第 55 卷 第 7 期 2006 年 7 月
1000-3290/2006/55(07)/3255-04

物 理 学 报
ACTA PHYSICA SINICA

Vol.55,No.7,July,2006


# 单个 $N$ 维量子系统的量子秘密共享*

杨宇光[1)†] 温巧燕[1)] 朱甫臣[2)]

1)(北京邮电大学理学院,北京 100876)

2)(现代通信国家重点实验室,成都 610041)

(2005 年 3 月 25 日收到;2005 年 6 月 16 日收到修改稿)

提出了一种单个 $N$ 维量子系统的量子秘密共享方案.在该方案中,利用对 Bennett 和 Brassard 协议(BB84 协议)中使用的两基四态扩展到多基多态,分发者对要共享的秘密采用多基多态编码,将被编码的单个 $N$ 维量子系统发送给他的两个代理人之一,该代理人利用一个 $N$ 维克隆机对接收到的粒子做幺正操作,然后把粒子发送给另一代理人.在得知最后一个代理人接收到该粒子之后,分发者告知两个代理人他所用的制备基,然后两个代理人分别对自己的系统进行测量并在合作之后获知分发者所发送的粒子的量子态.该方案的安全性基于量子不可克隆定理.另外该方案还具有信息量大效率高的特点.最后对该方案从两方扩展到 $N$ 方进行了讨论.

**关键词**:量子秘密共享,多基多态编码,$N$ 维克隆机,量子不可克隆定理

**PACC**:0365

## 1. 引 言

把一个秘密消息分割使得单个人不能重构该秘密消息是信息处理特别是高安全应用中常见的任务.现代密码学[1]提供了解决方案——秘密共享.它利用数学算法分割消息并将产生的块利用经典通信分发给两个或多个合法用户.然而目前使用的所有经典通信方式易于受到窃听攻击且不易被合法用户检测到.幸运地是,量子秘密共享协议[2—5]可以利用多光子纠缠实现信息安全分发.最近,人们提出了许多利用纠缠的量子秘密共享协议[6—8].量子密钥分发(QKD)[9]和经典秘密共享协议的结合也可以实现安全的秘密共享.量子秘密共享协议通过使合法用户能够确定在秘密共享过程中是否存在窃听来提供安全的秘密共享.但实现这种多方秘密共享[2,6]不太容易,这是因为制备甚至三方或四方纠缠态的效率都是非常低的,同时利用量子纠缠的现有的量子秘密共享协议的效率仅仅达到 50%.

最近,Guo 和 Guo[10]已提出了一种没有纠缠的量子秘密共享协议.他们直接对量子密钥分发协议的量子比特编码并把一个消息分割成许多部分来仅仅利用乘积态达到多方秘密共享.该理论效率达到 100%.还有其他没有纠缠的量子秘密共享协议被提出[11,12].目前大多数研究集中在基于两维量子变量(量子比特)的量子秘密共享.对于高维系统,所得到的研究成果很少.

本文提出了一种单个 $N$ 维量子系统的量子秘密共享方案.在该方案中,利用对 Bennett 和 Brassard 协议(BB84 协议)中使用的两基四态扩展到多基多态,分发者对要共享的秘密采用多基多态编码,将被编码的单个 $N$ 维量子系统发送给他的两个代理人之一,该代理人利用一个 $N$ 维克隆机对接收到的粒子做幺正操作,然后把粒子发送给另一代理人.在得知最后一个代理人接收到该粒子之后,分发者告知两个代理人他所用的制备基,然后两个代理人分别对自己的系统进行测量并在合作之后获知分发者所发送的粒子的量子态.该方案的安全性基于量子不可克隆定理.另外该方案还具有信息量大效率高的特点.最后对该方案从两方扩展到 $N$ 方进行了讨论.

## 2. $N$ 维量子系统的量子秘密共享方案

利用对 Bennett 和 Brassard 协议(BB84 协议)中使用的两基四态扩展到多基多态,分发者首先从 $M$

* 国家自然科学基金(批准号:60373059,90604023),教育部博士点基金(批准号:20040013007)资助的课题.

