基于W态的量子安全直接通信协议

杨新元[1] 马 智[1,2] 吕 欣[3]
(信息工程大学 郑州 450002)[1] (河南省科学院应用物理研究所 郑州 450008)[2]
(国家信息中心 北京 100045)[3]

摘 要 提出了一种新的两方量子安全直接通信协议。该方案利用有序的四粒子W态作为信息载体,利用幺正变换对秘密消息进行编码,通过当地Bell基测量和经典通信直接传递秘密消息。在理想信道下,协议对于非相干攻击是安全的。该方案的优点在于利用W态作为信息载体,较GHZ态而言,损耗要小得多,并且不需要在量子信道中传输载有秘密消息的量子比特。

关键词 量子密码,量子安全直接通信,W态,幺正变换
中图法分类号 TN918 **文献标识码** A

Quantum Secure Direct Communication Protocol Based on W State

YANG Xin-yuan[1] MA Zhi[1,2] LU Xin[3]
(University of Information Engineering, Zhengzhou 450002, China) [1]
(Institute of Applied Physics of Henan Academy of Sciences, Zhengzhou 450008, China) [2] (State Information Center, Beijing 100045, China) [3]

Abstract A novel two-party quantum secure direct communication protocol was proposed. By using ordered four-particle W state as carrier of information, encoding the secret message with unitary transformation, we can directly transmit secret message with local Bell-basis measurement and classical communication. In ideal channel, the protocol is secure against incoherent attack. The advantage of this scheme is that using W state is more little than GHZ state in energy loss and no quantum bit carrying secret message is transmitted in quantum channel.

Keywords Quantum cryptography, Quantum secure direct communication, W state, Unitary transformation

1 引言

受美国人Wiesner[1]量子货币思想的启发,Bennett和Brassard于1984年提出了量子密码的概念,并提出了第一个量子密码协议——BB84协议[2]。作为密码学与量子力学相结合的产物,量子密码以量子力学为基础,利用量子特性——"海森堡测不准原理"、"量子相干性"和"量子不可克隆原理"来保证通信的安全性。BB84协议是一个量子密钥分配协议,它以量子态作为信息载体,利用量子力学原理,通过量子信道传输,在保密通信双方之间建立共享的经典密钥,简单地说就是利用量子通信实现经典的密钥分发。2000年,BB84协议的无条件安全性得到了证明[3]。在经典密码里,只有"一次一密"具有无条件安全性[4],但由于效率不高,无法应用于实际,而量子密码能提供无条件安全且高效的密码协议,因而受到了人们的广泛重视。BB84协议之后,人们提出了许多量子密钥分配协议[5-12]。

量子安全直接通信(Quantum secure direct communication,简称QSDC),是继量子密钥分配之后提出的又一重要量子密码方案。不同于量子密钥分配,QSDC要求通信双方不需要预先共享密钥就可以实现秘密消息的安全传递。目前提出的量子安全直接通信协议[13-26]按信息载体可以分为两类,一类是基于单光子系统的QSDC,另一类是基于纠缠系统的QSDC。2002年,BEIGE等人基于单光子提出了一个QSDC方案[13],每个光子传输一比特经典信息,解读一个量子比特的秘密消息需要额外传输一个经典比特。Deng等人给出了一个基于一次一密的QSDC协议[14],该方案使用单光子作为信息载体。王剑等人基于单光子序列的顺序重排提出了一种两方通信的QSDC协议[15]和一种多方控制的QSDC协议[16],协议的安全性由量子不可克隆原理和单光子序列的秘密传输顺序所保证。目前来说大多数QSDC协议都采用纠缠态作为信息载体。Boström等人用Einstein-Podolsky-Rosen(EPR)对作为信息载体给出了一个Ping-Pang量子安全直接通信方案[17],该方案可以在传输过程中解密秘密消息而不需要传输额外的经典信息。Deng等人借鉴Long-Liu 2002两步量子密钥分配方案[8]的思想,利用有序的EPR对提出了一个两步QSDC协议[18]。后来,Deng等人又利用有序的EPR对提出了两种网络通信的QSDC协议[19],第一种方案是一量子比特可以携带两比特经典信息,但是量子比特需要传输两次,增加了潜在的窃听者Eve获得量子比特的机会;第二种方案利用了纠缠转移技术,一量子比特携带一比特经典信息,但

到稿日期:2008-11-14 返修日期:2009-01-22 本文受国家自然科学基金(60403004),河南省杰出青年科学基金项目(0612000500)资助。
杨新元(1980—),男,硕士生,主要研究方向为信息安全和量子密码等,E-mail:yangstarstar@163.com;马 智(1973—),女,博士,副教授,主要研究方向为信息安全和量子密码等;吕 欣(1977—),男,博士,副研究员,主要研究方向为信息安全和量子密码等。

