第 54 卷 第 12 期 2005 年 12 月
1000-3290/2005/54(12)/5549-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.12,December,2005

一种新的利用不可扩展乘积基和严格纠缠基的量子密钥分配方案*

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)(现代通信国家级重点实验室,成都 610041)

(2005 年 2 月 6 日收到;2005 年 6 月 30 日收到修改稿)

提出了一种新的利用 $3\otimes3$ Hilbert 空间的不可扩展乘积基和严格纠缠基的量子密钥分配方案.对窃听者的窃听成功概率进行了分析.该方案具有许多诸如容量大以及效率高等独特的特点.

关键词:量子密钥分配,不可扩展乘积基,严格纠缠基,正交完备基

PACC:0365,4230

1. 引 言

自从 Bennett 和 Brassard[1] 在 1984 年提出第一个利用量子力学分发密钥的量子密钥分配协议(BB84)以来,人们已提出了大量的量子密钥分配协议[2—6].对量子密钥分配实验的研究也迅速发展,例如,BB84 协议和 B92 协议的光纤实验已达到 48 km[7],在自由空间中的 B92 协议的实验已超过 1 km[8].文献[9]首次提出了一种基于正交态的量子密码协议.这些方案的基本技术是把 1 个比特的信息分成两步传送以确保每次仅有部分的信息被传送.正交态的不可克隆定理[10] 保证了方案的安全性.所谓正交态的不可克隆定理,是指由 A 和 B 组成系统的两个(或多个)正交态 $\rho_i(AB)$ 不能被克隆,条件是首先获得的(比如 A)子系统的约化密度矩阵 $\rho_i(A)=\mathrm{Tr}_B[\rho_i(AB)]$ 非正交且不相同,且第二个子系统的约化密度矩阵是非正交的.在两个子系统组成复合系统的情况下,如果子系统仅仅是一个接一个地被接收,那么存在多种正交态不能被克隆的情况.

对于多态系统,Bennett 等[11] 已经表明存在 $3\otimes3$ Hilbert 空间的正交乘积纯态且证明这些态可能具有没有纠缠的非局域性.人们已经实现了三个相互正交极化态的实验演示[12],其中两光子被用作多态系统.文献[13]建议了一种利用正交乘积态的量子密钥分配方案.

2. $3\otimes3$ Hilbert 空间的量子密钥分配协议

为便于提出量子密钥分配协议,先描述几个概念和结果.多方量子态的 Hilbert 空间的乘积基(PB)是一个正交乘积纯态的集合.多方量子态的 Hilbert 空间 H 的不可扩展乘积基(UPB)是一个 PB S,S 张起 H 的子空间 H_S,补空间 $H-H_S$ 不包括乘积态.

定义[14] 多方量子系统 $H=\otimes_{i=1}^{M}H_i$,各方的维度分别为 d_i,H 的总维度是

$$N=\prod_{i=1}^{M}d_i.$$

如果纯态 $|\varphi_j\rangle(j=0,\cdots,n-1)$ 的任意联合仍是一个纠缠纯态,则纯态 $|\varphi_j\rangle(j=0,\cdots,n-1)$ 构成一个纠缠基(EB) $T=\{|\varphi_0\rangle,\cdots,|\varphi_{n-1}\rangle\}$.被 EB T 张起的子空间 H_T(H_T 不包括任何分离的纯态)被称作纠缠空间(ES).如果存在一个包含 $m=N-n$ 个乘积态的 UPB $S=\{|\psi_0\rangle,\cdots,|\psi_{m-1}\rangle\}$,使得 $B=S\cup T=\{|\psi_0\rangle,\cdots,|\psi_{m-1}\rangle,|\varphi_0\rangle,\cdots,|\varphi_{n-1}\rangle\}$ 形成 H 的一个

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

† E-mail:yangyang7357@sina.com

正交完备基，则 EBT 被称作严格纠缠基(EEB)，子空间 H_T 被称作严格纠缠空间(EES)，其中所有的态和 UPBS 相互正交. B 称作具有不可扩展乘积基的完备基(CBUPB).

文献[14]已证明了 EEB 的存在.

2.1. 构造 3⊗3 Hilbert 空间的 UPB 和 EEB

现在考虑 $3\otimes3$ 系统. 该 Hilbert 空间的 UPB 的一般集合形式如下：

$$\begin{aligned}
|\psi_0\rangle &= |0\rangle(a|0\rangle + b|1\rangle),\\
|\psi_1\rangle &= (e|0\rangle + f|1\rangle)|2\rangle,\\
|\psi_2\rangle &= |2\rangle(c|1\rangle + d|2\rangle),\\
|\psi_3\rangle &= (g|1\rangle + h|2\rangle)|0\rangle,\\
|\psi_4\rangle &= \frac{1}{3}(|0\rangle+|1\rangle+|2\rangle)\\
&\quad\times(|0\rangle+|1\rangle+|2\rangle),
\end{aligned} \tag{1}$$

式中 a,b,c,d,e,f,g,h 是复数且 $|a|^2+|b|^2=|c|^2+|d|^2=|e|^2+|f|^2=|g|^2+|h|^2=1$.

