可靠[5]。

参考文献

〔1〕陈鲁生，沈世镒. 现代密码学[M]，北京：科学出版社 2002.7：P.41—63，P.69—78

〔2〕Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. Proc. of 35th Symposium on Foundation of Computer Science, 1994:124~134

〔3〕马瑞霖. 量子密码通信[M]，北京：科学出版

社 2006.6：P.33—35
〔4〕Poppe A, Peev M, Maurhart O, *et al*. Outline of the Secoqc quantumn-key-distribution netwark in Vienna [EB/OL]. Arxiv.org/pdf/0804.0122v1, 2008-04-01
〔5〕www.idquantique.com