第 36 卷 第 2 期 计 算 机 工 程 2010 年 1 月
Vol.36 No.2 Computer Engineering January 2010
·安全技术· 文章编号：1000—3428(2010)02—0170—03 文献标识码：A 中图分类号：TN918.1

基于部分纠缠态的量子安全直接通信协议

徐红云[1]，杨新元[2]，马 智[2]，吕 欣[3]
(1. 乌鲁木齐总医院，乌鲁木齐 830000；2. 信息工程大学应用数学系，郑州 450002；3. 国家信息中心，北京 100045)

摘 要：提出一种新的带认证的三方量子安全直接通信协议。该方案利用共享的三粒子部分纠缠态和 CNOT 门来编码和译码，两方可同时向第三方传递秘密消息，共享的部分纠缠态可重复使用。在理想信道下，协议对于非相干攻击是安全的。该方案通过认证可以验证客户端身份的合法性，部分纠缠态在实际中容易制备和保存，能够实现两方同时跟第三方直接通信。
关键词：密码学；量子密码学；量子安全直接通信；部分纠缠态

Quantum Secure Direct Communication Protocol Based on Partially Entangler State

XU Hong-yun[1], YANG Xin-yuan[2], MA Zhi[2], LV Xin[3]
(1. Urumchi General Hospital, Urumchi 830000; 2. Department of Applied Mathematics, Information Engineering University, Zhengzhou 450002; 3. State Information Center, Beijing 100045)

【Abstract】 This paper proposes a new three-party quantum secure direct communication protocol with authentication. The scheme uses three-particle partially entangled states and CNOT gate to encode and decode. Two users can simultaneously transmit secret message to the third party, and partially entangled states shared can be used repeatedly. In ideal channel, the protocol is secure against incoherent attack. The advantage of the scheme is that through authentication, one can confirm the client's legitimate identity, partially entangled states are easy to prepare and store in practice, and two users can simultaneously communicate with the third party.
【Key words】 cryptography; quantum cryptography; quantum secure direct communication; partially entangler state

1 概述

从 1984 年文献[1]提出第 1 个量子密码协议——BB84 量子密钥分配协议以来，量子密码、量子通信技术和量子计算取得了飞速发展，已形成了自身完整的理论体系，成为国际学术界关注的焦点之一。经典密码体制是以数学为基础的，其安全性是基于计算安全的，只有经典的一次一密[2]被证明是无条件安全的，但因为在密钥分发方面效率很低，无法应用于实际。量子密码作为一种新型的密码，是密码学与量子力学相结合的产物，具有 2 个基本特征：无条件安全性和对窃听的可检测性[3]。与经典密码的安全性基础不同，量子密码的安全性基于量子力学的基本原理。从安全性的角度出发，量子密码带来了新的思路。Shor 的大整数因子分解算法使现在互联网常用的 RSA 公钥密码体制受到了潜在的威胁，如果量子计算机研制成功，RSA 体制将在多项式时间内被攻破。人们看到了量子密码的潜在优势，越来越多的研究人员都加入了量子密码的研究行列。

在提出量子密钥分配之后，人们又提出了量子安全直接通信(Quantum Secure Direct Communication, QSDC)的概念。量子密钥分配是通信双方通过量子通信来实现经典的密钥分发[4]。通信双方共享经典的密钥后，再加密解密秘密消息来进行通信。不同于量子密钥分配，QSDC 不需要通信双方预先共享经典的密钥，通过量子通信就可以直接实现秘密消息的安全传递，并且不会向潜在的窃听者泄露任何信息。目前提出的量子安全直接通信协议按信息载体可以分为 2 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。

