文章编号：0253-2239(2008)03-0556-04

# 束缚纠缠态量子秘密共享的不安全性分析

於亚飞 张智明*

（华南师范大学信息光电子科技学院 广东省光子信息技术重点实验室，广东 广州 510006）

**摘要** 分析了以 Smolin 束缚纠缠态作为通道量子态的量子秘密共享方案的安全性。给出了一个简单的来自通信方内部的截获重发攻击策略，这个攻击策略是依赖比对单量子比特测量结果的窃听检测程序所不能检测出来的。结果表明，仅以束缚纠缠 Smolin 态作为通道量子态的量子秘密共享方案对于来自内部的窃听攻击不是无条件的。

**关键词** 量子光学；量子信息；量子秘密共享；束缚纠缠 Smolin 态；独立相干攻击

**中图分类号** O413 **文献标识码** A

# Analysis on Unsecurity of Quantum Secret Sharing Based on Smolin Bound Entangled States

Yu Yafei Zhang Zhiming

(*Guangdong Provincial Key Laboratory of Photonic Information Technology, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou, Guangdong* 510006, *China*)

**Abstract** We analyze the security of quantum secret sharing (QSS) with bound entangled Smolin states as the channel quantum state. An intercept-resend strategy of the inner legal communicators is proposed to attack the security without being detected by the checking procedure compared with the results of single-qubit measurement. It is concluded that QQS only with Smolin bound entangled states as the channel quantum state is not unconditionally secure.

**Key words** quantum optics; quantum information; quantum secret sharing; bound entangled Smolin state; coherent individual attack

## 1 引 言

近十几年来关于量子纠缠在量子信息过程中的研究取得了蓬勃发展，量子离物传态[1,2]是量子纠缠在信息传输过程中最重要的应用。量子离物传态是以自由的量子纠缠作为量子通道，借助量子操控和经典通信使量子态脱离原来的承载系统而在另一个量子系统中出现。自由的量子纠缠是指可以借助局域操作和经典通信的手段从纠缠态中提取出 Einstein-Podolsky-Rosen (EPR) 纠缠态；量子世界中还存在一种利用局域操作和经典通信的方法不能从中提纯出 EPR 纠缠态的束缚纠缠态[3]。由于束缚纠缠态的不可提纯性质，束缚纠缠对处理量子信息似乎是无用的，但近年来理论研究发现一类束缚纠缠态可以作为通道量子态应用于纠缠凝聚过程，所取得的效果明显优于 Greenberger-Horne-Zeilinger (GHZ) 态和 W 态[4~6]。关于束缚纠缠态是否可以用于量子安全通信的问题也被深入地讨论，Horodechi 等的研究表明可以从束缚纠缠态中提取安全的密钥，束缚纠缠可以应用于量子密钥分发(Quantum key distribution)[7]；Augusiak 等发现束缚纠缠 Smolin 态能够最大违背两设置 Bell 不等式，并讨论了将这类束缚纠缠态应用于量子秘密共享(Quantunm secret sharing, QSS)[8,9]的可行性。不同于量子密钥分发过程，量子秘密共享[10~12]是多方(三方及三方以上)通信过程，不但要排除外部的窃听行为，还要防范通信各方潜在的内部欺骗行为，所以量子秘密共享过程对所使用的通道量子态的纠缠特征有更为严格的要求。本文研究了基于 Smolin 束缚纠缠态的量子秘密共享方案的安全性，发现这种方案虽能够有效地对抗来自外部的窃听，

**收稿日期**：2007-07-11；**收到修改稿日期**：2007-10-08

**基金项目**：国家自然科学基金(10404007,60578055)资助课题。

**作者简介**：於亚飞(1975—)，女，副教授，主要从事理论物理教学和量子信息方面的研究。E-mail：yfyuks@yahoo.com.cn

* 通信联系人。E-mail：zmzhang@scnu.edu.cn

但对来自通信方内部的截获重发攻击却是非常脆弱的。给出一个 Smolin 束缚纠缠态量子秘密共享的内部截获重发攻击方案，理论证明了基于 Smolin 束缚纠缠态的量子秘密共享方案不是无条件安全的。

