量子物理与量子技术

光纤量子密码网络

温 浩　　郭光灿

数字通信和数字信号处理领域的快速发展直接推动了 20 世纪后半叶兴起的信息革命。今天的数字信息系统仍然只在经典物理范畴。每一个比特的信息都能完全被经典器件描述,比如用一个晶体管或者微处理器的输入电压高低来代表 0 或者 1。然而,信息也能通过量子力学方式处理和传输,这就产生了全新的量子信息科学。量子信息科学的一个典型应用就是量子密码术,它在过去的十几年中发展十分迅速,美国和欧洲甚至已有比较成熟的商业产品。那么,什么是量子密码术、它的基本工作原理是什么、量子密码网络又是解决什么问题的……希望读者能通过本文大致了解这些问题。在了解量子密码之前,让我们首先回顾一下现代密码技术。

现代密码学都是基于数学和信息理论,根据加密密钥和解密密钥是否相同,可分为非对称密钥体系和对称密钥体系。非对称密钥体系是基于一些困难的数学问题,比如大数质因数分解问题,最典型的代表就是 RSA 公钥系统,采用公钥加密、私钥解密。这种体系的安全性都是计算安全性,即虽然理论上可以破解,但是在有限的计算资源和计算能力下,需要漫长的时间才能完成,因为求解这类问题所进行的计算步数通常与问题规模成指数关系。但是随着现代计算机计算能力的迅速增长和算法的改进,破解这种问题变得越来越容易,例如 1979 年对一个 129 位的合数进行因子分解需要 4×10^6 年,到 1994 年只需要 8 个月,而在 2006 年只需不到 1 个月的时间。另外,将来的量子计算机和量子并行算法也将分解大数的步数变成多项式关系,速度将比现行计算机快得多。由此可见,非对称密钥体系确实面临潜在的安全问题。在对称密钥体系下,尽管有各种各样的加密算法(DES、AES 等),但大多也是基于计算安全性。到目前为止,唯一被证明具有无条件安全性的加密算法是一次一密(One Time Pad)算法。

在一次一密中,明文与密钥进行比特异或得到密文,密文再与同一个密钥进行比特异或就恢复出明文了。算法虽然很简单,但对密钥有着严格要求:密钥长度必须和明文长度相同、密钥必须是真随机数、密钥不得重复使用。一次一密和所有的对称加密算法一样,需要通信双方在通信之前共享同一密钥,即密钥分配过程。密钥分配是个大问题,只有保证密钥安全才能保证系统的安全性。传统通信中密钥分配通常依靠信任的载体或者事先约定来完成,但这种办法既不高效、又要承担很大风险。当然也可采用非对称加密算法传递对称加密的密钥,现在因特网广泛采用的 IPSec 技术,事实上就是以此类算法传递密钥的。但是这种情况下产生的密钥安全性也取决于算法复杂度,并不绝对安全。

量子密钥分配(Quantum Key Distribution, QKD)突破了传统加密方法的束缚,采用量子态作为密钥的传输载体,根据量子力学原理,任何企图窃听量子密钥的操作都会改变量子状态,而通信的合法接收者从量子态的改变可以判断传送过程中是否存在窃听者,以决定是否采用该次传送的密钥。由于这种安全性不是基于计算安全性而是基于物理基础,所以即使是今后的量子计算机也不能破解,这就从根本上解决了密钥分配的安全性问题。

量子密码的原理

量子密码学的鼻祖是美国人威斯纳(S. Wiesner)。1976 年,美国哥伦比亚大学的威斯纳最早提出将量子力学与密码术相结合,并撰写了一篇《共轭编码》的论文。也许这种思想在当时看来过于离奇,甚至没有一家科学杂志愿意发表他的研究成果。直到 1983 年,他才有机会将论文发表在一家刊物上。幸运的是,IBM 公司的本内特(C. H. Bennett)和加拿大蒙特利尔大学的布拉萨德(G. Brassard)对此深入研究,于 1984 年在一次 IEEE 会议上提出第一个量子密钥分配协议,阐述了如何在一个不安全的公开信道上利用量子态使通讯双方安全地交换密钥(即著名的"BB84"协议),这是一个广泛应用于各种量子密码系统的协议,其安全性得到了理论证明。

