文章编号: 1001-3806(2004)03-0281-05

自由空间量子密码术的发展状况

张光宇[1,2],马 晶[1],谭立英[1]

(1. 哈尔滨工业大学 可调谐激光技术国家级重点实验室,哈尔滨 150001; 2. 哈尔滨理工大学 应用科学学院,哈尔滨 150080)

摘要: 综述了自由空间量子密码术的发展状况。其中包括自由空间量子密码术协议和量子密钥分配过程,以及自由空间量子密码术实验分析。

关键词: 量子密码术;量子密钥分配;自由空间;单光子技术

中图分类号: O431.2 **文献标识码**: A

Developments of free-space quantum cryptography

ZHANG Guang-yu[1,2], *MA Jing*[1], *Tan Li-ying*[1]

(1. National Key Laboratory of Tunable Laser Technology, Harbin Institute of Technology, Harbin 150001, China; 2. College of Applied Sciences, Harbin University of Science and Technology, Harbin 150080, China)

Abstract: The recent development of free-space quantum cryptography is reviewed, which includes free-space quantum cryptography protocols and the process of quantum key distribution. Free-space quantum cryptography is analyzed experimentally.

Key words: quantum cryptography; quantum key distribution; free-space; single photon technique

引 言

当今时代,保密通信享有特殊的重要性。如何建立最安全的全球卫星通信系统更具有重要意义。量子密码术(quantum cryptography, QC)因其在保密通信中的绝对安全性而备受关注,并预期成为将来对信息进行加密的重要手段。它打破了经典密码通信的极限,将量子物理与密码学相结合,很好地解决了通信的可靠性问题。

目前,从数学或经典物理还无法找出一种绝对安全的密码通信系统。虽然量子计算机还没有成为现实,但已经对传统密码术构成了巨大的威胁。只有量子密码术能够抵挡量子计算机的攻击。

保密通信中的关键是密钥,通信安全就在于保证密钥的安全。量子密码术,更确切地说是量子密钥分配(quantum key distribution, QKD),采用单光子通信技术,通信双方 Alice 和 Bob 通过共同的量子信道(如光纤或自由空间等)和经典信道(如以太网或电话线等)建立、传输密钥。根据量子力学的测不准原理和量子不可克隆原理,任何窃听者 Eve 的存在都会被发现,从而保证密钥的绝对安全,也就保证了加密信息的绝对安全。

现在,对量子密钥分配的研究主要集中在两个方面:基于光纤量子信道和基于自由空间量子信道。对于自由空间量子信道,激光通信链路包括地面点对点、卫星-地面站和卫星间链路。为了实现全球最安全的卫星通信,就需要将量子密钥在自由空间(卫星)传送。这就提出要进行地面点对点、卫星-地面站和卫星间激光通信链路的量子密钥分配问题。

1 自由空间量子密码术

量子密码术是密码术与量子力学相结合的产物,它的理论首先是由美国哥伦比亚大学的 WIESNER 于 1970 年提出的[1]。在他的思想启发下,美国 IBM 公司的 BENNETT 和加拿大 Montreal 大学的 BRASSARD 于 1984 年提出了第 1 个量子密码术协议。它是基于两组共轭基,采用单光子偏振态编码的四态量子密钥分配方案,现称之为 BB84 协议[2]。1992 年,BENNETT 又提出一种比 BB84 协议简单、但量子效率减半的协议。它采用任何两个非正交的光

作者简介:张光宇(1971-),男,讲师,博士研究生,主要从事卫星光通信和量子密码术方面的研究。

E-mail: zhangguangyu@hit.edu.cn

收稿日期:2003-08-12;收到修改稿日期:2003-10-18

子偏振态编码,称为 B92 协议[3]。基于 einstein-podolsky-rosen(EPR)佯谬,英国的 EKERT 于 1991 年提出用双量子纠缠态来实现量子密码术,称为 EPR 协议[4]。1995 年,以色列的 GOLDENBERG 和 VAIDMAN 又提出基于正交态的量子密码术协议,其绝对安全性由正交态的量子不可克隆原理保证[5,6]。在这些协议基础上,各个国家的科研人员又提出了不少其它协议[7~11],但大都在现有实验条件下还很难实现,在这里不做进一步的讨论。

