文章编号:1001 - 2486(2007)02 - 0056 - 05

# 基于纠缠交换的量子安全通信协议*

王 剑,陈皇卿,张 权,唐朝京
(国防科技大学 电子科学与工程学院,湖南 长沙 410073)

摘 要:基于纠缠交换和 Einstein-Podolsky-Rosen 纠缠对,提出一种量子安全直接通信协议和一种多方量子秘密共享协议。量子安全直接通信协议利用光子分组传输方法,与现有协议不同的是通信方可以直接将秘密消息编码为四个 Bell 态之一,从而不需要在保证量子信道的安全之后再对秘密消息编码。在多方量子秘密共享协议中,通信方以一定的概率选择检测模式和编码模式。协议的实现只需要 Einstein-Podolsky-Rosen 对而不需要制备多粒子纠缠态。与已有的协议相比较,该协议不需要局域幺正操作,协议的效率得到了显著提高。两个协议的安全性均等同于 BBM92 协议的安全性。

关键词:量子信息;量子密码;量子安全直接通信;量子秘密共享;纠缠交换
中图分类号:TP309.7 文献标识码:A

# Quantum Secure Communication Protocols on the Basis of Entanglement Swapping

WANG Jian, CHEN Huang-qing, ZHANG Quan, TANG Chao-jing
(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

**Abstract**: A quantum secure direct communication protocol and a multiparty quantum secret sharing protocol based on Einstein-Podolsky-Rosen pairs and entanglement swapping are presented. The present quantum secure direct communication protocol makes use of the ideal of block transmission. Different from the proposed quantum secure direct communication protocols, the sender can encode one's secret message as one of the four Bell states without ensuring the security of the quantum channel firstly. In the multiparty quantum secret sharing protocol, the communication parties adopt checking mode or encoding mode with some probability. It does not need multi-particles entangled state but only Einstein-Podolsky-Rosen pair to realize the protocol. Compared with the proposed quantum secret sharing protocol with entanglement swapping, it is unnecessary for the protocol to perform local unitary operation. The efficiency for the protocol is greatly improved. The securities for both the protocols are the same as that for BBM92 protocol.

**Key words**: quantum information; quantum cryptography; quantum secure direct communication; quantum secret sharing; entanglement swapping

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就是由量子力学基本原理保证的无条件安全的量子密码学。量子密码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。量子密码主要包括量子密钥分配(QKD)[3-4]、量子数据加密、量子秘密共享(QSS)[4]、量子身份认证、量子数字签名以及量子安全直接通信(QSDC)[5-7]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。QSS 是经典秘密共享的量子版本,利用量子力学的基本原理可以实现无条件安全的秘密共享。

本文基于纠缠交换和 EPR 对提出了一种 QSDC 协议和一种 QSS 协议。其中 QSDC 协议利用了光子分组传输的思想。不同于已有的 QSDC 协议,发送方可以直接将秘密消息编码在 EPR 对上,从而不

* 收稿日期:2006 - 05 - 15
基金项目:国家自然科学基金资助项目(60472032)
作者简介:王剑(1975—),男,工程师,博士生。

需要首先保证量子信道的安全再进行消息编码。在多方 QSS 协议中,通信方以一定的概率选择检测模式和编码模式,协议只需要 ERP 对即可实现,而不需要难以制备的多粒子纠缠的 GHZ 态,因此协议具有较强的可实现性。与文献[8]相比,本文的协议不需要进行局域幺正操作,协议更为简单实用。我们同时说明了这两个协议是安全的。

## 1　纠缠交换的基本原理

纠缠交换(ES)能够使没有直接相互作用的两个量子系统纠缠起来。由于 ES 使得远距离分布纠缠成为可能,所以 ES 在量子信息中起着相当重要的作用。首先对纠缠交换进行简单的描述。四个 Bell 态表示为:

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),\quad |\Psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle) \tag{1}$$