现在给定 UPB $S=\{|\psi_0\rangle,\cdots,|\psi_4\rangle\}$，使用 Schmidt 正交化的方法获得一个 EEB. 任意选取 H 中的四个态 $\{|f_0\rangle,|f_1\rangle,|f_2\rangle,|f_3\rangle\}$ 使得 $\{|\psi_0\rangle,\cdots,|\psi_4\rangle,|f_0\rangle,|f_1\rangle,|f_2\rangle,|f_3\rangle\}$ 形成 H 中的一个线性独立群. 可以选取

$$\begin{aligned}
|f_0\rangle &= |0\rangle(b^*|0\rangle - a^*|1\rangle),\\
|f_1\rangle &= (f^*|0\rangle - e^*|1\rangle)|2\rangle,\\
|f_2\rangle &= |2\rangle(d^*|1\rangle - c^*|2\rangle),\\
|f_3\rangle &= (h^*|1\rangle - g^*|2\rangle)|0\rangle.
\end{aligned}$$

通过推导定义 $|\varphi_k\rangle(k=0,1,2,3)$ 如下所示：

$$|\varphi_0\rangle = \eta_0\{|f_0\rangle - \sum_{i=0}^{4}\langle\psi_i|f_0\rangle|\psi_i\rangle\}, \tag{2}$$

$$|\varphi_k\rangle = \eta_k\{|f_k\rangle - \sum_{i=0}^{4}\langle\psi_i|f_k\rangle|\psi_i\rangle - \sum_{j=0}^{k-1}\langle\varphi_j|f_k\rangle|\varphi_j\rangle\} \quad (k=1,2,3), \tag{3}$$

式中 η_k 是归一化系数，它可由推导确定. 令

$$T = \{|\varphi_0\rangle,\cdots,|\varphi_3\rangle\},$$

因此

$$\begin{aligned}
B &= S\cup T\\
&= \{|\psi_0\rangle,\cdots,|\psi_4\rangle,|\varphi_0\rangle,\cdots,|\varphi_3\rangle\}
\end{aligned}$$

形成一个正交完备基. 由于 S 是一个 UPB，所以 T 是一个 EEB，B 是一个 CBUPB.

在冗长的计算之后，获得结果 $|\varphi_k\rangle(k=0,1,2,3)$.

$$|\varphi_0\rangle = \eta_0\Big\{|0\rangle\Big(\frac{8b^*+a^*}{9}|0\rangle - \frac{b^*+8a^*}{9}|1\rangle - \frac{b^*-a^*}{9}|2\rangle\Big) - \frac{b^*-a^*}{9}(|1\rangle+|2\rangle)(|0\rangle+|1\rangle+|2\rangle)\Big\}, \tag{4}$$

$$|\varphi_1\rangle = Z_1|0\rangle|0\rangle + Z_2|0\rangle|1\rangle + Z_3|0\rangle|2\rangle + Z_4|1\rangle(|0\rangle+|1\rangle) + Z_4|2\rangle(|0\rangle+|1\rangle+|2\rangle) + Z_5|1\rangle|2\rangle, \tag{5}$$

$$|\varphi_2\rangle = Y_1|0\rangle|0\rangle + Y_2|0\rangle|1\rangle + Y_3|0\rangle|2\rangle + Y_4|1\rangle|0\rangle + Y_4|1\rangle|1\rangle + Y_5|1\rangle|2\rangle + Y_4|2\rangle|0\rangle + Y_6|2\rangle|1\rangle + Y_7|2\rangle|2\rangle, \tag{6}$$

$$\begin{aligned}
|\varphi_3\rangle &= \Big(A + X_1\frac{8b^*+a^*}{9} + X_2Z_1 + X_3Y_1\Big)|0\rangle|0\rangle + \Big(A - X_1\frac{b^*+8a^*}{9} + X_2Z_2 + X_3Y_2\Big)|0\rangle|1\rangle\\
&+ \Big(A - X_1\frac{b^*-a^*}{9} + X_2Z_3 + X_3Y_3\Big)|0\rangle|2\rangle + \Big(B - X_1\frac{b^*-a^*}{9} + X_2Z_4 + X_3Y_4\Big)|1\rangle|0\rangle\\
&+ \Big(A - X_1\frac{b^*-a^*}{9} + X_2Z_4 + X_3Y_4\Big)|1\rangle|1\rangle + \Big(A - X_1\frac{b^*-a^*}{9} + X_2Z_5 + X_3Y_5\Big)|1\rangle|2\rangle\\
&+ \Big(C - X_1\frac{b^*-a^*}{9} + X_2Z_4 + X_3Y_4\Big)|2\rangle|0\rangle + \Big(A - X_1\frac{b^*-a^*}{9} + X_2Z_4 + X_3Y_6\Big)|2\rangle|1\rangle\\
&+ \Big(A - X_1\frac{b^*-a^*}{9} + X_2Z_4 + X_3Y_7\Big)|2\rangle|2\rangle.
\end{aligned} \tag{7}$$

