光电子·激光 第12卷 第1期 2001年1月
Journal of Optoelectronics · Laser Vol. 12 No. 1 Jan. 2001

文章编号:1005-0086(2001)01-0105-04

量子密码的原理、应用和研究进展

池 灏,章献民,朱华飞,陈抗生
(浙江大学信息与电子工程学系,浙江 杭州 310027)

摘要:基于量子物理原理的量子密码术已被证明是保密信中密钥安全分配的有效手段。本文介绍了量子密码的基本原理,探讨了实现量子密码的3种方案,并研究了各自的密钥分配机制。还讨论了近年来的理论和实验研究进展,并指出现存的问题以及今后研究重点。鉴于其应用前景,最后建议我国尽快开展量子密码的实验研究。

关键词:量子密码;密钥分配;光纤信道;光网络;光通信
中图分类号:O431.2 **文献标识码**:A

Principles, Applications and State-of-the-arts of Quantum Cryptography

CHI Hao, ZHANG Xian-min, ZHU Hua-fei, CHEN Kang-sheng
(Dept. of Infor. & Electron. Eng. Zhejiang Univ. Hangzhou 310027, China)

Abstract: Quantum cryptography, which is based on fundamental physical principles, has been proved to be an effective technique for secure key distribution. In this paper, the authors introduce the fundamental theory of quantum cryptography, then discussed the three main schemes for quantum cryptography and their key distribution policies respectively. Recent improvements in theory and experiment are discussed, and the existng problems and developing directions are also pointed out. For its application potential, it's suggested to construct experimental system of quantum cryptography in China.

Key words: quantum cryptography; key distribution; fiber channel; optical network; optical communications

1 引 言

在快速走向信息化社会的今天,人们日益关注信息的安全性问题。许多保密通信系统的安全性往往最终依赖于密钥的安全分配。密钥的安全分配这一关键性问题一直困扰着人们。

量子密码技术为密钥分配提供了解决的办法[1]。量子密码依赖于两点:一是基本量子力学效应(如测不准原理,Bell原理);二是量子密钥分配协议。量子密码系统能够保证:1)任何窃听者最多只能获取部分信息;2)任何窃听行为都能被合法的发收双方检测到。70年代,美国哥伦比亚大学的S. Wiesner创造性地提出了共轭编码的概念。80年代以来,源于共轭编码概念的量子密码术取得了令人惊异的进步与成就,近年来,欧、美、日等许多大学和研究机构竞相投入到量子密码的研究中。

2 量子密码的实现方案及原理

目前为止,主要有3类量子密码实现方案[2]:1)基于单光子量子信道中测不准原理的Bennett-Brassard-Wiesner(BBW)方案;2)基于量子相关信道中Bell原理的Ekert方案;3)基于两个非正交量子态性质的Bennett方案。

2.1 基于测不准原理的量子密码方案

量子力学中,任意两个可观测力学量可由厄密算符 $\hat{A}$ 和 $\hat{B}$ 表示。若它们不对易,或者说不能有共同的本征态,必满足测不准关系式:

$$\Delta\hat{A}\cdot\Delta\hat{B}\geqslant\frac{1}{2}|\overline{[\hat{A},\hat{B}]}| \tag{1}$$

