量子保密通信的技术现状及安全性

王向斌[1] 尹 浩[2] 马怀新[2] 彭承志[1] 杨 涛[3] 潘建伟[3]

(1 清华大学物理系 北京 100084)

(2 中国电子设备系统工程公司 北京 100039)

(3 中国科学技术大学微尺度物质科学国家实验室 合肥 230026)

摘 要 理论上,量子密钥分发可以带来绝对安全的保密通信. 但是真实系统的量子密钥分发的安全性需要进一步证明. 现有的基于弱相干态的量子密码实验在光子数分离攻击下是完全不安全的. 诱骗信号方案(decoy - state method)及纠缠对分发方案可以实现基于现有技术的、真实系统的绝对安全量子密钥分发.

关键词 量子保密通信,安全性,BB84 方案,诱骗信号方案,光子数分离攻击

The security and recent technology of QKD

WANG Xiang-Bin[1] YIN Hao[2] MA Huai-Xin[2] PENG Cheng-Zhi[1]

YANG Tao[3] PAN Jian-Wei[3]

(1 *Department of Physics, Tsinghua University, Beijing* 100084, *China*)

(2 *China Electronic System Engineering Company, Beijing* 100039, *China*)

(3 *Hefei National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Hefei* 230026, *China*)

Abstract In principle, quantum key distribution (QKD) can be used to make unconditionally secure private communication. However, the security of existing real system for QKD needs to be carefully examined. Actually, the existing experiments based on weak coherent states are insecure under photon-number-splitting attack. Fortunately, the decoy-state method and the entanglement-distribution method can be used to realize the unconditionally secure QKD based on real-life system with existing technology.

Keywords QKD, security, BB84 method, decoy-state method, photon-number-splitting attack

1 背景

保密通信最直接的办法是让通信双方先共享一串密码,然后以此密码对通信内容加密、解密. 然而,他们必需使用秘密信道才能建立共同密码. 经典通信不存在可证实的绝对安全的秘密信道,因为窃听者原则上总可以做到获取信息而又不留痕迹. 或者说,当我们使用秘密信道作密钥分发(key distribution)时,我们无法证实密钥没有被窃听. 换言之,我们无法证明任何经典密钥分发(classical key distribution)是安全的.

20 世纪 70 年代,数学家提出了用于保密通信的"公钥"方法("public key" system). 这种方法不需要保密通信的发信方(Alice)接受方(Bob)拥有共享密码. 在此系统中,Bob 公开其公钥 X,但隐藏密钥 K. 任何人,比如 Alice 想向 Bob 发送密信 P,可先利用公钥 X 对 P 编码而形成 $E\_X(P)$. 只要拥有 X,$E\_X(P)$ 可简单算出. 但是,$E\_X(P)$ 的解码,即 $D\_K(E\_X(P)) = P$ 运算极其复杂,除非拥有密钥 K,而 Bob 是唯一拥有密钥 K 的人. 然而,这种解码的复杂性迄今并无数学证明. 以被广泛使用的 RSA 法为例,其核心是对大数分解运算的复杂性假定. 其安全性隐患在于这种假定从未获得证明. 更坏的消息是,使用量子算法,大数分解可以被有效地给出. 这就是说,在经典算法范围内,RSA 系统的安全性未获证

2006 - 01 - 08 收到

明:在量子算法范围内,RSA 系统肯定不安全[1]. 山东大学王小云等[2—4]人近年来以经典算法对两种经典密码系统的成功破解加剧人们对经典密码系统安全性的忧虑,即便窃听者仅采用经典算法.

当然,经典公钥系统并非保密通信的唯一方法. 为实现绝对安全的保密通信,C. H. Benett 与 G. Brassard 与 1984 年提出了量子密钥分发方案[5]. 这种方案的安全性基于量子力学基本原理. Benett 与 Brassard 的具体量子密钥分发方案后来被称为 BB84 方案[5]. 我们将从 BB84 方案[1]开始,综述量子密码的方案,安全性[6—8],以及真实系统的实验现状[10—12,18—20]和安全性[13—17].