量子密码术的绝对安全性由量子力学基本原理保证。所谓绝对安全性[12]是指窃听者智商极高,采用最高明的窃听策略,使用一切可能的先进仪器,在这些条件下,密钥仍然是安全的。窃听者的基本策略有两类:一是通过对载有经典信息的量子态进行测量,从其测量的结果来获取所需的信息。但是由量子力学的测不准原理可知,对量子态的测量会干扰量子态的本身,因此,这种窃听方式必然会留下痕迹而被合法用户所发现。二是避开直接量子测量而采用量子拷贝机(对量子态进行复制)来拷贝载有信息的量子态,窃听者将原量子态传送给接收者,而留下拷贝的量子态进行测量以窃取信息,这样就不会留下任何被发现的痕迹。但是量子不可克隆原理保证窃听者不会成功,任何物理上可行的量子拷贝机都不可能克隆出与输入量子态完全一样的量子态来。因此,量子密码术原则上可以提供不可破译、不可窃听的密码通信系统。

目前,自由空间量子密码术的研究主要集中在两个方面:(1)自由空间信道地面点对点大气激光通信链路量子密钥分配实验的研究[13~19];(2)卫星-地面站和卫星-卫星间激光通信链路量子密钥分配的可行性分析研究[20]。如何在卫星-地面站和卫星-卫星间建立绝对安全的量子密钥,将是未来该领域的主要研究方向。

在自由空间信道地面点对点大气激光通信链路量子密钥分配实验方面,目前国外进展很快。美国 Johns Hopkins 大学采用 BB84 协议,用 He-Ne 激光器和电光调制器产生光脉冲,成功地在白天室外条件下传输单光子,自由空间光程为 75m,比特传输率为 1kHz,误码率为 2%。美国 Los Alamos 国家实验室首先进行了自由空间室内光路 205m 的量子密码术实验。随后,他们采用 B92 协议,进行了夜晚条件下室外光路 950m 和白天室外光路 500m 的量子密码术实验,误码率分别为 1.5%和 1.6%。后来,他们又进行了 1.6km 自由空间量子密码术实验。该实验是在白天室外条件下,采用 B92 协议,平均误码率为 5.3%。近年来,德国 Ludwig-Maximilian 大学等单位合作创造了自由空间量子密钥分配的新记录,达到 23.4km。该实验采用 BB84 协议,光源为每个脉冲 0.08 个光子,光损耗约为 18dB,误码率低于 6%。

在中国,自由空间量子密码术的研究还处于起步阶段。1995 年,邵进等人采用 BB84 协议在国内首次做了演示性实验[21],华东师范大学张涌采用 B92 协议做了实验[22],这都是在距离较短的自由空间里进行的。

2 自由空间量子密码术协议

根据自由空间量子信道的特点,对于自由空间量子密钥分配,主要采用 BB84 协议和 B92 协议。

2.1 BB84 协议

BB84 协议是第 1 个量子密码术协议,属于基于两个非对易可观测量的量子密钥分配。它的特点是采用 4 个非正交态作为量子态,且这 4 个态分属于两组共轭基,每组共轭基中的 2 个态是相互正交的。两组基互为共轭指的是,一组基的任一基矢在另一组基的任何基矢上的投影都相等。因此,对于某一组基的基矢量子态,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。BB84 协议通过量子信道传输具有一定偏振态的光子,通过经典信道来传输经典信息。下面以光子的偏振态为例说明 BB84 协议的基本原理,如表 1 所示。

表 1 BB84 协议的基本原理

Alice 用线偏振基发送的光子	Bob 用线偏振基接收	Bob 完全确定光子偏振态:水平或垂直
	Bob 用圆偏振基接收	以 5%概率得到左旋或右旋圆偏振态
Alice 用圆偏振基发送的光子	Bob 用线偏振基接收	以 5%概率得到水平或垂直线偏振态
	Bob 用圆偏振基接收	Bob 完全确定光学偏振态:左旋或右旋

