文章编号: 1007-2985(2010) 03-0051-04

基于 GHZ 态的四量子位秘密共享方案*

王朋朋, 周小清, 李小娟, 赵 晗, 杨小琳
(吉首大学物理科学与信息工程学院, 湖南 吉首 416000)

摘 要: 利用 GHZ 态作为量子信道, 再辅以经典信道传送经 GHZ 态测量后的信息, 便可实现量子位的秘密共享. 基于上述思想, 充分利用六粒子 GHZ 纠缠态的相关性, 通过 1 次 Bell 基测量、4 次单粒子测量和相应的幺正变换, 从而实现了 4 个量子位的秘密共享方案.

关键词: 隐形传态; GHZ 态; 秘密共享
中图分类号: O413.2; TN915.0 文献标志码: A

近年来, 以计算机为核心的大规模信息网路, 尤其是互联网的建立与发展, 使得人类对信息的传输和数据计算的质量要求更高了, 不但要求传输信息的效率高, 而且要求传送信息过程中具有高的安全保密性. 因此, 高效性、保密性、可靠性和认证性四项指标是现在通信系统的基本要求[1]. 在量子通信中, 量子秘密共享方案最早由 Shamir 和 Blakely 于 1979 年独立提出[2-3]; Hilley, Buzek 和 Berthiaume 最早提出利用 GHZ 三重态实现量子秘密共享方案(HBB 协议)[4], HBB 协议的非确定性, 指明要传输 1 bit 经典消息需 2 个 GHZ 态才能完成传送, 理论上效率较低. 后来又有人提出基于 2 粒子非正交纠缠态的 QSS 方案(KKI 协议)[5], 如 Grover 算法和基于纠缠交换的文献[6-7], 在 QSS 方案的基础上有人又提出基于直基态的 QSS 方案且在实验上运用单光子实现了 QSS 方案[8-9]. 现已有利用 GHZ 态传送 3 个量子位的秘密共享方案[10]. EPR 佯谬在近 60 多年量子力学发展过程中起着推动作用[11], 实验的本质在于: 真实世界是遵从爱因斯坦的局域论, 还是波尔的非局域性论, 1982 年, 法国学者 Aspect 第 1 个在实验上验证了 Bell 不等式可以违背(即证实了微观世界是遵从波尔的非局域性论). 笔者利用六粒子的 GHZ 态实现四量子位秘密共享方案, 解决了四粒子的 GHZ 态进行测量的具体理论计算步骤和计算结果, 并给出与现有的经典通信网络结合起来实现四量子位的秘密共享方案.

1 四粒子 GHZ 态测量的物理原理

对于 2 个两态粒子的量子系统, 给出如下 Bell 基:

$$\begin{cases} |\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}, \\ |\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}. \end{cases} \quad (1)$$

利用 Bell 基可对任意两粒子态 $|\Psi\rangle_{AB}$ 实施正交测量, 称为 Bell 基测量.

对于 GHZ 态的制备有很多方法, GHZ 态的制备有很多方法, 文献[12] 中指出制备远程 N 光子 GHZ 纠缠态的方案. GHZ 常用的四重态如下:

* 收稿日期: 2010-03-21
基金项目: 湖南省科技计划项目(2008FJ3078)
作者简介: 王朋朋(1985-), 男, 陕西铜川人, 吉首大学物理科学与信息工程学院硕士生, 主要从事凝聚态物理研究
通讯作者: 周小清(1963-), 男, 湖南常德人, 吉首大学物理科学与信息工程学院教授, 硕导, 主要从事量子信息研究.

$$|\Psi\rangle = 1/\sqrt{2}(|0\rangle|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle|1\rangle), \quad (2)$$

(2) 式中脚码 0、1、2、3 代表不同的 4 个粒子.