2 BB84 方案及其绝对安全性

2.1 BB84 方案

在 BB84 密钥分发方案中[5],以量子态对应于经典二进制码(bit). 为简单起见,我们考虑一种最简单的量子态:光子偏振(见图 1). 水平或 45°偏振对应于经典比特 0;竖直或 135°偏振对应于经典比特 1. Alice 向 Bob 发射一系列单光子偏振态. 每个光子的偏振从水平,竖直,45°或 135°中随机选出. 或者说,Alice 随机使用了两组基,我们称之为直角基(水平,竖直偏振)及斜角基(45°偏振或 135°偏振). 对每个飞入光子,Bob 随机选用直角或斜角基测量其偏振(对每个飞入光子 Bob 只能选用一组基测量). 这样,在 BB84 方案中,对每个飞入光子,有一半概率 Bob 使用错误基测量,即 Bob 的测量基与 Alice 的态制备基不一样. 他们通过经典公开通道比较每个光子的制备基与测量基. Bob 丢弃那些使用了错误基得到的测量结果. 对于剩下的测量记录,Bob 随机抽取一部分与 Alice 对照,检验每组基下各态的误码率并丢弃这些公开宣布的用作检验的测量结果. 若误码率过大,他们放弃所有数据. 否则,他们再对剩余数据(我们称之为初始码,即 raw key)通过纠错(error correction),隐私放大(privacy amplification)而提炼出最终码(final key).

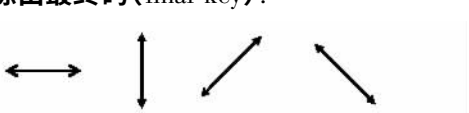

图 1 光子的 4 个偏振态可以用来作量子密码

现有的对 BB84 方案绝对安全性的严格数学证明,基本都采用了繁复的数学或者是涉及了极其精巧的物理概念. 为清楚起见,我们从量子力学原理开始对 BB84 方案的安全性作一粗略回顾.

2.2 零噪声通道下 BB84 方案的安全性

先考虑特殊情况,Alice 与 Bob 之间用于传递量子态的物理通道没有噪声[5]. 在此情况下,他们要求误码检验的结果必须是零误码率,否则丢弃所有初始码. 窃听者(eavesdropper)要获取部分密码信息,她必须在量子态自 Alice 向 Bob 传递过程中对这些量子态作某种观察. 对于每个光子,由于她不知道该光子偏振态是在直角基或是斜角基下制备的. 她的任何观察至少对其中一种基下制备的态产生干扰从而导致 Alice 与 Bob 在误码检验中发现大于零的误码率. 例如,窃听者选择直角基观测每个量子态. 此观测不会干扰直角基下制备的态,但是每个斜角基下制备的态将有一半的可能性变成误码. 具体的说,假定 Alice 以斜角基制备了第 i 个光子的偏振态,45°偏振:

$$|45°\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle),$$

这里 H 与 V 分别代表水平偏振态与竖直偏振态. 若在传输过程中任何人包括窃听者对此态在直角基下测量,依量子力学的测量原理,此态将要么塌缩至水平偏振态要么塌缩至竖直偏振态. 将来若 Bob 在斜角基下测量其偏振,其测量结果有一半可能性与 Alice 的制备记录不符. 同理,若 Alice 所制备的态为 135°偏振,在传递过程中受到直角基测量,此光子亦有一半可能性导致误码. 如果在误码检验中,Alice 选用了 n 个在斜角基下制备的偏振记录,则窃听者对所有光子偏振以直角基测量而又不被察觉的概率为 2^{-n}. 只要 n 值不太小,窃听者在 BB84 方案中成功通过误码率检验的可能性几乎为零. 或者说,只要有窃听,Alice 与 Bob 总能察觉.

在实践中,由于现有技术无法实现零噪声物理通道,这种零噪声通道事实上并不存在. 噪声在量子态制备,传输及测量过程中是不可避免的. 因此,更为重要的问题是噪声通道下的安全性证明.

