文章编号:1004-4213(2010)11-2083-5

利用 *N* 粒子纠缠态的量子秘密共享*

邓晓冉[1],杨帅[2],闫凤利[3]

(1 天津工程师范学院 理学院,天津 300222)

(2 天津理工大学 理学院,天津 300191)

(3 河北师范大学 物理科学与信息工程学院,石家庄 050016)

摘 要:为了高效实现多方之间的量子秘密共享,引入了一种纠缠度较高的 N 粒子纠缠态,并提出了利用该 N 粒子纠缠态在一方与($N-1$)方之间形成共享秘密位串的方案.该方案在建立秘密位串的过程中,Alice 对发送的粒子随机选择么正操作 I 和 σ_x,并选择一部分粒子用于检测信道的安全;之后 Alice 根据($N-1$)方选择的操作又选择了一部分粒子用于对参与者诚实度检测及信道安全检测.通过多次对窃听者的检测,很好地保证了信道的安全性及产生的秘密位串的可用性.最终在 Alice 及另外($N-1$)方之间可形成 $n[1-(N-1)/2^{N-1}]/6$ 个共享秘密位.

关键词:量子秘密共享;纠缠态;量子位;信道

中图分类号:O41 **文献标识码**:A **doi**:10.3788/gzxb20103911.2083

0 引言

量子通信是近年来迅速发展起来的研究领域,它以量子态作为信息载体和通信信道进行通信.量子通信为信息科学的发展提供了新的方法,它具有容量大、速度快、保密性强等优点,对信息的处理比经典方法具有更快的速度和更高的效率[1].

量子安全通信是将保密通信建立在量子物理客观规律基础上的交叉学科,是一个具有重要意义的研究课题.随着对数学难题求解的经典算法和量子算法的深入研究,基于数学上计算复杂性的经典安全通信面临着严峻的挑战.随着经典计算机技术的飞速发展和量子计算机的实验进展,破译数学密码的难度逐渐降低.一些数学密码体制受到很大威胁,如 R. Rivest、A. Shamir 和 L. Adleman 提出的 RSA 公钥密码体制以及 ElGamal 公钥密码体制,可以在多项式时间内被量子计算机破解.量子力学中不可克隆定理、测不准原理和纠缠特性可以保证量子密钥分发的无条件安全性和对窃听的可检测性,使得量子安全通信具有良好的性能和前景.

量子密钥分配是量子安全通信的核心.1984 年 Bennett 和 Brassard 利用四个沿不同偏振方向的单光子态提出第一个量子密钥分配方案[2].1992 年,Bennett 又提出一种更简单的方案.以上两种方案均使用的是单光子态.1991 年,Ekert 提出了一种基于两粒子最大纠缠态的量子密钥分配方案.随着对密钥分配研究的深入和实际需要,人们开始关注多方之间的量子秘密共享.在已提出的量子密钥分配方案[3-13]中,一方与多方之间的量子秘密共享大多利用了多光子纠缠态,如 Greenberger-Horne-Zeilinger(GHZ)态、W 态等,但它们的纠缠度较低.本文通过引入一种纠缠度较高且制备过程简单的 N 粒子纠缠态,提出了一种利用该 N 粒子纠缠态[7]在 Alice 和另外($N-1$)个经典方之间形成共享的秘密位串的方案,该方案的效率会随着 N 粒子态数 n 和粒子数 N 的增加而提高.

1 新引入的 *N* 粒子纠缠态

为了说明 N 粒子纠缠态的制备过程,以四粒子纠缠态和五粒子纠缠态的制备为例.

1.1 四粒子纠缠态

四粒子纠缠态的形式为

$$|\Psi\rangle=\frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|0101\rangle+|0110\rangle+|1001\rangle+|1010\rangle+|1100\rangle+|1111\rangle)$$

此态具有一个重要的特性:对任意一个量子位实施局域测量,则其余三个量子位将被转换成一个纠缠度较 GHZ 态高的三粒子纠缠态.即此态可被写成

$$|\Psi\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle\frac{|000\rangle+|011\rangle+|101\rangle+|110\rangle}{2}+|1\rangle\frac{|001\rangle+|010\rangle+|100\rangle+|111\rangle}{2}\right) \tag{1}$$

而且此态的纠缠度较一般的四粒子纠缠态要高,即至少需实施三次局域操作才能完全消纠缠.