为了在发送者 Alice 和接收者 Bob 之间建立密钥,Alice 随机地在两组共轭基,圆偏振基和线偏振基,4 个非正交态,左旋圆偏振态和右旋圆偏振态,水平线偏振态和垂直线偏振态中选择一个发送给 Bob。为了确定 Alice 发送的态,Bob 随机地选择两个偏振量进行测量。假定 Alice 发送的态是垂直线偏振态。如果 Bob 选择线偏振测量量,则其可以完全确定 Alice 发送的态。若 Bob 选择圆偏振测量量,

由于线偏振量和圆偏振量互为共轭,线偏振态在圆偏振量的测量之下,投影到圆偏振基中的一个态上,而原来的态被完全破坏了。水平线偏振态在圆偏振测量量测量后各有 50 %的概率得到左旋或右旋圆偏振态。根据量子测量理论,若事先不知道量子态的偏振状态,则仅由一次测量结果是无法确定被测体系测量前的状态,因而 Bob 不能根据他的测量结果确定 Alice 发送的态。下面给出具体的密钥分配过程:(1) Alice 发送给 Bob 一系列偏振方向随机选择的单光子序列;(2) Bob 随机选择线偏振基或者圆偏振基对光子的偏振方向进行测量;(3) Bob 通过经典信道公布所用的测量基(线偏振或圆偏振),但不公布测量结果;(4) Alice 通过经典信道告诉 Bob 哪些测量基是正确的;(5) Alice 和 Bob 保留测量基一致时的结果,放弃其它数据,从而建立起密钥。

2.2　B92 协议

B92 协议是基于任何两个非正交量子态的量子密钥分配方案。下面以光子的偏振态为例,说明 B92 协议的基本原理,如表 2 所示。

表 2　B92 协议的基本原理

Alice 用 45°偏振片发送的光子(1)	Bob 用 45°偏振片接收	Bob 接收不到光子
	Bob 用 90°偏振片接收	某些光子通过被 Bob 接收到
Alice 用 0°偏振片发送的光子(0)	Bob 用 45°偏振片接收	某些光子通过被 Bob 接收到
	Bob 用 90°偏振片接收	Bob 接收不到光子

为了传送密钥,Alice 以 0°和 45°两个偏振方向的光子代表二进制比特值 0 和 1,向 Bob 随机发送单光子脉冲序列,而 Bob 随机选择 90°或 - 45°两个偏振方向进行接收。如果 Bob 的偏振片方向垂直于 Alice 发送方向(50 %几率),Bob 接收不到任何光子;若成 45°,则有 50 %几率接收到光子。而一旦接收到光子,Bob 就会知道光子的偏振方向,因为只有一种可能性。因此,Bob 以 90°(- 45°) 方向接收到光子,他就知道 Alice 发送的偏振方向是 45°(0°),对应着比特 1 (0)。平均而言,有 3/4 的光子将不能被 Bob 接收到,但是,Bob 却可以确切地知道那少数通过偏振片而被他接收到的光子的比特值。在接收完 Alice 所发送的偏振光子后,Bob 可以通过经典信道告诉 Alice 哪些光子被他接收到了。这样,双方就建立起密钥。

3　量子密钥分配过程

量子密码术协议在理论上都具有绝对安全性,这由量子力学基本原理保证。但是,在实际量子密码通信系统中,为了产生安全的量子密钥,量子密码术协议需要完成 5 个过程:身份认证;单光子传输;数据筛选;数据纠错;保密加强。整个过程如图 1 所示。