是量子比特只需传输一次，载有秘密消息的量子比特不用在量子信道中传输，使窃听者 Eve 无法获得载有秘密消息的量子比特。Hwayean 等人提出了两种带认证的 QSDC 协议[20]，第一种方案通信双方之间存在量子线路，第二种方案通信双方之间不存在量子线路，两种方案都采用 Greenberger-Horne-Zeilinger(GHZ)态作为信息载体，一量子比特可以携带一比特经典信息。吕欣等人利用量子 CSS 纠错码和未知量子态不可克隆等性质提出了一种 QSDC 方案[21]，该方案的安全性建立在求解一般的线性码的译码问题是一个 NP 完全问题，部分线性码存在快速的译码算法和量子图灵机不能有效求解 NP 完全问题基础之上，与已有的 QSDC 方案相比，该方案不需要交换任何额外的经典信息和建立量子纠缠信道。文献[22-25]都以 GHZ 态作为信息载体给出了 QSDC 方案，前 3 个方案利用了纠缠转移技术，实现了秘密消息的直接同时交换，这 4 个方案的优点在于不需要传输载有秘密消息的量子比特。

2000 年，一种新的纠缠态 W 态[27]被提出。GHZ 态和 W 态是两种不同的纠缠态，W 态在量子比特的损耗方面比 GHZ 态要小，因而受到了人们的重视。2006 年，CAO 等人基于四粒子 W 态提出了一种新的 QSDC 方案[26]，但是方案本身存在很多漏洞。

本文同样采用四粒子 W 态作为信息载体，利用幺正变换和 Bell 基测量提出了一种新的两方 QSDC 协议。注意到 CAO 方案的漏洞，我们的方案修补了这些漏洞。该方案的优点在于选用了相对于 GHZ 态而言损耗较小的 W 态作为信息载体，不需要在量子信道中传输带有秘密消息的量子比特，量子比特只需传输一次。在理想信道下，通过窃听检测保证了信道的安全，协议在非相干攻击下是安全的。

2 预备知识

$\{|0\rangle,|1\rangle\}$是一组标准正交基，称为 Z 基，记：

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

易知$\{|+\rangle,|-\rangle\}$也是一组标准正交基，我们称为 X 基。根据式(1)有：

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

4 个 EPR 对表示为：

$$|\beta_{xy}\rangle=\frac{1}{\sqrt{2}}(|0,y\rangle+(-1)^x|1,y\oplus 1\rangle) \tag{3}$$

式中，$x,y\in\{0,1\}$，$\oplus$表示域 F_2 上的模 2 加运算。根据式(3)，4 个 Bell 态可以写为：

$$\begin{aligned}&|\beta_{00}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),|\beta_{01}\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)\\&|\beta_{10}\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle),|\beta_{11}\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)\end{aligned} \tag{4}$$

4 个 Bell 态也构成了一组标准正交基。由式(3)可以得到：

$$|x,y\rangle=\frac{1}{\sqrt{2}}(|B_{0,x\oplus y}\rangle+(-1)^x|B_{1,x\oplus y}\rangle) \tag{5}$$

根据式(5)有：

$$\begin{aligned}&|00\rangle=\frac{1}{\sqrt{2}}(|\beta_{00}\rangle+|\beta_{10}\rangle),|01\rangle=\frac{1}{\sqrt{2}}(|\beta_{01}\rangle+|\beta_{11}\rangle)\\&|10\rangle=\frac{1}{\sqrt{2}}(|\beta_{01}\rangle-|\beta_{11}\rangle),|11\rangle=\frac{1}{\sqrt{2}}(|\beta_{00}\rangle+|\beta_{10}\rangle)\end{aligned} \tag{6}$$

4 个 Pauli 算子记为：

$$\begin{aligned}&\sigma_0=I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\\&\sigma_y=i\sigma_x\sigma_z=\begin{pmatrix}0&-i\\i&0\end{pmatrix}\end{aligned} \tag{7}$$

四个 Pauli 算子作用在 Z 基$|0\rangle$和$|1\rangle$上有：

$$\sigma_0|0\rangle=|0\rangle,\sigma_0|1\rangle=|1\rangle \tag{8}$$

$$\sigma_x|0\rangle=|1\rangle,\sigma_x|1\rangle=|0\rangle \tag{9}$$

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

$$\sigma_y|0\rangle=i|1\rangle,\sigma_y|1\rangle=-i|0\rangle \tag{11}$$

四粒子 W 态记为：

$$|W_4\rangle=\frac{1}{2}(|1000\rangle+|0100\rangle+|0010\rangle+|0001\rangle)_{1234} \tag{12}$$

利用式(2)把四粒子 W 态用 X 基表示，式(12)可以变形为：

$$\begin{aligned}|W_4\rangle=\frac{1}{4}[&|+\rangle_1|+\rangle_2(2|+\rangle|+\rangle+|+\rangle|-\rangle+|-\rangle|\\&+\rangle)_{34}-|-\rangle_1|-\rangle_2(2|-\rangle|-\rangle+|+\rangle|-\rangle+|\\&-\rangle|+\rangle)_{34}+|+\rangle_1|-\rangle_2(|+\rangle|+\rangle-|-\rangle|\\&-\rangle)_{34}+|-\rangle_1|+\rangle_2(|+\rangle|+\rangle-|-\rangle|-\rangle)_{34}]\end{aligned} \tag{13}$$

