第 29 卷 第 4 期 量 子 电 子 学 报 Vol.29 No.4
2012 年 7 月 CHINESE JOURNAL OF QUANTUM ELECTRONICS July 2012

DOI: 10.3969/j.issn.1007-5461. 2012.04.007

基于三粒子纠缠态的未知单粒子态量子秘密共享

张群永

(淮阴工学院数理学院, 江苏 淮安 223003)

摘 要: 提出了两个未知单粒子态的量子秘密共享方案, 分别使用一个对称的三粒子纠缠态和一个不对称的三粒子纠缠态作为量子信道来实现态的共享。在发送者和协助者分别对各自所拥有的粒子实施 Bell 基测量、单粒子态测量之后, 接收者对所拥有的粒子作相应的幺正操作才能实现初始量子态的重构。方案可以推广至任意两粒子和多粒子纠缠态的量子秘密共享。在安全性方面, 考虑了来自外部和共享者内部的盗窃情况, 经讨论可认为所提出的方案是安全可靠的。

关 键 词: 量子光学; 量子秘密共享; 幺正操作; 量子态共享; 量子信息分离

中 图 分 类 号: O431.2 **文 献 标 识 码:** A **文章编号:** 1007-5461(2012)04-0421-06

Quantum secret sharing of single-qubit state via tripartite entangled states

ZHANG Qun-yong

(Faculty of Mathematics and Physics, Huaiyin Institute of Technology, Huai'an 223003, China)

Abstract: Two schemes for quantum secret sharing of single-qubit state were proposed. A symmetric three-qubit entangled state and an asymmetric three-qubit entangled state were used as quantum channel, respectively. The sender performs Bell-basis measurements on her particles, and the cooperator operates single-particle measurements on his particles, then the state receiver can reconstruct the original state by applying the appropriate unitary operation. The schemes can also be generalized to the case of arbitrary two-qubit and multi-particle entangled state. The security against certain eavesdropping attacks is also considered. These protocols are considered to be secure.

Key words: quantum optics; quantum secret sharing; unitary operation; quantum state sharing; quantum information splitting

1 引 言

量子秘密共享是量子信息学的核心内容之一。秘密共享的含义是秘密以适当的方式拆分, 拆分后的每一个子秘密由不同的参与者管理, 只有若干个参与者共同协作才能恢复出秘密信息。量子秘密共享是经典秘密共享的量子版本, 它不仅可以共享经典信息, 还可以共享量子态信息。 1999 年, Hillery, Buzek 和 Berthiaume 首次提出了用量子物理方法实现量子秘密共享和量子信息分离的概念, 并基于 GHZ 态的纠缠关联性设计了第一个量子秘密共享协议 [1] (简称 HBB 协议) 。这种方案克服了经典秘密共享的安全性缺

作者简介: 张群永 (1984 -), 江苏涟水人, 硕士, 主要从事量子信息与量子计算方面的研究。 **E-mail:** zhangqunyong@126.com

收稿日期: 2012–02–24; **修改日期:** 2012–03–22

点，而且具有较高的效率，它所蕴含的从物理学性质到密码学应用的思想对后来的量子秘密共享研究有着深远的影响。此后，无论在理论方面还是在实验方面，各种各样的量子秘密共享方案相继被提出[2~12]。本文分别以一个对称的三粒子纠缠态和不对称的三粒子纠缠态作为量子信道，提出了两个未知单粒子态的量子秘密共享方案。

2 基于三粒子对称纠缠信道未知单粒子态的共享方案

假如存在三个合法的使用者 Alice, Bob 和 Charlie。Alice 想要给 Bob 或者 Charlie 发送一个未知单粒子态的量子信息

$$|\varphi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1 , \tag{1}$$

系数 α 和 β 都是复数，且满足 $|\alpha|^2 + |\beta|^2 = 1$。Alice 已知 α 和 β 的信息，而 Bob 和 Charlie 却不知道。现在 Alice 准备把该量子态信息拆分成两部分，分发给接收者 Bob 和 Charlie。当且仅当两个接收者相互合作时被授权接收信息的一方才能恢复出初始的未知单粒子态。任一接收者在没有信息交流和合作的情况下都无法单独获取未知量子态信息。