假设通信方 Alice 和 Bob 相距很远,他们共享了两个 Bell 态,$|\phi_{12}^{+}\rangle$和$|\phi_{34}^{+}\rangle$,其中光子 1 和 4 属于 Alice,Bob 拥有光子 2 和 3。$|\phi_{12}^{+}\rangle$和$|\phi_{34}^{+}\rangle$的乘积态可以表示为:

$$|\phi_{12}^{+}\rangle\otimes|\phi_{34}^{+}\rangle=\frac{1}{2}(|\phi_{14}^{+}\rangle|\phi_{23}^{+}\rangle+|\phi_{14}^{-}\rangle|\phi_{23}^{-}\rangle+|\Psi_{14}^{+}\rangle|\Psi_{23}^{+}\rangle+|\Psi_{14}^{-}\rangle|\Psi_{23}^{-}\rangle) \tag{2}$$

如果 Alice 对光子 1 和 4 进行 Bell 基测量,则光子 1,2,3,4 的态分别以 1/4 的概率塌缩为$|\phi_{14}^{+}\rangle|\phi_{23}^{+}\rangle$,$|\phi_{14}^{-}\rangle|\phi_{23}^{-}\rangle$,$|\Psi_{14}^{+}\rangle|\Psi_{23}^{+}\rangle$或$|\Psi_{14}^{-}\rangle|\Psi_{23}^{-}\rangle$。当然,如果 Alice 和 Bob 共享其他的 Bell 态也可以得到类似的结果。本文需要用到的其他纠缠交换关系式包括:

$$|\phi_{12}^{-}\rangle\otimes|\phi_{34}^{+}\rangle=\frac{1}{2}(|\phi_{14}^{+}\rangle|\phi_{23}^{-}\rangle+|\phi_{14}^{-}\rangle|\phi_{23}^{+}\rangle+|\Psi_{14}^{-}\rangle|\Psi_{23}^{+}\rangle+|\Psi_{14}^{+}\rangle|\Psi_{23}^{-}\rangle) \tag{3}$$

$$|\Psi_{12}^{+}\rangle\otimes|\phi_{34}^{+}\rangle=\frac{1}{2}(|\phi_{14}^{+}\rangle|\Psi_{23}^{+}\rangle-|\phi_{14}^{-}\rangle|\Psi_{23}^{-}\rangle+|\Psi_{14}^{+}\rangle|\phi_{23}^{+}\rangle-|\Psi_{14}^{-}\rangle|\phi_{23}^{-}\rangle) \tag{4}$$

$$|\Psi_{12}^{-}\rangle\otimes|\phi_{34}^{+}\rangle=\frac{1}{2}(|\phi_{14}^{-}\rangle|\Psi_{23}^{+}\rangle-|\phi_{14}^{+}\rangle|\Psi_{23}^{-}\rangle+|\Psi_{14}^{-}\rangle|\phi_{23}^{+}\rangle-|\Psi_{14}^{+}\rangle|\phi_{23}^{-}\rangle) \tag{5}$$

## 2　基于纠缠交换的 QSDC 协议

在 QSDC 协议中,假设发送方 Alice 想要将 $2(n-m)$ 比特的秘密消息直接发送给接收方 Bob。Alice 和 Bob 编码四个 Bell 态$|\phi^{+}\rangle$,$|\phi^{-}\rangle$,$|\Psi^{+}\rangle$,$|\Psi^{-}\rangle$为两比特的消息"00"↔"01"↔"10"和"11"。协议的具体步骤为:

(1)Alice 直接将秘密消息编码在 $n-m$ 个 EPR 对上。如果 Alice 的秘密消息为 00(01,10,11),她制备态$|\phi^{+}\rangle$($|\phi^{-}\rangle$,$|\Psi^{+}\rangle$,$|\Psi^{-}\rangle$)。这样,编码了秘密消息的 $n-m$ 个 EPR 对构成了一个有序的编码序列。Alice 同时制备 $m$ 个 EPR 对作为检测序列,每一个 EPR 对均处于态$|\phi_{12}^{+}\rangle$。Alice 将这 $m$ 个 EPR 对随机地插入到编码序列中,构成 $n$ 个有序的 EPR 对 $\{[P_1(1),P_1(2)],[P_2(1),P_2(2)],\cdots,[P_n(1),P_n(2)]\}$,其中下标表示每一个 EPR 对在序列中的顺序,1 和 2 表示 EPR 对的两个光子。Alice 从每一个 EPR 对中提取出一个光子构成一个有序的光子序列,$[P_1(1),P_2(1),\cdots,P_n(1)]$称为 $S_1$ 序列,其余的光子构成 $S_2$ 序列$[P_1(2),P_2(2),\cdots,P_n(2)]$。Bob 同样制备 $n$ 个有序的 EPR 对,只不过每一个 EPR 对的态为$|\phi_{34}^{+}\rangle$。与 Alice 一样,Bob 将他制备的 $n$ 个 EPR 对分为 $S_3$ 序列$[P_1(3),P_2(3),\cdots,P_n(3)]$和 $S_4$ 序列$[P_1(4),P_2(4),\cdots,P_n(4)]$。Alice 将 $S_2$ 序列发送 Bob,Bob 将 $S_4$ 序列发送给 Alice。

(2)在确认双方都接收到光子序列后,Alice 随机地选择 $Z$ 基($|0\rangle$,$|1\rangle$)或 $X$ 基($|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$,$|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$)对检测序列中的光子 1 进行测量。测量完后,Alice 告诉 Bob 检测序列的位置、她选择的测量基以及测量结果。Bob 采用与 Alice 相同的测量基对检测序列中的光子 2 进行测量并将他的测量结果与 Alice 公布的结果进行比较。由于检测序列中光子的态均为$|\phi_{12}^{+}\rangle$,$|\phi_{12}^{+}\rangle$可以用 $X$ 基表示为:$|\phi_{12}^{+}\rangle=\frac{1}{\sqrt{2}}(|++\rangle+|--\rangle)_{12}$。如果没有窃听,无论是用 $Z$ 基还是 $X$ 基测量,双方的结果

必定是一致的。这样,Bob 可以估计出 $S_2$ 序列传输中的错误率。类似地,通信双方采用相同的窃听检测方法来保证 $S_4$ 序列传输的安全。如果错误率超过双方预先设定的错误门限,通信双方放弃协议,否则继续执行协议的下一步。

(3) Alice 对编码序列中的光子 1 和 4 执行 Bell 基测量,并公布测量结果。Bob 对编码序列中的光子 2 和 3 执行 Bell 基测量。由式(2)~(5),Bob 根据自己的测量结果可以得到 Alice 的秘密消息,如表 1 所示。例如,如果 Alice 的测量结果为 $|\phi_{14}^-\rangle$,Bob 的测量结果为 $|\phi_{23}^+\rangle$,那么 Alice 的秘密消息为"01"。