一条典型的量子密钥分配链路如图 1 所示。通常秘密通信的双方为 Alice(发送方)和 Bob(接收方)。用来传输密钥的载体通常是单个光子,可以用其偏振状态(极化方向)、相位或者频率等物理量来携带信息。除了一个量子信道用于传输量子信号外,还需要一个经典信道从事相关的经典通信,经典

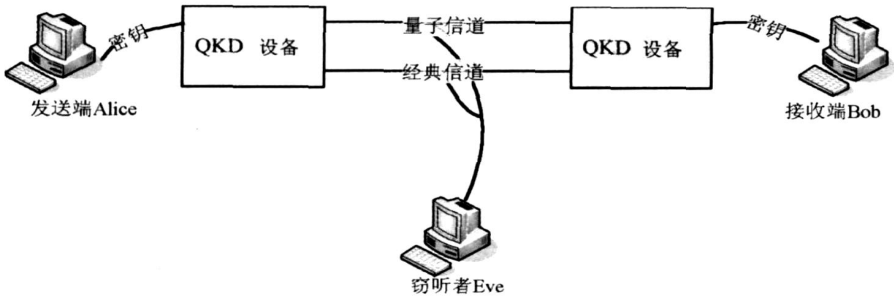


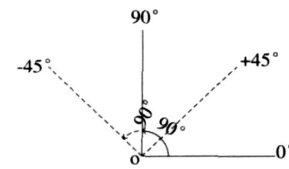
图 1　简化的量子密钥分配模型

信道可以不用保密,也就是说通信信息是公开的。而中途的窃听者 Eve 能很方便地窃听经典信道,但是不能随意对数据进行篡改(这个假定是比较合理的,可以通过消息认证等手段来保证)。

量子密码的安全性是由量子力学的几个基本规律决定的。第一是海森堡不确定性原理,也叫作测不准原理,即不可能同时精确测量两个非对易的物理量。经典物理学中粒子的坐标和动量可同时取确定值,但在量子力学中就不行,当其中一个完全确定时,另外一个就完全不确定。另外还有时间和能量的不确定性等。不确定关系是粒子波动性的必然结果,是微观粒子的固有性质,与测量仪器精度无关。第二是测量塌缩原理,即对量子态进行测量会不可避免地使该量子态塌缩到某一个本征态上。除非被测量的量子态正好是某个本征态,否则测量前后的量子态是不同的,这意味着对量子态进行测量都会留下痕迹。测量即破坏的道理在经典物理里面也是很奇怪的事情,但在微观世界却很普遍。第三就是量子不可克隆定理,即一个未知的量子态是无法被精确克隆的。这个定理虽然颠覆了我们平时数据可以任意拷贝的直观印象,但是却真实存在于量子世界。可以这样来理解:假设有一个未知的量子态,我们能够完全拷贝它,这就意味着能得到足够多的完全拷贝,可以任意精确地测出它的任两个不对易力学量(不断重复测量),但这与海森堡不确定关系矛盾,所以精确拷贝未知量子态是不可能的,量子不可克隆定理也是量子力学推导的必然结果。这三个原理是量子密钥分配安全性的物理保障。

下面我们简单介绍一下 BB84 协议,为了易于理解,我们以偏振编码系统为例,类似结果可以推广到相位编码系统中。BB84 协议采用单光子的 4 个偏振态(参见图 2),包括{水平偏振态 0°,垂直偏振态 90°, + 45°偏振态, - 45°偏振态},分别代表将单光子调制到相应的状态,可通过简单的偏振片来实现。其中{0°,90°}为一组相互正交的 2 个量子态,构成一组水平垂直基,不妨叫作 base0,{ ±45°}为另一组相互正交的量子态,构成斜对角基 base1。但 base0 和 base1 是非正交不兼容的,换句话说,就是拿斜对角基去测量 0°态时,会各有一半几率塌缩到 ±45°两个态上,得到不确定的结果,而拿水平垂直基去测量时,会确定地得到原始态。同样情况也发生在其他态上。