定义 4 个态矢 $|x+\rangle$, $|x-\rangle$, $|y+\rangle$, $|y-\rangle$ 并用基矢表示如下:

$$|x\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle), \quad (3)$$

$$|y\pm\rangle = 1/\sqrt{2}(|0\rangle \pm i|1\rangle). \quad (4)$$

联立(3) 至(4) 式求解可得

$$|0\rangle = 1/\sqrt{2}(|x+\rangle + |x-\rangle), \quad (5)$$

$$|1\rangle = 1/\sqrt{2}(|x+\rangle - |x-\rangle), \quad (6)$$

$$|0\rangle = 1/\sqrt{2}(|y+\rangle + |y-\rangle), \quad (7)$$

$$|1\rangle = -i/\sqrt{2}(|y+\rangle - |y-\rangle). \quad (8)$$

现要确定各粒子的态需要进行 2 次测量. 将(7) 至(8) 式代入(2) 式, 则

$$|\Psi\rangle = \frac{1}{2}\sqrt{2}[(|x+\rangle+|x-\rangle)(|x+\rangle+|x-\rangle)|0\rangle|0\rangle + (|x+\rangle-|x-\rangle)(|x+\rangle-|x-\rangle)|1\rangle|1\rangle] =$$

$$\frac{1}{2}\sqrt{2}[(|x+\rangle|x+\rangle+|x+\rangle|x-\rangle+|x-\rangle|x+\rangle+|x-\rangle|x-\rangle)|0\rangle|0\rangle +$$

$$\frac{1}{2}\sqrt{2}[(|x+\rangle|x+\rangle-|x+\rangle|x-\rangle-|x-\rangle|x+\rangle+|x-\rangle|x-\rangle)|1\rangle|1\rangle =$$

$$\frac{1}{2}\sqrt{2}[(|x+\rangle|x+\rangle+|x-\rangle|x-\rangle)(|0\rangle|0\rangle+|1\rangle|1\rangle) +$$

$$(|x+\rangle|x-\rangle+|x-\rangle|x+\rangle)(|0\rangle|0\rangle-|1\rangle|1\rangle)]. \quad (9)$$

从(9) 式可看出 4 个粒子仍然处于纠缠态, 可以对粒子 0 和粒子 1 进行测量, 根据测量结果可以知道粒子 2、粒子 3 所处的量子纠缠状态, 例如, 若对粒子 0、1 测量结果是 $|x+\rangle$, $|x+\rangle$, 那么粒子 2, 3 的量子态为 $1/\sqrt{2}(|0\rangle|0\rangle+|1\rangle|1\rangle)$; 如果对粒子 0, 1 的测量结果是 $|x+\rangle$, $|x-\rangle$, 那么粒子 2, 3 的量子态为 $1/\sqrt{2}(|0\rangle|0\rangle-|1\rangle|1\rangle)$. 同理, 将(5) ~ (8) 式两两分别代入(2) 式便可得粒子 2, 3 的量子态, 绘制成表 1. 从表中可以看出第 1 次对粒子 0 和粒子 1 进行 Bell 基联合测量, 可以得到粒子 2 和粒子 3 所处的量子态.

表 1 粒子 2, 3 量子态的测量结果

粒子 2, 3 的量子态		粒子 0 的量子态测量结果			
		$\|x+\rangle$	$\|x-\rangle$	$\|y+\rangle$	$\|y-\rangle$
粒子 1 量子态的测量结果	$\|x+\rangle$	$\|0\rangle\|0\rangle+\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle-\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle-i\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle+i\|1\rangle\|1\rangle$
	$\|x-\rangle$	$\|0\rangle\|0\rangle-\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle+\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle+i\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle-i\|1\rangle\|1\rangle$
	$\|y+\rangle$	$\|0\rangle\|0\rangle-i\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle+i\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle-\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle+\|1\rangle\|1\rangle$
	$\|y-\rangle$	$\|0\rangle\|0\rangle+i\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle-i\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle+\|1\rangle\|1\rangle$	$\|0\rangle\|0\rangle-\|1\rangle\|1\rangle$

假如第 1 次对粒子 0、粒子 1 测量后得到粒子 2、粒子 3 处于 $1/\sqrt{2}(|0\rangle|0\rangle+|1\rangle|1\rangle)$ 纠缠态, 为得到粒子 3 的量子态. 第 2 次可对粒子 2 进行 von Neumann 测量[13]. 在新的基底 $|x\rangle$, $|y\rangle$ 下, 粒子 2 的量子态可分解为

$$|0\rangle = \sin\theta|x\rangle + \cos\theta|y\rangle, \quad (10)$$

$$|1\rangle = \sin\theta|x\rangle - \cos\theta|y\rangle, \quad (11)$$

其中 θ 为分析角, 若取 $\theta = 45°$, 将第 1 次测量后所得到的量子态经归一化后得

$$a|0\rangle|0\rangle + b|1\rangle|1\rangle, \quad (12)$$

其中 $a^2 + b^2 = 1$. 将(10) ~ (11) 式代入(12) 式, 则

$$a|0\rangle|0\rangle + b|1\rangle|1\rangle = (a|x\rangle + a|y\rangle)|0\rangle + (b|x\rangle - b|y\rangle)|1\rangle =$$

$$a|x\rangle|0\rangle + a|y\rangle|0\rangle + b|x\rangle|1\rangle - b|y\rangle|1\rangle =$$

$$(a|0\rangle + b|1\rangle)|x\rangle + (a|0\rangle - b|1\rangle)|y\rangle. \quad (13)$$