† E-mail:yangyang7357@sina.com

个互补基中随机选取一个基,然后从该基的 $N$ 个正交归一化态中随机选取一个态来编码他的经典秘密.$M$ 个基以及每一基中的 $N$ 个正交归一化态的选取都是等概率的,也就是说 $NM$ 个态中每一个态出现的概率均为 $1/(MN)$.我们首先在 $N$ 维空间上定义基 $\{\varphi\}$ 和 $\{\psi\}$ 是相互互补的,条件是所有可能的矢量(不同基中的态)对之间的内积具有相同的大小,即

$$|\langle\varphi_i|\psi_j\rangle| = 1/\sqrt{N} \quad i,j = 0,1,\cdots,N-1, \tag{1}$$

如果一个量子态制备在 $\{\varphi\}$ 基,但在互补基($\psi$)上被测量,那么所得结果是完全随机的.Wootters 和 Fields[13] 已表明,当 $N = p^k$($p$ 是质数且 $k$ 是一个正整数)时,存在一组 $M = N+1$ 个相互互补的基[13].

### 2.1. $N$ 维量子系统的量子秘密共享方案

在该方案中,第一个接收者使用 Bužek 和 Hillery[14] 提出的 $N$ 维对称通用量子克隆机的不对称模型对接收到的 $N$ 维粒子作幺正操作.该不对称克隆机[15,16] 可以用来得到具有不同忠实度的分发者的量子态的两个拷贝.接收者保留一个拷贝,将另一拷贝发送给另一接收者.然后,在分发者公布他的制备基之后,这两个接收者使用所公布的基对自己的系统测量.实现该不对称克隆机的量子电路见文献[17].

我们分析一下第一个接收者使用诸如文献[15,16]中所述的 $N$ 维克隆机的情形.如果分发者把被编码的 $|\varphi_k\rangle$ 发送给第一个接收者,该接收者使用 UQCM 对接收到的 $N$ 维粒子作幺正操作,输出的态为

$$|\varphi_k\rangle_s \to \sum_{m,n=0}^{N-1} a_{m,n} U_{m,n} |\varphi_k\rangle_2 |\Phi_{m,N-n}\rangle_{1M}, \tag{2}$$

其中幅度 $a_{m,n}$($m,n = 0,1,\cdots,N-1$) 表明克隆机,$s$,2,1 和 $M$ 分别代表分发者、第二个接收者、第一个接收者和克隆机.在这儿 $|\Phi_{m,n}\rangle_{1M}$,是推广的 Bell 态,也就是一组两个 $N$ 维系统的 $N^2$ 个正交归一化的最大纠缠态:

$$|\Phi_{m,n}\rangle_{1M} = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{2\pi i(ln/N)} |\varphi_l\rangle_1 |\varphi_{l+m}\rangle_M, \tag{3}$$

其中 $m$ 和 $n$($m,n = 0,1,\cdots,N-1$) 表明 $N^2$ 个态.在这儿以及下面,态矢标志模 $N$.算子 $|U_{m,n}\rangle$ 被定义为

$$|U_{m,n}\rangle = \sum_{k=0}^{N-1} e^{2\pi i(kn/N)} |\varphi_{k+m}\rangle\langle\varphi_k|. \tag{4}$$

它形成了 $N$ 维态上的一个错误算子群,推广了适于量子比特的 Pauli 矩阵:$m$ 表示'位移'错误(推广了比特翻转 $\sigma_x$),$n$ 表示相位错误(推广了相位翻转 $\sigma_y$).使用 $|\Phi_{m,n}\rangle$ 和 $|U_{m,n}\rangle$ 的定义,方程(2)可以重新表示为

$$|\varphi_k\rangle_s \to \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} |\varphi_{k+m}\rangle_2 \sum_{l=0}^{N-1} c_{m,k-l} |\varphi_l\rangle_1 |\varphi_{l+m}\rangle_M, \tag{5}$$

其中

$$c_{m,j} = \sum_{n=0}^{N-1} a_{m,n} e^{2\pi i(jn/N)}. \tag{6}$$

现在,令上述的克隆机是通用的,也就是[15,16]

$$a_{m,n} = \alpha\delta_{m,0}\delta_{n,0} + \frac{\beta}{N}, \tag{7}$$

归一化关系为

$$\alpha^2 + \frac{2}{N}\alpha\beta + \beta^2 = 1, \tag{8}$$

其中 $\alpha$ 与 $\beta$ 确定了不对称克隆机的参数.