表明力学量 $\hat{A}$ 和 $\hat{B}$ 不能同时具有完全确定的值,精确测定其中一个量必然以另一个力学量的模糊为代价,即测不准原理。

收稿日期:2000-04-10 修订日期:2000-06-07

A和B是欲建立通信联系的双方，他们首先通过量子密码系统共享密钥，当然通信信道上可能会有窃听者(Eve)。图1是BBW方案模型原理图，类似于Mach-Zehnder干涉仪，A和B分别控制相位调制器Φ_A和Φ_B。为了发送密钥流，A发送定时单光子脉冲序列到干涉仪中，并随机选择4个相移中的1个对光子进行编码，即$\Phi_A=0$或$=180°$(基1)；$\Phi_A=90°$或$270°$(基2)。对于每组基，A选择较小的相移即$\Phi_A=0$或$90°$代表0；较大的相移$\Phi_A=180°$或$270°$代表1。B同样也在两个相移$\Phi_B=0$(基1)或$90°$(基2)中进行随机选择，并根据在哪个输出端探测到光子分别记录为0或1。传送过程结束后，A和B通过公开信道分别公布自己的每个编码和解码基。然后将数据分为2组：一组是相移差$\Phi_A-\Phi_B$为0或$180°$的结果，在这个情况下，光量子在最后分束器上的行为是确定的，结果可能被用做密钥流；另一组是那些相移差为$90°$或$270°$的数据，由于在这种情况下，光子在最后分束器上的行为是完全随机的，即被记录为0和1的概率是一样的。然后双方同意保留第1组数据而弃用第2组数据[3]。

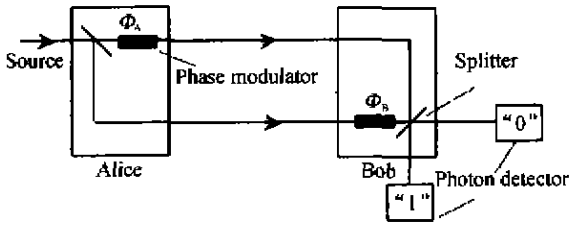

图1　基于干涉测量的BBW方案模型

Fig. 1　The model of BBW scheme based on interferometry

考虑信道上存在Eve的情况，他有2个目标：一是正确读取信息从而分享密钥；二是希望窃听行为不为A和B发觉。如果A发送的是真正的单光子，那么Eve唯一的办法是截入信道期望正确读取每一个光子态，并将副本发送给B，从而不被发觉。然而，类似B，Eve每次测量也必须从两组基中选择其一，并且约有一半的情况选择错误，这时得到0和1的概率是相等的。这样，Eve发送错误的状态给B，并且使B记录出错(即A发0，B记为1，或反之)的概率为0.25。如果A和B从第1组数据中选择足够多的bit进行比较，那么Eve不被发觉的概率可降到足够小的程度。如比较100 bit/s的数据，Eve逃脱的概率是$(1-0.25)^{100}=3.2\times10^{-13}$。当然若未发现窃听行为，第1组余下的数据就可安全地用做密钥。在这里，密钥的安全性是由量子力学的基本定律—测不准原理来保证的。

2.2　基于Bell原理的量子密码方案

Bell原理源自量子力学完备性的问题。光子源沿$\pm Z$方向发出具有负相关特性的光子对，即处于单态(singlet state)的光子对，探测器1、2可分别选用x-y平面的探测A、B、C(可理解为3个检偏方向)进行探测。如果探测器1、2选择同样的探测基A时，每一个探测器所得的结果都是随机的(A^+或$\overline{A}^-$，分别表示光子偏振态平行或垂直于探测基A的情况)，但两个结果总是负相关的，也就是说，当一个是A^+时，另一个必为A^-，反之亦然。若探测器1、2同时选择其他探测基B或C时，情况相同，结果分别记为B^+、B^-和C^+、C^-。在实际的每次实验中，探测器1、2都互相独立且随机地选择探测基，经过大量的实验后，若用$n(A^+B^+)$表示探测器1用探测基A测得A^+，且同时探测器2用探测基B测得B^+的数目；$n(A^+C^+)$，$n(B^+C^+)$的意义亦然。Ekert指出，如果量子力学本身是不完备的，3个量应满足Bell不等式：

$$n(A^+B^-)\leqslant n(A^+C^+)+n(B^+C^+) \qquad (2)$$

而基于量子力学完备性的观点，(2)式不能成立。后来，大量实验的多数结果表明，量子力学本身是完备的，Bell不等式不能成立。

Ekert[4]从上述实验中得到启发，提出了基于Bell原理的量子密码方案。系统包括能发送单态光子对的光源，光子对在分离后分别沿$\pm Z$方向发送到合法用户A和B，A和B分别沿处于x-y平面的量子基方向α_i和β_j($i,j=1,2,3$)测量，其中α_i和β_j的3个量子基方位角分别为：$\Phi_{1a}=0$，$\Phi_{2a}=\pi/4$，$\Phi_{3a}=\pi/2$和$\Phi_{1b}=\pi/2$，$\Phi_{3b}=3\pi/4$，其中a、b分别表示A和B的分析仪。双方均随机并独立地选用量子基测量每一对光子，每一次测量的结果只能是$+1$或-1(分别表示光子的偏振态平行或垂直于所选的测量基方向)，定义测量基方向α_i和β_j的相关系数为