2.3 噪声通道下量子密码的绝对安全性证明

由于篇幅所限,我们在此只能介绍证明的基本思想. 我们从绝对安全性(unconditional security)开始.

定义:若任何窃听者对最终码的信息量大于 δ 的概率小于 ε,其中 ε,δ 为指数接近于零点小量,如

100 亿分之一,则称之为具有绝对安全性.

早期文献常有计算误码率与窃听者对初始码信息量的关系的研究. 然而这样的研究无法论证窃听者对最终码的信息量. 注意,由于窃听者可以储存其量子态而直接攻击最终码,经典信息论中的有关压缩窃听者信息量的结论不适用.

严格的安全性证明最早由 D. Mayers 于 1996 年给出[6]. Mayers 的证明极其繁复. 我们在此基于 Koashi 的简化解释对其基本思想[7]做扼要介绍:用经典 CSS 码对 BB84 方案中的初始码进行提炼(含纠错与隐私放大两步),在关键性的隐私放大部分,Mayers 引入两种方案:虚方案与实方案. 在虚方案中,用户最终得到 k 个光子在斜角基上的纯态因此窃听者对虚方案的最终码信息量为零. 由于虚方案要求他们在直角基下测量获得最终码,所以 Alice 与 Bob 在虚方案中不能形成共同最终码. 实方案中,Alice 以直角基的态取代斜角基. 由于对称性,对窃听者而言,虚方案与实方案全等,以此窃听者对实方案的 k 光子在直角基上的信息量必然也为零. 而此时由于初始态是在直角基下制备,所以 Alice 与 Bob 可形成全同最终码.

Shor 与 Preskill 与 1999 年给出了大为简化的证明[8]. 其基本出发点为纠缠态提纯. 假如 Alice 与 Bob 共享 k 对(偏振)纠缠对:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$$

那么他们分别对各自的光子偏振在直角基下测量,所得结果必然全同且任何第三者对他们的测量结果必然完全无知. 在噪声通道下的纠缠分发不可能让他们享有纯纠缠对,但是纠缠提纯理论告诉我们,用 CSS 量子纠错码可将低质量纠缠对提炼成较少数量的高质纠缠对直至纯纠缠对. 然而,获得绝对安全的最终码并不必须完成纠缠提纯的全过程. 事实上,位相错误由于不影响最终码,因此毋需最终矫正. 只要他们作了适当的操作使得他们原则上知道如何矫正即可. 这样,量子 CSS 码被经典化,而代之以先测量再使用经典 CSS 码对测量数据进行操作. 既然可以先测量,则初始纠缠对的制备亦无必要. Alice 可以直接制备并向 Bob 传递单光子 BB84 偏振态.

提炼出的最终码如果只把它用作一次性便笺式密码(one - time - pad)的话,那么它是绝对安全的. 如果对最终码进行扩张或多次使用,则安全性无法保证,从而丧失了量子密码对经典密码的最大优势.

最终码的产出率取决于通道误码率. 就 BB84 方案而言,以经典 CSS 码提炼的产出率为

$$r = 1 - 2h(t),$$

$$h(t) = -t\log_2 t - (1-t)\log_2(1-t),$$

其中 t 为平均误码率. 此公式给出量子密钥分发误码率上限值为 11%.

2.4 真实系统与理想系统的差别

需要强调的是,虽然 BB84 方案已经被证明是绝对安全的,这并不意味着任何以该方案为基础的实验都是安全的. 这是因为所进行的实验未必真正符合 BB84 安全性证明中所要求的前提条件. 证明中假设了单光子源,由于技术难度极高,现有的实验多采用单一强度弱相干态或下转化产生的纠缠态. 下面对这两种做法的技术现状及安全性作一介绍.

