第 57 卷 第 5 期 2008 年 5 月
1000-3290/2008/57(05)/2680-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.5,May,2008

用非最大纠缠信道对任意二粒子纠缠态的量子秘密分享*

刘玉玲 满忠晓 夏云杰†

(曲阜师范大学物理工程学院,曲阜 273165)

(2007 年 4 月 15 日收到;2007 年 10 月 9 日收到修改稿)

提出一个对任意二粒子纠缠态在 N 者之间的量子秘密分享方案,该方案利用非最大纠缠 Einstein-Podolsky-Rosen(EPR)对作为量子信道,利用广义的贝尔基进行测量.接收者通过引入辅助粒子,并对其做选择性测量,就会概率性地得到最初的量子态.

关键词:非最大纠缠的 Einstein-Podolsky-Rosen(EPR)对,广义的贝尔测量

PACC:0365,4250

1. 引 言

秘密分享[1]最初的基本思想是发送者 Alice 把一个经典的秘密分成两部分,一部分给 Bob,一部分给 Charlie,他们两个人只有真诚合作其中一人(而不是两人)才能获得秘密,否则谁也无法得到.在经典物理中,一个经典信号可以毫无保留地不露任何蛛丝马迹地被复制,所以经典物理无法保证秘密分享的安全性.但是当量子力学进入信息领域之后,情况就改变了.量子秘密分享是量子通讯的一个重要分支,是经典秘密分享的推广.概括起来量子秘密分享有 3 个目标,1)用来在多个人中分配一个密钥(QKD)[2—8];2)用来分享一个经典秘密(QSS)[2,3,9—15];3)借助纠缠交换来分享一个未知的量子态(QSTS)[16—25],可控制的量子隐形传态[26—30]也属于此类.在空间分离的两个或多个人之间,QKD 确实提供了一个产生和分配密钥的安全方法.QSS 和 QKD 的区别[31]在于当存在多个人分享一个秘密时前者能够减少资源的利用,因此 QSS 比 QKD 更易实现[5].1999 年 Hillery,Buzek 和 Berthiaume[2]开创了 QSS 的先河,第一次分别用三个和四个粒子的 GHZ 态分享了一个经典秘密,后来被称为 HBB99 协议.此后很多 QSS 方案被提出,然而它们只注重分享一个或多个比特的经典信息[9—15].但是,在很多量子信息科学中,尤其是在量子计算中,需要分享或传递的是一个未知的量子态.因此本文将要论述与 QSS 有些不同,即一个未知量子态的秘密分享(QSTS)[16—30].最简单的 QSTS 只涉及到一个量子比特的分享[16,23,27],文献[17—22,24—26,28—30]推出了分享任意 $N(N\geqslant 2)$ 个比特的秘密,在上述文章中它们多数用的信道是处于最大纠缠的 EPR 对或 GHZ 态.但在实际情况中,由于产生纠缠态的仪器并不完美,因此信道不可能处于绝对的最大纠缠状态,这时通常是采取纯化的方式进行提纯,这样势必会造成资源的浪费.并且 Deng 等人[32]证明了传统的量子秘密分享(包括 QSS 和 QSTS)在噪声情况下是不安全的.另外上面多数方案采取的测量都是标准的 Bell 测量,这实际是对 Bell 测量的一种限制.Deng 等人[25]已经研究了利用最大纠缠的两光子对(EPR 对)完成高效率的量子态共享.为了不失一般性,下面我们对文献[25]进行推广,用处于非最大纠缠[33]的 EPR 对作为信道,用广义的 Bell 基进行测量,讨论任意两个纠缠粒子态的秘密分享.由于信道变为非最大纠缠状态,Bell 测量是广义的而不是标准的,所以我们为之而付出的代价是接收者收到的秘密是概率性的.但是经过接收者引入辅助粒子并做幺正操作 U_2 之后,接收概率会明显提高.

* 国家自然科学基金重点项目(批准号:10534030)资助的课题.