2006 年，文献[5]提出了 2 种带认证的量子安全直接通信协议，协议中验证了通信方的合法身份，2 种方案都基于 GHZ 态：一种利用了量子纠缠转移技术，通信方之间不需要量子线路；另一种方案通信方之间需要量子线路。2007 年，文献[6]提出了带量子加密的两方量子安全直接通信协议，通信方重复使用共享的部分纠缠态作为量子密钥来加密和解密传输光子上的秘密消息。部分纠缠态的优点是在实际应用方面，更容易制备和保存。受文献[5-6]的启发，本文提出了带认证的基于三粒子部分纠缠态的量子安全直接通信方案，通信方重复使用共享的部分纠缠态和 CNOT 门来加密和解密传输光子上的秘密消息。与文献[6]的方案相比，把通信方扩展到三方，并且验证了客户端身份的合法性。

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，称为 X 基。

基金项目：国家自然科学基金资助项目(60403004)；河南省杰出青年科学基金资助项目(0612000500)
作者简介：徐红云(1981－)，女，技师，主研方向：信息安全；杨新元，助理研究员、硕士；马 智，副教授、博士；吕 欣，副研究员、博士
收稿日期：2009-10-20 **E-mail**：xu_hongyun1981@163.com

协议中用到 2 个 Pauli 算子 I 和 σ_x，还有 Hadamard 变换 H，其中，

$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \sigma_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{2}$$

令 $|\psi\rangle_{ABT}=a|000\rangle_{ABT}+b|111\rangle_{ABT}$，其中，$a$, b 为复数且 $|a|^2+|b|^2=1$。有下列等式：

$$|\psi'\rangle_{ABT}=(\sigma_x\otimes\sigma_x\otimes\sigma_x)|\psi\rangle_{ABT}=b|000\rangle_{ABT}+a|111\rangle_{ABT} \tag{3}$$

CNOT 门的作用可以表示为

$$|x,y\rangle\to|x,x\oplus y\rangle$$

其中，$x,y\in\{0,1\}$；$|x\rangle$ 为控制比特；$|y\rangle$ 为目标比特；$\oplus$ 表示域 $\mathbb{F}_2$ 上的模 2 加运算。

3 协议描述

协议里通信方包括可信服务器 Trent、客户端 Alice 和 Bob，这里假设服务器 Trent 是安全的，协议实现的目的是 Trent 验证 Alice 和 Bob 的合法身份，然后 Alice 和 Bob 同时向服务器 Trent 发送秘密消息。

协议分为认证、窃听检测部分和直接通信部分。

3.1 认证、窃听检测部分

在通信之前，Trent 拥有安全的 hash 函数 $h:\mathbb{F}_2^m\to\mathbb{F}_2^n$，其中，$\mathbb{F}_2^m$ 为 2 元 m 维向量空间；$\mathbb{F}_2^n$ 为 2 元 n 维向量空间，且 $m>n$，这里 m 和 n 都是正整数。另外 Trent 还存储着 Alice 和 Bob 的秘密身份序列 ID_A 和 ID_B.，其中，$ID_A, ID_B\in\mathbb{F}_2^m$，这里 ID_A, ID_B 是保密的。Alice(Bob)也拥有 hash 函数 h 和自己的秘密身份序列 ID_A (ID_B)。

Alice 和 Bob 想要向 Trent 发送秘密消息，首先向服务器发出申请，Trent 收到申请后，制备 $2n$ 个三粒子部分纠缠态 $|\psi\rangle_{ABT}=a|000\rangle_{ABT}+b|111\rangle_{ABT}$，然后对三粒子部分纠缠态随机执行幺正变换 U_I 或 U_x，其中，$U_I=I\otimes I\otimes I$, $U_x=\sigma_x\otimes\sigma_x\otimes\sigma_x$。变换完成后，Trent 从制备的部分纠缠态中随机选取 n 个态作为校验态并记录下它们的位置，再计算 Alice 的认证密钥 K_A 和 Bob 的认证密钥 K_B，其中，K_A=h(ID_A); K_B=h(ID_B); $K_A, K_B\in\mathbb{F}_2^n$。Trent 根据 K_A (K_B)各比特分位的值 0 或 1 对校验态中的粒子 A(B)执行幺正变换 I 或 H。例如，若 K_A 的比特分位的值为 0(1)，则 Trent 对 A 粒子执行 I(H)变换。变换完成后，Trent 按照原先制备的部分纠缠态的顺序将所有 $2n$ 个 A 粒子和 B 粒子分别发给 Alice 和 Bob，自己保留 T 粒子。