$c_{m,j}$ 可以重新写为

$$c_{m,j} = \alpha\delta_{m,0} + \beta\delta_{j,0}, \tag{9}$$

因此我们得到了克隆变换

$$\begin{aligned}|\varphi_k\rangle_s \to & \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} |\varphi_{k+m}\rangle_2 (\alpha\delta_{m,0} \sum_{l=0}^{N-1} |\varphi_l\rangle_1 |\varphi_l\rangle_M \\ & + \beta|\varphi_k\rangle_1 |\varphi_{k+m}\rangle_M \\ = & |\varphi_k\rangle_2 \Big( \frac{\alpha}{\sqrt{N}} \sum_{l=0}^{N-1} |\varphi_l\rangle_1 |\varphi_l\rangle_M \\ & + \frac{\beta}{\sqrt{N}} |\varphi_k\rangle_1 |\varphi_k\rangle_M \Big) \\ & + \sum_{m=0}^{N-1} |\varphi_{k+m}\rangle_2 \Big( \frac{\beta}{\sqrt{N}} |\varphi_k\rangle_1 |\varphi_{k+m}\rangle_M \Big). \end{aligned} \tag{10}$$

该方案描述如下:

1) 分发者从 $M$ 个互补基中随机选取一个基,然后从该基的 $N$ 个正交归一化态中随机选取一个态来编码他的经典秘密.然后把编码的 $N$ 维粒子发送给第一个接收者.

2) 第一个接收者使用 UQCM 对接收到的 $N$ 维粒子作幺正操作,将其中一个拷贝发送给第二个接收者.

3) 在第二个接收者接收到该 $N$ 维粒子之后,他宣布他已接收到.

4) 分发者通过一公开信道公布他的制备基.

5) 这两个接收者使用与分发者相同的基测量自己的粒子,也就是,第一个接收者对他的拷贝和克隆机作相关测量,第二个接收者对他的拷贝测量.

6) 通过合作,两个接收者得到共享的秘密信息.

7) 重复以上步骤,生成所需要的数量.

8) 为了检测是否存在窃听或欺骗的攻击,分发者随机地选取已发送的 $N$ 维粒子所在位置的一个子集,他宣布该子集中的位置序号.然后这两个接收者分别宣布他们的测量结果(宣布他们测得的量子态,而不是经典密钥).这两个接收者在每一粒子位置宣布他们的测量结果的顺序由分发者随机决定.如果没有窃听或欺骗存在,分发者所分发的态和两个接收者的测量结果满足(10)式的相关性,否则他们放弃所获得的结果,重新开始协议.

### 2.2. 协议的安全性分析

假设一个偷听者 Eve 先截取分发者所发送的 $N$ 维量子态并对之进行测量,然后将之发送给第一个接收者 $R_1$,或者第一个接收者 $R_1$ 试图通过在对分发者所发送的量子态作幺正操作之前测量该量子态来推断所发送的态而没有第二个接收者 $R_2$ 的帮助或授权.我们假设 Eve($R_1$)从 $M$ 个基中选择一个基对接收到的态进行测量.由于发送者是随机地从 $NM$ 个态中选取的,所发送的态是 Eve($R_1$)所选择的基的本征态的概率为 $1/M$.在 $(M-1)/M$ 的概率下,Eve($R_1$)的测量结果将是随机的,它满足 $|\langle\varphi_i|\psi_j\rangle| = 1/\sqrt{N}$.这意味着 Eve($R_1$)不能获得分发者所发送的态的信息.在步骤(8),假设分发者随机选取了 $n$ 个位置进行检测,Eve($R_1$)偷听不被检测到的概率为 $P_1 = \left(\frac{1}{M} + \frac{M-1}{M} \times \frac{\alpha^2 + \beta^2}{N^3}\right)^n$.但在这种情况下,Eve($R_1$)得不到分发者所发送的量子态的信息.只会带来被检测到的风险.

假设第一个接收者是不诚实的.他还可以采取另一欺骗策略.从(10)式可以看出,如果第一个接收者测量他的拷贝和克隆机且发现这两个结果不一致,那么他可以得到正确的态而不需要第二个接收者的帮助,我们可以计算出第一个接收者得到正确的态的概率为 $P_s = \frac{N-1}{N}\beta^2$.在步骤(8),假设分发者随机选取了 $n$ 个位置进行检测,第一个接收者欺骗成功且不被检测到的概率为 $P_2 = (1 - P_s)^n$.为了尽可能地减小这种欺骗攻击,我们应适当地选取 $\alpha$ 和 $\beta$ 的值.另外,我们可以让分发者将每一编码的 $N$ 维粒子随机地发送给一个接收者.

从该方案可以看出它还具有信息量大以及效率高等特点,这是由于除了用于检测的密钥之外剩余的密钥都是有用的.另外,每一 $N$ 维粒子代表了 $\log_2 N$ 个比特的信息.

