第 56 卷 第 2 期 2007 年 2 月
1000-3290/2007/56(02)/0673-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.2,February,2007

多方控制的量子安全直接通信协议*

王 剑† 陈皇卿 张 权 唐朝京

(国防科学技术大学电子科学与工程学院,长沙 410073)

(2006 年 5 月 10 日收到;2006 年 6 月 12 日收到修改稿)

基于单光子序列的顺序重排,提出了一种可应用于一些特殊的场景的多方控制的量子安全直接通信协议.协议中,接收方只有在得到所有控制方的同意之后,才能恢复出发送方的秘密消息.协议的安全性由量子不可克隆定理和单光子序列的秘密传输顺序所保证.此外,除了用于窃听检测的部分光子,所有的光子都用于编码秘密消息,而且协议的实现不需要使用纠缠态,该协议具有效率高和实现简单等特点.

关键词:量子密码,量子安全直接通信,顺序重排,单光子

PACC:0365,4230,4250

1. 引 言

量子信息学是近 20 年发展起来新型交叉学科,是量子理论、信息科学以及计算机科学相结合的产物[1].量子信息学中发展速度最快的分支学科是量子密码,它是以经典密码学和量子力学为基础、利用量子效应实现无条件安全的信息交互的一种新型密码体制.经典密码体制的安全性基于某些数学难题,如大整数因子分解、离散对数问题等.1994 年,Shor[2] 提出一种量子并行算法,该算法利用量子计算机可以轻而易举地破解大整数因子分解这类数学难题.Shor 的发现对现有的密码体制提出了严峻的挑战,同时掀起了量子密码学研究的热潮.由于量子密码能提供无条件安全的通信,量子密码学成为量子信息学中最引人注目的分支,并形成了系统的量子密码理论体系.量子密码主要包括量子密钥分配(QKD)[3—8]、量子数据加密、量子秘密共享(QSS)[9]、量子身份认证、量子数字签名以及量子安全直接通信(QSDC)[10—21] 等方面.QKD 即通信双方以量子态为信息载体,利用量子力学原理在通信双方之间建立无条件安全的共享密钥.不同于 QKD,QSDC 可以实现秘密消息的直接传送而不需要首先建立密钥再对秘密消息进行加密.由于 QSDC 可以应用于某些特殊的加密任务,QSDC 在最近几年得到了飞速的发展.可以将 QSDC 分为两类,即基于单粒子的 QSDC 和基于纠缠的 QSDC.Deng[10] 等人将单光子序列作为一次一密来实现 QSDC;Cai 等人[11] 基于处于混合态的单量子位提出了一个 QSDC 协议.当然,基于纠缠的 QSDC 占据了 QSDC 协议的主流.Bostrom 等人[12] 提出了一个非安全的 QSDC 模型;Deng 等人[13] 借鉴 Long-Liu 2002 两步 QKD 方案[5] 的物理思想,利用有序的 EPR 对提出了一个两步 QSDC 协议;我们提出了一个基于量子隐形传态的 QSDC 协议和一个基于 Greenberger-Horne-Zeilinger(简写 GHZ)态的多方控制的 QSDC 协议[14,15].

2003 年,Deng 等人[6] 利用控制的顺序重排加密实现了一个 QKD 方案.在他们的方案中,通信双方共享了一个用于控制顺序重排操作的控制密钥.最近,Zhu 等人[16] 利用纠缠粒子的秘密传输顺序提出了一种 QSDC 协议,其安全性基于纠缠关联和传输粒子顺序的秘密性.利用 Zhu 等人的方法,王剑等提出了一个基于单光子序列秘密顺序重排的 QSDC 协议[17].本文基于这种方法提出了一种多方控制的 QSDC 协议,该协议可以应用于某些特殊的加密任务.发送方通过量子信道将秘密消息发送给接收方,但是接收方必须在控制方的同意之下才能恢复出发送方的秘密消息.由于该协议只需要使用单光子而不需要纠缠态,与基于纠缠的 QSDC 协议相比较,协议的实现更为简单.在我们的协议中,除了用于窃听

* 国家自然科学基金(批准号:60472032)资助的课题.