Alice 和 Bob 收到所有 $2n$ 个 A 粒子和 B 粒子序列后，通知 Trent，Trent 再公布校验态的具体位置。Alice 和 Bob 分别计算自己的认证密钥 K_A 和 K_B，再根据 K_A 和 K_B 各比特分位的值对 n 个校验态中的 A 粒子和 B 粒子执行幺正变换 I 或 H，然后分别用 Z 基测量，并公开测量结果。Trent 也用 Z 基测量校验态中的 T 粒子，与 Alice 和 Bob 公开的测量结果进行比较，分析错误率。如果错误率比预期的小，在可接受的范围内，继续进行下一步；否则，终止通信，重新开始。

3.2 直接通信部分

Alice 和 Bob 根据所要发送的秘密消息的比特值 0 或 1 制备量子态 $|0\rangle$ 或 $|1\rangle$，称这些态为传输态，实际发送时是一个一个的粒子，称这些粒子为传输粒子。如果 Alice 和 Bob 的秘密消息的长度大于 n，可以分段发送，每段长为 n。传输粒子制备好后，Alice(Bob)用 CNOT 门作用 A_i(B_i)粒子和传输粒子 $M_{A,i}$($M_{B,i}$)，这里粒子 A_i(B_i)作为控制比特，传输粒子 $M_{A,i}$($M_{B,i}$)作为目标比特。然后在传输粒子中随机插入 n 个诱骗光子，诱骗光子随机从 $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ 中选，并且记录它们的位置和具体的态。Alice 和 Bob 将插入诱骗光子的 $2n$ 个粒子分别发给 Trent，Trent 收到 Alice 和 Bob 发送的所有粒子后，通知 Alice 和 Bob。然后 Alice 和 Bob 公开诱骗态具体的位置和相应的态，Trent 根据 Alice 和 Bob 公开的信息对诱骗光子进行测量，并与 Alice 和 Bob 公开的结果进行比较，分析错误率。如果 Alice(Bob)发过来的粒子的错误率比预期的小，Trent 用 CNOT 门作用 T_i 粒子和传输粒子 $M_{A,i}$($M_{B,i}$)，这里粒子 T_i 作为控制比特，传输粒子 $M_{A,i}$($M_{B,i}$)作为目标比特，然后用 Z 基进行测量，读出 Alice(Bob)的秘密消息；否则，丢掉传输粒子，要求 Alice(Bob)重新发送。

Trent 也可以用同样的方法向 Alice 和 Bob 发送秘密消息，同样地，任意两方都可以同时向第三方发送秘密消息。如果在量子信道中没有窃听，则共享的部分纠缠态作为加密密钥和解密密钥可重复使用。

注：公开的信息可以通过经典信道公布，但是公开的信息不能被篡改。比如经典信道可以用电话或者无线电广播等方式。

4 安全性分析

首先分析潜在的攻击者 Eve 不采取任何措施，只是被动窃听所能获得的信息量。通过认证、窃听检测后，Alice 和 Bob 根据秘密消息 0 或 1 制备相应的量子态 $|0\rangle$ 或 $|1\rangle$，这里假设 Alice 和 Bob 发送秘密消息比特 0 或 1 的概率都是 1/2，由于编码和译码过程不需要任何经典信息的辅助，因此 Eve 得不到任何有用的经典信息，那么 Eve 猜对 Alice 和 Bob 发送的秘密消息的概率只能是 1/2，于是，有 Alice 和 Eve 的互信息：

$$I(A,E)=H(A)-H(A|E)=1-\frac{1}{2}H\left(\frac{1}{2}\right)-\frac{1}{2}H\left(\frac{1}{2}\right)=0 \tag{4}$$