利用式(6)把四粒子 W 态用 Bell 基表示，式(12)又可以变形为：

$$\begin{aligned}|W_4\rangle=\frac{1}{2}[&|\beta_{01}\rangle_{12}\otimes(|\beta_{00}\rangle+|\beta_{10}\rangle)_{34}+(|\beta_{00}\rangle+|\beta_{10}\rangle)_{12}\\&\otimes|\beta_{01}\rangle_{34}]\end{aligned} \tag{14}$$

式中，$\otimes$表示张量积。用四个幺正变换 $\sigma_0\otimes\sigma_0\otimes\sigma_0\otimes\sigma_0$，$\sigma_0\otimes\sigma_z\otimes\sigma_0\otimes\sigma_0$，$\sigma_x\otimes\sigma_0\otimes\sigma_0\otimes\sigma_0$ 和 $\sigma_x\otimes\sigma_z\otimes\sigma_0\otimes\sigma_0$ 作用在四粒子 W 态上，利用式(8)、(9)、(10)和(14)得到：

$$(\sigma_0\otimes\sigma_0\otimes\sigma_0\otimes\sigma_0)|W_4\rangle=\frac{1}{2}[(|\beta_{00}\rangle+|\beta_{10}\rangle)_{12}\otimes|\beta_{01}\rangle_{34}+|\beta_{01}\rangle_{12}\otimes(|\beta_{00}\rangle+|\beta_{10}\rangle)_{34}] \tag{15}$$

$$(\sigma_0\otimes\sigma_z\otimes\sigma_0\otimes\sigma_0)|W_4\rangle=\frac{1}{2}[(|\beta_{00}\rangle+|\beta_{10}\rangle)_{12}\otimes|\beta_{01}\rangle_{34}-|\beta_{11}\rangle_{12}\otimes(|\beta_{00}\rangle+|\beta_{10}\rangle)_{34}] \tag{16}$$

$$(\sigma_x\otimes\sigma_0\otimes\sigma_0\otimes\sigma_0)|W_4\rangle=\frac{1}{2}[(|\beta_{01}\rangle-|\beta_{11}\rangle)_{12}\otimes|\beta_{01}\rangle_{34}+|\beta_{00}\rangle_{12}\otimes(|\beta_{00}\rangle+|\beta_{10}\rangle)_{34}] \tag{17}$$

$$(\sigma_x\otimes\sigma_z\otimes\sigma_0\otimes\sigma_0)|W_4\rangle=\frac{1}{2}[(|\beta_{01}\rangle-|\beta_{11}\rangle)_{12}\otimes|\beta_{01}\rangle_{34}+|\beta_{10}\rangle_{12}\otimes(|\beta_{00}\rangle+|\beta_{10}\rangle)_{34}] \tag{18}$$

3 协议描述

协议的目的是为了实现发送方 Alice 通过量子信道安全地传递秘密消息(0 或 1)序列给接收方 Bob。这里，不考虑通信方 Alice 和 Bob 的身份认证问题，Alice 和 Bob 的身份认证通过经典的身份认证和量子身份认证都可以实现。

3.1 准备阶段

由发送方 Alice 制备有序的 n 个四粒子 W 态，$n\geqslant 1$。Alice 将 3 和 4 粒子组成的序列 S_B 发给接收方 Bob，自己保存 1 和 2 粒子序列 S_A，这里

$$S_A=\{P_1(1)\otimes P_1(2),\cdots,P_n(1)\otimes P_n(2)\} \tag{19}$$

$$S_B=\{P_1(3)\otimes P_1(4),\cdots,P_n(3)\otimes P_n(4)\} \tag{20}$$

下标表示 n 个 W 态的序号。当 Bob 收到全部 S_B 序列后告知 Alice，这样发送方 Alice 和接收方 Bob 共享了四粒子 W 态，

建立了量子纠缠信道。

3.2 窃听检测阶段

Alice 确认 Bob 收到全部 S_B 序列后，从 S_A 序列中随机选定一个充分大的子集序列，并通过经典信道告知接收方 Bob 在 S_B 序列中相应的位置，选出的序列作为校验序列。Alice 随机选取 Z 基或 X 基测量序列 S_A 中的校验序列，测量完成后告知 Bob 她选取的基的信息，Bob 选取相应的基测量序列 S_B 中的校验序列，测量完成后 Bob 将测量结果通过经典信道告知 Alice，由 Alice 根据四粒子 W 态的纠缠特性，利用式(12)和式(13)来分析错误率，如果错误率高出预先给定的值，那么放弃此次通信，从第一步重新开始。否则，对剩下的四粒子 W 态进行量子纠缠提纯[28]和量子保密增强[29]，然后继续下一步。