图 2　BB84 协议采用 4 个量子态,实线的两个正交态构成 base0、虚线的两个正交态构成 base1,base0 和 base1 是非正交的



双方可以约定{0°, + 45°}代表 bit0,{90°, - 45°}代表 bit1。Alice 端随机制备成其中一个态,比方水平偏振。经过传输后,Bob 也随机选取一组基来测量。如果选取和 Alice 制备态相兼容的基,比如水平垂直基,那么就会确定地测量到该量子态,获得 1bit 信息(上例就是 bit0);如果选取的基是斜对角基,则根据测量塌缩原理会各有一半概率坍塌到两个量子态上,得到两个不同的值。因此,Alice 和 Bob 为了传递信息,应选取制备基和测量基兼容的光子分配密钥。在实际操作中,由于传输信道对光子的衰减,只有一部分光子能够到达 Bob 端被探测器响应,Bob 在光子到达后公布他选取的测量基信息(是 base0 还是 base1),Alice 告诉他只保留和自己制备基一致的结果,这个过程就叫做对基,这样最后大概有 50 %的 bit 串被抛弃(参见图 3)。

现在我们来看看 Eve 的窃听是怎样被双方发现的。首先量子不可克隆定理禁止 Eve 通过复制量子态来重复测量,因此他必须采取截获光子测量再重发的策略。除非 Eve 和 Alice、Bob 的基都一致,他才会成功获得 1bit 信息。而当他选择和 Alice 不一致的测量基(50 %的概率)时(比如 Alice 是 base0、Eve 是 base1),如果 Bob 选择 base0 测量,根据对基协议,Alice 和 Bob 会生成 1bit 密钥,但是他们有一半的几率会得到不同结果。同样的情况也发生在

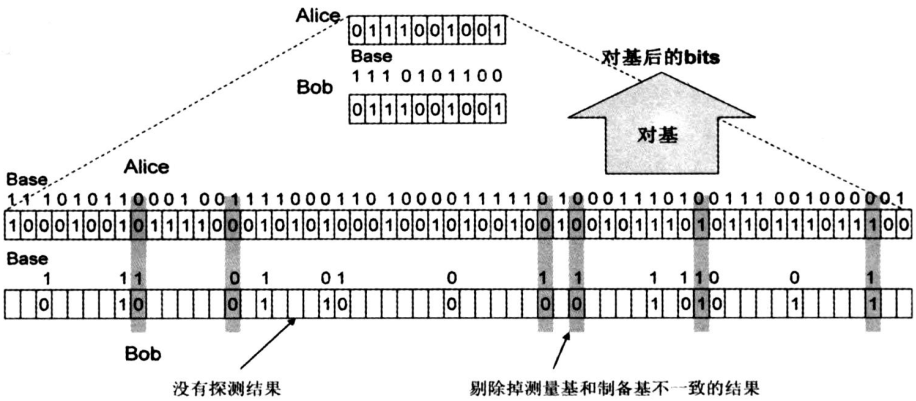


图3 对基过程:图中方框代表发送和探测到的数据,方框上面是相应的制备基(对应 Alice 端)或者测量基(对应 Bob 端),对于到达 Bob 端的光子(探测器有响应的时候),只保留制备基和测量基一致结果

简单的保密放大可以这样进行:假设 Alice 和 Bob 共享 2bit 信息,而 Eve 知道其中的 1bit 信息,那么 Alice 和 Bob 可以简单操作,比如把前 1bit 和后 1bit 异或,然后再把这个结果作为安全密钥,因为 Eve 无从知道另外 1bit 信息,所以对于结果也只能随机猜测。这样就消耗掉一部分密钥得到 Eve 完全无法知道的安全密钥。Alice 和 Bob 经过这些协议才能得到一个安全密钥,用于任何对称密钥系统。如果采用一次一密的加密算法,理论上则可实现绝对安全的加密系统。