† 通信联系人. E-mail:yjxia@mail.qfnu.edu.cn

2. 用非最大纠缠 EPR 对在两者之间对任意二粒子纠缠态的量子秘密分享

首先，假定 Alice 有一个任意 2 个比特的秘密状态

$$|\chi\rangle_{ab} = \alpha|00\rangle_{ab} + \beta|01\rangle_{ab} + \gamma|10\rangle_{ab} + \delta|11\rangle_{ab}, \quad (1)$$

为了简单起见，先假定 Alice 有两个代理人，于是她想把这个秘密分成两部分，一部分给 Bob，一部分给 Charlie. 他们只有真诚合作，其中一个(而不是两个)才能得到这个秘密，否则谁也无法获得. 为此 Alice，Bob 和 Charlie 相邻的两者之间各分享一个 EPR 对其形式如下：

$$|Q\rangle_{ij} = \mu|01\rangle_{ij} + \nu|10\rangle_{ij}, \quad (2)$$

其中 $ij \in \{(1,2),(3,4),(5,6)\}$ $|\mu|^2 + |\nu|^2 = 1$. 同时我们也定义 4 个完全正交的 Bell 态也称广义的 Bell 态：

$$|B_{00}\rangle_{XY} = a|00\rangle_{XY} + b|11\rangle_{XY}, \quad (3)$$

$$|B_{11}\rangle_{XY} = b|00\rangle_{XY} - a|11\rangle_{XY}, \quad (4)$$

$$|B_{01}\rangle_{XY} = c|01\rangle_{XY} + d|01\rangle_{XY}, \quad (5)$$

$$|B_{10}\rangle_{XY} = d|01\rangle_{XY} - c|10\rangle_{XY}, \quad (6)$$

其中 $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$, ${}_{XY}\langle B_{ii'}||B_{jj'}\rangle_{XY} = \delta_{ii'}\delta_{jj'}$.

假定 Alice，Bob 和 Charlie 都能进行广义 Bell 态的测量(GBM).

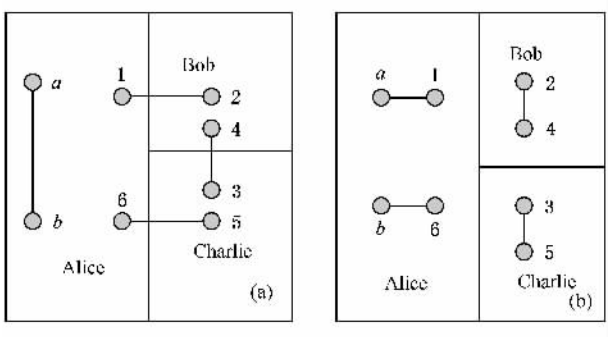

图 1　一个实心球代表一个粒子，实线代表粒子之间的纠缠

整个过程可以按照以下几步进行：

1) 首先 Alice 准备两对 EPR 对(1 和 2，5 和 6)，然后分别将粒子 2 与 5 发给 Bob 和 Charlie 图 1(a)，为了确保信道的安全性，Alice 会在其中掺入一部分诱骗光子[34—36] 使它们分别处于 $|0\rangle$，$|1\rangle$，$|+\rangle$ 和 $|-\rangle$ 态上，即将粒子 2 与 5 和诱骗光子一块分别发给 Bob 和 Charlie，也就是采取块传输[37] 的方法进行传递. 当 Bob 和 Charlie 收到所有粒子之后，Alice 告诉 Bob 和 Charlie 在什么位置进行测量并公布其测量结果，通过分析 Alice 会判断信道是否是安全的.

2) 我们假定 Charlie 想获得秘密，那么他就准备 EPR 对 3 和 4 并将 4 发给 Bob(图(a))，安全性检查与 1) 相同.

3) 当确定信道安全无误后，Alice 分别在粒子 a，1(用 ij 表示) 和 b，6(用 kl 表示) 上做 GBM 的测量，于此同时 Bob 在粒子 2，4 上做 GBM 的测量(用 mn 表示)(图(b)).

4) 根据他们的测量结果，Charlie 首先会选择合适的幺正操作 U_1 具体形式见表 1，分别在粒子 3，5 上操作，然后引入一个辅助粒子 A，让其初态处于 $|0\rangle_A$ 的状态，接着 Charlie 在粒子 3，5 和 A 上进行幺正操作 U_2 具体形式见表 2 的操作，这时 Charlie 会以一定的概率得到 $|\chi\rangle$.

