文章编号: 1001- 2486(2009) 02- 0051- 04

基于纯纠缠态的量子安全直接通信协议*

王 剑, 张 盛, 张守林, 张 权
(国防科技大学 电子科学与工程学院, 湖南 长沙 410073)

摘 要: 基于纯纠缠态, 提出一种量子安全直接通信协议。通信方利用 decoy 光子来检测窃听。在保证量子信道的安全后, 发送方通过控制非操作和 von Neumann 测量将秘密消息编码在纯纠缠态上并发送给接收方。由于所有的纯纠缠态都用于传输秘密消息, 该协议具有较高的量子比特效率。就实验的可行性来说, 该协议可以用当前的技术实现。此外, 该协议在噪声量子信道中也是安全的。

关键词: 量子密码; 量子安全直接通信; 纯纠缠态
中图分类号: TP309. 7 文献标识码: A

Quantum Secure Direct Communication Protocol with Pure Entangled States

WANG Jian, ZHANG Sheng, ZHANG Shou-lin, ZHANG Quan
(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: We present a quantum secure direct communication protocol where the channels are not the maximally entangled states. The communication parties utilize decoy photons to check eavesdropping. After ensuring the security of the quantum channel, the sender encodes the secret message and transmits it to the receiver by using controlled-NOT operation and von Neumann measurement. The protocol is efficient in that all pure entangled states are used to transmit the secret message. As for the experimental feasibility, our protocol can be realized with today's technologies. The protocol is also verified to be secure for a noise quantum channel.

Key words: quantum cryptography; quantum secure direct communication; pure entangled states

量子密码是以量子力学和经典密码学为基础, 利用微观粒子的量子属性实现信息保护的一种新型密码体制, 其安全性由量子不可克隆定理和测不准原理所保证[1]。量子密码主要包括量子密钥分配(QKD)[2]、量子数据加密、量子秘密共享、量子身份认证、量子数字签名以及量子安全直接通信(QSDC)[3-10]等方面。QKD 是指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。与 QKD 不同的是, 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。目前, 针对 QSDC 的研究成为量子密码学中的一个研究热点。

QSDC 协议可以分为基于纠缠粒子系统的 QSDC 协议和基于单粒子系统的 QSDC 协议两类。基于纠缠粒子系统的 QSDC 协议大多采用最大纠缠态。由于消相干及噪声, 往往很难得到最大纠缠态, 利用纠缠提纯也只能从部分纠缠的态中提取出近似的最大纠缠态。本文利用非最大纠缠的量子信道实现了一个 QSDC 协议。类似于文献[10], 通信方利用 decoy 光子来保证量子信道的安全。如果传输量子信道中没有窃听, 则发送方通过控制非操作将秘密消息编码在纯纠缠态上, 通信各方然后对各自的光子执行 von Neumann 测量, 接收方根据发送方公布的测量结果就可以得到发送方的秘密消息。协议中传输的光子序列并不携带秘密信息, 我们同时指出该协议在噪声量子信道中也是安全的。

1 协议描述

假设发送方 Alice 想要将秘密消息直接传送给接收方 Bob, 协议由以下几步组成:

* 收稿日期: 2008- 10- 27
基金项目: 国家自然科学基金资助项目(60872052)
作者简介: 王剑(1975—), 男, 讲师, 博士。

(S1) Alice 制备 N 个有序的两光子态, 每一个两光子态为 $|\varphi\rangle_{AB}=a|00\rangle_{AB}+b|11\rangle_{AB}$, 其中 $|a|^2+|b|^2=1$。这 N 个有序的态可以表示为 $[P_1(A),P_1(B)]$、$[P_2(A),P_2(B)]$、…、$[P_N(A),P_N(B)]$, 其中下标表示两光子态在序列中的顺序, A 和 B 表示态的两个光子。Alice 从每个态中提取一个光子构成一个有序的光子序列 $[P_1(A),P_2(A),\cdots,P_N(A)]$, 称为 A 序列。其余的光子组成 B 序列, $[P_1(B),P_2(B),\cdots,P_N(B)]$。

(S2) Alice 制备一些 decoy 光子用于窃听检测。每一个 decoy 光子随机地处于 $\{|0\rangle,|1\rangle,|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\}$ 中的一个态。Alice 将这些 decoy 光子随机地插入到 B 序列中并将这个新的 B 序列发送给 Bob。