显然测量结果有 2 种可能, 若测得粒子 2 结果为 $|x\rangle$, 则粒子 3 的量子态为 $a|0\rangle+b|1\rangle$; 若测得粒子 2 的结果为 $|y\rangle$, 则粒子 3 的量子态为 $a|0\rangle-b|1\rangle$. 同理, 可得其他粒子的量子态, 如表 2 所示. 从表 2 中可以看出第 2 次对粒子 2 进行单粒子测量, 可以得到粒子 3 的量子态. 例如, 按照前面方法, 第 1 次对粒子 0 和粒子 1 进行联合测量得到粒子 2 和粒子 3 的量子态为 $a|0\rangle|0\rangle+b|1\rangle|1\rangle$, 第 2 次对粒子 2 进行单粒子测量, 假如测量结果为 $|x\rangle$, 则粒子 3 的量子态为 $a|0\rangle+b|1\rangle$, 此时, 变换的幺正矩阵为 $\boldsymbol{U}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, 其中 $\boldsymbol{U}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

表 2　粒子 3 的量子态

第 1 次粒子 2, 3 量子态	第 2 次粒子 2 量子态	粒子 3 所处量子态	幺正变换矩阵 $\boldsymbol{U}$	逆矩阵 $\boldsymbol{U}^{-}$
$a\|0\rangle_2\|0\rangle_3+b\|1\rangle_2\|1\rangle_3$	$\|x\rangle_2$	$a\|0\rangle_3+b\|1\rangle_3$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$
	$\|y\rangle_2$	$a\|0\rangle_3-b\|1\rangle_3$	$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$
$a\|0\rangle_2\|0\rangle_3-b\|1\rangle_2\|1\rangle_3$	$\|x\rangle_2$	$a\|0\rangle_3-b\|1\rangle_3$	$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$
	$\|y\rangle_2$	$a\|0\rangle_3+b\|1\rangle_3$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$
$a\|0\rangle_2\|0\rangle_3-\mathrm{i}b\|1\rangle_2\|1\rangle_3$	$\|x\rangle_2$	$a\|0\rangle_3-\mathrm{i}b\|1\rangle_3$	$\begin{pmatrix}1&0\\0&-\mathrm{i}\end{pmatrix}$	$\begin{pmatrix}1&0\\0&\mathrm{i}\end{pmatrix}$
	$\|y\rangle_2$	$a\|0\rangle_3+\mathrm{i}b\|1\rangle_3$	$\begin{pmatrix}1&0\\0&\mathrm{i}\end{pmatrix}$	$\begin{pmatrix}1&0\\0&-\mathrm{i}\end{pmatrix}$
$a\|0\rangle_2\|0\rangle_3+\mathrm{i}b\|1\rangle_2\|1\rangle_3$	$\|x\rangle_2$	$a\|0\rangle_3+\mathrm{i}b\|1\rangle_3$	$\begin{pmatrix}1&0\\0&\mathrm{i}\end{pmatrix}$	$\begin{pmatrix}1&0\\0&-\mathrm{i}\end{pmatrix}$
	$\|y\rangle_2$	$a\|0\rangle_3-\mathrm{i}b\|1\rangle_3$	$\begin{pmatrix}1&0\\0&-\mathrm{i}\end{pmatrix}$	$\begin{pmatrix}1&0\\0&\mathrm{i}\end{pmatrix}$

2　四量子位秘密共享的理论方案

文献[10] 提出利用 GHZ 态传送 3 个量子位的秘密共享方案, 在此基础上, 用六粒子的 GHZ 态 $|\Psi\rangle_{56789}=1/\sqrt{2}(|000000\rangle+|111111\rangle)_{456789}$ 完成四粒子纠缠的 GHZ 态 $|\Psi\rangle_{0123}=(a|0000\rangle+b|1111\rangle)_{0123}$ 的隐形传态, 进而实现 4 个量子位的秘密共享方案.