其中，H 为 Shannon 熵，$H(p)=-p\mathrm{lb}p-(1-p)\mathrm{lb}_2(1-p)$。同理有 Bob 与 Eve 的互信息 $I(B,E)=0$。

因为最优化非相干攻击是非相干攻击里最强的一种攻击方式，所以这里仅对最优化非相干攻击的情况进行分析。假设 Eve 在量子信道中给发送的每一个粒子都安放一个探测器，等 Alice 和 Bob 发送传输粒子后，再通过探测器来窃取 Alice 和 Bob 发送的秘密消息。不妨设探测器的初态为 $|0\rangle_e$，探测器与部分纠缠态相互作用后，Alice, Bob, Trent 和 Eve 组成的整个系统的密度算子为 $\rho_{ABTE}=U|\psi\rangle|00\rangle\langle00|\langle\psi|U^\dagger$，其中，$U$ 为 Eve 执行的幺正变换。Eve 在安放探测器的同时，必然会扰动部分纠缠态，也就是说幺正变换 $U\neq I$，I 是单位变换。对于单个粒子与探测器相互作用，根据 Schmidt 分解定理[7]有

$$U(|0\rangle\otimes|0\rangle_e)=|0\rangle|a_{00}\rangle_e+|1\rangle|a_{01}\rangle_e \tag{5}$$

$$U(|1\rangle\otimes|0\rangle_e)=|0\rangle|a_{10}\rangle_e+|1\rangle|a_{11}\rangle_e \tag{6}$$

$$U(|+\rangle\otimes|0\rangle_e)=|+\rangle|b_{00}\rangle_e+|-\rangle|b_{01}\rangle_e \tag{7}$$

$$U(|-\rangle\otimes|0\rangle_e)=|+\rangle|b_{10}\rangle_e+|-\rangle|b_{11}\rangle_e \tag{8}$$

其中，$\langle a_{00}|a_{01}\rangle=0$；$\langle a_{10}|a_{11}\rangle=0$；$\langle b_{00}|b_{01}\rangle=0$；$\langle b_{10}|b_{11}\rangle=0$。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：

$$\langle a_{00}|a_{00}\rangle = \langle a_{11}|a_{11}\rangle$$
$$\langle a_{01}|a_{01}\rangle = \langle a_{10}|a_{10}\rangle$$
$$\langle b_{00}|b_{00}\rangle = \langle b_{11}|b_{11}\rangle$$
$$\langle b_{01}|b_{01}\rangle = \langle b_{10}|b_{10}\rangle \quad (9)$$

由对称性条件(2)可得：

$$\langle a_{00}|a_{00}\rangle = \langle b_{00}|b_{00}\rangle,\ \langle a_{01}|a_{01}\rangle = \langle b_{01}|b_{01}\rangle \quad (10)$$

根据式(9)、式(10)可得：

$$F = \langle a_{00}|a_{00}\rangle = \langle a_{11}|a_{11}\rangle = \langle b_{00}|b_{00}\rangle = \langle b_{11}|b_{11}\rangle > 0 \quad (11)$$

$$D = \langle a_{01}|a_{01}\rangle = \langle a_{10}|a_{10}\rangle = \langle b_{01}|b_{01}\rangle = \langle b_{10}|b_{10}\rangle > 0 \quad (12)$$

对(5)式 2 边取各自的内积可得：

$$F+D=1 \quad (13)$$

令 $|a_{ii}\rangle = \sqrt{F}|\hat{a}_{ii}\rangle$，$|b_{ii}\rangle = \sqrt{F}|\hat{b}_{ii}\rangle$，$i \in \{0,1\}$，其中，$\langle \hat{a}_{ii}|\hat{a}_{ii}\rangle = 1$；$\langle \hat{b}_{ii}|\hat{b}_{ii}\rangle = 1$。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 $i \neq j$，其中，$\langle \hat{a}_{ij}|\hat{a}_{ij}\rangle = 1$；$\langle \hat{b}_{ij}|\hat{b}_{ij}\rangle = 1$。