(S3) 确认 Bob 收到 B 序列后, Alice 公布 decoy 光子的位置信息以及所处基的信息。Bob 根据 decoy 光子的测量基信息, 对其执行 von Neumann 测量并公布测量结果。Alice 根据 Bob 的测量结果, 对 B 序列传输过程中的错误率进行估计。如果错误率低于他们预先设定的门限, Alice 则认为传输信道中没有窃听, 通信方继续执行协议的下一步; 反之, 通信方中断协议。

(S4) Alice 根据其秘密消息比特值, 对应每一光子对分别制备一个光子 a, 即如果 Alice 的秘密消息比特为 0(1), 则她制备一个态为 $|0\rangle(|1\rangle)$ 的光子。这样, Alice 对应 N 个有序的光子对制备了 N 个光子 $[P_1(a),P_2(a),\cdots,P_N(a)]$, 称为 a 序列。如果光子 $P_i(a)$ $(i=1,2,\cdots,N)$ 的态为 $|0\rangle$, 则由光子 $P_i(a)$、$P_i(A)$ 以及 $P_i(B)$ 构成的复合系统的态为

$$|\Phi_0\rangle_{aAB}=|0\rangle_a\overleftarrow{(a|00\rangle+b|11\rangle)}_{AB} \tag{1}$$

其中下标 a 表示光子 $P_i(a)$。如果 $P_i(a)$ 处于态 $|1\rangle$, 则 $[P_i(a),P_i(A),P_i(B)]$ 的态为

$$|\Phi_1\rangle_{aAB}=|1\rangle_a\overleftarrow{(a|00\rangle+b|11\rangle)}_{AB} \tag{2}$$

(S5) Alice 对光子 $P_i(A)$ 和 $P_i(a)$ $(i=1,2,\cdots,N)$ 执行控制非操作 ($P_i(A)$ 为控制位, $P_i(a)$ 为靶位)。控制非操作使得态 $|\Phi_0\rangle_{aAB}$ 变为

$$|\Phi_0'\rangle_{aAB}=(a|000\rangle+b|111\rangle)_{aAB} \tag{3}$$

态 $|\Phi_1\rangle_{aAB}$ 变为

$$|\Phi_1'\rangle_{aAB}=(a|100\rangle+b|011\rangle)_{aAB} \tag{4}$$

(S6) 执行完控制非操作后, Alice 和 Bob 分别对光子 $P_i(a)$ 和 $P_i(B)$ 执行 σ_z 基测量。由式(4)和(5), 虽然 Bob 得到了测量结果, 但他还是无法获取 Alice 的秘密消息。

(S7) Alice 公布 a 序列中光子的测量结果。如表 1 所示, Bob 根据 Alice 公布的测量结果可以恢复出 Alice 的秘密消息。例如, 假设 Bob 的测量结果为 $|0\rangle$, 如果 Alice 的测量结果为 $|0\rangle(|1\rangle)$, Bob 可以推断出 Alice 的秘密消息为 0(1)。

表 1 Alice 秘密消息的恢复

Tab. 1 The recovery of Alice's secret message

秘密消息	Alice 的测量结果	Bob 的测量结果
0	$\|0\rangle$	$\|0\rangle$
1	$\|0\rangle$	$\|1\rangle$
1	$\|1\rangle$	$\|0\rangle$
0	$\|1\rangle$	$\|1\rangle$

为使通信双方的测量结果对称分布于 0 和 1, 而不是出现大概率的 0 或 1, 可以对协议的第(S1)步进行稍许修改, 即 Alice 在第(S1)步制备 N 个有序的两光子态, 每一个两光子态随机地处于 $|\varphi\rangle_{AB}$ 或 $|\phi\rangle_{AB}=a|11\rangle_{AB}+b|00\rangle_{AB}$, 以代替制备 N 个态为 $|\varphi\rangle_{AB}$ 的光子对。

2　效率及安全性分析

Cabello 从信息论的角度定义量子密码协议的效率为 $\xi = b_s/(q_t + b_t)$, 其中 b_s 为通信方得到的秘密比特数, q_t 和 b_t 分别为协议中交互的量子比特数和经典比特数(这里省略了用于窃听检测的经典比特数) 。根据 Cabello 定义的效率公式, 该协议的总效率为 50% 。