## 2　Smolin 束缚纠缠态量子秘密共享的内部截获重发攻击

Smolin 束缚纠缠态是一类不可锁束缚纠缠态，即在允许两体间的联合操作时可从中提纯出 Bell 纠缠态[13]。一个四体 Smolin 束缚纠缠态可表示为

$$\begin{aligned}\rho_{ABCD}=\frac{1}{4}(&|\Phi^+\rangle_{AB}\langle\Phi^+|\otimes|\Phi^+\rangle_{CD}\langle\Phi^+|+\\&|\Phi^-\rangle_{AB}\langle\Phi^-|\otimes|\Phi^-\rangle_{CD}\langle\Phi^-|+\\&|\Psi^+\rangle_{AB}\langle\Psi^+|\otimes|\Psi^+\rangle_{CD}\langle\Psi^+|+\\&|\Psi^-\rangle_{AB}\langle\Psi^-|\otimes|\Psi^-\rangle_{CD}\langle\Psi^-|),\end{aligned}\quad(1)$$

其中 $|\Phi^{\pm}\rangle$ 和 $|\Psi^{\pm}\rangle$ 分别表示四个 Bell 态。显然，量子比特 $C$ 和 $D$ 上的联合 Bell 测量会使分离的量子比特 $A$ 和 $B$ 处于与测量结果相同的 Bell 态上。四个量子比特间存在着关联：假设任意选取一个泡利(Pauli)算子对每个量子比特进行测量，分别得到一个 $r_i\in\{0,1\}$，$i=A,B,C,D$，则 $r_A\oplus r_B\oplus r_C\oplus r_D=0$($\oplus$ 表示模 2 加)。每个 $r_i$ 的取值都是随机的，只能通过比对其他量子比特上的测量输出 $r_j(j\neq i)$ 的取值来决定。

假设四个量子比特 $A,B,C,D$ 分别由进行通信的四方 Alice，Bob，Charlie 和 Diana 所持有，其中 Alice 则利用这个 Smolin 态作为通道量子态使 Bob，Charlie 和 Diana 共享她的秘密信息。通信的四方各任选一个 Pauli 算子对其持有的量子比特进行投影测量，并公布所选的 Pauli 算子。与量子密钥分发 EPR 协议[14]类似，相同的测量基下的测量结果将用来在通信各方之间建立密钥。这个量子秘密共享方案能够有效对抗外部的窃听[8]。假设存在一个窃听者 Evan 采用相干独立攻击，若窃听不引入错误，由四量子比特系统和窃听系统组成的复合系统将演化到 $|\Omega\rangle=\frac{1}{\sqrt{4}}\sum_{i=1}^{4}|\Psi^i_{ABCD}\rangle|\phi^i_E\rangle$，其中 $|\Psi^i_{ABCD}\rangle(i=1,2,3,4)$ 表示 Smolin 态 $\rho_{ABCD}$ 的四个本征态，$|\phi^i_E\rangle$ 表示区分每个本征态的窃听系统状态。将复合系统的量子态 $|\Omega\rangle$ 对量子比特 $B,C,D$ 求迹，得到 $\rho_{AE}=\rho_A\otimes\rho_E$。因为 $\rho_{AE}$ 是个直积态，Evan 的窃听系统与量子比特 $A$ 并没有量子关联，Alice 的单量子比特测量不影响窃听系统地量子态，所以 Evan 从窃听系统中得不到 Alice 的秘密信息。