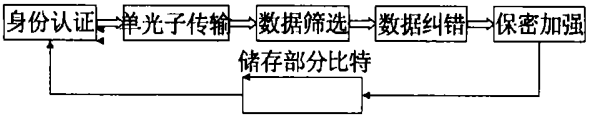

图 1　量子密钥分配过程

3.1　身份认证

进行身份认证的目的是让通信的一方 Alice 知道她实际上是和另一方 Bob 在通信。如果 Alice 和 Bob 不能证明他们彼此保持通信,那么聪明的窃听者 Eve 就能够使 Alice 相信他就是 Bob,使 Bob 相信她就是 Alice,这就是所谓的中间人攻击。若不进行身份认证就无法避免 Eve 的这种攻击。Alice 和 Bob 通常使用以前密钥中的部分比特进行核对彼此的身份。

3.2　单光子传输

经过身份认证,Alice 和 Bob 确信他们已经彼此通信,Alice 就通过量子信道开始协议。对于 BB84 协议或 B92 协议,Alice 发送给 Bob 一串随机选取的具有确定偏振态的光子。理想情况下,一个密钥比特用一个光子发送。但是,采用高度衰减激光脉冲作为单光子源,偶尔也多于一个光子。

3.3　数据筛选

Bob 接收到 Alice 发送来的光子后,Alice 和 Bob 就通过经典信道进行数据筛选。对于 BB84 协议,Alice 和 Bob 互相通报他们用来制备或测量每个光子使用的基。这样大约有一半的机会,他们对同一光子使用了同样的基。从而保留这些光子而舍弃其它光子。对于 B92 协议,Bob 只需告诉 Alice 他测量到了哪些光子。从而保留这些光子作为原始密钥。

对于上面两个协议,Alice 和 Bob 并不需要通报光子的比特值 0 或 1。因此,Eve 通过经典信道不能获得 Alice 和 Bob 拥有的比特序列的任何信息。代替被动窃听,Eve 就不得不通过量子信道采取主动攻击。因为单光子是不可分的,所以 Eve 不能用光束分离器窃听密钥的传输。又因为量子不可克隆原理,也不能进行拷贝。而且,量子态的非正交性保证,如果 Eve 进行测量,那么由于波函数态的不可逆

坍缩,她将被探测到,从而在 Alice 和 Bob 筛选的密钥中引起误码率的增加。因此,Alice 和 Bob 可以通过量子信道监视 Eve 的窃听。

3.4 数据纠错

在数据筛选之后,Alice 和 Bob 并不能保证剩下的数据没有误码。单光子源和探测器将引入误码,背景不能完全被消除。他们必须采取措施验证数据。Alice 和 Bob 通常采用奇偶校验法,即比较一个公开约定的随机子集的奇偶性。

3.5 保密加强

保密加强是一种蒸馏技术。Alice 和 Bob 经过身份认证、单光子传输、数据筛选和纠错后,得到一个部分保密的密钥。为了使 Eve 对密钥比特获得尽可能少的信息量,采取保密放大技术,即通过一定的编码规则,缩短密钥比特串,从而使得 Eve 所掌握的密钥信息量减少到 1bit 以下。

最后,储存一些密钥比特用于制备下一个密钥的身份认证。

4 自由空间量子密码术实验及分析

目前,自由空间量子密码术实验主要集中在地面点对点大气激光通信链路。1989 年,BENNETT 和 BRASSARD 等人完成了自由空间量子密钥分配的第一个演示性实验[23]。实验中光子在空气中传播了 32cm,误码率为 4 %,比特率为 105bits/ 10min。在随后 10 多年的时间内,自由空间量子密码术实验取得了很大进展。表 3 中列出的是主要进展情况。

表 3 已进行的自由空间量子密码术实验

实验小组	光路	光程	协议	误码率	比特率
Johns Hopkins	白天室外	75m	BB84	2 %	1kHz
Los Alamos	白天室外	500m	B92	1.6 %	5kHz
Los Alamos	白天室外	1.6km	B92	5.3 %	3kHz
Qineti Q	夜晚室外	1.9km	BB84	6.5 %	81Hz
Ludwig-Maximilian	夜晚室外	23.4 km	BB84	4.77 %	367Hz