Alice 制备 base1 时。综上所述,Eve 窃听一次引入误码的概率是 50 % ×50 % = 25 %,即不被发现的概率是 75 %。但如果 Alice 和 Bob 公开比较了 100bit,那么 Eve 不被发现的几率仅为 $(3/4)^{100}$(约 3×10^{-13}),可谓无处藏身。当然实际中 Eve 也可能做更复杂的攻击,以降低其引入的误码率,但 1999 年加拿大的 Lutkenhaus 从理论上证明当一组密钥的误码率不超过 11.5 %时密钥就是安全的。因此为了检测 Eve 的存在,Alice 和 Bob 只要选取对基之后的一段密钥(随后可以抛弃掉)进行误码率评估,看其是否超过安全上限,以决定这次产生的密钥是否保留。针对窃听者的检测过程正是量子密钥分配安全性的有力保障。

经过对基之后,理论上 Alice 和 Bob 产生的随机串相同,但由于 Eve 的窃听、实际系统的非对称性以及传输信道的噪声影响,还会存在一定误码,这个误码率通常在几个百分点左右,跟传统光通信 10^{-9} 量级的误码率差别很大,所以通常用 QBER(Quantum Bit Error Rate)来说明。由于任何对称加密算法都要求通讯双方所使用的密钥完全相同,因此必需一个消除误码的纠错过程。量子信息专家已提出多种纠错算法,这些算法在算法复杂度、通信效率上各有差别,目前尚无最佳方案。

做完纠错并未结束,因为 Eve 还可能获得一部分信息,这就需要一个保密放大(Privacy Amplification)过程将 Eve 的信息量降为零。保密放大最初虽是应量子密码的需求而研制的,但却是纯粹的经典信息处理过程,而且还能应用到经典通信的相关领域中,这充分说明量子信息交叉学科的性质。最

量子密码网络

尽管量子密码有着诱人的应用前景,但是受技术条件限制,目前的实际系统仍然存在很多问题。在密钥传送过程中,作为信息载体的光子在光纤传输时易受环境干扰而改变量子态,导致系统不稳定。另外,量子信号强度也会随传输距离增大而指数性衰减,因此实现远距离量子密钥传送难度很大。目前为止,报道的最远距离是 2007 年 5 月日本 NTT 公司和美国刚刚合作完成的 200 千米光纤实验,但仍不理想。

未来量子中继和自由空间技术可能会解决这个问题。量子中继是基于量子纠缠态的原理,通过传输光子保存到量子存储器中,再和别的中继一起进行 Bell 态联合测量传输光子,理论上可以把用户间的距离扩展到无穷远,但目前的技术难度非常大,大多还只是理论研究。而自由空间技术则是直接利用光子在大气层中传输,实现地面和近地卫星的通信,利用卫星的中转扩大传输距离。同样由于技术限制,目前还没有星地通信实验的报道,实验都集中在两个地面接收点之间,最近奥地利的研究小组已经将大气中的传输距离提高到了 144 千米。

除了距离,更需要解决的问题是如何满足多用户需求。因为目前的量子密码技术主要是点对点连接,只能是单一用户间的通信。对于多用户来说,如果完全靠这种连接非常耗费资源,1 个网络如果有 N 个用户的话就需要有 $N(N-1)/2$ 个连接,这对

于网络建设来说是不能承受的。如何有效降低多用户连接的成本,正是亟待解决的问题。建设网络还有一个重要原因就是网络能增强用户间通信的可靠性,因为任何两个用户之间可能存在多条可用路径,当一条路径因为窃听或者故障不能正常工作时,其他路径可迅速接替其工作,保证用户的正常通信。

正因为其重要性,近年来美欧日等国家和地区都不约而同加强对量子网络的投入和研究。2006年,美国国防部高级研究项目管理局(DARPA)宣布建设一个拥有8个节点的QKD网络,包括哈佛大学、波士顿大学、BBN公司和美国国家标准技术局(NIST)多家研究机构,目前该网络还在不断完善和扩建。欧洲的英法德意等多个国家则参与了基于量子密码的安全通信项目(SECOQC),计划到2008年建设一个覆盖欧洲大陆的实际可用的量子密码网络,包括了数条自由空间的星地通信链路。日本三菱公司和NEC公司于去年合作完成实际通信线路上不同设备之间的兼容性测试,为今后的网络建设做好准备。