对于一个来自通信方内部的窃听攻击，这个方案是十分脆弱的，一个不忠诚的秘密分享者可以简单地利用截获重发策略成功击破其安全性[15]。假设这个不忠诚的秘密分享者是 Bob。在 Alice 向 Bob，Charlie 和 Diana 发送量子比特 $B$，$C$ 和 $D$ 的过程中 Bob 截获量子比特 $C$ 和 $D$，这样他拥有量子比特 $B$，$C$ 和 $D$。Bob 对 Alice 发来的每个序列中的量子比特 $C$ 和 $D$ 做联合 Bell 测量，使量子比特 $B$ 和 $A$ 纠缠起来，并处于与测量结果相同的 Bell 态上。Bob 记录下每个序列中的 Bell 测量结果，并根据测量结果重新制备一对最大纠缠的量子比特 $C'$ 和 $D'$ 发送给 Charlie 和 Diana。从(1)式可以看出束缚纠缠 Smolin 态是两个相同 Bell 态矢量直乘的四种形式的等概率混合。可以解释为，某人制备了两对处于相同 Bell 态的量子比特，却忘记了具体是四个 Bell 态中的哪一个。如果他对其中一对量子比特做 Bell 测量，他就能知道另一对纠缠量子比特的具体 Bell 态形式。所以 Bob 在 Bell 基下测量量子比特 $C$ 和 $D$ 后，他立即知道他和 Alice 之间共享的 Bell 态的具体形式，因此在发送量子比特 $C'$ 和 $D'$ 之后每一个序列中通信四方共享的量子态对 Bob 而言只是两个相同 Bell 态的矢量直积。但是对于 Alice，Charlie 和 Diana，由于缺乏 Bell 测量结果的信息，每个序列中共享的量子态还是两个相同 Bell 态矢量直积的四种形式的等概率混合，即 Bob 的 Bell 测量没有改变通信四方共享的 Smolin 态。这与使用纠缠 GHZ 态作为信道量子态的情况不同；在使用 GHZ 态作为信道量子态的量子秘密共享方案中 Bob 的测量将使通信方共享的量子态由 GHZ 纠缠纯态变演为一个混合量子态，引入大量错误，在检测窃听的过程中 Bob 的截获重发会被发现。但在使用 Smolin 纠缠态作为通道量子态的量子秘密共享方案中，Bob 的测量行为不改变共享的通道量子态，常规检测不能发现 Bob 的窃听行为；Bob 只要像一个诚实的通信者一样选择测量基测量自己的粒子并公布测量结果。在 Alice 公布用于建立密钥的序列号和测量基之后，Bob 根据在相应序列的 Bell 测量结果知道量子比特 $B$ 和量子比特 $A$ 的关联状态，从而由单量子比特测量结果推知 Alice 的密钥而不需要其他通信方的帮助。

基于一般束缚纠缠 Smolin 态更多通信方的量子秘密共享方案，截获重发策略也可击破其安全性，不同的是 Bob 需要做更多的两体 Bell 测量来确定

Bob 和 Alice 之间的纠缠状态。一般的多体纠缠 Smolin 态可以表达为一种递归形式[8]

$$\rho_4 = \frac{1}{4}\sum_{m=0}^{3} U_2^m \rho_2 U_2^m \otimes U_2^m \rho_2 U_2^m ,$$

$$\rho_{2(n+1)} = \frac{1}{4}\sum_{m=0}^{3} U_{2n}^m \rho_{2n} U_{2n}^m \otimes U_2^m \rho_2 U_2^m , \quad (2)$$

其中 $\rho_2 = |\Psi^-\rangle\langle\Psi^-|$，$U_{2n}^m = I^{\otimes(2n-1)} \otimes \sigma_m$（$m = 0, 1, 2, 3$，$n = 1, 2, 3, \cdots$）表示对第 $2n$ 个粒子做 Pauli 算子 $\sigma_m$ 操作，其中 $\sigma_0 = I$。从这种递归的表示中可看出，对 $2(n+1)$ 个粒子的 Smolin 纠缠态，通过将其中 $2n$ 个粒子两两配对进行 Bell 测量，会使剩下的两个分离的粒子处于确定的 Bell 态上。Bob 截获所有 Alice 发送的粒子，并两两配对作 Bell 测量，根据测量结果，确定出自己和 Alice 之间所共享的 Bell 态，并按测量结果制备 Bell 态重新发送给合法接收者。与利用四体 Smolin 态的情况相同，Bob 通过这些 Bell 测量能够确定他与 Alice 之间共享的 Bell 态，从而当用于建立密钥的测量基公布出来的时候 Bob 可以根据单量子比特测量结果推知 Alice 的密钥而不需其他通信方的协助；相对于其他的通信方，由于缺乏 Bell 测量结果的信息，通信各方共享的还是 $2(n+1)$ 粒子的 Smolin 态，因此 Bob 无需额外的操作来逃避窃听检测，只要按照诚实的通信方的行为选择测量基做单量子比特测量并如实公布测量结果。