表 1 Alice 秘密消息的恢复

Tab. 1 The recovery of Alice's secret message

| Alice 的秘密消息 | | {Alice 的测量结果,Bob 的测量结果} |
|---|---|---|
| 00 | $(\|\phi^+\rangle)$ | $\{\|\phi_{14}^+\rangle,\|\phi_{23}^+\rangle\}$, $\{\|\phi_{14}^-\rangle,\|\phi_{23}^-\rangle\}$, $\{\|\Psi_{14}^+\rangle,\|\Psi_{23}^+\rangle\}$, $\{\|\Psi_{14}^-\rangle,\|\Psi_{23}^-\rangle\}$ |
| 01 | $(\|\phi^-\rangle)$ | $\{\|\phi_{14}^+\rangle,\|\phi_{23}^-\rangle\}$, $\{\|\phi_{14}^-\rangle,\|\phi_{23}^+\rangle\}$, $\{\|\Psi_{14}^-\rangle,\|\Psi_{23}^+\rangle\}$, $\{\|\Psi_{14}^+\rangle,\|\Psi_{23}^-\rangle\}$ |
| 10 | $(\|\Psi^+\rangle)$ | $\{\|\phi_{14}^+\rangle,\|\Psi_{23}^+\rangle\}$, $\{\|\phi_{14}^-\rangle,\|\Psi_{23}^-\rangle\}$, $\{\|\Psi_{14}^+\rangle,\|\phi_{23}^+\rangle\}$, $\{\|\Psi_{14}^-\rangle,\|\phi_{23}^-\rangle\}$ |
| 11 | $(\|\Psi^-\rangle)$ | $\{\|\phi_{14}^-\rangle,\|\Psi_{23}^+\rangle\}$, $\{\|\phi_{14}^+\rangle,\|\Psi_{23}^-\rangle\}$, $\{\|\Psi_{14}^-\rangle,\|\phi_{23}^+\rangle\}$, $\{\|\Psi_{14}^+\rangle,\|\phi_{23}^-\rangle\}$ |

该协议的安全性基于 $S_2$ 序列和 $S_4$ 序列传输的安全性,即只要保证传输序列的安全,协议就是安全的。Alice 和 Bob 对检测光子采用随机的 $Z$ 基和 $X$ 基测量来检测窃听,这种窃听检测方法类似于 BBM92 协议的窃听检测方法[3]。BBM92 协议已经被证明是无条件安全的,而且只有在保证传输序列的安全之后,Alice 才会执行 Bell 基测量并公布她的测量结果,因此该协议的安全性等同于 BBM92 协议的安全性。从信息论的角度对协议的安全性进行分析,可以更加清楚地说明窃听者 Eve 的窃听行为无法逃脱通信双方的窃听检测。互信息定义为 $I(X:\ Y)=H(X)-H(X\mid Y)$,其中 $H(X)=-\sum_i p(x_i)\log_2 p(x_i)$ 为香农熵,$H(X\mid Y)$ 为条件熵。如果没有窃听,Alice 和 Bob 之间的互信息 $I_{AB}=2$,Alice 和 Eve 之间的互信息 $I_{AE}=0$ 如果 Eve 截获通信方的传输光子,并将自己制备的纠缠粒子对分别发送给各通信方,则 Alice 和 Eve 之间的互信息 $I_{AE}=2$,Alice 和 Bob 之间的互信息 $I_{AB}=0$。因此,Alice 和 Bob 很容易就可以检测到 Eve 的存在。

该协议也可以用局域幺正操作来实现,下面简单阐述其基本原理。Alice 和 Bob 分别制备 $n$ 个有序的 EPR 对,每一个 EPR 对均处于态 $|\phi^+\rangle$。Alice 将四个幺正操作 $I,\sigma_x,i\sigma_y,\sigma_z$ 分别编码为"00""01""10"和"11"。类似于该协议的第(1)步,每一方将各自 EPR 序列中的一组光子序列发送给另一方。在保证传输序列的安全之后,Alice 根据她的秘密消息采用相应的幺正操作将两比特的秘密信息编码在 EPR 对上。Alice 然后执行 Bell 基测量并公布其测量结果。Bob 根据 Alice 的测量结果和他自己的测量结果就可以得到 Alice 的秘密消息。

该协议最突出的特点是在传输光子序列之前就可以直接将秘密消息编码在纠缠对上,而不需要事先保证量子信道的安全。协议的缺点是需要用到量子存储器来存储传输光子序列。此外,由于需要制备纠缠对和进行 Bell 基测量,该协议比基于单光子的 QSDC 协议要复杂一些。