为了从理论上详细地论述这一观点，我们可以把整个过程用以下公式表示：

$$\begin{aligned}|\psi\rangle &= |\chi\rangle_{ab}|Q\rangle_{12}|Q\rangle_{34}|Q\rangle_{56} \\ &= \sum_{i,j,k,l,m,n=0}^{l} |B_{ij}\rangle_{a1}|B_{kl}\rangle_{b6}|B_{mn}\rangle_{24} \\ &\quad \times |\phi_{ijklmn}\rangle_{35}, \end{aligned} \quad (7)$$

其中

$$\begin{aligned}|\phi_{ijklmn}\rangle_{35} &= \xi_{ijklmn}|00\rangle_{35} + \zeta_{ijklmn}|01\rangle_{35} \\ &\quad + \sigma_{ijklmn}|01\rangle_{35} + \tau_{ijklmn}|11\rangle_{35}. \end{aligned} \quad (8)$$

从表 1 中可以看到 U_1 为一些泡利矩阵的操作，U_2 的形式如下：

$$U_2 = \begin{bmatrix} A_1 & A_2 \\ A_2 & -A_1 \end{bmatrix} \quad (9)$$

其中

$$A_1 = \begin{bmatrix} a_0 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_3 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} \sqrt{1-a_0^2} & 0 & 0 & 0 \\ 0 & \sqrt{1-a_1^2} & 0 & 0 \\ 0 & 0 & \sqrt{1-a_2^2} & 0 \\ 0 & 0 & 0 & \sqrt{1-a_3^2} \end{bmatrix}.$$

表 1 Alice 和 Bob 的测量结果($ijklmn$)及 Charlie 所采取的相应的幺正变换 U_1 和 U_2

情况	$ijklmn$	U_1	U_2	情况	$ijklmn$	U_1	U_2
1	000100		(1)	33	010100		(33)
2	000111		(2)	34	010111		(34)
3	001000		(3)	35	011000		(35)
4	001011		(4)	36	011011		(36)
5	110100		(5)	37	100100		(37)
6	110111		(6)	38	100111		(38)
7	111000		(7)	39	101000		(39)
8	111011	$I^3\otimes I^5$	(8)	40	101011	$\sigma_X^3\otimes I^5$	(40)
9	010101		(9)	41	000101		(41)
10	010110		(10)	42	000110		(42)
11	011001		(11)	43	001001		(43)
12	011010		(12)	44	001010		(44)
13	100101		(13)	45	110101		(45)
14	100110		(14)	46	110110		(46)
15	101001		(15)	47	111001		(47)
16	101010		(16)	48	111010		(48)
17	000000		(17)	49	000001		(49)
18	000011		(18)	50	000010		(50)
19	001100		(19)	51	001101		(51)
20	001111		(20)	52	001110		(52)
21	110000		(21)	53	110001		(53)
22	110011		(22)	54	110010		(54)
23	111100		(23)	55	111101		(55)
24	111111	$I^3\otimes\sigma_X^5$	(24)	56	111110	$\sigma_X^3\otimes\sigma_X^5$	(56)
25	010001		(25)	57	010000		(57)
26	010010		(26)	58	010011		(58)
27	011101		(27)	59	011100		(59)
28	011110		(28)	60	011111		(60)
29	100001		(29)	61	100000		(61)
30	100010		(30)	62	100011		(62)
31	101101		(31)	63	101100		(63)
32	101110		(32)	64	101111		(64)