这里，

$$\eta_0 = \frac{9}{\sqrt{|8b+a|^2+|b+8a|^2+7|b-a|^2}},$$

$$Z_1 = \eta_1\left(-\frac{f^* - e^*}{9} - \eta_0^2\frac{(b-a)(e^* - f^*)(8b^* + a^*)}{81}\right),$$

$$Z_2 = \eta_1\left(-\frac{f^* - e^*}{9} + \eta_0^2\frac{(b-a)(e^* - f^*)(b^* + 8a^*)}{81}\right),$$

$$Z_3 = \eta_1\left(\frac{8f^* + e^*}{9} + \eta_0^2\frac{|b-a|^2(e^* - f^*)}{81}\right),$$

$$Z_4 = \eta_1\left(-\frac{f^* - e^*}{9} + \eta_0^2\frac{|b-a|^2(e^* - f^*)}{81}\right),$$

$$Z_5 = \eta_1\left(-\frac{f^* + 8e^*}{9} + \eta_0^2\frac{|b-a|^2(e^* - f^*)}{81}\right),$$

$$Y_1 = \eta_2\left[-\frac{1}{9} + \eta_0^2\frac{(b-a)(8b^* + a^*)}{81} - Z_1Z_4^*\right](d^* - c^*),$$

$$Y_2 = \eta_2\left[-\frac{1}{9} - \eta_0^2\frac{(b-a)(b^* + 8a^*)}{81} - Z_2Z_4^*\right](d^* - c^*),$$

$$Y_3 = \eta_2\left[-\frac{1}{9} - \eta_0^2\frac{|b-a|^2}{81} - Z_3Z_4^*\right](d^* - c^*),$$

$$Y_4 = \eta_2\left[-\frac{1}{9} - \eta_0^2\frac{|b-a|^2}{81} - |Z_4|^2\right](d^* - c^*),$$

$$Y_5 = \eta_2\left[-\frac{1}{9} - \eta_0^2\frac{|b-a|^2}{81} - Z_5Z_4^*\right](d^* - c^*),$$

$$Y_6 = \eta_2\left[\frac{8d^* + c^*}{9} - \eta_0^2\frac{|b-a|^2(d^* - c^*)}{81} - |Z_4|^2(d^* - c^*)\right],$$

$$Y_7 = \eta_2\left[-\frac{d^* + 8c^*}{9} - \eta_0^2\frac{|b-a|^2(d^* - c^*)}{81} - |Z_4|^2(d^* - c^*)\right],$$

$$X_1 = \eta_2\eta_0^2\frac{(b-a)(h^* - g^*)}{9},$$

$$X_2 = -\eta_3\eta_1\left[\frac{1}{9} + \eta_0^2\frac{(b-a)^2}{81}\right](e-f)(h^* - g^*),$$

$$X_3 = \eta_3\eta_2\left[\frac{1}{9} + \eta_0^2\frac{(b-a)^2}{81} + |Z_4|^2\right](d-c)(h^* - g^*),$$

$$A = -\eta_3\frac{h^* - g^*}{9},$$

$$B = \eta_3\frac{8h^* + g^*}{9},$$

$$C = -\eta_3\frac{h^* + 8g^*}{9}.$$

2.2. 量子密钥分配协议

我们提出了以下的量子密钥分配协议.在该量子密钥分配方案中,传送过程类似于利用普通正交态[9]的量子密钥分配方案和利用正交乘积态的量子密钥分配方案[13].

(1) Alice 随机地将粒子 A 和粒子 B 制备于如上所示的 9 个正交态中的一个,把粒子 A 发送给粒子 B.当 Bob 接收到粒子 A 时,他通过一个公开的经典信道通知 Alice.然后 Alice 发送粒子 B.当 Bob 拥有粒子 A 和粒子 B 时,他在(1),(4)—(7)式中的基上作联合的正交测量来确定这两个粒子制备在哪个态上.在该过程的多次重复之后,他们可以共享一个随机比特串,该比特串作为原始密钥.

(2)为了检测窃听,Alice 和 Bob 随机地比较一些比特来验证相关性是否被破坏.如果错误率低于某一个他们可以容忍的门限值,就可以认为没有窃听存在,剩下的结果经过错误纠正和秘密放大之后可以作为密钥.相反,他们抛弃所有的密钥,重新进行该量子密钥分配协议.