事实上, 量子比特的制备和传输较之经典比特要复杂得多, Cabello 的效率公式(通常称为总效率) 并不能充分描述量子密码协议的效率。量子比特效率是分析量子密码协议效率的有益补充, 其定义为 $\eta = q_u/q_t$, 其中 q_u 为有用的量子比特, q_t 为传输的总的量子比特。在评估量子密码协议效率时通常要结合这两个参数。由量子比特效率公式, 该协议量子比特的效率为 100% 。

该协议利用 decoy 光子使得窃听者 Eve 无法进行成功的窃听, 而且窃听者的窃听行为将在窃听检测过程中被发现。由于 decoy 光子随机地处于$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$中的一个态, 该协议的安全性等价于 BB84 协议的安全性。如果保证了量子信道的安全, 那么该协议就是完全安全的。

根据 Stinespring Dilation 定理, Eve 的攻击可以视为在一个大的 Hilbert 空间 $H_{AB} \leftarrow H_E$ 上执行幺正操作 $\hat{E}$。假设 Eve 的辅助态为$|\varepsilon\rangle$, 则

$$\hat{E}|0, \varepsilon\rangle = \alpha|0, \varepsilon_{00}\rangle + \beta|1, \varepsilon_{01}\rangle \tag{5}$$

$$\hat{E}|1, \varepsilon\rangle = \beta'|0, \varepsilon_{10}\rangle + \alpha'|1, \varepsilon_{11}\rangle \tag{6}$$

$$\begin{aligned}\hat{E}|+, \varepsilon\rangle &= \frac{1}{\sqrt{2}}[\alpha|0, \varepsilon_{00}\rangle + \beta|1, \varepsilon_{01}\rangle + \beta'|0, \varepsilon_{10}\rangle + \alpha'|1, \varepsilon_{11}\rangle] \\ &= \frac{1}{2}[|+\rangle(\alpha|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle + \beta'|\varepsilon_{10}\rangle + \alpha'|\varepsilon_{11}\rangle) \\ &\quad + |-\rangle(\alpha|\varepsilon_{00}\rangle - \beta|\varepsilon_{01}\rangle + \beta'|\varepsilon_{10}\rangle - \alpha'|\varepsilon_{11}\rangle)]\end{aligned} \tag{7}$$

$$\begin{aligned}\hat{E}|-, \varepsilon\rangle &= \frac{1}{\sqrt{2}}[\alpha|0, \varepsilon_{00}\rangle + \beta|1, \varepsilon_{01}\rangle - \beta'|0, \varepsilon_{10}\rangle - \alpha'|1, \varepsilon_{11}\rangle] \\ &= \frac{1}{2}[|+\rangle(\alpha|\varepsilon_{00}\rangle + \beta|\varepsilon_{01}\rangle - \beta'|\varepsilon_{10}\rangle - \alpha'|\varepsilon_{11}\rangle) \\ &\quad + |-\rangle(\alpha|\varepsilon_{00}\rangle - \beta|\varepsilon_{01}\rangle - \beta'|\varepsilon_{10}\rangle + \alpha'|\varepsilon_{11}\rangle)]\end{aligned} \tag{8}$$

Eve 的幺正操作可以写为

$$\hat{E} = \begin{pmatrix} \alpha & \beta' \\ \beta & \alpha' \end{pmatrix} \tag{9}$$

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 $|\alpha|^2 = |\alpha'|^2$, $|\beta|^2 = |\beta'|^2$, 那么, Eve 的攻击引入的错误率为 $e = |\beta|^2 = 1 - |\alpha|^2$。

从信息论的角度来看, 在一个量子系统中, 可得到的信息不超过 Holevo 限 $\chi(\rho) = S(\rho) - \sum_i p_i S(\rho_i)$, 其中 $S(\rho)$ 为态 ρ 的 von-Neumann 熵, $\rho = \sum_i p_i \rho_i$ (ρ_i 为 Alice 以概率 p_i 制备的量子态)。如果 Alice 分别以 1/4 的概率制备 4 个 decoy 光子, 那么 decoy 光子的 Shannon 熵为 $H(\rho) = -\sum_i p_i \log_2 p_i = 2$, Eve 可得到的信息