式(5)~式(8)可表示为

$$U\left(|0\rangle \otimes |0\rangle_e\right) = \sqrt{F}|0\rangle|\hat{a}_{00}\rangle_e + \sqrt{D}|1\rangle|\hat{a}_{01}\rangle_e \quad (14)$$

$$U\left(|1\rangle \otimes |0\rangle_e\right) = \sqrt{F}|1\rangle|\hat{a}_{11}\rangle_e + \sqrt{D}|0\rangle|\hat{a}_{10}\rangle_e \quad (15)$$

$$U\left(|+\rangle \otimes |0\rangle_e\right) = \sqrt{F}|+\rangle|\hat{b}_{00}\rangle_e + \sqrt{D}|-\rangle|\hat{b}_{01}\rangle_e \quad (16)$$

$$U\left(|-\rangle \otimes |0\rangle_e\right) = \sqrt{F}|-\rangle|\hat{b}_{11}\rangle_e + \sqrt{D}|+\rangle|\hat{b}_{10}\rangle_e \quad (17)$$

其中，F 是保真度；D 是误码率。假设 Trent 根据 K_A 和 K_B 的值对手中的量子态进行变换，变换后量子态仍是 $|\psi\rangle_{ABT} = a|000\rangle_{ABT} + b|111\rangle_{ABT}$，即 Trent 对部分纠缠态 $|\psi\rangle_{ABT}$ 执行幺正变换 U_I，同时 K_A 和 K_B 比特分位的值都为 0 的情况。按照协议 Trent 把 A 粒子和 B 粒子发给 Alice 和 Bob，然后 Eve 在量子信道中给发送的每一个粒子都安放一个探测器，Alice, Bob, Trent 和 Eve 组成的整个系统的量子态 $|\Psi\rangle_{ABTE}$ 用 Z 基表示为

$$\begin{aligned}|\Psi\rangle_{ABTE} = a\Big(&F|000\rangle_{ABT}|\hat{a}_{00}\rangle_{e_A}|\hat{a}_{00}\rangle_{e_B} + \sqrt{FD}|010\rangle_{ABT}|\hat{a}_{00}\rangle_{e_A}|\hat{a}_{01}\rangle_{e_B} + \\ &\sqrt{FD}|100\rangle_{ABT}|\hat{a}_{01}\rangle_{e_A}|\hat{a}_{00}\rangle_{e_B} + D|110\rangle_{ABT}|\hat{a}_{01}\rangle_{e_A}|\hat{a}_{01}\rangle_{e_B}\Big) + \\ b\Big(&F|111\rangle_{ABT}|\hat{a}_{11}\rangle_{e_A}|\hat{a}_{11}\rangle_{e_B} + \sqrt{FD}|101\rangle_{ABT}|\hat{a}_{11}\rangle_{e_A}|\hat{a}_{10}\rangle_{e_B} + \\ &\sqrt{FD}|011\rangle_{ABT}|\hat{a}_{10}\rangle_{e_A}|\hat{a}_{11}\rangle_{e_B} + D|001\rangle_{ABT}|\hat{a}_{10}\rangle_{e_A}|\hat{a}_{10}\rangle_{e_B}\Big)\end{aligned} \quad (18)$$

因此，Trent, Alice 和 Bob 用 Z 基测量校验态时，错误率为 D^2+2FD。同理可知，当 Trent 对部分纠缠态随机执行幺正变换 U_I 或 U_x，再根据 K_A 和 K_B 的值将手中的量子态变换成其他态时，错误率也为 D^2+2FD。通过以上分析，在认证、窃听检测阶段分析错误率时，理论上错误率为 $D^2+2FD>0$，那么在理想信道下，可以发现 Eve 的存在。