3.3 编码阶段

经过窃听检测后剩下的四粒子 W 态称为编码序列。Alice 对秘密消息进行编码，若 Alice 想要发送消息比特 0(1)，则对编码序列的粒子 1 执行 σ_0(σ_1)变换，这里 $\sigma_1=\sigma_x$。然后再对编码序列的粒子 2 随机执行 I 或 σ_z 变换。编码方案可以表示为：

$$\begin{cases} 0\rightarrow\sigma_0=I \\ 1\rightarrow\sigma_1=\sigma_x \end{cases} \tag{21}$$

3.4 译码阶段

Alice 和 Bob 分别用 Bell 基测量各自的编码序列，然后 Alice 通过经典信道告知 Bob 她的测量结果，Bob 根据 Alice 的测量结果和自己的测量结果参照表 1 解读出 Alice 发送的秘密消息。Bob 也可以按照下列规则解读 Alice 发送的秘密消息比特：若 Alice 的测量结果是 $|\beta_{xy}\rangle$，Bob 的测量结果是 $|\beta_{x'y'}\rangle$，$x,y,x',y'\in\{0,1\}$，则 Alice 发送的秘密消息比特为 $y\oplus y'\oplus 1$，这里$\oplus$为域 F_2 上的模 2 加运算。

表 1

A \ B	$\|\beta_{01}\rangle$	$\|\beta_{00}\rangle$或$\|\beta_{10}\rangle$
0	$\sigma_0\otimes\sigma_0\otimes\sigma_0\otimes\sigma_0$	$\|\beta_{00}\rangle$或$\|\beta_{10}\rangle$	$\|\beta_{01}\rangle$
0	$\sigma_0\otimes\sigma_z\otimes\sigma_0\otimes\sigma_0$	$\|\beta_{00}\rangle$或$\|\beta_{10}\rangle$	$\|\beta_{11}\rangle$
1	$\sigma_x\otimes\sigma_0\otimes\sigma_0\otimes\sigma_0$	$\|\beta_{01}\rangle$或$\|\beta_{11}\rangle$	$\|\beta_{00}\rangle$
1	$\sigma_x\otimes\sigma_z\otimes\sigma_0\otimes\sigma_0$	$\|\beta_{01}\rangle$或$\|\beta_{11}\rangle$	$\|\beta_{10}\rangle$

注 1：通过经典信道公开的结果不能被篡改，比方说经典信道可以用电话或者无线电广播等方式。

注 2：3.3 节里对粒子 2 随机执行 I 或 σ_z 变换本身对于编码秘密消息没有任何关系，只是为了使 Alice 在译码阶段公开的 Bell 基测量结果在理论上出现$|\beta_{00}\rangle$，$|\beta_{10}\rangle$，$|\beta_{01}\rangle$或$|\beta_{11}\rangle$的概率相等，防止 Eve 从 Alice 公开的测量结果中获取任何信息。

4 协议分析

4.1 协议的正确性

协议的正确性是指，如果通信双方都遵循协议规则，在没有共享密钥的情况下，可以完成秘密消息的安全传递。在理想条件下，也就是说没有噪声和能量损失的情况下，如果窃听检测时的错误率大于 0，说明量子信道中存在敌手 Eve 的窃听，那么通信双方放弃此次通信，重新开始；如果错误率等于 0，说明量子信道中不存在敌手 Eve 的窃听，这时可以不必执行量子纠缠提纯和量子保密增强，直接进行后面的编码和译码，实现秘密消息的安全传递。在实际条件下，如果窃听检测时的错误率高出预先给定的值，说明存在敌手 Eve 的窃听，那么通信双方放弃此次通信，重新开始；如果错误率低于预先给定的值，因为噪声和能量损失的影响，这时错误率就不一定为 0，为了保证消息的正确传递，要求执行量子纠缠提纯和量子保密增强，保证四粒子 W 态的纠缠特性。

假设发送方 Alice 想要发送消息比特“1”，Alice 根据编码方案对粒子 1 执行 σ_1 变换，然后对粒子 2 随机执行 I 或 σ_z 变换，不妨设 Alice 选择 σ_z 对粒子 2 进行变换。Alice 和 Bob 分别用 Bell 基测量各自的粒子，根据式(18)，不妨设 Bob 的测量结果为 $|\beta_{00}\rangle$，Alice 的测量结果为 $|\beta_{10}\rangle$。Alice 通过经典信道将她的测量结果“10”告知 Bob，Bob 根据 Alice 的测量结果和自己的测量结果，按照译码规则解读出 Alice 发送的秘密消息比特为“1”。同理，可以得到 Alice 发送“0”给接收方 Bob 的情况。