假设甲地的 Alice 有粒子 0, 1, 2, 3. 量子态为 $|\Psi\rangle_{0123}=(a|0000\rangle+b|1111\rangle)_{0123}$, 其中 $a^2+b^2=1$. 现要将此量子态传送给丙地的 Cliff, Cliff 持有粒子 6, 7, 8, 9. 为此必须建立量子信道, 方法如下:

(1) 量子信道的建立. 由制备中心 (乙地的 Bob 为 GHZ 态制备中心) 制备量子态 $|\Psi\rangle_{56789}=1/\sqrt{2}(|000000\rangle+|111111\rangle)_{456789}$, 将粒子 4 传给甲地的 Alice, 粒子 5, 6, 7, 8, 9 给丙地的 Cliff. 则总的态矢为

$$|\Psi\rangle=|\Psi\rangle_{0123}\otimes|\Psi\rangle_{56789}=(a|0000\rangle+b|1111\rangle)_{0123}\otimes1/\sqrt{2}(|000000\rangle+|111111\rangle)_{456789}=$$
$$|\Psi^{+}\rangle_{04}/\sqrt{2}(a|00000000\rangle+b|11111111\rangle)_{12356789}+|\Psi^{-}\rangle_{04}/\sqrt{2}(a|00000000\rangle-$$
$$b|11111111\rangle)_{12356789}+|\Phi^{+}\rangle_{04}/\sqrt{2}(a|00000000\rangle+b|11111111\rangle)_{12356789}$$
$$+|\Phi^{-}\rangle_{04}/\sqrt{2}(a|00000000\rangle-b|11111111\rangle)_{12356789}.$$

(2) 量子测量. Alice 对粒子 0, 4 采用 Bell 基进行联合测量, 假设测量结果为 $|\Psi^{-}\rangle$, 将测量结果发送到公用的经典信道 (如中国移动、中国电信等), 则

$$|\Psi\rangle_{2356789}=(a|00000000\rangle+b|11111111\rangle)_{12356789}. \quad (14)$$

Alice 对粒子 1, 2 分别进行如(3)式的单粒子测量, 并假设测量结果为| $x-$ ⟩| $y+$ ⟩, 并将测量结果发送到公用的经典信道, 则

$$|\Psi\rangle_{356789} = (a|000000\rangle - ib|111111\rangle)_{356789}. \quad (15)$$

Alice 对粒子 3, 5 分别进行如(3), (4)式的单粒子测量, 并假设测量结果为| $x-$ ⟩| $y+$ ⟩, 并将测量结果发送到公用的经典信道, 则

$$|\Psi\rangle_{6789} = (a|0000\rangle - b|1111\rangle)_{6789}. \quad (16)$$

(3) 量子信息的接收. 丙地的 Cliff 把甲地 Alice 持有的粒子 0, 1, 2, 3 的量子态在粒子 6, 7, 8, 9 上恢复, 根据公用的经典信道上 Alice 的测量结果选择适当的幺正变换矩阵, 对现有的量子态| $\Psi\rangle_{6789} = (a|0000\rangle - b|1111\rangle)_{6789}$ 进行变换. 假设对粒子 6 做幺正变换$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, 就可以得到量子态| $\Psi\rangle_{6789} = (a|0000\rangle + b|1111\rangle)_{6789}$.

由通信过程可知, 只要用 1 个 GHZ 纠缠态, 进行 1 次 Bell 测量和 4 次单粒子测量, 就可实现 Alice 与 Cliff 之间的四粒子秘密共享方案. 方案操作简单, 通信过程易于实现.

3 结论

利用六粒子 GHZ 态作为量子信道, 再辅以经典信道, 提出了四粒子的 GHZ 态秘密共享方案, 该方案简单实用. 通过 1 次 Bell 测量和 4 次单粒子测量及相应的幺正变换, 从而实现了 4 个量子位的秘密共享方案. 解决了四粒子的 GHZ 态进行测量的具体理论计算步骤和计算结果, 提出了与现有的经典通信网络结合实现四量子位秘密共享方案, 为多粒子的密钥共享方案提供了理论基础.[14]

参考文献:

[1] 陈汉武. 量子信息与量子计算[M]. 南京: 东南大学出版社, 2006: 1-5.