* 天津工程师范学院校级科研项目(KJ0817)资助

† Tel:13920355717 Email:yangshuai@tjut.edu.cn

收稿日期:2010-05-17 修回日期:2010-06-13

为了获得$|\Psi\rangle$，需要事先准备两个$|0\rangle$态和一个Bell态$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$，并对第一、第二个量子位实施Hadamard门；然后分别以第一、第二个量子位为控制位，第三、第四个量子位为靶位实施控制-非门操作. 步骤如图1.

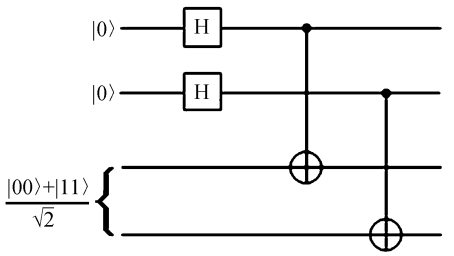


图1 四粒子纠缠态的制备

Fig. 1 Quantum circuit for generating four-particle entangled state

电路的输入态为

$$|\Psi_0\rangle=|0\rangle\otimes|0\rangle\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}},$$

使第一、第二个量子位通过Hadamard门后，可以得到

$$|\Psi_1\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}},$$

然后让一、三量子位和二、四量子位分别通过控制-非门，从而得到

$$|\Psi_2\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle\frac{|000\rangle+|011\rangle+|101\rangle+|110\rangle}{2}+|1\rangle\frac{|001\rangle+|010\rangle+|100\rangle+|111\rangle}{2}\right)=|\Psi\rangle \quad (2)$$

1.2 五粒子纠缠态

五粒子纠缠态的形式为

$$|\Psi\rangle=\frac{1}{4}(|00000\rangle+|00011\rangle+|00101\rangle+|00110\rangle+|01001\rangle+|01010\rangle+|01100\rangle+|01111\rangle+|11000\rangle+|10100\rangle+|10010\rangle+|10001\rangle+|11110\rangle+|11011\rangle+|11101\rangle+|10111\rangle) \quad (3)$$

此态具有一个重要的特性：对任意一个量子位实施局域测量，则其余四个量子位将被转换成一个纠缠度较高的四粒子纠缠态. 即此态可被写成

$$|\Psi\rangle=\frac{1}{\sqrt{2}}\left[|0\rangle\left(\frac{|0000\rangle+|0011\rangle+|0101\rangle+|0110\rangle}{2\sqrt{2}}+\frac{|1001\rangle+|1010\rangle+|1100\rangle+|1111\rangle}{2\sqrt{2}}\right)\right]+\frac{1}{\sqrt{2}}\left[|1\rangle\left(\frac{|1000\rangle+|0100\rangle+|0010\rangle+|0001\rangle}{2\sqrt{2}}+\frac{|1110\rangle+|1011\rangle+|1101\rangle+|0111\rangle}{2\sqrt{2}}\right)\right] \quad (4)$$

而且此态的纠缠度较一般的五粒子纠缠态要高，即至少需实施四次局域操作才能完全消纠缠.

为了获得$|\Psi\rangle$，需要事先准备三个$|0\rangle$态和一个Bell态$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$，并对第一、第二、第三个量子位实施Hadamard门；然后分别以第二、第三个量子位为控制位，第四、第五个量子位为靶位实施控制-非门操作，最后再以第一个量子位为控制位、第二个量子位为靶位实施控制-非门操作. 具体步骤如图2.