以上分析了协议的正确性。

4.2 协议的安全性

首先分析 Eve 不采取任何措施只是被动窃听的情况下所能获得的信息量。通过窃听检测后，Alice 对秘密消息进行编码，假设 Alice 发送秘密消息比特“0”或“1”的概率为 1/2，也就是说对粒子 1 执行幺正变换 σ_0 或 σ_1 的概率是 1/2，然后对粒子 2 随机执行 σ_0 或 σ_z 变换，那么 Alice 对粒子 1 和粒子 2 执行幺正变换 $\sigma_0\otimes\sigma_0$，$\sigma_0\otimes\sigma_z$，$\sigma_1\otimes\sigma_0$ 或 $\sigma_1\otimes\sigma_z$ 的概率为 1/4，译码时，Alice 和 Bob 分别用 Bell 基测量各自的粒子，Bob 的测量结果出现 $|\beta_{01}\rangle$($|\beta_{00}\rangle$或$|\beta_{10}\rangle$)的概率为 1/2，Alice 的测量结果出现 $|\beta_{00}\rangle$，$|\beta_{10}\rangle$，$|\beta_{01}\rangle$或$|\beta_{11}\rangle$的概率都是 1/4，由于 Bob 的测量结果不公开，Eve 能利用的有效信息只有 Alice 通过经典信道公开的测量结果，因此 Eve 猜对 Bob 的测量结果按照译码规则解读出 Alice 发送的秘密消息比特的概率为 1/2。此时，Alice 与 Eve 的互信息 $I(A,E)$有：

$$\begin{aligned} I(A,E)&=H(A)-H(A|E)\\ &=1-\frac{1}{2}H\left(\frac{1}{2}\right)-\frac{1}{2}H\left(\frac{1}{2}\right)=0 \end{aligned} \tag{22}$$

式中，H 为 Shannon 熵，

$$H(p)=-p\log_2 p-(1-p)\log_2(1-p)。$$

同理有 Eve 与 Bob 的互信息 $I(E,B)=0$。

4.2.1 截取重发攻击

若攻击者 Eve 截取 3.1 节中 Alice 发送给 Bob 的 SB 序列，自己制备 n 个四粒子 W 态序列，按照 Alice 的做法，也将四粒子 W 态分成序列 S_A' 和 S_B'，然后将序列 S_B' 发给 Bob。假设 Eve 通过窃听检测，由于 Eve 截获了所有的 S_B 序列，在译码阶段，Eve 同样用 Bell 基测量 S_B 序列，根据 Alice 公开的测量结果，Eve 按照译码规则可以得到 Alice 发送的秘密消息，但是这种攻击在窃听检测阶段是可以发现的。

Bob 收到的序列 S_B' 与 Alice 保留的序列 S_A 不具有纠缠特性，在窃听检测阶段，Alice 和 Bob 随机选用 Z 基或 X 基测量校验序列，利用式(12)和式(13)分析四粒子 W 态的纠缠特性时，选用 Z 基时理论上错误率为 1/2，选用 X 基时理论上错误率为 11/32，因此总体上错误率为：

$$P_e=\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{11}{32}=\frac{27}{64}=0.421875$$

通过以上分析，经过窃听检测，就可以发现攻击者 Eve 的存在。

4.2.2 测量重发攻击

攻击者 Eve 截获并用 Bell 基测量 3.1 节中 Alice 发送给 Bob 的 S_B 序列后，根据测量结果选取相应的量子态发给 Bob。具体地，若 Eve 测得结果 $|\beta_{01}\rangle$，则发送量子态 $|\beta_{01}\rangle$ 给 Bob；若 Eve 测得结果 $|\beta_{00}\rangle$ 或 $|\beta_{10}\rangle$，则发送量子态 $|00\rangle$ 给 Bob。假设 Eve 通过了窃听检测，此时 Eve 根据测得的结果和 Alice 公开的测量结果，很容易按照译码规则解读出 Alice 发送的秘密消息，但是这种攻击在窃听检测阶段也是可以发现的。

当 Eve 以 1/2 概率测得结果 $|\beta_{01}\rangle$ 时，将量子态 $|\beta_{01}\rangle$ 发给 Bob，此时 Alice 保留的粒子坍塌到量子态 $|00\rangle$。Alice 和 Bob 组成的复合系统的量子态可以表示为：

$$\begin{aligned}|00\rangle_{12}\otimes|\beta_{01}\rangle_{3'4'}&=\frac{1}{\sqrt{2}}[(|\beta_{00}\rangle+|\beta_{10}\rangle)_{12}\otimes|\beta_{01}\rangle_{3'4'}]\\&=\frac{1}{\sqrt{2}}[|0001\rangle+|0010\rangle)_{123'4'}\\&=\frac{1}{2\sqrt{2}}[(|++\rangle+|+-\rangle+|-+\rangle+\\&\quad|--\rangle)_{12}\otimes(|++\rangle-|--\rangle)_{3'4'}]\end{aligned}\tag{23}$$