表 2　U_2 中 a_0, a_1, a_2, a_3 具体形式

U_2	a_0	a_1	a_2	a_3	U_2	a_0	a_1	a_2	a_3
(1)	1	$\frac{\mu^2}{\nu^2}$	$\frac{\mu c}{\nu d}$	$\frac{\mu^3 c}{\nu^3 d}$	(33)	1	$\frac{\nu^2 ca}{\mu^2 bd}$	$\frac{\mu c}{\nu d}$	$\frac{\nu c^2 a}{\mu bd^2}$
(2)	1	$-\frac{\mu^2 a^2}{\nu^2 b^2}$	$\frac{\mu c}{\nu d}$	$-\frac{\mu^3 a^2 c}{\nu^3 b^2 d}$	(34)	1	$-\frac{\nu^2 cb}{\mu^2 ad}$	$\frac{\mu c}{\nu d}$	$-\frac{\nu c^2 b}{\mu ad^2}$
(3)	1	$\frac{\mu^2}{\nu^2}$	$-\frac{\mu b}{\nu c}$	$\frac{\mu^3 d}{\nu^3 c}$	(35)	1	$\frac{\nu^2 ca}{\mu^2 bd}$	$-\frac{\mu d}{\nu c}$	$-\frac{\nu a}{\mu b}$
(4)	1	$-\frac{\mu^2 a^2}{\nu^2 b^2}$	$-\frac{\mu d}{\nu c}$	$\frac{\mu^3 a^2 c}{\nu^3 b^2 d}$	(36)	1	$-\frac{\nu^2 cb}{\mu^2 ad}$	$-\frac{\mu d}{\nu c}$	$\frac{\nu b}{\mu a}$
(5)	1	$-\frac{\mu^2 b^2}{\nu^2 a^2}$	$\frac{\mu c}{\nu d}$	$-\frac{\mu^3 b^2 c}{\nu^3 a^2 d}$	(37)	1	$-\frac{\nu^2 ad}{\mu^2 bc}$	$\frac{\mu c}{\nu d}$	$-\frac{\nu a}{\mu b}$
(6)	1	$\frac{\mu^2}{\nu^2}$	$\frac{\mu c}{\nu d}$	$\frac{\mu^3 c}{\nu^3 d}$	(38)	1	$\frac{\nu^2 bd}{\mu^2 ac}$	$\frac{\mu c}{\nu d}$	$\frac{\nu b}{\mu a}$
(7)	1	$-\frac{\mu^2 b^2}{\nu^2 a^2}$	$-\frac{\mu d}{\nu c}$	$-\frac{\mu^3 b^2 d}{\nu^3 a^2 c}$	(39)	1	$-\frac{\nu^2 ad}{\mu^2 bc}$	$-\frac{\mu d}{\nu c}$	$\frac{\nu ad^2}{\mu bc^2}$
(8)	1	$\frac{\mu^2}{\nu^2}$	$-\frac{\mu d}{\nu c}$	$-\frac{\mu^3 d}{\nu^3 c}$	(40)	1	$\frac{\nu^2 bd}{\mu^2 ac}$	$-\frac{\mu d}{\nu c}$	$-\frac{\nu bd^2}{\mu ac^2}$
(9)	1	$\frac{c^2}{d^2}$	$\frac{\mu c}{\nu d}$	$\frac{\mu c^3}{\nu d^3}$	(41)	1	$\frac{ad}{bc}$	$\frac{\mu c}{\nu d}$	$\frac{\mu a}{\nu b}$
(10)	1	-1	$\frac{\mu c}{\nu d}$	$-\frac{\mu c}{\nu d}$	(42)	1	$-\frac{ac}{bd}$	$\frac{\mu c}{\nu d}$	$-\frac{\mu ac^2}{\nu bd^2}$
(11)	1	$\frac{c^2}{d^2}$	$-\frac{\mu d}{\nu c}$	$-\frac{\mu c}{\nu d}$	(43)	1	$\frac{ad}{bc}$	$-\frac{\mu d}{\nu c}$	$\frac{\mu ad^2}{\nu bc^2}$
(12)	1	-1	$-\frac{\mu d}{\nu c}$	$\frac{\mu d}{\nu c}$	(44)	1	$-\frac{ac^2}{bd^2}$	$-\frac{\mu}{\nu}$	$\frac{\mu ac}{\nu bd}$
(13)	1	-1	$\frac{\mu c}{\nu d}$	$-\frac{\mu c}{\nu d}$	(45)	1	$-\frac{bd}{ac}$	$\frac{\mu c}{\nu d}$	$-\frac{\mu b}{\nu a}$
(14)	1	$\frac{d^2}{c^2}$	$\frac{\mu c}{\nu d}$	$\frac{\mu d}{\nu c}$	(46)	1	$\frac{bc}{ad}$	$\frac{\mu c}{\nu d}$	$\frac{\mu bc^2}{\nu ad^2}$
(15)	1	-1	$-\frac{\mu d}{\nu c}$	$\frac{\mu d}{\nu c}$	(47)	1	$-\frac{bd}{ac}$	$-\frac{\mu d}{\nu c}$	$\frac{\mu bd^2}{\nu ac^2}$
(16)	1	$\frac{d^2}{c^2}$	$-\frac{\mu d}{\nu c}$	$-\frac{\mu d^3}{\nu c^3}$	(48)	1	$\frac{bc}{ad}$	$-\frac{\mu d}{\nu c}$	$-\frac{\mu b}{\nu a}$