若 Alice, Bob 和 Charlie 共享一个对称三粒子纠缠态作为量子信道[13]

$$|\phi\rangle_{234} = \frac{1}{2}(|000\rangle + |110\rangle + |101\rangle + |001\rangle)_{234} , \tag{2}$$

粒子 2, 3, 4 分别属于 Alice, Bob 和 Charlie, 量子信息和信道构成的四粒子系统可写为

$$|\Psi\rangle_{1234} = |\varphi\rangle_1|\phi\rangle_{234} =$$
$$\frac{1}{2}(\alpha|0\rangle_1 + \beta|1\rangle_1)(|000\rangle + |110\rangle + |101\rangle + |011\rangle)_{234} . \tag{3}$$

首先，Alice 对所拥有的粒子 1, 2 进行 Bell 态测量，Bell 态的具体形式为

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{12} , \ |\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{12} , \tag{4}$$

测量之后，Bob 和 Charlie 所拥有的粒子将会对应塌缩到以下四种纠缠态之一

$${}_{12}\langle\Phi^+|\Psi\rangle_{1234} = \frac{1}{2\sqrt{2}}[\alpha(|00\rangle + |11\rangle)_{34} + \beta(|10\rangle + |01\rangle)_{34}] , \tag{5}$$

$${}_{12}\langle\Phi^-|\Psi\rangle_{1234} = \frac{1}{2\sqrt{2}}[\alpha(|00\rangle + |11\rangle)_{34} - \beta(|10\rangle + |01\rangle)_{34}] , \tag{6}$$

$${}_{12}\langle\Psi^+|\Psi\rangle_{1234} = \frac{1}{2\sqrt{2}}[\alpha(|10\rangle + |01\rangle)_{34} + \beta(|00\rangle + |11\rangle)_{34}] , \tag{7}$$

$${}_{12}\langle\Psi^-|\Psi\rangle_{1234} = \frac{1}{2\sqrt{2}}[\alpha(|10\rangle + |01\rangle)_{34} - \beta(|00\rangle + |11\rangle)_{34}] . \tag{8}$$

由于纠缠交换的作用，Alice 要发送的量子信息已经被传递到 Bob 和 Charlie 所拥有的量子态之中，此时量子信息的分发过程已经完成。Bob 和 Charlie 中任何一个人如果不通过相互合作和信息交流而仅仅依靠对自己的粒子进行局域测量都无法获得 Alice 的未知量子态。根据不可克隆定理，只能有一个接收者获得初始态信息。不失一般性，我们假设 Alice 的 Bell 态测量结果为 $|\Phi^+\rangle_{12}$, 根据式 (5), 我们可以把 Bob 和 Charlie 拥有的对应粒子态写成

$$|\Phi\rangle_{34}=\frac{1}{2\sqrt{2}}[\alpha(|00\rangle+|11\rangle)_{34}+\beta(|10\rangle+|01\rangle)_{34}]=$$
$$\frac{1}{4}[|0\rangle_3(\alpha|0\rangle+\beta|1\rangle)_4+|1\rangle_3(\alpha|1\rangle+\beta|0\rangle)_4]\ . \tag{9}$$

不妨假设 Alice 委任 Charlie 重构量子态信息，如果 Bob 同意协助 Charlie 恢复初始量子态，那么 Bob 需要对粒子 3 进行单粒子态测量，并且公布测量结果。如果 Bob 的测量结果是 $|0\rangle_3$, 那么 Charlie 的粒子 4 将会塌缩到态 $\alpha|0\rangle_4+\beta|1\rangle_4$, 这正是 Alice 送出的初始量子态。 Charlie 不需要对粒子 4 进行任何操作就可以得到初始量子态；如果 Bob 的测量结果是 $|1\rangle_3$, 那么粒子 4 将会塌缩到态 $\alpha|1\rangle_4+\beta|0\rangle_4$, 此时 Charlie 需要对粒子 4 实施一个幺正操作 U_2 便可以获得初始量子信息。幺正操作如下

$$U_0=|0\rangle\langle 0|+|1\rangle\langle 1|\ ,\ U_1=|0\rangle\langle 0|-|1\rangle\langle 1|\ ,$$
$$U_2=|0\rangle\langle 1|+|1\rangle\langle 0|\ ,\ U_3=|0\rangle\langle 1|-|1\rangle\langle 0|\ . \tag{10}$$