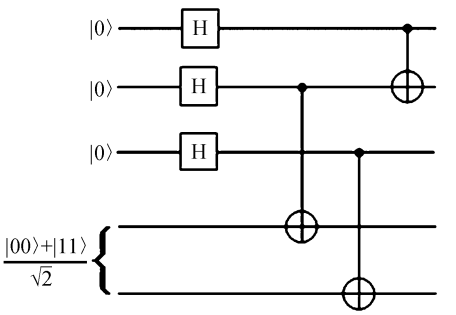


图2 五粒子纠缠态的制备

Fig. 2 Quantum circuit for generating five-particle entangled state

电路的输入态为

$$|\Psi_0\rangle=|0\rangle\otimes|0\rangle\otimes|0\rangle\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}} \quad (5)$$

使第一、第二、第三个量子位通过Hadamard门后，可以得到

$$|\Psi_1\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}} \quad (6)$$

然后让二、四量子位和三、五量子位分别通过控制-非门，从而得到

$$|\Psi_2\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\left(\frac{|0000\rangle+|0011\rangle+|0101\rangle+|0110\rangle}{2\sqrt{2}}+\frac{|1001\rangle+|1010\rangle+|1100\rangle+|1111\rangle}{2\sqrt{2}}\right) \quad (7)$$

最后以第一个量子位为控制位，第二个量子位为靶位实施控制-非门操作，即可获得

$$|\Psi_3\rangle=\frac{1}{\sqrt{2}}\left[|0\rangle\left(\frac{|0000\rangle+|0011\rangle+|0101\rangle+|0110\rangle}{2\sqrt{2}}+\frac{|1001\rangle+|1010\rangle+|1100\rangle+|1111\rangle}{2\sqrt{2}}\right)\right]+\frac{1}{\sqrt{2}}\left[|1\rangle\left(\frac{|1000\rangle+|0100\rangle+|0010\rangle+|0001\rangle}{2\sqrt{2}}+\frac{|1110\rangle+|1011\rangle+|1101\rangle+|0111\rangle}{2\sqrt{2}}\right)\right]=|\Psi\rangle \quad (8)$$

1.3 N粒子纠缠态

将四粒子、五粒子纠缠态的制备过程推广，为了获得N粒子纠缠态，需要准备$(N-2)$个$|0\rangle$态和一

个 Bell 态 $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$，并对第一至第($N-2$)个量子位实施 Hadamard 门；然后分别以第($N-3$)、第($N-2$)个量子位为控制位，第($N-1$)、第 N 个量子位为靶位实施控制-非门操作；最后分别以第($N-4$)、第($N-5$)、…、第 1 个量子位为控制位，第($N-3$)、第($N-4$)、…、第 2 个量子位为靶位逐个依次实施控制-非门操作，即可获得纠缠度较高的 N 粒子纠缠态.

2　量子秘密共享协议

1) Alice 制备 n 个 N 粒子纠缠态 $|\Psi\rangle_i$($i=1,2,\cdots,n$)，然后 Alice 分别对每个纠缠态的 2、3、…、N 粒子随机的实施么正操作 $I=|0\rangle\langle 0|+|1\rangle\langle 1|$ 或 $\sigma_x=|1\rangle\langle 0|+|0\rangle\langle 1|$，之后再将其分别发送给 Bob1、Bob2、…、Bob($N-1$)，剩下的第一个粒子留给自己.

2) 接到 Alice 发送过来的所有量子位后，Bob1、Bob2、…、Bob($N-1$)通过公共信道告知 Alice. 然后 Alice 将只有某一个量子位实施操作为 σ_x，其余均实施的是 I 操作的量子位通过公共信道告知 Bob1、Bob2、…、Bob($N-1$)，并要求他们直接将这些对应量子位返还给她. Alice 收到这些粒子后对他们进行联合 N 粒子测量，若出错率较高，则协议取消，重新开始；若出错率低，则协议继续.

3) 对剩下的量子位，Bob1、Bob2、…、Bob($N-1$)随机选择以下两种方式：①采用经典$\{|0\rangle,|1\rangle\}$基测量收到的量子位；②把量子位以新的顺序直接返还给 Alice.