3 基于弱相干态的量子密码系统安全问题

3.1 现有实验状况

由于光子偏振态在光纤里传播时噪声较大,通常对 BB84 态采用位相加载(phase coding). 这要求 Bob 在远端作单光子干涉测量,即观测两光束的干涉效应. 这要求对光程控制的精度小于 5% 波长. 最早的一种办法是 plug&play(P&P),采用双程光传输[9]. 这种方法可对光程误差作自动矫正. 在 P&P 系统中,光源与测量发生在密钥分发的同一侧. 由 Bob 向 Alice 发射强光,Alice 将强光衰减成平均强度为 0.1 光子左右的弱光并在加载 BB84 态后传回. 最早的日内瓦大学的实验[9]传输距离 67km,每秒形成初始码 160 个,误码率为 5%. 此后,P&P 法的实验结果又有进展,其密钥分发距离可达 100km. 可是,由于强光后向散射(backscattering)造成的测量噪声限制了传送距离. 或者说,若距离过长,由后向散射造成的误码率将会太大而不能生成最终码.

后来的实验放弃了 P&P 法而采用单向传输弱光(弱相干态). 单向传输的主要技术困难在于远端干涉装置的稳定性. 到目前为止,至少已有三个弱光单向传输实验. 剑桥实验[10,11]采用连续,主动矫正的方法保持干涉测量的准确性. 其传输距离达 122km,误码率为 8.9%. 日本电气公司(NEC)实验采用固化干涉装置(integrated - optic interferometer)并改进了单光子探测器信噪比,他们的传输距离为 150km[12—14]. 中国科技大学实验通过自动矫正偏振

起伏而加强了 MZ 干涉议的稳定性. 该实验实现传输距离 125km,误码率 6%,初始码产生速率 10^{-3} bit/s[15].

然而,所有这些弱光传输及检测实验还不足以形成安全的量子密钥分发. 事实上,若窃听者采用光子数分离攻击(photon - number - splitting attack)[16,17],则上述所有实验都是完全不安全的.

3.2 光子数分离攻击[16,17]

现有通道损耗率极大,对于 100km 以上的距离,加上探测效率,整体效率将小于千分之一. 根据理论证明,理想单光子源即便在高损耗通道下也是绝对安全的. 可是弱相干光源在高损耗通道下则结果完全不同 据此所建立的密码是完全不安全的,因为窃听者可以通过光子数分离攻击而获得全部密码. 如图 2 所示. 为表述方便,我们以偏振空间为例. 在光子数空间,强度为 μ,位相随机的相干态的数学式为

$$|\mu\rangle\langle\mu| = e^{-\mu}\sum_n \frac{\mu^n}{n!}|n\rangle\langle n|,$$

其中 n 为光子数. 此式的物理意义为,任意一个相干态脉冲可能是真空,可能是单光子,可能是多光子. 现有实验将相干态强度设为

$$\mu = 0.1,$$

即平均每个脉冲 0.1 个光子. 此即表明多光子脉冲的概率大约为单光子脉冲概率的 5%.

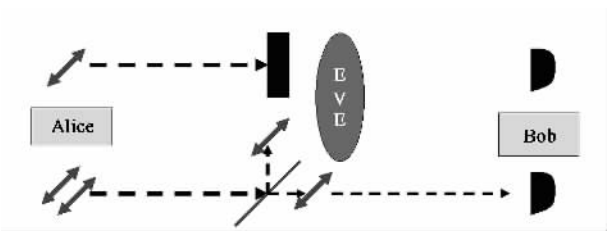

图 2 光子数分离攻击

窃听者在截获每一个脉冲之后,先观测其光子数. 若只有一个光子,则将其丢弃. 若有多个光子(两个或两个以上),窃听者保留其中一个而将剩余光子通过低损耗通道传给 Bob. 等到 Alice 与 Bob 公布每个脉冲的正确测量基后,窃听者再对她所保留的光子各自进行测量. 由于多光子脉冲所有光子偏振全同,窃听者可拥有 Bob 的所有光子的全部偏振信息. 窃听者在进行光子数分离时只对光子数测量而未对偏振测量,因此不会造成任何噪声. 另外,由于窃听者可以使用低损耗通道,窃听者总体上并未降低 Alice 与 Bob 所预期的通道透射率. 简而言之,对于现有相干态密钥分发实验[10—15],窃听者可获取全部信息而不留下任何痕迹. 事实上,量子密码发明者之一,G. Brassard 等人早在 2000 年就对弱相干态量子密码实验做出批评[17]. Brassard 等人在其著名论文[17]的摘要部分就指出:" Existing experimental schemes (based on weak pulses) currently do not offer unconditional security for the reported distances and signal strength. "即:" 现有基于(相干态)弱脉冲的做法,据其所报告的距离及所采用的脉冲强度,并不提供绝对安全性. "