该方案所有可能的结果如表 1 所示。 Alice 只需要对所拥有两个粒子进行 Bell 态测量，而被授权的量子信息接收者需要在另一方的协助下才可以获得初始量子态，协助者仅需要公布单粒子态测量的结果，信息接收者根据关联性表进行适当的幺正操作就可以完成量子态的恢复。表 1 中 M_{12} 指 Alice 对粒子 1 和 2 的 Bell 态测量结果， M_3 是 Bob 对粒子 3 的单粒子态测量结果， $|\phi\rangle_4$ 是 Bob 在单粒子测量之后粒子 4 塌缩的态， $U_{\rm c}$ 是 Charlie 要恢复 Alice 的初始量子态必须对粒子 4 所做的幺正操作。

Table 1 Relation between the local unitary operations and measurement results in the scheme of symmetric three-qubit entangled state

M_{12}	M_3	$\|\phi\rangle_4$	$U_{\rm c}$
$\|\Phi^+\rangle_{12}$	$\|0\rangle_3$	$\alpha\|0\rangle+\beta\|1\rangle$	U_0
	$\|1\rangle_3$	$\alpha\|1\rangle+\beta\|0\rangle$	U_2
$\|\Phi^-\rangle_{12}$	$\|0\rangle_3$	$\alpha\|0\rangle-\beta\|1\rangle$	U_1
	$\|1\rangle_3$	$\alpha\|1\rangle-\beta\|0\rangle$	U_3
$\|\Psi^+\rangle_{12}$	$\|0\rangle_3$	$\alpha\|1\rangle+\beta\|0\rangle$	U_2
	$\|1\rangle_3$	$\alpha\|0\rangle+\beta\|1\rangle$	U_0
$\|\Psi^-\rangle_{12}$	$\|0\rangle_3$	$\alpha\|1\rangle-\beta\|0\rangle$	U_3
	$\|1\rangle_3$	$\alpha\|0\rangle-\beta\|1\rangle$	U_1

3　基于三粒子不对称纠缠信道未知单粒子态的共享方案

如果 Alice, Bob 和 Charlie 共享一个不对称的三粒子纠缠态作为量子信道 [14]

$$|\phi\rangle_{\rm abc}=\Big(\frac{1}{\sqrt{2}}|000\rangle+\frac{1}{2}|101\rangle+\frac{1}{2}|110\rangle\Big)_{\rm abc}\ , \tag{11}$$

Alice 拥有粒子 1 和 a, 粒子 b 和 c 分别属于 Bob 和 Charlie, 整个量子系统的态可以写作

$$|\Psi\rangle_{1{\rm abc}}=|\varphi\rangle_1\otimes|\phi\rangle_{\rm abc}=(\alpha|0\rangle+\beta|1\rangle)_1\Big(\frac{1}{\sqrt{2}}|000\rangle+\frac{1}{2}|101\rangle+\frac{1}{2}|110\rangle\Big)_{\rm abc}\ . \tag{12}$$

为了使 Bob 和 Charlie 能够共享 Alice 的量子态信息， Alice 首先应当对自己的两个粒子进行 Bell 态测量，根据测量结果的不同， Bob 和 Charlie 拥有的粒子将对应地塌缩到以下四种态之一：

$$ {}_{1a}\langle\Phi^+|\Psi\rangle_{1abc}=\frac{1}{\sqrt{2}}\Big[\frac{\alpha}{\sqrt{2}}|00\rangle+\frac{\beta}{2}|01\rangle+\frac{\beta}{2}|10\rangle\Big]_{bc}, \tag{13} $$

$$ {}_{1a}\langle\Phi^-|\Psi\rangle_{1abc}=\frac{1}{\sqrt{2}}\Big[\frac{\alpha}{\sqrt{2}}|00\rangle-\frac{\beta}{2}|01\rangle-\frac{\beta}{2}|10\rangle\Big]_{bc}, \tag{14} $$