4) Alice 收到 Bob1、Bob2、…、Bob($N-1$)返回的序列后，通过公共信道告知 Bob1、Bob2、…、Bob($N-1$).

5) Bob1、Bob2、…、Bob($N-1$)分别公布没有测量而直接返回的量子位以及这些量子位的顺序.

6) 根据 Bob1、Bob2、…、Bob($N-1$)对各自量子位执行的操作，Alice 对自己的相应量子位执行以下三个操作之一：

① 假如 Bob1、Bob2、…、Bob($N-1$)都选择用$\{|0\rangle,|1\rangle\}$基测量，则 Alice 也使用$\{|0\rangle,|1\rangle\}$基测量，若起初 Alice 分别发送给 Bob1、Bob2、…、Bob($N-1$)的($N-1$)个粒子实施的么正操作中有偶数个 σ_x，则直接将 Alice 获得的测量结果作为共享位；若起初 Alice 分别发送给 Bob1、Bob2、…、Bob($N-1$)的($N-1$)个粒子实施的么正操作中有奇数个 σ_x，则要获得共享位 Alice 需对她的测量结果实施 σ_x 操作. 仅当 Bob1、Bob2、…、Bob($N-1$)合作，将各自测得的结果进行二进制加法运算(模二加)，即可获得对应的共享位.

② 假如 Bob1、Bob2、…、Bob($N-1$)中有一部分人(如 Bob1、Bob2)选择的是用$\{|0\rangle,|1\rangle\}$基测量，而其余的人选择的是直接将粒子返还给 Alice，则 Alice 对她自己的粒子和 Bob3、…、Bob($N-1$)返回的粒子执行联合测量，之后要求 Bob1、Bob2 公布其测量结果，可用于检测 Bob1、Bob2 的测量结果正确与否.

③ 假如 Bob1、Bob2、…、Bob($N-1$)都选择将粒子直接返还给 Alice，则 Alice 对她自己的粒子和被 Bob1、Bob2、…、Bob($N-1$)返回的粒子执行联合 N 粒子测量，可用于检测 N 粒子纠缠态是否被改变.

这三种情况出现的概率是相同的.

7) Alice 通过第②、③种情况来检测错误率，假如在任何一种情况中错误率较高且超过预定值，则协议将被废除.

8) 通过步骤 1)～7)在 Alice、Bob1、Bob2、…、Bob($N-1$)之间可产生大约 $\frac{1}{3}n(1-\frac{N-1}{2^{N-1}})$ 个共享秘密位. 为了进一步保证协议的安全性，Alice 要求在产生共享秘密位的序列中随机取出一个子序列(长度约为共享秘密位串的一半，即 $\frac{1}{6}n(1-\frac{N-1}{2^{N-1}})$)，并公布各自的测量结果. 假如 Bob1、Bob2、…、Bob($N-1$)对应位的值有偶数或奇数个 1，则可知，Alice 手中的对应位应是 0 或 1. 如果这次检测的错误率不高，则 Alice 的剩下的 $\frac{1}{6}n(1-\frac{N-1}{2^{N-1}})$ 个共享位就构成了最后的秘密位串，仅当 Bob1、Bob2、…、Bob($N-1$)合作才可获得秘密位.

3　安全性分析

该方案在形成秘密位串过程中以及产生秘密位串之后，多次进行了对窃听者的检测，所以该方案有较高的安全性.

3.1　截获-发送攻击

在 Bob1、Bob2、…、Bob($N-1$)中有一方是不诚实的，企图不与其他方合作而独自获取秘密信息.

假定不诚实的一方是 Bob1(或其他任何一方). 当 Alice 将实施了么正操作的 N 粒子纠缠态中的($N-1$)个粒子分别发送给 Bob1、Bob2、…、Bob($N-1$)时，Bob1(或其他任何一方)在中途将发送给其他各方的粒子截获，然后对这($N-1$)个粒子执行联合测量，再将截获的粒子分别发送给其他各方. 然而

Bob1(或其他任何一方)的这种窃听行为将在第二步信道安全性检测时被发现,所以 Bob1(或其他任何一方)的这种窃听行为几乎不能成功获取秘密信息.