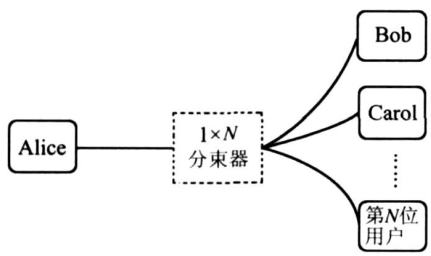


图4 1×N分束器的量子密码网络

最早的量子密码网络实验是汤生(Paul. D. Townsend)小组于1997年在《自然》杂志上发表的。他们采用无源光器件分束器(splitter)实现Alice和多个Bob的量子密钥分配,Alice发送的光子经过分束器时会有1/ N的概率达到特定的Bob端(见图4)。这个方案简便易行,Alice能够同时和多个Bob分配密钥,显而易见效率偏低,因为随着用户数增加到N,每个用户的码率都下降到单个用户的1/ N。除了效率问题外,网络的另外一个缺点是严重依赖于管理员Alice,如果Alice发生故障则整个网络就会瘫痪。此外,一般用户之间也不能直接进行量子通信,必须依靠Alice中转密钥,这样又会导致对Alice的信任问题。不管怎样,这个方案在需要低成本的环境下还是可行的。

除了分束器之外,利用商业上成熟的波分复用(Wavelength Division Multiplex,WDM)技术也能构建一个简单网络,Alice依靠波长可变的激光器,在同一根光纤上复用传输经过WDM后按照不同波长到达不同用户,这样做的好处是不会因用户增加而降低传输率。国外多个研究小组都提出了基于WDM技术的网络方案,但和分束器方案一样,没有很好地解决普通用户间的通信问题,而且整个网络依赖一个主控制端用户。由国内科研人员改进并设计的拥有自主知识产权的4端口量子路由器(其结构见图5),能够同时满足4用户间的量子密钥分配,并有效解决了通信效率问题。利用该路由器,任一用户都可通过3个波长(λ_1、λ_2、λ_3)的光子和另外3个用户同时通信,并且由分配给每个用户的波长自动寻址,而用户只需对外铺设一根光纤。值得注意的是,这个结构下每个用户的作用是等同的,从而减轻了网络对某一特定用户的依赖性。2007年3月,有关实验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在3个不同地点的4用户长时间稳定量子密钥分配和视频保密通信,初步验证了量子路由器的功能和密钥分配系统的实用性。当然该方案也有缺点,即要求每个用户都要有多个发射端和接收端设备,在成本方面会有一定劣势。综合来看,目前的量子网络都只是提出一些实验方案,并没有经典网络那样完善和成熟的技术标准。寻求在满足多用户前提下尽量提高通信效率并降低通信成本的网络仍是目前研究的一个热点课题。

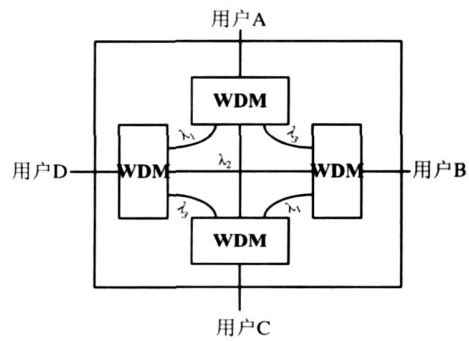


图5 4端口量子路由器结构图

除了自身发展之外,量子密码和经典网络的结合也是一个亟需完善之处。为进一步节省通信成本,可以让量子光和经典光在同一根光纤上传输(通过WDM耦合可以很容易办到),但是因为经典光信号强度太大,会极大干扰量子光,降低其信噪比,如何降低这些影响、设计出可靠的量子传输系统是必须面对的工程问题。同时由于目前光通信常用的中