$$ {}_{1a}\langle\Psi^+|\Psi\rangle_{1abc}=\frac{1}{\sqrt{2}}\Big[\frac{\alpha}{2}|01\rangle+\frac{\alpha}{2}|10\rangle+\frac{\beta}{\sqrt{2}}|00\rangle\Big]_{bc}, \tag{15} $$

$$ {}_{1a}\langle\Psi^-|\Psi\rangle_{1abc}=\frac{1}{\sqrt{2}}\Big[\frac{\alpha}{2}|01\rangle+\frac{\alpha}{2}|10\rangle-\frac{\beta}{\sqrt{2}}|00\rangle\Big]_{bc}. \tag{16} $$

在对粒子 a 和 1 进行 Bell 态测量之后，由于纠缠交换，量子信息已经被转移到 Bob 和 Charlie 所共享的纠缠态之中，此时量子信息的分发过程已经完成。需要指出的是，上述四个可能的塌缩概率是相同的，每一个发生的几率都为 1/4 。 Bob 和 Charlie 两者都无法通过局域操作来恢复未知单粒子态 $|\varphi\rangle_1$ 。为了重构初始的未知态， Bob 和 Charlie 应当相互协助才能重构量子态信息。不失一般性，我们假设 Alice 获得 Bell 态测量结果为 $|\Psi^-\rangle_{1a}$, 并将其公开宣布。我们假设 Alice 委任 Charlie 来重构初始的未知态，如果 Bob 同意协助 Charlie, 他将通过对自己的粒子 b 和 Charlie 的粒子 c 实施一次两粒子联合幺正操作

$$ \Omega=|00\rangle\langle 00|+|11\rangle\langle 11|+\frac{1}{\sqrt{2}}(|01\rangle\langle 01|+|10\rangle\langle 01|+|01\rangle\langle 10|-|10\rangle\langle 10|). \tag{17} $$

在实施幺正操作之后，两粒子 b 和 c 的态将可以写成

$$ \Omega|\phi\rangle_{bc}=\Big(\frac{\alpha}{2}|01\rangle-\frac{\beta}{2}|00\rangle\Big)_{bc}=\frac{1}{2}|0\rangle_b(\alpha|1\rangle_c-\beta|0\rangle_c), \tag{18} $$

从上式中可以看出，粒子 b 处于态 $|0\rangle_b$, 粒子 c 处于态 $\alpha|1\rangle_c-\beta|0\rangle_c$ 。这种情况下， Charlie 应当在粒子 c 上实施一个幺正操作 U_3, 幺正操作 $U_i(i=1,2,3)$ 同式 (10) 。在 Bob 的帮助下， Charlie 可以在粒子 c 上重构出初始量子态信息。对于其他情况的测量结果和重构未知量子态的局域幺正操作之间的关系也可以通过同样的方法获得。关联性如表 2 所示，其中 M_{1a} 指 Alice 对粒子 1 和 a 的 Bell 态测量结果， $|\phi\rangle_c$ 指粒子 c 塌缩后的量子态， U_i 指 Charlie 恢复量子信息需要进行的幺正操作。

Table 2 Relation between the local unitary operations and measurement results in the scheme of asymmetric three-qubit entangled state