3.2 存在第(N+1)方 Eve 的攻击

窃听者 Eve 同时截获了 Alice 发送给 Bob1、Bob2、…、Bob($N-1$)的量子位,并对此($N-1$)个量子位执行联合测量,然后再将处于测出态的($N-1$)个粒子分别发送给 Bob1、Bob2、…、Bob($N-1$).

以四粒子纠缠态为例:

根据式(1),假如 Alice 实施的么正操作为 III,则四粒子纠缠态保持不变,即 $|\Psi'\rangle_{1234}=|\Psi\rangle_{1234}$;假如 Alice 实施的么正操作为 $\mathrm{II}\sigma_x$ 或 $\mathrm{I}\sigma_x\mathrm{I}$ 或 $\sigma_x\mathrm{II}$,则四粒子纠缠态转化为

$$|\Psi''\rangle_{1234}=\frac{1}{\sqrt{2}}\left[|0\rangle_1\frac{(|001\rangle+|010\rangle+|100\rangle+|111\rangle)_{234}}{2}+|1\rangle_1\frac{(|000\rangle+|011\rangle+|101\rangle+|110\rangle)_{234}}{2}\right] \quad (9)$$

假如 Alice 实施的么正操作为 $\mathrm{I}\sigma_x\sigma_x$ 或 $\sigma_x\mathrm{I}\sigma_x$ 或 $\sigma_x\sigma_x\mathrm{I}$,则四粒子纠缠态保持不变,即

$$|\Psi''\rangle_{1234}=|\Psi\rangle_{1234}$$

假如 Alice 实施的么正操作为 $\sigma_x\sigma_x\sigma_x$,则四粒子纠缠态转化为

$$|\Psi'''\rangle_{1234}=\frac{1}{\sqrt{2}}\left[|0\rangle_1\frac{(|001\rangle+|010\rangle+|100\rangle+|111\rangle)_{234}}{2}+|1\rangle_1\frac{(|000\rangle+|011\rangle+|101\rangle+|110\rangle)_{234}}{2}\right] \quad (10)$$

由于存在多种情况,所以即使 Eve 进行联合测量,Eve 也难以知道 Alice 的量子位.而且 Eve 的这种窃听行为在第二步检测信道的安全性时也将被发现.另外,Eve 不知道 Bob1、Bob2、Bob3 会选择哪种操作,假如 Bob1、Bob2、Bob3 实施的操作为 1)Bob1、Bob2、Bob3 中一部分选择用$\{|0\rangle,|1\rangle\}$基测量,而另一部分选择直接返还给 Alice;2)Bob1、Bob2、Bob3 都选择直接返还给 Alice,在 Alice 进行联合测量时,Eve 的这种窃听行为将被发现,此结论同样适用于 N 粒子纠缠态.

4 结论

提出了一种利用纠缠度较高且实际可行的 N 粒子纠缠态在一方与($N-1$)方之间形成秘密共享的方案.该方案通过多次对窃听者的检测,很好地保证了信道的安全性及产生的秘密位串的可用性;并且随着 n 和 N 的增加,该方案的效率会逐渐提高.

参考文献

[1] XIONG Xue-shi, FU Jie, SHEN Ke. Controlled teleportation of an unknown two-particle partly entangled state [J]. *Acta Photonica Sinica*, 2006, **35**(5): 780-782.
熊学仕,付洁,沈柯. 二粒子部分纠缠未知态的量子受控传递[J]. 光子学报,2006,**35**(5):780-782.

[2] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing: proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984[C]. IEEE, 1984: 175-179.

[3] DENG Fu-guo, LIU Xiao-shu, MA Ying-jun, *et al*. A theoretical scheme for multi-user quantum key distribution with N Einstein-Podolsky-Rosen pairs on a passive optical network[J]. *Chinese Physics Letters*, 2002, **19**: 893-896.