当 Eve 以 1/2 概率测得结果 $|\beta_{00}\rangle$ 或 $|\beta_{10}\rangle$ 时，将量子态 $|00\rangle$ 发给Bob，此时 Alice 保留的粒子坍塌到量子态 $|\beta_{01}\rangle$。Alice 和 Bob 组成的复合系统的量子态可以表示为：

$$\begin{aligned}|\beta_{01}\rangle_{12}\otimes|00\rangle_{3'4'}&=\frac{1}{\sqrt{2}}[|\beta_{01}\rangle_{12}\otimes(|\beta_{00}\rangle+|\beta_{10}\rangle)_{3'4'}]\\&=\frac{1}{\sqrt{2}}(|0100\rangle+|1000\rangle)_{123'4'}=\frac{1}{2\sqrt{2}}[(|\\&\quad++\rangle-|--\rangle)_{12}\otimes(|+-\rangle+|+\\&\quad-\rangle+|-+\rangle+|--\rangle)_{3'4'}]\end{aligned}\tag{24}$$

在窃听检测阶段，Alice 和 Bob 随机选取 Z 基或 X 基测量校验序列，利用式(12)、(13)、(23)和(24)分析错误率时，选用 Z 基测量时理论上错误率为 0，这时 Eve 引入的错误无法侦测，选取 X 基测量时理论上错误率为 1/4，因此随机选取 Z 基或 X 基时理论上错误率 $P_e=\frac{1}{2}\times\frac{1}{4}=\frac{1}{8}=0.125$，也可以发现 Eve 的存在。

4.2.3 纠缠重发攻击[30]

若窃听者 Eve 在量子信道中给发送的每一个粒子安放一个探测器，等 Alice 编码完成后，准备窃取 Alice 发送给 Bob 的秘密消息。不妨设探测器的初态为 $|0\rangle_e$，探测器与四粒子 W 态相互作用后，整个系统的量子态为 $\rho_{ABE}=U|W_4\rangle|00\rangle\langle00|\langle W_4|U^*$，这里 U 为 Eve 执行的幺正变换。Bob 收到的量子态为 $\rho_B=Tr_A(Tr_E(\rho_{ABE}))$，这里 Tr_A 是对 Alice 拥有的粒子所组成的系统求偏迹，Tr_E 是对 Eve 的探测器所组成的系统求偏迹。Eve 安放的探测器存储的量子态 $\rho_E=Tr_A(Tr_B(\rho_{ABE}))$。Eve 在安放探测器的同时，必然会扰动四粒子 W 态，也就是说幺正变换 $U\neq I$，对于单个粒子与探测器相互作用，根据 Schmidt 分解定理[31]有：

$$U(|0\rangle\otimes|0\rangle_e)=|0\rangle|a_{00}\rangle_e+|1\rangle|a_{01}\rangle_e\tag{25}$$

$$U(|1\rangle\otimes|0\rangle_e)=|0\rangle|a_{10}\rangle_e+|1\rangle|a_{11}\rangle_e\tag{26}$$

$$U(|+\rangle\otimes|0\rangle_e)=|+\rangle|b_{00}\rangle_e+|-\rangle|b_{01}\rangle_e\tag{27}$$

$$U(|-\rangle\otimes|0\rangle_e)=|+\rangle|b_{10}\rangle_e+|-\rangle|b_{11}\rangle_e\tag{28}$$

式中，$\langle a_{00}|a_{01}\rangle=0$，$\langle a_{10}|a_{11}\rangle=0$，$\langle b_{00}|b_{01}\rangle=0$，$\langle b_{10}|b_{11}\rangle=0$。Eve 执行的幺正变换 U 满足下列对称性条件：

(1)当下标 0 与 1 互换时 $|a_{ij}\rangle$ 或 $|b_{ij}\rangle$ 的各种内积保持不变，$i,j\in\{0,1\}$。

(2)当 a 与 b 互换时 $|a_{ij}\rangle$ 或 $|b_{ij}\rangle$ 的各种内积保持不变，$i,j\in\{0,1\}$。

由对称性条件(1)可得：

$$\begin{aligned}&\langle a_{00}|a_{00}\rangle=\langle a_{11}|a_{11}\rangle,\langle a_{01}|a_{01}\rangle=\langle a_{10}|a_{10}\rangle\\&\langle b_{00}|b_{00}\rangle=\langle b_{11}|b_{11}\rangle,\langle b_{01}|b_{01}\rangle=\langle b_{10}|b_{10}\rangle\end{aligned}\tag{29}$$

由对称性条件(2)可得：

$$\langle a_{00}|a_{00}\rangle=\langle b_{00}|b_{00}\rangle,\langle a_{01}|a_{01}\rangle=\langle b_{01}|b_{01}\rangle\tag{30}$$