† E-mail:jwang@nudt.edu.cn

检测的光子,其余的光子均可用于编码秘密消息,协议具有较高的效率.本文同时分析了协议的安全性.

2. 协议描述

下面对多方控制的 QSDC 协议进行具体的描述.假设分区经理 Bob 想要将他的秘密消息直接传输给总经理 Alice,Bob 同时要求 Alice 在董事们(Charlie,Dick,…,York 和 Zach)的同意之下,才能得到秘密消息.我们假设协议中的控制方都是诚实的.

S1) Alice 制备一个包含 n 个光子的有序的光子序列,$[P_1,P_2,\cdots,P_n]$,称为 P 序列.序列中的每一个光子随机地处于以下四个态之一:

$$|H\rangle = |0\rangle, \tag{1}$$

$$|V\rangle = |1\rangle, \tag{2}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{3}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{4}$$

Alice 然后将 P 序列发送给 Charlie.

S2) Charlie 收到 P 序列后,对于序列中的每一个光子,他首先随机地选择幺正操作 I 或 U 对光子进行幺正变换,其中

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{5}$$

$$U = \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|. \tag{6}$$

对于序列中的每一个光子,Charlie 同时随机地选择幺正操作 I 或 H 对光子进行变换,这里

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|). \tag{7}$$

幺正操作 U 能够翻转 Z 基($|0\rangle$,$|1\rangle$)和 X 基($|+\rangle$,$|-\rangle$)中的态,即

$$U|0\rangle = -|1\rangle, U|1\rangle = |0\rangle, \tag{8}$$

$$U|+\rangle = |-\rangle, U|-\rangle = -|+\rangle. \tag{9}$$

幺正操作 H 可以实现 Z 基和 X 基之间的相互转换,即

$$H|0\rangle = |+\rangle, H|1\rangle = |-\rangle, \tag{10}$$

$$H|+\rangle = |0\rangle, H|-\rangle = |1\rangle. \tag{11}$$

Charlie 做完变换后,将光子序列发送给下一个控制方 Dick.类似地,Dick 和其余的控制方对光子序列中的每一个光子执行随机的 I,U 或 H 操作,直到 Zach 完成了他对光子序列的操作.Zach 然后将光子序列发送给 Bob.

S3) Bob 从 P 序列中选取一个充分大的子集用于窃听检测,称为检测序列(C 序列).P 序列中的其他光子构成消息编码序列(M 序列).Bob 对 C 序列中的每一个光子随机地执行 I 或 U 操作.他然后根据秘密消息的比特值对 M 序列中的每一个光子执行相应的 I 或 U 操作,从而将秘密消息编码在 M 序列的光子上.例如,如果 Bob 的秘密消息比特是 0(1),Bob 则对相应的光子执行幺正操作 I(U).

S4) 执行完随机操作和编码操作后,Bob 打乱检测序列和编码序列中光子的顺序,即对序列中的光子进行重新排列,产生一个新的光子序列,称为 P' 序列,$[P'_1,P'_2,\cdots,P'_n]$.他然后将 P' 序列发送给 Alice.除了 Bob 自己,P' 序列中光子的排列顺序对于其他人都是秘密的,这也是该方案安全性的重要保证.

S5) 在确认 Alice 收到 P' 序列后,Bob 首先公布检测序列的位置以及该序列中光子的秘密排列顺序;Bob 然后让 Alice 公布检测序列中光子的初始态.为防止 Alice 的截取重发攻击,对于每一个采样光子,Bob 随机选择一个控制方先公布他的 H 操作信息,然后再依次选择其他的控制方公布他们的 H 操作信息.确切地说,控制方只公布他们对采样光子进行 H 操作的信息,而并不公布 I 和 U 操作信息;根据控制方公布的信息,Alice 能够选择正确的测量基对采样光子进行测量;测量后,Alice 告诉 Bob 她的测量结果.对于每一个采样光子,Bob 随机地选择一个控制方公布他的 I 和 U 操作信息,再依次选择其他的控制方公布他们的 I 和 U 操作信息;这样 Bob 就能够判断 P 序列传输过程中产生的错误率;如果错误率低于他们预先设定的门限,通信各方继续执行下一步,否则,协议中止.