## 3 Smolin 束缚纠缠态量子秘密共享不安全性的证明

虽然研究发现可以从束缚纠缠态中提纯出安全的密钥，并且束缚纠缠 Smolin 态能够最大违背一类 Bell 不等式，但是上述的攻击方案说明量子秘密共享不像量子密钥分发是简单一对一通信，由于涉及的通信方增多，其安全性不是仅仅由信道量子态对 Bell 不等式的违背所能保证的。在此，采用文献[16]的方法以四粒子束缚纠缠 Smolin 态为例证明基于束缚纠缠 Smolin 态的量子秘密共享方案对来自于内部的相干独立攻击是不安全的。Bob 的最佳的相关独立攻击是让其辅助系统和 Alice 发送的三粒子 $BCD$ 系统共同经历一个幺正操作，这个幺正操作使四粒子 $ABCD$ 系统和辅助系统的量子态演化到一个新的量子态。

$$\begin{aligned}\rho_{ABCD} \otimes |\varphi\rangle_a\langle\varphi| \xrightarrow{U} |\Theta\rangle = \frac{1}{\sqrt{8}}\{&(|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_D + |1\rangle_A|1\rangle_B|1\rangle_C|1\rangle_D) \otimes |\varphi^1\rangle_a + \\ &(|0\rangle_A|1\rangle_B|0\rangle_C|1\rangle_D + |1\rangle_A|0\rangle_B|1\rangle_C|0\rangle_D) \otimes |\varphi^2\rangle_a + \\ &(|0\rangle_A|0\rangle_B|1\rangle_C|1\rangle_D + |1\rangle_A|1\rangle_B|0\rangle_C|0\rangle_D) \otimes |\varphi^3\rangle_a + \\ &(|0\rangle_A|1\rangle_B|1\rangle_C|0\rangle_D + |1\rangle_A|0\rangle_B|0\rangle_C|1\rangle_D) \otimes |\varphi^4\rangle_a\}, \end{aligned} \quad (3)$$

其中，

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_D + |1\rangle_A|1\rangle_B|1\rangle_C|1\rangle_D)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B|0\rangle_C|1\rangle_D + |1\rangle_A|0\rangle_B|1\rangle_C|0\rangle_D)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|1\rangle_C|1\rangle_D + |1\rangle_A|1\rangle_B|0\rangle_C|0\rangle_D)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B|1\rangle_C|0\rangle_D + |1\rangle_A|0\rangle_B|0\rangle_C|1\rangle_D)$$

是四粒子 Smolin 态 $\rho_{ABCD}$ 的四个本征态，而 $|\varphi^i\rangle (i = 1, 2, 3, 4)$ 是辅助系统与这四个本征态分别对应的正交归一量子态。将复合系统量子态 $|\Theta\rangle$ 对粒子 $C$ 和 $D$ 求迹得到

$$\begin{aligned}\rho_{ABa} = \frac{1}{4}\Bigg\{&\frac{(|\varphi^1\rangle_a + |\varphi^3\rangle_a)}{\sqrt{2}}\frac{({}_a\langle\varphi^1 + {}_a\langle\varphi^3|)}{\sqrt{2}} \otimes |\Phi^+\rangle_{AB}\langle\Phi^+| + \\ &\frac{(|\varphi^1\rangle_a - |\varphi^3\rangle_a)}{\sqrt{2}}\frac{({}_a\langle\varphi^1 - {}_a\langle\varphi^3|)}{\sqrt{2}} \otimes |\Phi^-\rangle_{AB}\langle\Phi^-| + \\ &\frac{(|\varphi^2\rangle_a + |\varphi^4\rangle_a)}{\sqrt{2}}\frac{({}_a\langle\varphi^2 + {}_a\langle\varphi^4|)}{\sqrt{2}} \otimes |\Psi^+\rangle_{AB}\langle\Psi^+| + \end{aligned}$$

$$\frac{(|\varphi^2\rangle_a - |\varphi^4\rangle_a)}{\sqrt{2}} \frac{({}_a\langle\varphi^2| - {}_a\langle\varphi^4|)}{\sqrt{2}} \otimes |\Psi^-\rangle_{AB}\langle\Psi^-|, \tag{4}$$

其中粒子 $A$ 为 Alice 所持有，而粒子 $B$ 和辅助系统 $a$ 均为 Bob 所持有，很明显 Bob 对辅助系统 $a$ 的局域测量使粒子 $A$ 和 $B$ 处于最大纠缠态，即 Bob 的局域操作可在系统 $AB$ 上产生纠缠，所以混合态 $\rho_{ABa}$ 是 $A-Ba$ 纠缠的。Bob 系统（粒子 $B$ 和辅助系统 $a$）与 Alice 系统之间存在量子关联，Bob 系统的状态依赖于 Alice 对粒子 $A$ 的测量结果，从而 Bob 可以非法获得 Alice 的秘密信息。