该方案实现的关键之处在于 Alice 仅仅在第一个粒子到达 Bob 之后发送第二个粒子以消除任何窃听者同时拥有两个粒子的可能性.由于所有的原始密钥除了用于检测窃听的比特被抛弃之外其他的密钥比特均可用,所以该协议效率高(接近 100%),且容量大,这是因为通过一个 $3\otimes 3$ 系统可以传送 $\log_2 9$ 的信息.

2.3. 窃听分析

在该量子密钥分配方案中使用了一个 CBUPB.该 CBUPB 由正交乘积态和纠缠态组成.我们首先考虑一个窃听策略.Eve 测量 Alice 发送给 Bob 的第一个粒子.Eve 根据第一个粒子的测量结果测量第二个粒子并将它发送给 Bob.窃听过程如下:Eve 截取粒子 A,在基 $\{|0\rangle,|1\rangle,|2\rangle\}$ 上作正交测量.假设粒子 A 被发现位于态 $|0\rangle$,粒子 A 和粒子 B 的两粒子态处于除了 $|\psi_2\rangle$ 和 $|\psi_3\rangle$ 之外的一个态上.然后她将之发送给 Bob.根据(1),(4)—(7)式,可以看出所发送的态被坍缩,除非所发送的态正好处于态 $|\psi_0\rangle$.当粒子 B 到来时,Eve 截取它.根据(1),(4)—(7)式,可以看出 Eve 不能找到一个可以区分所传送态的测量基.Eve 的测量不会给她带来关于所传送态的信息.相反,只会干扰所传送的态,而被 Alice 和 Bob 通过随机比较一些比特检测到.该方案的安全性大大提高.

通过一个具体的例子计算窃听者 Eve 窃听成功且不被检测到的概率.为了简单而不失一般性,我们令 $a=-b=e=-f=c=-d=g=-h=\frac{1}{\sqrt{2}}$.计算出 Eve 窃听成功且未被检测到的总概率为 $P_S(G)\approx 0.414165$.该值小于文献[13]中协议所计算的最小值 $\frac{7}{9}$,可见本方案的安全性优于文献[13].

另外,该方案也和文献[13]中的量子密钥分配方案一样,具有容量大的特点.

考虑另一窃听策略.Eve 截取第一个粒子,将自己已制备好的处于 CBUPB 中一个基态的两个粒子中的一个发送给 Bob.当粒子 B 到达时,Eve 截取它,然后将其已制备的另一粒子发送给 Bob.这样,虽然 Eve 在(1),(4)—(7)式中的基上作联合正交测量获得所传送态的信息,但是这可以被 Alice 和 Bob 通过随机比较一些比特检测到.

3. 结 论

本文提出了一种新的利用 $3\otimes 3$ Hilbert 空间的 UPB 和 EEB 的量子密钥分配方案.该方案具有许多独特的特点,如大容量、高效率.

方案中使用了非最大纠缠态.由于制备非最大纠缠态的困难性以及在传送过程中态的消相干,因此目前该方案的实现还具有一定的困难.

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE) pp 175—179

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[5] 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]

[6] Pasquinucci H B, Peres A 2000 *Phys. Rev. Lett.* **85** 3313

[7] Hughes R J, Morgan G L, Peterson C G 2000 *J. Mod. Opt.* **47** 533

[8] Butter W T 2000 *Phys. Rev. Lett.* **84** 5652

[9] Goldenberg L, Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239

[10] Mor T 1998 *Phys. Rev. Lett.* **80** 3137

[11] Bennett C H, Divincenzo D P, Fuchs C A *et al* 1999 *Phys. Rev.* A **59** 1070

[12] Tsegaye T, Soderholm J, Atature M *et al* 2000 *Phys. Rev. Lett.* **85** 5013

[13] Guo G P, Li C F, Shi B S *et al* 2001 *Phys. Rev.* A **64** 042301

[14] Zhong Z Z 2004 *Phys. Rev.* A **70** 044302

A novel quantum key distribution scheme with unextendible product basis and exact entanglement basis*

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 of Modern Communications*, *Chengdu* 610041, *China*)

(Received 6 February 2005; revised manuscript received 30 June 2005)

Abstract

A novel quantum key distribution scheme with unextendible product basis and exact entanglement basis in the $3\otimes3$ Hilbert space is proposed. The probability of successful eavesdropping by the eavesdropper is also analysed. This scheme has many distinct features such as great capacity, high efficiency.

Keywords: quantum key distribution, unextendible product basis, exact entanglement basis, orthogonal complete basis

PACC: 0365, 4230

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

† E-mail: yangyang7357@sina.com