(17)	1	$\frac{\mu^2}{\nu^2}$	$\frac{\nu a}{\mu b}$	$\frac{\mu a}{\nu b}$	(49)	1	$\frac{ad}{bc}$	$\frac{\nu a}{\mu b}$	$\frac{\nu da^2}{\mu cb^2}$
(18)	1	$\frac{\mu^2 a^2}{\nu^2 b^2}$	$\frac{\nu a}{\mu b}$	$-\frac{\mu a^3}{\nu b^3}$	(50)	1	$-\frac{ac}{bd}$	$\frac{\nu a}{\mu b}$	$-\frac{\nu ca^2}{\mu db^2}$
(19)	1	$\frac{\mu^2}{\nu^2}$	$-\frac{\nu b}{\mu a}$	$-\frac{\mu b}{\nu a}$	(51)	1	$\frac{ad}{bc}$	$-\frac{\nu b}{\mu a}$	$-\frac{\nu d}{\mu c}$
(20)	1	$-\frac{\mu^2 a^2}{\nu^2 b^2}$	$-\frac{\nu b}{\mu a}$	$\frac{\mu a}{\nu b}$	(52)	1	$-\frac{ac}{bd}$	$-\frac{\nu b}{\mu a}$	$\frac{\nu c}{\mu d}$
(21)	1	$-\frac{\mu^2 b^2}{\nu^2 a^2}$	$\frac{\nu a}{\mu b}$	$-\frac{\mu b}{\nu a}$	(53)	1	$-\frac{bd}{ac}$	$\frac{\nu a}{\mu b}$	$-\frac{\nu d}{\mu c}$
(22)	1	$\frac{\mu^2}{\nu^2}$	$\frac{\nu a}{\mu b}$	$\frac{\mu a}{\nu b}$	(54)	1	$\frac{bc}{ad}$	$\frac{\nu a}{\mu b}$	$\frac{\nu c}{\mu d}$
(23)	1	$-\frac{\mu^2 b^2}{\nu^2 a^2}$	$-\frac{\nu b}{\mu a}$	$\frac{\mu b^3}{\nu a^3}$	(55)	1	$-\frac{bd}{ac}$	$-\frac{\nu b}{\mu a}$	$\frac{\nu b^2 d}{\mu ca^2}$
(24)	1	$\frac{\mu^2}{\nu^2}$	$-\frac{\nu b}{\mu a}$	$-\frac{\mu b}{\nu a}$	(56)	1	$\frac{bc}{ad}$	$-\frac{\nu b}{\mu a}$	$-\frac{\nu cb^2}{\mu da^2}$
(25)	1	$\frac{c^2}{d^2}$	$\frac{\nu a}{\mu b}$	$\frac{\nu ac^2}{\mu bd^2}$	(57)	1	$\frac{\nu^2 ca}{\mu^2 bd}$	$\frac{\nu a}{\mu b}$	$\frac{\nu^3 a^2 c}{\mu^3 b^2 d}$
(26)	1	-1	$\frac{\nu a}{\mu b}$	$-\frac{\nu a}{\mu b}$	(58)	1	$-\frac{\nu^2 bc}{\mu^2 ad}$	$\frac{\nu a}{\mu b}$	$-\frac{\nu^3 c}{\mu^3 d}$
(27)	1	$\frac{c^2}{d^2}$	$-\frac{\nu b}{\mu a}$	$-\frac{\nu bc^2}{\mu ad^2}$	(59)	1	$\frac{\nu^2 ca}{\mu^2 bd}$	$-\frac{\nu b}{\mu a}$	$-\frac{\nu^3 c}{\mu^3 d}$
(28)	1	-1	$-\frac{\nu b}{\mu a}$	$\frac{\nu b}{\mu a}$	(60)	1	$-\frac{\nu^2 bc}{\mu^2 ad}$	$-\frac{\nu b}{\mu a}$	$\frac{\nu^3 b^2 c}{\mu^3 a^2 d}$
(29)	1	-1	$\frac{\nu a}{\mu b}$	$-\frac{\nu a}{\mu b}$	(61)	1	$-\frac{\nu^2 ad}{\mu^2 bc}$	$\frac{\nu a}{\mu b}$	$-\frac{\nu^3 a^2 d}{\mu^3 b^2 c}$
(30)	1	$\frac{d^2}{c^2}$	$\frac{\nu a}{\mu b}$	$\frac{\nu ad^2}{\mu bc^2}$	(62)	1	$\frac{\nu^2 bd}{\mu^2 ac}$	$\frac{\nu a}{\mu b}$	$\frac{\nu^3 d}{\mu^3 c}$
(31)	1	-1	$-\frac{\nu b}{\mu a}$	$\frac{\nu b}{\mu a}$	(63)	1	$-\frac{\nu^2 ad}{\mu^2 bc}$	$-\frac{\nu b}{\mu a}$	$\frac{\nu^3 d}{\mu^3 c}$
(32)	1	$\frac{d^2}{c^2}$	$-\frac{\nu b}{\mu a}$	$-\frac{\nu bd^2}{\mu ac^2}$	(64)	1	$\frac{\nu^2 bd}{\mu^2 ac}$	$-\frac{\nu b}{\mu a}$	$-\frac{\nu^3 b^2 d}{\mu^3 a^2 c}$