[2] SHAMIR A. How to Share a Secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[3] BLAKELY G. Safeguarding Cryptographic Keys [C]// Proceedings of the National Computer Conference, New York: AFIPS Press, 1979: 313-317.

[4] HILLERY M, BUZEK V, BERTHIAUME A. Quantum Secret Sharing [J]. Phys. Rev. A, 1999, 59: 1 829-1 834.

[5] KARLSSON A, KOASHI M, IMOTO N. Quantum Entanglement for Secret Sharing and Secret Splitting [J]. Phys. Rev. A, 1999, 59: 162-169.

[6] HSU L Y. Quantum Secret-Sharing Protocol Based Grover's Algorithm [J]. Phys. Rev. A, 2003, 68: 022306.

[7] KARIMIPOUR V, BAHRAMINASAB A, BAGHERINEZHAD S. Entanglement Swapping of Generalized Cat States and Secr-Sharing [J]. Phys. Rev. A, 2002, 65: 042320.

[8] LJUUGGREN D, BOURENNANE M, KARLSSON A. Authority-Based User Authentication in Quantum Key Distribution [J]. Phys. Rev. A, 2000, 62: 022305.

[9] ZHANG Z J, YONG L, MAN Z X. Multiparty Quantum Secret Sharing [J]. Phys. Rev. A, 2005, 71: 044301.

[10] LIU Y Q, SHI J, HU B L, et al. Scheme of Three Quantum Bit Secret Sharing Based on GHZ State [J]. Chinese Journal of Quantum Electronics, 2010, 27(1): 46-50.

[11] 陈汉武. 量子信息与量子计算[M]. 南京: 东南大学出版社, 2006, 19-27.

[12] ZHAO H, ZHOU X Q, YANG X L. Generation of Multiparticle Entangled State from Einstein-Podolsky-Rosen Photon Pairs Optics Communications [J]. Acta Phys. Sin., 2010, 283: 2 472-2 475.

[13] ZHOU X Q, WU Y W. Discussion on Building the Net of Quantum Teleportation Using Three-Particle Entangled States [J]. Acta Phys. Sin., 2007, 56(4): 1 881-1 887.

[14] BENNETT C H, BESSETTE F, BRASSARD G, et al. Experimental Quantum Cryptography [J]. Journal of Cryptography, 1992(5): 3-28.

(下转第 58 页)

[7] 彭良玉, 何怡刚, 黄满池. 连续时间电压型 CCII+ /- 双二阶滤波器 [J]. 电路与系统学报, 2000, 5(4): 90-92.
[8] 彭良玉, 何怡刚, 黄满池. 电压模式 CCII+ /- 双二阶滤波器 [J]. 电工技术学报, 2000, 15(4): 58-61.

A Novel Design of Voltage-Mode Three Inputs and One Output Biquadratic Filter

WU Xian-ming[1], WU Yun[2]
(1. College of Physics Science and Information Engineering, Jishou University, Jishou 416000, HunanChina; 2. College of Mechanical and Electronic Engineering in China University of Petroleum, Dongying 257061, Shandong China)

Abstract: A voltage-mode 3-input and 1-output universal biquadratric filter based on second generation current conveyor (CCII) is presented. The circuit consists of two CCIIs, three capacitors and two resistors, which can realize functions of second-order low-pass, band-pass, high-pass, notch and all-pass, and it has low passive and active sensitivities. The circuit is simulated with PSPICE, and results show that the design of circuit is correct.

Key words: voltage-mode; current conveyor; filter

(责任编辑 陈炳权)

(上接第 54 页)

Scheme of Four Quantum Bit Secret Sharing Based on GHZ State

WANG Peng-peng, ZHOU Xiao-qing, LI Xiao-juan, ZHAO Han, YANG Xiao-lin
(College of Physics Science and Information Engineering, Jishou University, Jishou 416000, Hunan China)

Abstract: With GHZ state as a quantum channel, quantum bit secret sharing can be realized after transmitting the information by a classical channel, which is measured by the GHZ state. Based on the above ideas, making full use of the correlation of a six-particle entanglement GHZ state, by a Bell measurement, four single-particle measurements and the corresponding unitary transformation, a four-qubit secret sharing scheme can be achieved.

Key words: teleportation; GHZ state; secret sharing

(责任编辑 陈炳权)