能 量 条 件 简 介

卢昌海

大家知道,广义相对论的场方程(即爱因斯坦场方程) $R_{\mu\nu} - (1/2) g_{\mu\nu}R = 8\pi G T_{\mu\nu}$是一组有关时空度规的二阶非线性偏微分方程,求解这样的方程组极其困难。在 20 世纪 60 年代初以前,物理学家对爱因斯坦场方程的很大一类研究都局限于在各种简化条件(比如特定的对称性)下求解场方程。这方面最著名的成果是施瓦西于 1916 年得到的施瓦西解,其度规为(m 为质量参数)

$$ds^2 = (1 - \frac{2m}{r})dt^2 - (1 - \frac{2m}{r})^{-1}dr^2 - r^2 d\Omega^2 ;$$

以及弗里德曼于 1922 年得到的弗里德曼解,其度规(通常被称为罗伯逊 - 沃克度规)为(R 为标度因子, k 取值为 0、- 1 或 1,分别对应于平直、负常曲率及正常曲率空间)

$$ds^2 = dt^2 - R^2(t)(\frac{dr^2}{1 - kr^2} + r^2 d\Omega^2) 。$$

这两个度规分别是广义相对论在天体物理及宇宙学上应用最为广泛的度规。但这两个解的发现也带来共同的问题,就是它们所对应的度规均具有奇异性。

施瓦西度规是一个静态度规,其奇异性(由上述表达式中易于看到)出现在 $r = 0$ 及 $r = 2m$ 处。其中 $r = 2m$ 处的奇异性(一度被称为施瓦西奇点),后来被证明只是坐标选择导致的表观奇异性,通过坐标变换可以消除;而 $r = 0$ 处的奇异性则是真正的物理奇点,时空曲率在趋近该点时趋于发散,这个奇点被称为曲率奇点。罗伯逊 - 沃克度规由于是一个动态度规,其情形稍微复杂些。当 $k = 1$(即空间具有正曲率)时这一度规在 $r = 1$ 处似乎具有奇异性,但这也是坐标选择导致的表观奇异性。除去这一表观奇异性,从形式上看,罗伯逊 - 沃克度规似乎没有其他显而易见的奇异性。但若将这一度规代入场方程中研究它的动力学演化,就会发现对于我们观测到的膨胀宇宙来说,只要宇宙当前的物质分布满足一个很宽泛的条件,罗伯逊 - 沃克度规中的标度因子 $R(t)$ 在过去某个有限时刻就必定等于零。在那个时刻(通常定义为 $t = 0$)宇宙的空间线度为零,物质密度则发散,因此那是一个物理奇点,被称为宇宙学奇点或大爆炸。

继器(比如掺铒光纤放大器 EDFA)不能处理量子信号,所以还必须设计一个旁路设备以方便量子光通过。在软件方面,针对目前因特网广泛使用的 VPN 协议(比如 IPSec、PPTP 等),还需做些修改以容纳量子密钥分配技术,这样量子密码才能得到更广泛的应用。

由此可见,建设量子密码网络并非易事,还涉及网络工程和现代光通信等领域,需要物理学家和网络工程师、通信工程师、软件工作者的通力合作。

量子密码技术作为量子信息科学的排头兵,在将信息安全提升到一个新高度的同时,也必将促进相关量子信息器件(如单光子源、单光子探测器、量子中继器等)的发展,为今后更加广阔的量子通信、量子计算打下深厚的技术基础。

(安徽省合肥市中国科学技术大学,中国科学院量子信息重点实验室 230026)

作者简介

温浩,男,1981 年 5 月生于四川自贡。2003 年获得中国科学技术大学电子信息科学与技术专业学士学位,后继续在该校中国科学院量子信息重点实验室攻读博士学位。主要研究兴趣在量子密码,量子密码网络的架构与实现。

郭光灿教授,男,1942 年 12 月 9 日生于福建惠安。1965 年毕业于中国科学技术大学无线电电子学系,2003 年当选为中国科学院院士。现任中国科学院量子信息重点实验室主任,中国物理学会量子光学专业委员会主任,国家科技部 973 项目“量子通信与量子信息技术”首席科学家,国家基金委创新研究群体学术带头人。