为了清楚起见，下面举例说明具体的过程：假定 Alice 测得 ij 的结果为 01，测得 kl 的结果为 10，Bob 测得 mn 的结果为 11，从表 1 中可以看到结果是第 36 种情况，也就是说整个状态 $|\psi\rangle$ 将会塌缩到

$$\begin{aligned}|\psi\rangle &= |B_{01}\rangle_{a1}|B_{10}\rangle_{b6}|B_{11}\rangle_{24}(\nu^2\mu bcd\alpha|10\rangle_{35}\\ &-\nu^3c^2b\beta|11\rangle_{35}-\mu^3ad^2\gamma|00\rangle_{35}\\ &+\mu^2\nu adc\delta|01\rangle_{35}\end{aligned}\tag{10}$$

这个状态．这时 Charlie 会在粒子 3 和 5 上分别进行 σ_X 和 I 的操作，那么粒子 3 和 5 会变为

$$\begin{aligned}|\chi\rangle_{35} &= \nu^2\mu bcd\alpha|00\rangle_{35}-\nu^3c^2b\beta|01\rangle_{35}\\ &-\mu^3ad^2\gamma|10\rangle_{35}+\mu^2\nu adc\delta|11\rangle_{35}.\end{aligned}\tag{11}$$

接着 Charlie 引入一个初态为 $|0\rangle$ 态的辅助粒子 A，在粒子 3，5 和 A 上进行表 2 中 $U_2(36)$ 的操作：

$$\begin{aligned}&U_2|\chi\rangle_{35}|0\rangle_A\\ &=\nu^2\mu bcd(\alpha|00\rangle_{35}+\beta|01\rangle_{35}\\ &+\gamma|10\rangle_{35}+\delta|11\rangle_{35})|0\rangle_A\\ &+(-\nu^2cb\sqrt{\nu^2c^2-\mu^2d^2}\beta|01\rangle_{35}\\ &-\mu d\sqrt{\mu^4a^2d^2-\nu^4c^2b^2}\gamma|10\rangle_{35}\\ &+\mu\nu dc\sqrt{\mu^2a^2-\nu^2b^2}\delta|11\rangle_{35})|1\rangle_A,\end{aligned}\tag{12}$$

其中取 $a_0=1$，$a_1=-\dfrac{\nu^2cb}{\mu^2ad}$，$a_2=-\dfrac{\mu d}{\nu c}$，$a_3=\dfrac{\nu b}{\mu a}$．

然后 Charlie 对粒子 A 做选择性测量．如果得到 $|1\rangle_A$，他就成功获得秘密，反之如果得到 $|1\rangle_A$ 他就失败，这样 Charlie 会以 $64(\nu^2\mu bcd)^2$ 的概率获得秘密．从上论述可以看到当 $a=b=c=d=\mu=\nu=\dfrac{1}{\sqrt{2}}$ 时，获得秘密的概率为 1．