自由空间量子密码术主要包括地面点对点、卫星-地面站和卫星间激光通信链路的量子密钥分配。对于地面点对点和卫星-地面站间的量子密钥分配,还要考虑大气湍流的影响。下面针对自由空间量子信道的特点,对量子密码术实验进行以下分析。

4.1 协议的选择

在已进行的自由空间量子密码术实验中,大都采用 BB84 协议和 B92 协议。这是因为,虽然量子密码术协议有很多种,但是对于自由空间激光通信链路,尤其是卫星-地面站间链路,BB84 协议和 B92 协议易于实现。B92 协议与 BB84 协议相比,实验中所需要的单光子源和探测器的数目减少了一半,偏振片的数目由 4 个减为 2 个,这就大大简化了实验装置。但代价是量子效率也减少了一半。

4.2 波长的选择

对于地面点对点和卫星-地面站间激光通信链路的量子密钥分配,大气湍流对光子的影响是主要因素,湍流效应主要发生在最底层大气。在这里,关键的问题是保证光子在穿过大气时不被吸收,并且在传播中要保持其偏振方向不发生改变。这就需要选择合适的大气窗口。NORDHOLT 等人[20]选择波长为 772nm 的光子。虽然波长更长的光子也不会被大气吸收,但是它们对大气扰动比较敏感。大气湍流会改变局域大气的折射系数,从而导致光子偏振方向的弯曲。大气湍流的典型尺度为几十厘米,772nm 已足够短,足以避免这种影响。而且在这一波长,大气传输率高达 80 %,单光子探测器的效率高达 65 %,大气的退极化效应可以忽略。

4.3 单光子源

在已进行的自由空间量子密钥分配实验中,单光子源均采用高度衰减激光脉冲,即弱激光脉冲。这样的光脉冲不是单光子数态而基本上是相干态,即光子不是一个个等间距地分布而是服从 Poisson 分布。这样就可能出现一个脉冲含有一个以上光子的情况。

为了得到单光子数态,采用具有极低平均光子数 μ 的相干态来近似单光子数态。用半导体激光器和衰减片产生的弱激光脉冲即可实现这样的相干态,并且为大多数实验所采用。在这样一个相干态中找到 n 个光子概率的 Poisson 分布为:

$$P(n,\mu) = \frac{\mu^n}{n!}e^{-\mu} \tag{1}$$

一个非空弱相干脉冲含有一个以上光子的概率为:

$$P(n>1 \mid n>0,\mu) = \frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)} \approx \mu/2 \tag{2}$$

这里 μ 可以控制得任意小。但当 μ 很小时,多数脉冲是空的,即:

$$P(n=0,\mu) \approx 1-\mu \tag{3}$$

目前,大多数实验取 $\mu=0.1$,这意味着约 5 %的非空脉冲含有一个以上的光子。如果 Alice 选择较少的平均光子数,那么大部分时间链路都处于闲置状态,量子信道效率很低。相反,如果 Alice 选择较多的平

均光子数,那么 Eve 原则上就可以窃听到多光子脉冲中的一个光子。对于自由空间量子信道,每个脉冲的平均光子数还与 Alice 和 Bob 间大气状况有关。因此,如何优化 μ 值,提高量子信道效率就显得非常重要。

4.4　单光子捕获技术

自由空间量子密钥分配强烈依赖于通过湍流大气在高背景下单光子的传输和检测。为了可靠地探测 Alice 发送来的光子,Bob 通常采用空域滤波、频域滤波和时域滤波。空域滤波要求小的接收视场角和接收机的精确瞄准。对于时域滤波,1550nm 参考脉冲(不载有密钥信息)被用来设置一个短的时间窗口(如 1ns)。参考脉冲后的 100ns,单个 QKD 光子到达。对于轨道高度为 800km 的低轨卫星,经过 100ns 卫星移动的距离还不到 1mm。因此,通过使用参考脉冲,光子到达时刻传达给接收机,并由此确定开启窗口的时间。这个短的时间窗口强烈地减少了背景光子数。采用窄带滤波背景可以被进一步地减弱。

5　结束语

自由空间量子密码术作为量子通信领域的一个新的生长点,无疑具有广泛的应用前景。但是,目前该领域在技术上的实现却面临着许多严重困难。但这无损于量子通信的发展趋势,反过来这正是对人类智慧和能力的又一次挑战。可以相信,自由空间量子密码术的实用化已为期不远。

参　考　文　献

[1] WIESNER S J. Conjugate coding [J]. SIGACT News, 1983, 15 (1):78～88.