综上所述，基于四粒子束缚纠缠 Smolin 态的量子秘密共享方案对于来自内部的攻击不是无条件安全的；基于一般束缚纠缠 Smolin 态的量子秘密共享方案不是无条件安全的证明可以用相同的方法获得。

## 4 结　论

分析了基于 Smolin 束缚纠缠态的量子秘密共享方案的安全性。给出了一个简单的来自通信方内部的截获重发攻击策略，这个攻击策略是常规的窃听检测程序所不能检测出来的。得出了基于束缚纠缠 Smolin 态的量子秘密共享方案对于来自内部的窃听攻击不是无条件安全的结论，并对此给出了一般性的证明。由此可见，涉及多方的量子安全通信情况复杂，由于纠缠混合态的纠缠结构和可提纯性的影响，在运用纠缠混态作为多方量子安全通信的量子通道时须十分谨慎。

## 参 考 文 献


1 Charles H. Bennett, Gilles Brassard, Clauale Crepeau *et al*.. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels[J]. *Phys. Rev. Lett.*, 1993, **70**(13): 1895～1899

2 Xiaoqin Su, Guangcan Guo. Quantum teleportation[J]. *Progress in Physics*, 2004, **24**(3): 259～273
苏晓琴，郭光灿. 量子隐形传态[J]. 物理学进展, 2004, **24**(3): 259～273

3 Michal Horodecki, Pawel Horodecki, Ryszard Horodecki. Mixed-state entanglement and distillation: is there a "bound" entanglement in nature? [J]. *Phys. Rev. Lett.*, 1998, **80**(24): 5239～5242

4 Mio Murao, Vlatko Vedral. Remote information concentration using a bound entangled state[J]. *Phys. Rev. Lett.*, 2001, **86**(2): 352～355

5 Yafei Yu, Jian Feng, Mingsheng Zhan. Remote information concentration by a Greenberger-Horne-Zeilinger state and by a bound entangled state[J]. *Phys. Rev. A*, 2003, **68**(2): 024303-1～024303-3

6 Yinhua Chen, Yafei Yu, Zhiming Zhang. Entangled states used in remote information concentration and their properties[J]. *Chin. Phys. Lett.*, 2006, **23**(12): 3158～3160

7 Karol Horodecki, Michal Horodecki, Pawel Horodecki *et al*.. Secure key from bound entanglement[J]. *Phys. Rev. Lett.*, 2005, **94**(16): 160502-1～160502-4

8 Remigiusz Augusiak, Pawel Horodecki. Generalized Smolin states and their properties[J]. *Phys. Rev. A*, 2006, **73**(1): 012318-1～012318-10

9 Remigiusz Augusiak, Pawel Horodecki. Bound entanglement maximally violating Bell inequalities: quantum entanglement is not fully equivalent to cryptographic security[J]. *Phys. Rev. A*, 2006, **74**(1): 010305-1～010305-4

10 Mark Hillery, Vladimír Bužek, André Berthiaume. Quantum secret sharing[J]. *Phys. Rev. A*, 1999, **59**(3): 1829～1834

11 Han Lianfang, Liu Yimin, Zhang Zhanjun. Multiparty quantum secret sharing of classical message using cavity quantum electrodynamic system[J]. *Chin. Phys. Lett.*, 2006, **23**(8): 1988～1991

12 Yang Yuguang, Wen Qiaoyan, Zhu Fuchen. Single $N$ dimensional qubit quantum secret sharing[J]. *Acta Physica Sinica*, 2006, **55**(7): 3255～3258
杨宇光，温巧燕，朱甫臣. 单个 $N$ 维量子系统的量子秘密共享[J]. 物理学报, 2006, **55**(7): 3255～3258

13 John A. Smolin. Four-party unlockable bound entangled state[J]. *Phys. Rev. A*, 2001, **63**(3): 032306-1～032306-4

14 Artur K. Ekert. Quantum cryptography based on Bell′s theorem[J]. *Phys. Rev. Lett.*, 1991, **67**(6): 661～663

15 Yafei Yu. Comment on "Generalized Smolin states and their properties"[J]. *Phys. Rev. A*, 2007, **75**(6): 066301-1～066301-2

16 Aditi Sen, Ujjwal Sen, Marek Zukowski. Unified criterion for security of secret sharing in terms of violation of Bell inequalities[J]. *Phys. Rev. A*, 2003, **68**(3): 032309-1～032309-7