3．用非最大纠缠的 EPR 对在 N 者之间分享任意两个纠缠粒子的秘密状态

上述方案很容易推广到 N 个代理人的情况，即 Bob_i（$i=1,2,\cdots,N-1$）和 Charlie，我们假定在 Bib_i（$i=1,2,\cdots,N-1$）帮助下，Charlie 是想获得秘密的人．整个过程用公式可以表示成如下的形式：

$$\begin{aligned}|\psi\rangle &= |\chi\rangle_{ab}|Q\rangle_{AC}|Q\rangle_{12}|Q\rangle_{34}\cdots\cdots|Q\rangle_{2N+1,2N+2}\\ &=|B_{k_1l_1}\rangle_{aA}|B_{k_2l_2}\rangle_{b1}|B_{k_3l_3}\rangle_{24}\cdots\cdots\\ &\times|B_{k_{N+1}l_{N+1}}\rangle_{2N-1,2N+1}\\ &\otimes|\phi_{k_1l_1\cdots k_{N+1}l_{N+1}}\rangle_{C,2N+2},\end{aligned}\tag{13}$$

其中

$$\begin{aligned}&|\phi_{k_1l_1\cdots k_{N+1}l_{N+1}}\rangle_{C,2N+2}\\ &=\xi_{k_1l_1\cdots k_{N+1}l_{N+1}}|00\rangle_{C,2N+2}\\ &+\zeta_{k_1l_1\cdots k_{N+1}l_{N+1}}|01\rangle_{C,2N+2}\\ &+\sigma_{k_1l_1\cdots k_{N+1}l_{N+1}}|10\rangle_{C,2N+2}\\ &+\tau_{k_1l_1\cdots k_{N+1}l_{N+1}}|11\rangle_{C,2N+2}.\end{aligned}\tag{14}$$

首先，Alice 与 Bob_1 分享一个 EPR 对 1 和 2，Bob_1 和 Bob_2 分享一个 EPR 对 3 和 4，……，Bob_{N-1} 和 Charlie 分享一个 EPR 对 $2N+1$ 和 $2N+2$，Charlie 和 Alice 分享一个 EPR 对 C 和 A．随后 Alice 在 a 和 1，b 和 A 上，Bob_i（$i=1,2,\cdots,N-1$）也分别在手中的两个粒子上做 GBM 的测量，然后将结果告诉 Charlie，根据结果 Charlie 会在他手中的两个粒子即 $|\phi_{k_1l_1\cdots k_{N+1}l_{N+1}}\rangle_{C,2N+2}$ 态上做相应的 U_1 和 U_2 操作，这样他会以一定的概率重现 Alice 要发送得秘密．其安全性与第 2 节的 1）步相同．

4．结 论

本文已经详细地论述了在两个代理人 Bob 和 Charlie 之间，用 3 个处于非最大纠缠状态的 EPR 对和广义的 Bell 基进行测量，如何实现任意两个纠缠粒子的秘密分享．当然，我们可以随意选取 Bob 或者 Charlie 为重现秘密者，其过程是一样的．并且以此为基础推广到 N 个代理人．也就是说从广义的角度提出了一个量子秘密分享的方案，它是一个一般性的方案，不受产生 EPR 对的仪器是否完美的影响，不需要进行纯化，因此可以节约能源．并且也对标准的 Bell 测量进行了推广，使测量更容易操作，EPR 对在实验中早已产生，因此只要确定信道是安全的，目标就很容易达到．当然由于信道是采用非最大纠缠的 EPR 对，我们会概率性地获得秘密，但是经过我们的处理，这个概率还是比较大的，因此，这个方案具有较大的实验意义．

[1] Blakley G R 1979 *Proceedings of the American Federationof Information Processing* 1979 *National Computer Conference* (American Federation of Information Processing, Arlington, VA, 1979) pp313—317
Shamir A 1979 *Commun*. ACM **22** 612

[2] Hillery M, Buzek, Berthiaume A 1999 *Phys*. *Rev*. A **59** 1829

[3] Karlsson A, Koashi M, Imoto N 1999 *Phys*. *Rev*. A **59** 162

[4] Xiao L, Long G L, Deng F G, Pan J W 2004 *Phys*. *Rev*. A **69** 052307
Deng F G, Zhou H Y, long G L 2005 *Phys*. *Lett*. A **337** 329
Deng F G, Long G L ,Zhou H Y 2005 *Phys*. *Lett*. A **340** 43
Deng F G, Wang Y, Xiao L 2004 *Chin*. *Phys*. *Lett*. **21** 2097

[5] Guo G P, Guo G C 2003 *Phys*. *Lett*. A **310** 247

[6] Yan F L, Gao T 2005 *Phys*. *Rev*. A **72** 012304

[7] Cabello A *e-print quant-ph*/0009025

[8] Yang C P, Gea-Banacloche J 2001 *J*. *Opt*. *B*: *Quantum Secmiclass*. *Opt*. **3** 407