$$I_E \leqslant S(\rho) - \sum_i p_i S(\rho_i) < H(P) \tag{10}$$

由此看来, Eve 无法得到 decoy 光子的完备信息, 通信方可以检测到 Eve 的窃听行为。

在噪声量子信道中, Eve 可以在第(S2) 步截获 B 序列中的部分光子, 并利用一个光子损失较少的低噪量子信道将 B 序列中其余的光子发送给接收方。在这种情况下, Eve 的攻击行为不会被通信方发现。但是, 在该协议中, 没有 Alice 的测量结果, Eve 即使截获 B 序列的部分粒子也无法得到 Alice 的秘密消息。Bob 只需在协议的第(S6) 步告诉 Alice 他收到了哪些粒子, 哪些粒子在传输过程中损失了。Alice 然后只公布 Bob 确实收到的那些光子对应的她的测量结果。例如, 如果 Bob 收到了 B 序列中的光子

$P_3(B)$、$P_6(B)$、…, 则 Alice 仅公布她对光子 $P_3(a)$、$P_6(a)$、…的测量结果。因此, 该协议在噪声量子信道下也是安全的。当然, 在噪声量子信道中, Alice 不能将秘密消息直接发送给 Bob。如果通信方在协议的第(S4)步, 即窃听检测通过之后, 采用某种方法能够判断双方是否共享了纠缠, 那么该协议在噪声量子信道中可以正常运行。

3 结束语

基于纠缠粒子系统的量子密码协议一般都使用最大纠缠态。但是, 由于消相干以及噪声, 往往很难得到最大纠缠态。本文基于纯纠缠态提出了一种 QSDC 协议并分析了协议的安全性。为检测传输量子信道中是否存在窃听, 秘密发送方在传输光子序列中插入了 decoy 光子。在确保量子信道的安全后, 发送方通过控制非操作将秘密消息编码在纯纠缠态上。然后通信各方对各自的粒子执行 σ_z 基测量。发送方公布其测量结果后, 接收方就可以根据自己的测量结果得出发送方的秘密消息。由于所有的纯纠缠态都用于传输秘密消息, 该协议具有较高的量子比特效率, 而且该协议在噪声量子信道中也是安全的。就实验的可行性来说, 该协议可以用当前的技术实现。

目前, 量子密码协议无论在理论上还是实验上的研究都取得了令人瞩目的成果。作者下一步的研究重点是设计高效、可实现性强、抗噪声以及具备特殊功能的多方多级的量子密码协议, 以拓展量子密码的研究范围, 加快量子密码的实用化进程。

参 考 文 献:

[1] 李承祖, 黄明球, 等. 量子通信与量子计算[M]. 长沙: 国防科技大学出版社, 2000.

[2] Bennett C H, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing[C]//IEEE Int. Conf. on Computers Systems and Signal Processing, Bangalore, India, 1984: 175- 179.

[3] Long G L, Liu X S. Theoretically Efficient High-capacity Quantum-key-distribution Scheme[J]. Phys. Rev. A, 2002, 65:032302.

[4] Bostr$\ddot{\text{o}}$m K, Felbinger T. Deterministic Secure Direct Communication Using Entanglement[J]. Phys. Rev. Lett., 2002, 89: 187902.

[5] Deng F G, Long G L, Liu X S. Two-step Quantum Direct Communication Protocol Using the Einstein-podolsky-rosen Pair Block[J]. Phys. Rev. A, 2003, 68(4): 042317.

[6] Cai Q Y, Li B W. Deterministic Secure Communication without Using Entanglement[J]. Chin. Phys. Lett., 2004, 21(4): 601- 603.

[7] Wang J, Zhang Q, Tang C J. Quantum Secure Direct Communication Based on Order Rearrangement of Single Photons[J]. Phys. Lett. A, 2006, 358: 256- 258.

[8] 王剑, 陈皇卿, 张权, 等. 多方控制的量子安全直接通信协议[J]. 物理学报, 2007, 56(2): 673- 677.

[9] Wang J, Zhang Q, Tang C J. Multiparty Controlled Quantum Secure Direct Communication using Greenberger-horne-zeilinger State[J]. Opt. Commun., 2006, 266: 732- 737.

[10] Li X H, Deng F G, et al. Deterministic Secure Quantum Communication without Maximally Entangled States[J]. J. Korean Phys. Soc., 2006, 49(4): 1354- 1359.