S6) Bob 公布 M 序列中光子的秘密排列顺序.如果控制方同意 Alice 恢复 Bob 的秘密消息,控制方则公布他们对 M 序列光子的操作信息.根据公布的信息,Alice 就能够选择正确的测量基对 M 序列的光子进行测量,从而得到 Bob 的秘密消息.

3. 安全性分析

下面我们对协议的安全性进行分析.协议的安全要求包括窃听者 Eve 得不到 Bob 的秘密消息以及接收方 Alice 只有在所有董事的同意之下才能得到 Bob 的秘密消息.

该协议的安全性由量子不可克隆定理和传输光子的秘密顺序所保证.类似于 BB84 协议[3],P 序列中每个光子随机地处于两组非正交测量基中的一个

态.根据 Stinespring dilation 定理[12],Eve 的窃听等价于 Eve 在由量子信号和辅助系统组成的一个大的 Hilbert 空间上执行幺正操作 $\hat{E}$.假设 Eve 的辅助态为 $|\varepsilon\rangle$,则

$$\hat{E}|0,\varepsilon\rangle = \alpha|0,\varepsilon_{00}\rangle + \beta|1,\varepsilon_{01}\rangle, \tag{12}$$

$$\hat{E}|1,\varepsilon\rangle = \beta'|0,\varepsilon_{10}\rangle + \alpha'|1,\varepsilon_{11}\rangle, \tag{13}$$

$$\begin{aligned}\hat{E}|+,\varepsilon\rangle &= \frac{1}{\sqrt{2}}[\alpha|0,\varepsilon_{00}\rangle + \beta|1,\varepsilon_{01}\rangle \\ &\quad + \beta'|1,\varepsilon_{10}\rangle + \alpha'|1,\varepsilon_{11}\rangle] \\ &= \frac{1}{2}[|+\rangle(\alpha|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle \\ &\quad + \beta'|\varepsilon_{10}\rangle + \alpha'|\varepsilon_{11}\rangle) \\ &\quad + |-\rangle(\alpha|\varepsilon_{00}\rangle - \beta|\varepsilon_{01}\rangle \\ &\quad + \beta'|\varepsilon_{10}\rangle - \alpha'|\varepsilon_{11}\rangle)],\end{aligned} \tag{14}$$

$$\begin{aligned}\hat{E}|-,\varepsilon\rangle &= \frac{1}{\sqrt{2}}[\alpha|0,\varepsilon_{00}\rangle + \beta|1,\varepsilon_{01}\rangle \\ &\quad - \beta'|0,\varepsilon_{10}\rangle - \alpha'|1,\varepsilon_{11}\rangle] \\ &= \frac{1}{2}[|+\rangle(\alpha|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle \\ &\quad - \beta'|\varepsilon_{10}\rangle - \alpha'|\varepsilon_{11}\rangle) \\ &\quad + |-\rangle(\alpha|\varepsilon_{00}\rangle - \beta|\varepsilon_{01}\rangle \\ &\quad - \beta'|\varepsilon_{10}\rangle + \alpha'|\varepsilon_{11}\rangle)].\end{aligned} \tag{15}$$

Eve 的幺正操作可以写为

$$\hat{E} = \begin{pmatrix} \alpha & \beta' \\ \beta & \alpha' \end{pmatrix}. \tag{16}$$

由于 $\hat{E}$ 是幺正操作,复数 α,β,α' 和 β' 必须满足 $\hat{E}\hat{E}^{\dagger} = I$,由此可得 $|\alpha|^2 = |\alpha'|^2$ 以及 $|\beta|^2 = |\beta'|^2$.那么 Eve 的窃听造成的错误率为 $e = |\beta|^2 = 1 - |\alpha|^2$.控制方采用随机的 I 和 H 操作能够使序列中光子的态在 Z 基和 X 基中随机地变换,相当于控制方重新用两组非正交基制备了一个光子序列.Bob 对光子序列的重新排列同样等价于制备了一个新的光子序列.Eve 无论窃听 Alice 发送的光子序列,还是控制方传输的光子序列,或是 Bob 发送给 Alice 的光子序列,都相当于窃听一个新的光子序列.Eve 的窃听将不可避免地产生一定的错误率,通信各方在窃听检测过程中会发现 Eve 的存在.