M_{1a}	$\|\phi\rangle_{bc}$	$\Omega\|\phi\rangle_{bc}$	$\|\phi\rangle_c$	U_i
$\|\Phi^+\rangle_{1a}$	$\frac{1}{\sqrt{2}}\Big[\frac{\alpha}{\sqrt{2}}\|00\rangle+\frac{\beta}{2}\|01\rangle+\frac{\beta}{2}\|10\rangle\Big]_{bc}$	$\frac{\alpha}{2}\|00\rangle+\frac{\beta}{2}\|01\rangle$	$\alpha\|0\rangle+\beta\|1\rangle$	U_0
$\|\Phi^-\rangle_{1a}$	$\frac{1}{\sqrt{2}}\Big[\frac{\alpha}{\sqrt{2}}\|00\rangle-\frac{\beta}{2}\|01\rangle-\frac{\beta}{2}\|10\rangle\Big]_{bc}$	$\frac{\alpha}{2}\|00\rangle-\frac{\beta}{2}\|01\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	U_1
$\|\Psi^+\rangle_{1a}$	$\frac{1}{\sqrt{2}}\Big[\frac{\alpha}{2}\|01\rangle+\frac{\alpha}{2}\|10\rangle+\frac{\beta}{\sqrt{2}}\|00\rangle\Big]_{bc}$	$\frac{\alpha}{2}\|01\rangle+\frac{\beta}{2}\|00\rangle$	$\alpha\|1\rangle+\beta\|0\rangle$	U_2
$\|\Psi^-\rangle_{1a}$	$\frac{1}{\sqrt{2}}\Big[\frac{\alpha}{2}\|01\rangle+\frac{\alpha}{2}\|10\rangle-\frac{\beta}{\sqrt{2}}\|00\rangle\Big]_{bc}$	$\frac{\alpha}{2}\|01\rangle-\frac{\beta}{2}\|00\rangle$	$\alpha\|1\rangle-\beta\|0\rangle$	U_3

4 安全性分析

我们从内外攻击两种情况来对上述方案的安全性进行分析。在基于三粒子对称纠缠信道的未知单粒子态共享方案中，假设存在一个盗窃者 (Eve), 她想在粒子分配过程中通过量子信道纠缠一个辅助粒子来盗取 Alice 所要传输的量子态信息。如果参与通讯的三方都没有发现来自 Eve 的攻击，那么，在 Alice 对其拥有的粒子进行 Bell 态测量之后， Bob, Charlie 和 Eve 构成的量子系统的态将塌缩到一个三粒子的纠缠态。然而，当 Bob 对他所拥有的粒子进行单粒子测量之后， Charlie 和 Eve 构成的系统将塌缩到一个直积态，

Eve 将不会获得任何未知量子态的信息。为了更清楚地阐述，我们假设 Eve 试图在纠缠信道上纠缠一个辅助粒子 $|0\rangle_5$, 如果 Alice 的 Bell 态测量结果为 $|\Phi^+\rangle_{12}$, 那么 Bob, Charlie 和 Eve 的混合态将会表示为

$$\alpha(|000\rangle + |110\rangle)_{345} + \beta(|100\rangle + |010\rangle)_{345} \ . \tag{19}$$

如果 Bob 实施一个基矢为 $|0\rangle_3$ 的测量， Charlie-Eve 组成的体系将塌缩到态 $(\alpha|0\rangle_4 + \beta|1\rangle_4)|0\rangle_5$ 。因此，Eve 的态并没有被改变，由于纠缠的对应特性，在此攻击中， Eve 没有任何获取未知量子态信息的机会。

另一种攻击情况是：我们假设参与者中就有一方是不诚实的，即如果 Charlie 便是盗窃者，或者他将和盗窃者 Eve 合作。 Charlie 通过拦截 Alice 发送给 Bob 的信道粒子，然后再将一个自己准备好的纠缠粒子发送给 Bob 。这样，仅当 Alice 委任 Charlie 来重构量子态时， Charlie 才能不被发现而窃取量子信息。如果 Alice 委任的是 Bob 而不是 Charlie 重构量子态，那么 Charlie 的盗窃行为将会被发现。由于 Charlie 未知 Alice 的测量结果，因此他发送给 Bob 的测量结果处于错误的量子态， Bob 重构的未知信息也将不同于 Alice 所发送的信息。当 Alice 和 Bob 公开对比一小部分量子信息时，他们将会发现通讯中存在着窃听的行为。

我们再考虑第二个方案的安全性，为了检查是否有盗窃者的存在， Alice 可以随机选择一个单粒子测量基对其粒子进行测量， Bob 和 Charlie 用同样的测量基对各自的粒子进行测量。由于纠缠一一对应的特性，他们测量的结果应该是相关的。如果在量子信道中存在盗窃者，那么当他们公开对比测量结果时将会发现存在着一些错误，这样将会发现来自外部的盗窃者。如果 Eve 的纠缠粒子没有给量子系统引入错误，那么系统的量子态将仍然是未知单粒子态和纠缠粒子的直积态。这样，盗窃者也无法获得 Alice 要发送的初始未知态。综上所述，对于某些盗窃者的攻击我们的量子秘密共享方案将是安全的。