## 3. 从两个接收者到 $N$ 个接收者的推广

现在我们考虑从两个接收者到 $N$ 个接收者的推广.这 $N$ 个接收者可以被标号为 $R_1, R_2, \cdots, R_n$.在每一轮,分发者将编码的 $N$ 维粒子随机发送给 $N$ 个接收者之一.为简化而不失一般性,每一接收者所使用的克隆机具有相同的参数.每一接收者(除了最后一个接收者)按序对接收到的 $N$ 维粒子作幺正操作,并将之发送给下一个接收者.包含 $N$ 个接收者的协议类似于两个接收者的协议,他们同样利用所测得的态之间的相关性检测窃听和欺骗.$N$ 个接收者对发送者所发送的态的克隆变换是(10)式的简单推广,具体表达式不再列出.随着接收者数量的增多,窃听或欺骗成功的概率越来越小.

## 4. 结　论

本文提出了一种单个 $N$ 维量子系统的量子秘密共享方案.在该方案中,利用对 Bennett 和 Brassard 协议(BB84 协议)中使用的两基四态扩展到多基多态,分发者对要共享的秘密采用多基多态编码,将被编码的单个 $N$ 维量子系统发送给他的两个代理人之一,该代理人利用一个 $N$ 维克隆机对接收到的粒子做幺正操作,然后把粒子发送给另一代理人.在得知最后一个代理人接收到该粒子之后,分发者告知两个代理人他所用的制备基,然后两个代理人分别对自己的系统进行测量并在合作之后获知分发者所发送的粒子的量子态.该方案的安全性基于量子不可克隆定理.另外该方案还具有信息量大效率高的特点.最后对该方案从两方扩展到 $N$ 方进行了讨论.

由于该方案没有使用高维纠缠态,因此实现起来相对要容易一些,并且可以在较长的距离内传送量子态.

[1] Schneier B 1996 *Applied Cryptography* (John Wiley & Sons, Inc.)
[2] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[3] Tittel W, Zbinden H, Gisin N 2001 *Phys. Rev.* A **63** 042301
[4] Gottesman D 2000 *Phys. Rev.* A **61** 042311
[5] Nasciment A C A, Quad J M, Imai H 2002 *Phys. Rev.* A **64** 042311
[6] Karlsson A, Koashi M, Imoto N 1999 *Phys. Rev.* A **59** 162
[7] Cleve R, Gottesmann D, Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[8] Karimipour V, Bahraminasab A, Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320
[9] Yang L, Wu L A, Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese) [杨 理、吴令安、刘颂豪 2002 物理学报 **51** 2446]
[10] Guo G P, Guo G C 2003 *Phys. Lett.* A **310** 247
[11] Christian S, Pavel T, Harald W arXiv: quant-ph/0502107
[12] Yan F L, Ting Gao arXiv: quant-ph/0502045
[13] Wootters W K, Fields B D 1989 *Ann. Phys.* **191** 363
[14] Bužek V, Hillery M 1998 *Phys. Rev. Lett.* **81** 5003
[15] Cerf N J 1998 *Acta Phys. Slov.* **48** 115
[16] Cerf N J 2000 *J. Mod. Opt.* **47** 187
[17] Braunstei S L, Bužek V, Hillery M 2001 *Phys. Rev.* A **63** 052313

# Single *N*-dimensional quNit quantum secret sharing*

Yang Yu-Guang[1)†] Wen Qiao-Yan[1)] Zhu Fu-Chen[2)]

1) (*School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876 *China*)

2) (*National Key Laboratory for Modern Communications, Chengdu* 610041, *China*)

(Received 25 March 2005; revised manuscript received 16 June 2005)

Abstract

A single *N*-dimensional quNit quantum secret sharing scheme is proposed. In this scheme, extending two bases and four states used in Bennett and Brassard protocol (BB84) to multi-bases and multi-states, a distributor sends the encoded *N*-dimensional quantum system to one of his two recipients. After receiving the quNit, the recipient makes a unitary operation on it using a *N*-dimensional cloning machine, and then sends it to the other recipient. After being informed that the second recipient has received the quNit, the distributor announces his preparing base, and then the two recipients perform measurements on their systems using the same base as the distributor and obtain the sent quantum state after collaboration. The security of the scheme is based on quantum non-cloning principle. In addition, this scheme has the features of great information flux and high efficiency. At last, the generalization from two recipients to *N* recipients is discussed.

**Keywords**: quantum secret sharing, multi bases and multi states encoding, *N*-dimensional cloning machine, quantum non-cloning principle

**PACC**: 0365

* Project supported by the National Natural Science Foundation of China (Grantss Nos. 60373059, 90604023) and the Doctoral Fund of Education Ministry of China (Grant No. 20040013007)

† E-mail: yangyang7357@sina.com