$$E(a_i,b_j)=P_{++}(a_i,b_j)+P_{--}(a_i,b_j)-P_{+-}(a_i,b_j)-P_{-+}(a_i,b_j) \qquad (3)$$

其中$P_{\pm\pm}(\alpha_i,\beta_j)$表示分别沿$\alpha_i$和$\beta_j$测得$\pm1$的联合概率。根据量子力学规律

$$E(a_i,b_j)=-a_i\cdot b_j \qquad (4)$$

定义：

$$S=E(a_1,b_1)-E(a_1,b_3)+E(a_3,b_1)+E(a_3,b_3) \qquad (5)$$

量子力学要求：

$$S=-2\sqrt{2} \qquad (6)$$

传送过程结束后，A和B通过公开信道宣布他们每次测量选用的量子基，这样可将测量结果分为2组：

第 1 组为双方选择量子基方位角不同的结果(如 A 选 Φ_{1a},B 选择 Φ_{1b});第 2 组为方位角相同的结果(如 A 选 Φ_{2a}、B 选择 Φ_{1b})。这些数据就可能作为将来的密钥数据。然后,他们公布第 1 组数据,这就使双方可根据方程(3)和(5)计算得 S 值。如果信道未被扰动或者说没有被窃听,双方计算得到 S 值应与方程(6)吻合,那么就可确信第 2 组的数据是严格负相关的,这组数据就可以作为密钥。

如果有 Eve,他将得不到任何信息,因为只是在 A 和 B 公开讨论后,信息才真正产生。Eve 窃听时,他可能会先截获光子,然后再将自己准备好的数据发送给 A 和 B 以图误导他们,但由于不可能事先得知他们如何选择量子基,Eve 的窃听行为将不可避免被检测到。事实上,窃听行为等价于引入了所谓的物理真实因素(elements of physical reality)[5],这将导致 S 值不再满足(6)式,经过物理推导,不管 Eve 采取何种窃听策略,都有

$$-\sqrt{2}\leqslant S\leqslant\sqrt{2} \tag{7}$$

这其实是 Clauser 等人将 Bell 原理一般化后的结果。这样,A 和 B 通过对测量结果的统计分析就能够发现是否有 Eve。这表明,系统密钥传送的安全性依赖于 Bell 原理,也就是说只要量子力学是完备的,方法就是安全的。

该方案尚未实现,事实上,在上述验证量子力学完备性的实验的基础上,再加上相应的软件,以及声光开关作为选择量子基的分析仪等设备,实验是不难完成的。

2.3　基于二状态传输的量子密码方案

C. H. Bennett[6]创造性地提出了只用 2 个非正交量子态的量子密码方案:

$$P_0|u_0\rangle=\sqrt{1-|\langle u_0|u_1\rangle|^2}\,|u_1^*\rangle \tag{8}$$

设 $|u_0\rangle$、$|u_1\rangle$ 分别代表两个非正交量子态,而 $|u_0^*\rangle$ 和 $|u_1^*\rangle$ 表示分别与 $|u_0\rangle$、$|u_1\rangle$ 正交的量子态。构造投影算符 $P_0=1-|u_1\rangle\langle u_1|$ 和 $P_1=1-|u_0\rangle\langle u_0|$,它们的作用分别是将量子态投影到 $|u_1^*\rangle$ 和 $|u_0^*\rangle$ 上。P_0 分别作用于 $|u_0\rangle$、$|u_1\rangle$,有