从信息论的角度来看,在量子系统中可访问的信息量受限于 Holevo 限[1]

$$\chi(\rho) = S(\rho) - \sum_i p_i S(\rho_i), \tag{17}$$

其中 $S(\rho)$ 为态 ρ 的 Von-Neumann 熵,$\rho = \sum_i p_i\rho_i$,ρ_i 是通信方以概率 p_i 制备的量子态.如果通信方分别以 1/4 的概率制备态 $|H\rangle$,$|V\rangle$,$|+\rangle$ 和 $|-\rangle$,则序列中光子的二元熵为 $H(P) = -\sum_i p_i \lg p_i = 2$,从而 Eve 可得到的信息

$$I_E \leqslant S(\rho) - \sum_i p_i S(\rho_i) < H(P). \tag{18}$$

由此看来,Eve 的窃听不可能得到光子序列的完备信息,她所得到的信息小于通信方传输的信息,所以通信方能够在窃听检测中发现 Eve 的窃听.

事实上,该协议的安全性等同于 BB84 协议的安全性,只不过 BB84 协议采用随机的 Z 基和 X 基测量来检测窃听,而我们的协议则利用光子序列的重新秘密排列来防止 Eve 获取发送方的秘密消息.假设 Eve 截获 P 序列并制备一个假的光子序列发送给 Bob,她再截获 Bob 发送给 Alice 的光子序列.如果 Bob 没有对光子序列进行重新排列,那么 Eve 通过测量假的光子序列从而得到 Bob 的秘密消息.正是因为 Bob 打乱了光子序列的排列顺序,Eve 无法得知传输光子序列的正确顺序,她只能得到一些毫无意义的乱码,而且在窃听检测过程中,Eve 的窃听会被通信方发现.由于传输光子的顺序的秘密性,显然如果 Eve 采用联合攻击,协议也是安全的.

由于 H 操作可以实现 Z 基和 X 基的相互转换,控制方对传输光子执行随机的 I 和 H 操作可以防止 Eve 获取控制方的控制信息.如果控制方只执行 I 和 U 操作,Eve 可以通过截取重发攻击来获取控制方的控制信息.例如,Eve 截获 P 序列并将一个假的光子序列发送给控制方;该控制方对光子序列执行随机的 I 或 U 操作后将其发送给下一个控制方;Eve 截获该序列并对序列进行测量就可以获取控制方的控制信息.在窃听检测过程中,Bob 首先让控制方公布他们的 H 操作信息,使得 Alice 能够选择正确的测量基来测量检测序列中的光子.在 Alice 公布她的测量结果后,Bob 才让控制方公布他们的 I 和 U 操作信息.这样做的目的是为了防止 Alice 在没有得到控制方的许可的情况下而获取 Bob 的秘密消息.如果控制方首先就公布他们所有的操作信息,Alice 采用截取重发攻击从而不需要控制方的控制就可以获取 Bob 的秘密消息.例如,Alice 将制备好的 P 序列直接发送给 Bob,同时发送一个假的光子序列给控制方 Charlie;Alice 截获 Zach 发送给 Bob 的光子序列;这样根据控制方公布的控制信息,Alice 可以在窃听检测过程中成功地欺骗 Bob,从而不需要控制方的同意而得到 Bob 的秘密消息.此外,在窃

听检测过程中,对于每一个采样光子,Bob 随机地选择一个控制方先公布他的操作信息,然后再依次选择其他的控制方,这样可以确保每一个控制方真正起到控制作用.当然,在我们的协议中,控制方都是诚实可信的.基于以上分析,我们的协议是安全的.