5　结束语

本文中我们对于三粒子纠缠态作为量子信道的未知单粒子态的共享问题，分别提出了一个基于对称的三粒子信道和不对称的三粒子信道的秘密共享方案。从内部和外部两种盗窃情况对方案的安全性进行了分析，得出我们所提出的量子秘密共享方案是安全可靠的。方案同样可以推广至共享任意未知两粒子态和未知多粒子态的情况 [15,16] 。最近， Bae 等提出了一个基于不对称量子信道的三方量子隐形传态方案 [14], 该方案显示出基于不对称量子信道的隐形传态可以比对称信道的隐形传态传递更多的量子信息，即不对称纠缠态作为量子信道有时可能更加有用。因此，我们下一步的工作将是更加深入地研究不对称量子信道在量子秘密共享中的应用。

参考文献：

[1] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing [J]. *Phys. Rev. A*, 1999, 59: 1829-1834.

[2] Gaertner S, Kurtsiefer C, *et al.* Experimental demonstration of four-party quantum secret sharing [J]. *Phys. Rev. Lett.*, 2007, 98: 020503.

[3] Deng F G, Li X H, Zhou H Y. Efficient high-capacity quantum secret sharing with two-photon entanglement [J]. *Phys. Lett. A*, 2008, 372: 1957.

[4] Hou K, Li Y B, Shi S H. Quantum state sharing with a genuinely entangled five-qubit state and Bell-state measurements [J]. *Opt. Commun.*, 2010, 283: 1961-1965.

[5] Shi R H, Huang L S, *et al.* Multiparty quantum secret sharing with Bell states and Bell measurements [J]. *Opt. Commun.*, 2010, 283: 2476-2480.

[6] 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* (量子电子学报), 2010, 27(1): 41-46 (in Chinese).

[7] Pan G X. Minimal measurement complexity for quantum information splitting of two-qubit state [J]. *Chinese Journal of Quantum Electronics* (量子电子学报), 2010, 27(2): 180-186 (in Chinese).

[8] Pan G X. Quantum information splitting of arbitrary two-particle state using two GHZ states [J]. *Chinese Journal of Quantum Electronics* (量子电子学报), 2010, 27(5): 573-579 (in Chinese).

[9] Shi R H, Huang L S, *et al.* Asymmetric multi-party quantum state sharing of an arbitrary m-qubit state [J]. *Quantum Information Processing*, 2011, 10: 53-61.

[10] Scherpelz P, Resch R, Berryrieser D, *et al.* Entanglement-secured single-qubit quantum secret sharing [J]. *Phys. Rev. A*, 2011, 84: 032303.

[11] Li M L, Ye L. Quantum information splitting of a product state of a single-qubit state via GHZ states [J]. *Chinese Journal of Quantum Electronics* (量子电子学报), 2011, 28(6): 693-696 (in Chinese).

[12] Nie Y Y, Li Y H, Liu J C, *et al.* Quantum information splitting of an arbitrary three-qubit state by using a genuinely entangled five-qubit state and a Bell-state [J]. *Quantum Information Processing*, 2012, 11: 563-569.

[13] Walther P, Resch K J, Zeilinger A. Local conversion of Greenberger-Horne-Zeilinger states to approximate W states [J]. *Phys. Rev. Lett.*, 2005, 94: 240501.

[14] Bae J, Jin J, Kim J, *et al.* Three-party quantum teleportation with asymmetric states [J]. *Chaos, Solitons and Fractals*, 2005, 24: 1047-1052.

[15] Zhang Q Y, Zhan Y B, Zhang L L, *et al.* Schemes for splitting quantum information via tripartite entangled states [J]. *Int. J. Theor. Phys.*, 2009, 48: 3331-3338.

[16] Zhan Y B, Zhang Q Y, Wang Y W, *et al.* Schemes for teleportation of an unknown single-qubit quantum state by using an arbitrary high-dimensional entangled state [J]. *Chin. Phys. Lett.*, 2010, 27(1): 010307.