$$P_0|u_1\rangle=0 \tag{9}$$

(8)、(9)式表明,P_0 投影到 $|u_1\rangle$ 的结果为零;而投影到 $|u_0\rangle$ 上得到正值的概率为 $\sqrt{1-|\langle u_0|u_1\rangle|^2}$。同样 P_1 作用到 $|u_0\rangle$、$|u_1\rangle$ 时,也有

$$P_1|u_0\rangle=0 \tag{10}$$

$$P_1|u_1\rangle=\sqrt{1-|\langle u_0|u_1\rangle|^2}\,|u_0^*\rangle \tag{11}$$

为传送密钥流,A 首先将随机比特流传送到量子信道中,量子态 $|u_0\rangle$ 和 $|u_1\rangle$ 分别代表 0 和 1。同样,B 随机并独立于 A 选择算符 P_0 或 P_1 进行测量,得到的结果有两种可能,即检测不到光子和检测到了光子;然后 B 通过公共信道宣布哪些 Bit 得到了正值(而不是选择了何种算符),双方只保留这一组数据,其余数据均弃用。如果没有 Eve,双方保留的数据(约占总数的 $\sqrt{1-|\langle u_0|u_1\rangle|^2}/2$)应该完全吻合,全是 A 发 $|u_0\rangle$、B 测 P_0 或者 A 发 $|u_1\rangle$、B 测 P_1。如果有窃听,将会使结果出错,如 A 发 $|u_0\rangle$、B 测 P_1 而得到正值,因为 Eve 无法知道通信双方所使用的量子态和测量算符。同样 A 和 B 只要比较足够多的数据,任何窃听行为都将被检测到。Bennett 提出了实现构想的干涉实验方案。

3　讨论以及研究进展

在量子力学中,对量子状态的测量并非只是外部过程,它将对被测量造成直接的影响。因此任何窃听行为都不可避免地会干扰通信系统的量子状态,从而留下蛛丝马迹。量子密码的优势在于密钥传输的安全性依赖于基本量子力学定律。光量子要么被合法接收者接受,要么被 Eve 接收。如果有 Eve,窃听动作本身将会对通信系统造成干扰,对通信系统的量子状态带来不可挽回的变化,从而通信双方就可得知有人在窃听。在实际的量子通信系统中,即使没有 Eve,调制器、检测器、量子信道也会由于各种原因引入一些错误,当然这些出错率应比 Eve 导入的错误率低得多,通信双方可通过子集校验纠错技术将错误过滤掉,确保所共享的随机序列完全吻合。但由于校验过程会不可避免地泄露部分信息,即安全性降低了,成为部分保密的随机序列。可通过所谓的机密放大技术(privacy amplification)的杂凑过程,提高序列的保密程度。以上我们叙述量子密码原理的时候,并未考虑 Eve 可能会采取更富攻击性的窃听策略,以图尽可能多地获取信息并尽量避免被发觉。如第 1 种方案,Breidbart 等人提出了 Eve 选择所谓的 Breidbart 基来测量和发送光子,就会使他正确读取所发的数据的概率提高到 85 %。不过,针对这种攻击策略,Barnett[7]提出了被抛弃数据协议(rejected-data protocol,简称 RDP),利用原方案中丢弃不用的数据(即相移差为 90°或 270°的数据)的统计性质,可轻而易举地检测到 Breidbart 基攻击。在实际应用中,RDP 可以与 BBW 协议联合使用。另外,L. Goldenberg 等