[4] LONG Gui-lu, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme[J]. *Phys Rev A*, 2002, **65**(3): 032302.

[5] DENG Fu-guo, LONG Gui-lu. Bidirectional quantum key distribution protocol with practical faint laser pulses[J]. *Phys Rev A*, 2004, **70**(1): 012311.

[6] LI Xi-han DENG Fu-guo, ZHOU Hong-yu. Efficient quantum key distribution over a collective noise channel[J]. *Phys Rev A*, 2008, **78**(2): 022321.

[7] HEN W, HAN Z F, MO X F, *et al*. Active phase compensation of quantum key distribution system [J]. *Chinese Science Bulletin*, 2008, **53**(9): 1310-1314.

[8] GAO F, GUO F Z, WEN Q Y, *et al*. Comparing the efficiencies of different detect strategies in the ping-pong protocol[J]. *Sci China Ser G-Phys Mech Astron*, 2008, **51**(12): 1853-1860.

[9] ZHOU Rui, ZHU Yu-lan, NIE Yi-you. One-way communication scheme based on superdense coding of four dimension two particles[J]. *Acta Photonica Sinica*, 2010, **39**(1): 156-159.
周锐,朱玉兰,聂义友. 四维二粒子超密编码的单向通信方案[J]. 光子学报,2010,**39**(1):156-159.

[10] HILLERY M, BUZEK V, BERTHIAUME A. Quantum secret sharing[J]. *Phys Rev A*, 1999, **59**(3): 1829-1833.

[11] WEI D X, YANG X D, LUO J, *et al*. NMR experimental implementation of three-parties quantum superdense coding [J]. *Chin Sci Bull*, 2004, **49**(5): 423-426.

[12] YAN Feng-li, GAO Ting, LI You-cheng. Quantum secret sharing between multiparty and multiparty with four states [J]. *Sci China Ser G-Phys Mech Astron*, 2007, **50**(5): 572-580.

[13] LI Xiao, LONG Gui-lu, DENG Fu-guo, *et al*. Efficient multiparty quantum secret sharing schemes[J]. *Phys Rev A*, 2004, **69**(5): 052307.

[14] LI Qin, CHAN W H, LONG Dong-yang. Semi-quantum secret sharing using entangled states[J]. *Phys Rev A*, 2010, **82**(2): 022303-022308.

Quantum Secret Sharing with *N*-Particle Entangled State

DENG Xiao-ran[1], YANG Shuai[2], YAN Feng-li[3]

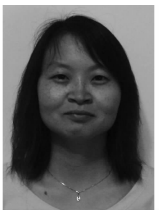
(1 *Department of Mathematics and Physics, Tianjin University of Technology and Education, Tianjin* 300222, *China*)

(2 *Department of Mathematics and Physics, Tianjin University of Technology, Tianjin* 300191, *China*)

(3 *College of Physics Science and Information Engineering, Hebei Normal University, Shijiazhuang* 050016, *China*)

Abstract: In order to construct quantum secret sharing protocols among many parts, a N-particle entangled state that has a large persistency of entanglement is introduced, and a quantum secret sharing protocol between one party and $(N-1)$ parties is presented using the proposed entangled state. During constructing secret sharing, Alice chooses randomly unitary operation I or σ_x for the sent particles, and chooses a part of the particles to check the safeness of channel; then Alice chooses another part of the particles to check the honesty of partners and the safeness of channel by the operations of $(N-1)$ parties. The protocol carries on examination to the eavesdropper for many times, so that it can insure the safeness of channel and the usability of the secret strings. Finally, there are $n[1-(N-1)/2^{N-1}]/6$ sharing secret bits among Alice and $(N-1)$ parties.

Key words: Quantum secret sharing; Entangled state; Quantum bit; Channel



DENG Xiao-ran was born in 1979. She received the M. S. degree from Hebei Normal University in 2005. Now she is a lecturer, and her research interests focus on quantum key distribution and quantum secret sharing in quantum information.