近年的新实验[10—15]虽在传输距离上有所提高但并未在安全性上有新的举措. Brassard 于 2000 年的评论对这些新实验依然适用. 若不解决 PNS 攻击的问题,现有相干态密钥分发实验[10—15]已失去量子密码的基本特征,绝对安全性.

虽然现有相干态密钥分发实验[10—15]不安全,但是这一事实并不意味着以现有技术做不出绝对安全的量子密钥分发. 理论上,采用诱骗信号方法(decoy - state method)和直接使用纠缠光源都可获得绝对安全的量子密码. 实验上,采用纠缠源的量子密钥分发不但在光纤中实现[24—27],而且在自由空间实现[28,29].

3.3 诱骗信号方法

该方法要求随机改变相干态脉冲强度而测出单光子计数率[18—20]. 以此为输入参数提炼出最终码. 采用该法所得最终码,其安全性与用理想单光子源所获最终码等价. 当然,诱骗信号方法未必就是唯一方法[20,21].

4 基于纠缠源的量子密钥分发

对于基于纠缠源的量子密钥分发方案,其最终码的绝对安全性是由量子纠缠对的提纯理论保证的. 纠缠对提纯理论结论是,只要初始分发的纠缠对噪声低于一定水平,就可以提炼出较少对的纯纠缠对,对纯纠缠对在两端进行同一基矢测量即可获得绝对安全的密码. 任何窃听者对纯纠缠对形成的密码不可能获取任何信息.

理论研究表明,若我们的目的仅是获取安全密码而不是纯纠缠对,我们不必进行真实的纠缠对提纯. 取而代之的是先对初始纠缠对直接测量,然后提炼测量数据,进而获得最终码. 在纠缠源量子密钥分

发实验中,纠缠源自身有噪声. 只要在纠缠分发后总体噪声低于一定水平,此噪声不影响最终码的安全性. 目前实验以下转换法制备纠缠源,此源包含多对态. 多对态不影响最终码的安全下. Gottesman 等人已经证明[7,23],只要采用双体态(bipartitestate),而 Alice 与 Bob 各自把自己一边的态当作量子比特(qubit)测量,所获最终码的安全性与纯纠缠对等价.

现有的基于纠缠对分发的量子密码实验主要有两类. 一种是基于能量 – 时间纠缠. 日内瓦 Gisin 小组用这种纠缠态完成了 8.5km 的量子密钥分发[24]. 另一种是基于光子对在偏振空间的纠缠. 近年来,这方面的实验研究十分活跃. 特别的,偏振空间的量子密钥分发实用于自由空间. 维也纳小组于 2003 年完成了 600m 距离的自由空间偏振纠缠分发[28]. 中国科学技术大学潘建伟小组于今年完成了 13km 距离的自由空间偏振纠缠分发[29]. 其纠缠源来自基于 BBO 晶体的 II 型参量下转换. 在经过滤波片后每秒约产出 10,000 个纠缠对,波长为 702.2nm. 在探测手段上采用了大型望远镜系统. 此实验结果一个标志性的意义在于首次证实光子纠缠对分发距离可以超过与大气层等效的大气距离. 这对尚在论证中的以卫星为中转站的洲际量子密钥分发的可行性无疑有着重要启示[30].

在量子密钥分发的全学科系统综述可参见文献[31].

5 总结与展望

采用量子算法[1],经典密码 RSA 系统肯定不安全. 即便在经典算法范围内,任何经典密码系统都有可能是不安全的,因为至今没有哪一个经典密码系统的安全性得数学证明,王小云等人近年来对若干经典密码系统的破解更加剧了人们对经典密码安全性的忧虑.