人[8]提出了基于二正交态传输的量子密码方案。

由于光纤的低损耗、稳定性好及能够实现长距离传输的特点，所以如何在光纤中实现量子密钥分配成为人们研究的重点[9]。目前，英国的BT实验室已通过30 km的商用光纤信道实现20 kbit/s的密钥传送，向实用化方向迈进了重要的一步[10]。量子密码的实验技术的关键是单光子探测技术。目前探测光子的APD需要液氮制冷以降低噪声，这就需要庞大的设备，并且成本也很高。期望在不久的将来，单光子探测技术能取得进步。考虑到点对点密钥分配方式的局限性，光网络能够容纳多用户，所以光网络中的量子密码术的研究得到了重视。国外已开展这方面的研究工作，BT实验室已提出树形和环形无源光网络中的量子密钥分配方案[11]，并完成了演示实验[12]。瑞士的日内瓦大学利用已埋设的标准通信光纤23 (km)，开展了量子密钥交换实验，获得了良好的结果[13]。奥地利因斯布鲁克大学利用光子编振编码，也获得了kHz级的密钥交换速率[14]。BT实验室在一根已敷设的光纤上同时实现了数据传输和量子密钥交换的波分复用实验[15]。同时，有关量子密码协议的研究仍在继续，日本NTT实验室提出了基于两个正交态的简单协议，在协议中，发端在两个正交态中混入第3态(真空态)以防止窃听[16]。不久前，美国的Los Alamos国家实验室完成了在自由空间950 m的量子密码实验，并指出在短期内可将距离扩展至2 km，这预示着量子密码技术在卫星通信中的潜在应用[17]。

参考文献：

[1] C H Bennett, G Brassard, A K Ekert. Quantum Cryptography[J]. *Scientific American*, 1992, **267**(4): 26-33.

[2] K J Blow, S J D Phoenix. On a fundamental theorem of quantum cryptography [J]. *J. of Mod. Opt*, 1993, **40**(1): 33-36.

[3] P D Townsend, I Thompson. A quantum key distribution channel based on optical fibre[J]. *J. of Mod. Opt*, 1994, **41**(12): 2425.

[4] A K Ekert. Quantum cryptography based on Bell's theorem[J]. *Phy. Rev. Lett*, 1991, **67**(6): 661-663.

[5] B d Espagnat. The quantum theory and reality[J]. *Scientific American*. 1979, **247**(52): 158-181.

[6] C H Bennett. Quantum cryptography using any two nonorthogonal states [J]. *Phy. Rev. Lett*, 1992, **68**(21): 3121-3124.

[7] S M Barnett, B Hunttner, S J D Phoenix. Eavesdropping strategies and rejected-data protocols in quantum cryptography[J]. *J. of. Mod. Opt*, 1993, **40**(12): 2501-2513.

[8] L Goldenberg, Lev Vaidman. Quantum cryptography based on orthogonal states[J]. *Phy. Rev. Lett*, 1995, **75**(7): 1239-1243.

[9] P D Townsend. Secure key distribution systems based on quantum cryptography[J]. *Electron. Lett*, 1994, **30**(10): 809-811.

[10] C Marand, P D Townsend. Quantum key distribution over distances as long as 30 km[J]. *Opt. Lett*, 1995, **20**(16): 1695-1697.

[11] S J D Phoenix, S M Barnett, P D Townsend, *et al*. Multi-user quantum cryptography on optical networks Electronics Letters [J]. 1995, **42**(6): 1155-1163.

[12] P D Townsend. Secure communications on passive optical networks using quantum cryptography[A]. *European Conference on Optical Communication*[C]. Piscata way. NJ. USA, IEEE, 1996, **3**: 335-338.

[13] N Gisin, Experimental studies of quantum cryptography in optical fiber communication systems[A]. *Proceedings of SPIE*[C]. 1999, **3749**: 342-343.

[14] S Chiangga, *et al*. Towards practical quantum cryptography[J]. *Applied Physics B: Lasers and Optics*, 1999, **69**(5): 389-393.

[15] P D Townsend. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing[J]. *Electronics Letters*, 1997, **33**(3): 188-190.

[16] M Koashi, *et al*. Simple protocol of quantum cryptography based on two truly orthogonal states [A]. *Technical Digest-European Quantum Electronics Conference*[C]. Piscataway NJ. USA, IEEE, 1998, 90-92.

[17] W T Buttler, *et al*. Practical quantum cryptography in free space[A]. *Technical Digest-European Quantum Electronics Conference* [C]. Piscataway, NJ. USA IEEE, 1998. 89-90.

作者简介：

池　丽　(1972—)，男，浙江温州人，1994年毕业于西安交通大学应用物理系获学士学位，1997年毕业于浙江大学光电信息工程学系获硕士学位，浙江大学信息与电子工程学系在读博士生，主要从事光网络、光纤光栅在光通信和传感中应用的研究。