4. 结束语

基于单光子序列的顺序重排,提出了一种可以应用于某些特殊任务的多方控制的 QSDC 协议,并分析了协议的安全性.在该协议中,接收方首先随机地用两组非正交基制备一个有序的光子序列,然后将光子序列发送给控制方;控制方在对序列中的光子进行幺正变换后,再将序列发送给发送方;发送方将光子序列分为检测序列和编码序列,并分别执行随机操作和编码操作;执行完操作后,发送方对光子序列进行重新排列产生一个新的序列,然后将序列发送给接收方;协议的参与方进行窃听检测.如果光子序列在传输过程中产生的错误率低于预先设定的门限,发送方公布编码序列中光子的排列顺序.这样在得到所有控制方的同意之后,接收方能够获取发送方的秘密消息.协议的安全性基于量子不可克隆定理和单光子序列的秘密传输顺序.考虑实验的可行性,我们的协议只需要用到单光子源、单光子检测器和一些线性光学器件.目前,关于单光子源和单光子检测器的研究已经较为深入,而且很多研究成果已应用于量子密码协议[22—25].根据现有的技术,量子逻辑操作可采用线性光学器件来实现.如参考文献[13]所述,光子的存储可以用光纤中的光延时来解决.这样我们的协议可以用现有的技术实现.

[1] Nielsen M A, Chuang I L 2000 *Quantum Computation and Quantum information* (Cambridge: Cambridge University Press)

[2] Shor P W 1994 *Proceeding of the* 35*th Annual Symposium on the Foundations of Computer Science* (New York: IEEE Press) p124

[3] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, (New York: IEEE Press) p175

[4] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[5] Long G L, Liu X S 2002 *Phys. Rev.* A **65** 032302

[6] Deng F G, Long G L 2003 *Phys. Rev.* A **68** 042315

[7] Yang L, Wu L A, Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese) [杨 理、吴令安、刘颂豪 2002 物理学报 **51** 2446]

[8] Ma H Q, Li Y L, Zhao H, Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese) [马海强、李亚玲、赵 环、吴令安 2005 物理学报 **54** 5014]

[9] Hillery M, Buzek V, Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[10] Deng F G, Long G L 2004 *Phys. Rev.* A **69** 052319

[11] Cai Q Y, Li B W 2004 *Chin. Phys. Lett.* **21** 601

[12] Bostrom K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[13] Deng F G, Long G L, Liu X S 2003 *Phys. Rev.* A **68** 042317

[14] Wang J, Zhang Q, Tang C J 2006 *Int. J. Mod. Phys.* C **17** 685

[15] Wang J, Zhang Q, Tang C J 2006 *Opt. Commun.* **266** 732

[16] Zhu A D, Xia Y, Fan Q B, Zhang S 2006 *Phys. Rev.* A **73** 022338

[17] Wang J, Zhang Q, Tang C J 2006 *Phys. Lett.* A **358** 256

[18] Man Z X, Zhang Z J, Li Y 2005 *Chin. Phys. Lett.* **22** 18

[19] Gao T, Yan F L, Wang Z X 2004 *Nuovo Cimento* B **119** 313

[20] Gao T, Yan F L, Wang Z X 2005 *J. Phys.* A **38** 5761

[21] Gao T, Yan F L, Wang Z X 2005 *Chin. Phys.* **14** 893

[22] Kim J, Benson O, Kan H, Yamamoto Y 1999 *Nature* **397** 500

[23] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[24] Beveratos A, Brouri R, Gacoin T, Villing A, Poizat J P, Grangier P 2002 *Phys. Rev. Lett.* **89** 187901

[25] Ribordy G, Gautier J D, Gisin N, Guinnard O, Zbinden H 2000 *J. Mod. Opt.* **47** 517

Multiparty controlled quantum secure direct communication protocol*

Wang Jian†　Chen Huang-Qing　Zhang Quan　Tang Chao-Jing

(*School of Electronic Science and Engineering, National University of Defense Technology, Changsha* 410073, *China*)

(Received 10 May 2006; revised manuscript received 12 June 2006)

Abstract

Based on the order rearrangement of single photon sequence, we present a multiparty controlled quantum secure direct communication protocol. The present protocol can be applied to some special scenario. In the protocol, the sender's secret message can only be recovered by the receiver under the permission of all the controllers. The security for the protocol is ensured by the quantum no-cloning theorem and the secret transmitting order of the single photon sequence. Moreover, all photons are used to encode the secret message except those chosen for eavesdropping check and it is unnecessary for the protocol to use entanglement. Our protocol is efficient and practicable.

Keywords: quantum cryptography, quantum secure direct communication, order rearrangement, single photon

PACC: 0365, 4230, 4250

* Project supported by the National Natural Science Foundation of China (Grant No. 60472032).

† E-mail: jwang@nudt.edu.cn