## 3 基于纠缠交换的多方 QSS 协议

我们首先给出一个三方 QSS 协议,然后将其扩展到多方 QSS 协议。假设 Alice 想要与 Bob 和 Charlie 共享一组随机密钥,Bob 和 Charlie 只有联合起来才能得到与 Alice 共享的随机密钥。协议由以下几步组成:

(1) Alice、Bob 和 Charlie 将四个 Bell 态 $|\phi^+\rangle,|\phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle$ 分别编码为"00""01""10"和"11"。Alice(Bob,Charlie)制备一个 EPR 对处于态 $|\phi_{12}^+\rangle$($|\phi_{34}^+\rangle,|\phi_{56}^+\rangle$)。Alice(Bob,Charlie)将光子 2(4,6)发送给 Bob(Charlie,Alice),并保留光子 1(3,5)。

(2) Alice 以概率 $p$ 选择检测模式,以概率 $1-p$ 选择编码模式。如果 Alice 选择检测模式,则通信双

方执行(C3);否则,跳转至(E3)。

(C3) Bob 随机地选择两组测量基($Z$ 基和 $X$ 基)对光子 2 进行测量。测量完后,Bob 告诉 Alice 他选择的测量基以及相应的测量结果。Alice 然后采用与 Bob 相同的测量基对光子 2 进行测量,并将她的测量结果与 Bob 的结果相比较。如果不存在窃听者,Alice 和 Bob 的结果是一致的。Alice 和 Charlie 用同样的方法来检测光子 6 传输过程中是否存在窃听。为了保证光子 4 传输的安全并防止不诚实的通信方的攻击,Alice 随机地指定 Bob 或者是 Charlie 去选择一个随机的测量基对光子 3 或 4 进行测量并公布相应的测量结果。如果光子 2,4,6 的传输都是安全的,协议转到第(1)步;否则协议中止。

(E3) Alice(Bob,Charlie)对光子 1 和 6(2 和 3,4 和 5)执行 Bell 基测量。根据式(2)~(5),光子 1,2,3,4,5 和 6 的态可以表示为:

$$\begin{aligned}|\phi_{12}^{+}\rangle\otimes|\phi_{34}^{+}\rangle\otimes|\phi_{56}^{+}\rangle=\frac{1}{4}(&|\phi_{16}^{+}\rangle|\phi_{23}^{+}\rangle|\phi_{45}^{+}\rangle+|\phi_{16}^{+}\rangle|\phi_{23}^{-}\rangle|\phi_{45}^{-}\rangle\\&+|\phi_{16}^{+}\rangle|\Psi_{23}^{+}\rangle|\Psi_{45}^{+}\rangle+|\phi_{16}^{+}\rangle|\Psi_{23}^{-}\rangle|\Psi_{45}^{-}\rangle\\&+|\phi_{16}^{-}\rangle|\phi_{23}^{+}\rangle|\phi_{45}^{-}\rangle+|\phi_{16}^{-}\rangle|\phi_{23}^{-}\rangle|\phi_{45}^{+}\rangle\\&+|\phi_{16}^{-}\rangle|\Psi_{23}^{-}\rangle|\Psi_{45}^{+}\rangle+|\phi_{16}^{-}\rangle|\Psi_{23}^{+}\rangle|\Psi_{45}^{-}\rangle\\&+|\Psi_{16}^{+}\rangle|\phi_{23}^{+}\rangle|\Psi_{45}^{+}\rangle-|\Psi_{16}^{+}\rangle|\phi_{23}^{-}\rangle|\Psi_{45}^{-}\rangle\\&+|\Psi_{16}^{+}\rangle|\Psi_{23}^{+}\rangle|\phi_{45}^{+}\rangle-|\Psi_{16}^{+}\rangle|\Psi_{23}^{-}\rangle|\phi_{45}^{-}\rangle\\&+|\Psi_{16}^{-}\rangle|\phi_{23}^{-}\rangle|\Psi_{45}^{+}\rangle-|\Psi_{16}^{-}\rangle|\phi_{23}^{+}\rangle|\Psi_{45}^{-}\rangle\\&+|\Psi_{16}^{-}\rangle|\Psi_{23}^{-}\rangle|\phi_{45}^{+}\rangle-|\Psi_{16}^{-}\rangle|\Psi_{23}^{+}\rangle|\phi_{45}^{-}\rangle)\end{aligned}\tag{6}$$