[2] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing [A]. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing [C]. New York: IEEE, 1984. 175～179.

[3] BENNETT C H. Quantum cryptography using any two nonorthogonal states [J]. Phys Rev Lett, 1992, 68(21):3121～3124.

[4] EKERT A K. Quantum cryptography based on Bell's theorem [J]. Phys Rev Lett, 1991, 67(6):661～663.

[5] GOLDENBERG L, VAIDMAN L. Quantum cryptography based on orthogonal states [J]. Phys Rev Lett, 1995, 75(7):1239～1243.

[6] MOR T. No cloning of orthogonal states in composite systems [J]. Phys Rev Lett, 1998, 80(14):3137～3140.

[7] INOUE K, WAKS E, YAMAMOTO Y. Differential phase shift quantum key distribution [J]. Phys Rev Lett, 2002, 89(3):037902-1～037902-3.

[8] GROSSHANS F, GRANGIER P. Continuous variable quantum cryptography using coherent states [J]. Phys Rev Lett, 2002, 88(5):057902-1～057902-4.

[9] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. Phys Rev, 2002, A65: 032302-1～032302-3.

[10] SILBERHORN C, KOROLKOVA N, LEUCHS G. Quantum key distribution with bright entangled beams [J]. Phys Rev Lett, 2002, 88(16):167902-1～167902-4.

[11] FUNK A C, RAYMER M G. Quantum key distribution using nonclassical photon-nmuber correlations in macroscopic light pulses [J]. Phys Rev, 2002, A65:042307-1～042307-5.

[12] 郭光灿. 量子信息引论 [J]. 物理, 2001, 30(5):286～293.

[13] JACOBS B C, FRANSON J D. Quantum cryptography in free space [J]. Opt Lett, 1996, 21(22):1854～1856.

[14] BUTTLER W T, HUGHES R J, KWIAT P G *et al*. Free-space quantum-key distribution [J]. Phys Rev, 1998, A57(4):2379～2382.

[15] HUGHES R J, BUTTLER W T, KWIAT P G *et al*. Quantum cryptography for secure free-space communications [J]. SPIE, 1999, 3615:98～103.

[16] HUGHES R J, BUTTLER W T, KWIAT P G *et al*. Free-space quantum cryptography in daylight [J]. SPIE, 2000, 3932:117～126.

[17] BUTTLER W T, HUGHES R J, LAMOREAUX S K *et al*. Daylight quantum key distribution over 1.6km [J]. Phys Rev Lett, 2000, 84(24):5652～5655.

[18] RARITY J G, GORMAN P M, TAPSTER P R. Secure key exchange over a 1.9km free-space range using quantum cryptography [J]. Electron Lett, 2001, 37:512～514.

[19] KURTSIEFER C, ZARDA P, HALDER M *et al*. Long distance free space quantum cryptography [J]. SPIE, 2002, 4917:25～31.

[20] NORDHOLT J E, HUGHES R J, MORGAN G L *et al*. Present and future free-space quantum key distribution [J]. SPIE, 2002, 4635:116～126.

[21] 邵　进,吴令安. 用单光子偏振态的量子密码通信实验 [J]. 量子光学学报, 1995(1):41～44.

[22] 张　涌. 量子保密通信研究 [D]. 上海:华东师范大学, 1997. 40～61.

[23] BENNETT C H, BESSETTE F, BRASSARD G *et al*. Experimental quantum cryptography [J]. Cryptology, 1992, 5:3～28.