根据式(29)、(30)记：

$$F=\langle a_{00}|a_{00}\rangle=\langle a_{11}|a_{11}\rangle=\langle b_{00}|b_{00}\rangle=\langle b_{11}|b_{11}\rangle\tag{31}$$

$$D=\langle a_{01}|a_{01}\rangle=\langle a_{10}|a_{10}\rangle=\langle b_{01}|b_{01}\rangle=\langle b_{10}|b_{10}\rangle\tag{32}$$

对式(25)两边取各自的内积可得：

$$F+D=1\tag{33}$$

令 $|a_{ii}\rangle=\sqrt{F}|\hat{a}_{ii}\rangle$，$|b_{ii}\rangle=\sqrt{F}|\hat{b}_{ii}\rangle$，$i\in\{0,1\}$，这里 $\langle\hat{a}_{ii}|\hat{a}_{ii}\rangle=1$，$\langle\hat{b}_{ii}|\hat{b}_{ii}\rangle=1$。令 $|a_{ij}\rangle=\sqrt{D}|\hat{a}ij\rangle$，$|b_{ij}\rangle=\sqrt{D}|\hat{b}ij\rangle$，$i,j\in\{0,1\}$ 且 $i\neq j$，这里 $\langle\hat{a}_{ij}|\hat{a}_{ij}\rangle=1$，$\langle\hat{b}_{ij}|\hat{b}_{ij}\rangle=1$。式(25)、(26)、(27)、(28)可表示为：

$$U(|0\rangle\otimes|0\rangle_e)=\sqrt{F}|0\rangle|\hat{a}_{00}\rangle_e+\sqrt{D}|1\rangle|\hat{a}_{01}\rangle_e\tag{34}$$

$$U(|1\rangle\otimes|0\rangle_e)=\sqrt{F}|1\rangle|\hat{a}_{11}\rangle_e+\sqrt{D}|0\rangle|\hat{a}_{10}\rangle_e\tag{35}$$

$$U(|+\rangle\otimes|0\rangle_e)=\sqrt{F}|+\rangle|\hat{b}_{00}\rangle_e+\sqrt{D}|-\rangle|\hat{b}_{01}\rangle_e\tag{36}$$

$$U(|-\rangle\otimes|0\rangle_e)=\sqrt{F}|-\rangle|\hat{b}_{11}\rangle_e+\sqrt{D}|+\rangle|\hat{b}_{10}\rangle_e\tag{37}$$

式中，F 是保真度，D 是误码率。这样在 Alice 分析四粒子 W 态的纠缠特性时，Eve 不可避免地会引起错误，在理想信道下，只要校验序列的长度足够长，通过窃听检测，Alice 就可以检测出 Eve 的存在。

结束语 通过以上分析，在理想信道下，协议在常见的非相干攻击下是安全的；在实际条件下，协议的安全性依赖于实际信道的噪声水平。本文利用有序的四粒子 W 态作为信息载体，利用幺正变换进行编码，通过当地 Bell 基测量和经典通信提出了一种新的两方量子安全直接通信方案。在理论上，除了校验用的 W 态，一个四粒子 W 态可以传输一比特经典信息。该方案的优点在于使用 W 态作为信息载体，较 GHZ 态而言，W 态损耗要小得多，且不需要传输载有秘密消息的量子比特。目前设计 QSDC 方案，可以利用量子稠密编码、量子纠缠转移和量子隐形传态等技术，下一步工作可以考虑结合这些技术实现多方通信的 QSDC。

参 考 文 献

[1] WiesnerS. Conjugatecoding[J]. ACMSIGACTNews, 1983, 15(1): 78-88

[2] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [A]// Proceedings of IEEE International Conference on Computers, Systems and Signal Processing[C]. Bangalore, India, 1984: 175-179

[3] Shor P W, Preskill J. Simple Proof of Security of the BB 8 4 Quantum Key Distribution Protocol[J]. Physical Review Letters, 2000, 85(2): 441-444

[4] 冯登国，裴定一. 密码学导引[M]. 北京：科学出版社，1998

[5] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121-3124

(下转第 76 页)

参 考 文 献

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C]// 1996 IEEE Symposium on Security and Privacy. Washington DC, USA, 1996: 164-173

[2] 徐锋，吕建. Web 安全中的信任管理研究与进展[J]. 软件学报，2002，13(11)：2057-2064

[3] 张志勇，黄涛. 信任管理中基于角色的委托授权研究进展[J]. 计算机应用研究，2008，25(6)：1601-1605，1610

[4] Barka E, Sandhu R S. Framework for role-based delegation models[C]// The 6th Annual Computer Security Application Conference. New Orleans, Louisiana, USA, 2000: 168-176

[5] Zhang X W, Oh S, Sandhu R. PBDM: A flexible delegation model in RBAC[C]// The 8th ACM Symposium on Access Control Models and Technologies. New York, USA, 2003: 149-157