当 Alice、Bob 和 Charlie 分别对各自的光子执行 Bell 基测量后,光子 1,2,3,4,5 和 6 的态以相同的概率 1/16 塌缩到式(6)16 个态中的一个态。这样,Alice 就与 Bob 和 Charlie 共享了一个随机密钥,如表 2 所示。假设 Bob 的测量结果为 $|\phi_{23}^{+}\rangle$,Charlie 的测量结果为 $|\phi_{45}^{-}\rangle$,Bob 联合 Charlie 就可以得知 Alice 的测量结果为 $|\phi_{16}^{-}\rangle$,这样三方就共享了两比特的密钥"01"。

表 2　三方共享密钥的建立

Tab. 2　The establishment of the three-party's sharing secret key

| 共享密钥 | Alice 的测量结果 | {Bob 的测量结果,Charlie 的测量结果} |
|---|---|---|
| 00 | $\|\phi_{16}^{+}\rangle$ | $\{\|\phi_{23}^{+}\rangle,\|\phi_{45}^{+}\rangle\}$, $\{\|\phi_{23}^{-}\rangle,\|\phi_{45}^{-}\rangle\}$, $\{\|\Psi_{23}^{+}\rangle,\|\Psi_{45}^{+}\rangle\}$, $\{\|\Psi_{23}^{-}\rangle,\|\Psi_{45}^{-}\rangle\}$ |
| 01 | $\|\phi_{16}^{-}\rangle$ | $\{\|\phi_{23}^{+}\rangle,\|\phi_{45}^{-}\rangle\}$, $\{\|\phi_{23}^{-}\rangle,\|\phi_{45}^{+}\rangle\}$, $\{\|\Psi_{23}^{-}\rangle,\|\Psi_{45}^{+}\rangle\}$, $\{\|\Psi_{23}^{+}\rangle,\|\Psi_{45}^{-}\rangle\}$ |
| 10 | $\|\Psi_{16}^{+}\rangle$ | $\{\|\phi_{23}^{+}\rangle,\|\Psi_{45}^{+}\rangle\}$, $\{\|\phi_{23}^{-}\rangle,\|\Psi_{45}^{-}\rangle\}$, $\{\|\Psi_{23}^{+}\rangle,\|\phi_{45}^{+}\rangle\}$, $\{\|\Psi_{23}^{-}\rangle,\|\phi_{45}^{-}\rangle\}$ |
| 11 | $\|\Psi_{16}^{-}\rangle$ | $\{\|\phi_{23}^{-}\rangle,\|\Psi_{45}^{+}\rangle\}$, $\{\|\phi_{23}^{+}\rangle,\|\Psi_{45}^{-}\rangle\}$, $\{\|\Psi_{23}^{-}\rangle,\|\phi_{45}^{+}\rangle\}$, $\{\|\Psi_{23}^{+}\rangle,\|\phi_{45}^{-}\rangle\}$ |

三方 QSS 协议的安全性基于传输光子 2,4,6 的安全性。只要光子传输的安全得到了保证,协议的安全就得到了保证。协议中的每一个通信方只传输了 EPR 对中的一个光子(即光子 2,4,6),为保证传输光子的安全性,每一方都随机地选择 $Z$ 基和 $X$ 基测量来检测窃听。这种窃听检测方法类似于 BBM92 协议中的检测方法,后者被证明是无条件安全的。协议中不诚实的通信方或者窃听者的攻击都会在检测模式中被发现。该协议的安全性与 BBM92 协议的安全性是等价的。协议的安全性分析参见文献[6]。