在直接通信部分，Alice, Bob 和 Trent 共享的部分纠缠态是 $|\psi\rangle_{ABT} = a|000\rangle_{ABT} + b|111\rangle_{ABT}$ 的概率为 1/2，$|\psi'\rangle_{ABT} = b|000\rangle_{ABT} + a|111\rangle_{ABT}$ 的概率也为 1/2。不妨设 Alice (Bob)要发送秘密消息 0，那么 Alice(Bob)制备量子态 $|0\rangle$，经过 CNOT 门作用后，Alice(Bob)制备的量子态会以 1/2 的概率变换为 $|a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|$，$|b|^2|0\rangle\langle 0| + |a|^2|1\rangle\langle 1|$，因此，用 Z 基测量时，会以 1/2 的概率得到 $|0\rangle$，$|1\rangle$。同理，Alice(Bob)发送秘密消息 1 的情况也是类似的。因此，Eve 得不到关于秘密消息的任何信息。另外由于在传输粒子中随机插入诱骗态的缘故，其安全性由量子不可克隆原理和量子测不准原理保证，本质上其安全性等价于 BB84 协议的安全性，因此 Eve 的窃听也会被发现。

5 结束语

通过安全性分析，在理想信道下，协议对于非相干攻击是安全的。在实际条件下，协议的安全性依赖于实际信道的噪声水平。若在量子信道中没有窃听，则部分纠缠态作为加密和解密密钥可重复使用。协议的优点在于通过认证，验证了客户端身份的合法性，部分纠缠态在实际中容易制备和保存，能够实现两方同时跟第三方直接通信。在理论上，如果能制备 N 粒子(N>3)的部分纠缠态，同样的方法，能够实现 N-1 方同时跟第 N 方直接通信。

参考文献

[1] Bennett C H, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing[C]//Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India: [s. n.], 1984: 175-179.

[2] 冯登国, 裴定一. 密码学导引[M]. 北京: 科学出版社, 1998.

[3] 曾贵华. 量子密码学[M]. 北京: 科学出版社, 2006.

[4] 王淑梅, 马鸿洋. 量子网络中多用户量子密钥共享协议[J]. 计算机工程, 2007, 33(10):155-157.

[5] Lee Hwayean, Lim Jongin, Yang HyungJin. Quantum Direct Communication with Authentication[J]. Physical Review A, 2006, 73(1).

[6] Li Xihan, Li Chunyan, Deng Fuguo, et al. Quantum Secure Direct Communication with Quantum Encryption Based on Pure Entangled States[J]. Chinese Physics, 2007, 16(8): 2149-2153.

[7] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information[M]. Cambridge, England, UK: Press of the University of Cambridge, 2000.

编辑　索书志

(上接第 169 页)

[7] 陈思宝. 基于 t-混合模型和扩展保局投影的聚类与降维方法研究[D]. 合肥: 安徽大学, 2005.

[8] Lee C H, Chen L H. Fast Closest Codeword Search Algorithm for Vector Quantization[J]. IEE Processings of Vision, Image and Signal Processing, 1994, 141(3): 143-148.

[9] 向德生, 熊岳山, 朱更明. 基于视觉特性的灰度水印自适应嵌入和提取算法[J]. 中国图象图形学报, 2006, 11(7): 1026-1025.

[10] 孙宏伟, 顾　明, 孙家广. 改进的基于主分量分析的码书设计算法[J]. 计算机辅助设计与图形学学报, 2005, 17(10): 2245-2250.

[11] Wu Sien-Chu, Chang Chin-Chen. A Novel Digital Image Watermarking Scheme Based on the Vector Quantization Technique[J]. Computers & Security, 2005, 24(6): 460-471.

编辑　金胡考