[6] 张宏，贺也平，石志. 基于周期时间限制的自主访问控制委托模型[J]. 计算机学报，2006，29(8)：1427-1437

[7] 徐震，李斓，冯登国. 基于角色的受限委托模型[J]. 软件学报，2005，16(5)：970-978

[8] Li N H, Feigenbaum J, Grosof N B. A logic-based knowledge representation for authorization with delegation[C]// The 12th IEEE Computer Security Foundations Workshop. Mordano, Italy, 1999: 162-174

[9] Li N H, John C M, William H W. Design of a Role-based Trust-management Framework[C]// 2002 IEEE Symposium on Security and Privacy. Berkeley, California, USA, 2002: 114-130

[10] 廖俊国，洪帆，朱更明，等. 基于信任度的授权委托模型[J]. 计算机学报，2006，29(8)：1265-1270

[11] Sandhu R S, Zhang X W, Kumar R, et al. Client-side access control enforcement using trusted computing and PEI models[J]. Journal of High Speed Network, 2006(15): 229-245

[12] 高迎，程涛远，王珊. 对等网信任管理模型及安全凭证回收方法的研究[J]. 计算机学报，2006，29(8)：1282-1289

[13] Shane B, Amit D L, Kenneth G P. Trusted Computing: Providing Security for Peer-to-Peer Networks[C]// The 5th IEEE International Conference on Peer-to-Peer Computing. Konstanz, Germany, 2005: 117-124

(上接第 71 页)

[6] Ekert A. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661-663

[7] Bennett C H, Brassard G, Mermin N D. Quantum Cryptography without Bell's Theorem[J]. Physical Review Letters, 1992, 68(5): 557-559

[8] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution schemes[J]. Physical Review A, 2002, 65(3): 032302

[9] Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution[J]. Physical Review A, 2003, 68(4): 042315

[10] Deng F G, Long G L. Bidirectional quantum key distribution protocol with practical faint laser pulses[J]. Physical Review A, 2004, 70(1): 012311

[11] Yang Y G, Wen Q Y, Zhu F C. An efficient two-step quantum key distribution protocol with orthogonal product states[J]. Chinese Physics, 2007, 16(4): 910-914

[12] Yang Y G, Wen Q Y. An efficient quantum key distribution protocol with orthogonal product states[J]. Chinese Physics, 2007, 16(8): 2215-2218

[13] Beige A, Englert B G, Kurstsierer CH, et al. Secure Communication with a Publicly Known Key[J]. ACTA PHYSICA POLONICA A, 2002, 101(3): 357-368

[14] Deng F G, Long G L. Secure direct communication with a quantum one-time-pad[J]. Physical Review A, 2004, 69(5): 052319

[15] Wang J, Zhang Q, Tang C J. Quantum secure direct communication based on order rearrangement of single photons[J]. Physics Letters A, 2006, 358(4): 256-258

[16] 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

[17] Boström K, Felbinger T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18): 187902

[18] Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block [J]. Physical Review A, 2003, 68(4): 042317

[19] Deng F G, Li X H, Li C Y. Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs[J]. Physics Letters A, 2006, 359(5): 359-365

[20] Hwayean L, Jongin L, Hyungjin Y. Quantum direct communication with authentication[J]. Physical Review A, 2006, 73(4): 042305

[21] 吕欣，马智，冯登国. 基于量子 Calderbank-Shor-Steane 纠错码的量子安全直接通信[J]. Journal of Software, 2006, 17(3): 509-515

[22] Gao T, Yan F L, Wang Z X. A Simultaneous Quantum Secure Direct Communication Scheme between the Central Party and Other M parties[J]. Chinese Physics Letters, 2005, 22(10): 2473-2476

[23] Gao T, Yan F L, Wang Z X. Deterministic secure direct communication using GHZ states and swapping quantum entanglement [J]. Journal of Physics A: Mathematical and General, 2005, 38(25): 5761-5770

[24] Man Z X, Xia Y J, Nguyen B A. Quantum secure direct communication by using GHZ states and entanglement swapping[J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2006, 39(18): 3855-3863

[25] Wang H F, Zhang S. Quantum Secure Direct Communication by Using a GHZ State[J]. Journal of the Korean Physical Society, 2006, 49(2): 459-463

[26] Cao H J, Song H S. Quantum Secure Direct Communication with W State[J]. Chinese Physics Letters, 2006, 23(2): 290-292

[27] Dur W, Vidal G, Cirac J I. Three qubits can be entangled in two inequivalent ways[J]. Physical Review A, 2000, 62(6): 062314

[28] Bennett C H, Brassard G, Popescu S, et al. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels [J]. Physical Review Letters, 1996, 76(5): 722-725

[29] Deutsch D, Ekert A, Jozsa R, et al. Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels[J]. Physical Review Letters, 1996, 77(13): 2818-2821

[30] Cirac J I, Gisin N. Coherent eavesdropping strategies for the four state quantum cryptography protocol[J]. Physics Letters A, 1997, 229(1): 1-7

[31] Nielsen M A, Chuang I L. Quantum computation and quantum information[M]. Cambridge, England: Press of the University of Cambridge, 2000