三方 QSS 协议可以很容易地扩展到多方 QSS 协议。假设 Alice 想要与 Bob、Charlie、Dick…York 和 Zach 共享随机密钥。类似地,每一个通信方制备一个态为 $|\phi^{+}\rangle$ 的 EPR 对,并依次将 EPR 对中的一个光子发送给下一方,即 Alice 发送一个光子给 Bob,Bob 然后发送一个光子给 Charlie…York 发送一个光子给 Zach,Zach 最后发送一个光子给 Alice。类似于三方 QSS 协议,Alice 分别以概率 $p$ 和 $1-p$ 选择检测模式和编码模式。在检测模式中,通信各方利用随机的 $Z$ 基和 $X$ 基测量来保证传输光子的安全。Alice 同样随机地指定 Bob,Charlie…York 和 Zach 选择测量基并公布测量结果。在编码模式中,每一个

通信方对各自拥有的两个光子执行 Bell 基测量。Bell 基测量后,Alice 与 Bob…Zach 就建立了共享密钥。Bob,Charlie…Zach 只要联合起来就可以得到与 Alice 共享的密钥。多方 QSS 协议的具体过程与三方 QSS 协议非常类似,其安全性也等同于三方 QSS 协议,在此不再赘述。

该协议的优点是只需要 EPR 对就可以实现多方 QSS 协议,不需要难以制备的多粒子纠缠态。此外,该协议较之文献[8]中的协议,省略了幺正操作的环节,协议的效率更高。当然与基于单光子的 QSS 协议相比较,由于需要制备纠缠光子,而且还要进行 Bell 基测量,因此该协议的可实现性要差一些。

## 4 结束语

基于纠缠交换和 EPR 对,我们提出了两个量子安全通信协议——QSDC 协议和多方 QSS 协议。在这两个协议中,通信各方分别传送 EPR 对中的一个光子给另一方,然后采用 Bell 基测量各自拥有的两个光子,即利用纠缠交换将没有直接相互作用的两个量子系统关联起来,通信双方从而能够利用纠缠关联进行秘密消息的传送。协议的窃听检测方法采用随机的基和基测量,这种方法等同于 BBM92 协议的窃听检测方法。只要保证了传输光子的安全性,这两个协议就是完全安全的。QSDC 协议将光子分组传输的方法与纠缠交换技术结合起来,发送方可以直接将两比特的秘密消息编码为四个 Bell 态之一,从而不需要在保证量子信道安全之后再进行消息编码,这也是该协议最大的特色。多方 QSS 协议的实现只需要利用 Bell 态,而不需要利用制备和测量区分都较为困难的多粒子纠缠的 GHZ 态,这样协议实现起来比较容易。在多方 QSS 协议中,通信各方均制备一个相同的 Bell 态,而且协议不需要进行局域的幺正操作,与文献[8]相比较,协议的过程得到了简化,效率得到了提高。目前,量子安全通信协议的研究在理论上和实验上都取得令人瞩目的成果,如何在噪声条件下设计高效的量子安全通信协议是作者下一步研究的重点。

## 参考文献:


[1] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information[M]. London: Cambridge University Press, 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] Bennett C H, Brassard G, Mermin N D. Quantum Cryptography without Bell's Theorem[J]. Phys. Rev. Lett., 1992, 68: 557 – 569.

[4] Hillery M, Buzek V, Berthiaume A. Quantum Secret Sharing[J]. Phys. Rev. A, 1999, 59: 1829 – 1834.

[5] Bostrom K, Felbinger T. Deterministic Secure Direct Communication Using Entanglement[J]. Phys. Rev. Lett., 2002, 89: 187902.

[6] 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.

[7] 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.

[8] Zhang Z J, Man X Z. Multiparty Quantum Secret Sharing of Classical Messages Based on Entanglement Swapping[J]. Phys. Rev. A, 2005, 72: 022 – 303.