量子密码在理论上是绝对安全的,无论窃听者拥有多大的经典或量子计算机. 量子密钥分发系统毋需量子计算机,甚至毋需量子存储器. 唯一需要的仅是量子态制备,传送与测量.

虽然以弱相干态为源的现有系统[10—15]对其所报告的密钥分发距离并不安全,但我们仍然有其他办法用现有技术实现绝对安全的量子密码系统,例如诱骗信号方法[18—20],纠缠对分发方法[24—29]等.

就未来而言,理想单光子源或纠缠源技术的发展将会大大提高量子密码系统的效率与实用性能.

参 考 文 献

[1] Shor P. Proc. 35th Ann. Symp. on Found. Of Computer Science. IEEE Comp. Soc. Press. Los Alomitos, CA, 1994. 124 – 134

[2] Wang X Y *et al*. Efficient collision attacks on SHA – 0, Crypto 05

[3] Wang X Y *et al*. Finding collisions in the full SHA – 1 Collision search attacks on SHA1, Crypto05

[4] Wang X Y *et al*. Collision for some hash functions MD4, MD5, HAVAL – 128, Crypto04

[5] Bennett C H *et al*. In: Proc. IEEE Int. Conf. on Computers, systems, and signal processing. Bangalore. IEEE, New York, 1984. 175

[6] Mayers D *et al*. Comput. Mach., 2001, 48: 351 (Its preliminary version appeared in "Advances in Cryptology – Proc. Crypto"96, Vol. 1109 of Lecture Notes in Computer Science. New York: Springer – Verlag, 1996. 343

[7] Koashi M. quant – ph/0507154

[8] Shor P W *et al*. Phys. Rev. Lett., 2000, 85: 441

[9] Stucki D *et al*. New J. Phys., 2002, 4: 41

[10] Gobby C *et al*. Appl. Phys. Lett., 2004, 84: 3762

[11] Yuan Z L *et al*. Optics Express, 2005, 13: 660

[12] Nambu Y *et al*. Jpn. J. Appl. Phys., 2004, 43: L1109

[13] Kimura T *et al*. Jpn. J. Appl. Phys., 2004, 43: L1217

[14] Hasegawa T *et al*. Proceedings of the 2005 Symposium on Cryptography and Information Security, 2F – 3 (in Japanese). Maiko Kobe, Japan, Jan. 25 – 28, 2005

[15] Mo X – F *et al*. Optics Letters, 2005, 30: 2632

[16] Huttner B *et al*. Phys. Rev. A, 1995, 51: 1863

[17] Brassard G *et al*. Phys. Rev. Lett., 2000, 85: 1330

[18] Hwang W – Y. Phys. Rev. Lett., 2003, 91: 057901

[19] Wang X – B. Phys. Rev. Lett., 2005, 94: 230503

[20] Lo H – K *et al*. Phys. Rev. Lett., 2005, 94: 230504

[21] Scarani V *et al*. Phys. Rev. Lett., 2004, 92: 057901

[22] Acin A *et al*. Phys. Rev. A, 2004, 69: 012309

[23] Gottesman D *et al*. Phys. Rev. A, 2001, 63: 022309

[24] Ribordy G *et al*. Phys. Rev. A, 2001, 63: 012309

[25] Tittle W *et al*. Phys. Rev. Lett., 2000, 84: 4737

[26] Jennewein T *et al*. Phys. Rev. Lett., 2000, 84: 4729

[27] Naik D S *et al*. Phys. Rev. Lett., 2000, 84: 4733

[28] Aspelmeyer M *et al*. Science, 2003, 301: 621

[29] Peng C Z *et al*. Phys. Rev. Lett., 2005, 94: 150501

[30] 张军等. 物理, 2005, 34 (10): 701 [Zhang J *et al*. Wuli (Physics), 2005, 34(10): 701 (in Chinese)]

[31] Gisin N *et al*. Rev. Mod. Phys., 2002, 74: 145; quant – ph/0101098