[9] Zhang Z J, Man Z X 2005 *Phys*. *Rev*. A **72** 022303

[10] Gottesman D 2000 *Phys*. *Rev*. A **61** 042311

[11] Cleve R, Gottesman D, Lo H K 1999 *Phys*. *Rev*. *Lett*. **83** 648

[12] Zhang Z J 2005 *Phys*. *Lett*. A **342** 60

[13] Bandyopadhyay S 2000 *Phys*. *Rev*. A **62** 012308

[14] Karimipour V, Bahraminasab A, Bagherinezhad S 2002 *Phys*. *Rev*. A **65** 042320

[15] Zhang Z J, Li Y, Man Z X 2005 *Phys*. *Rev*. A **71** 044301
Deng F G, Li X H, Zhou H Y, Zhang Z 2005 *Phys*. *Rev*. A **72** 044302

[16] Li Y M, Zhang K S , Peng K C 2004 *Phys*. *Lett*. A **324** 420

[17] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2005 *Phys*. *Rev*. A **72** 044301

[18] Deng F G, Li C Y, Li Y S, Zhou H Y, Wang Y 2005 *Phys*. *Rev*. A **72** 022338

[19] Man Z X, Xia Y J, An NB 2007 *Eur*. *Phys*. *J*. D **42** 333

[20] Li X H, Zhou P, Li C Y, Zhou H Y, Deng F G 2006 *J*. *Phys*. B **39** 975

[21] Zhang Y Q, Jin X R, Zhang S 2006 *Chin Phys*. **15** 2252

[22] Chen P, Deng F G, Long G L 2006 *Chin Phys*. **15** 2228

[23] Bandyopadhyay S 2000 *Phys*. *Rev*. A **62** 012308

[24] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2005 *Phys*. *Rev*. A **72** 044301

[25] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2006 *Eur*. *Phys*. *J*. D **39** 459

[26] Li X H, Deng F G, Zhou H Y 2007 *Chin*. *Phys*. *Lett*. **24** 1151

[27] Yuan H C, Qi K G 2005 *Chin Phys*. **14** 898

[28] Huang Z P, Li H C 2005 *Chin Phys*. **14** 974

[29] Yuan H C, Qi K G 2005 *Chin Phys*. **14** 1716

[30] Yang J 2005 *Chin Phys*. **14** 2149

[31] Gisin N, Ribordy G, Tittel W , Zbinden H 2002 *Rev*. *Mod*. *Phys*. **74** 145

[32] Deng F G, Li X H, Zhou H Y *arXiv*:0705.0279

[33] Man Z X , Xia Y J 2007 *Chin*. *Phys*. **16** 1197

[34] Li C Y, Zhou H Y, Wang Y, Deng F G 2005 *Chin*. *Phys*. *Lett*. **22** 1049

[35] Li C Y, Li X H, Deng F G, Zhou P, Liang Y J, Zhou H Y 2006 *Chin*. *Phys*. *Lett*. **23** 2896

[36] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P, Zhou H Y 2006 *Journal of the Korean Physical Society* **49** 1354

[37] Long G L, Liu X S 2002 *Phys*. *Rev*. A **65** 032302

Quantum secret sharing of an arbitrary two-particle entangled state via non-maximally entangled channels *

Liu Yu-Ling Man Zhong-Xiao Xia Yun-Jie†

(*College of Physics and Engineering, Qufu Normal University, Qufu* 273165, *China*)

(Received 15 April 2007; revised manuscript received 9 October 2007)

Abstract

In this paper, a quantum secret sharing scheme is proposed for an arbitrary two-particle entangled state among N agents. The scheme adopts the non-maximally entangled Bell states as quantum channels and the generalized Bell states as the measurement basis. By introducing an auxiliary particle and making selective measurement on it, the receiver can obtain the original quantum state with a probability less than unity.

Keywords: non-maximally entangled Einstein-Podolsky-Rosen (EPR) pair, generalized Bell state measurement

PACC: 0365, 4250

* Project supported by the Key Program of National Science Foundation of China (Grant No. 10534030).

† Corresponding author. E-mail: yjxia@mail.qfnu.edu.cn