第 56 卷 第 4 期 2007 年 4 月
1000-3290/2007/56(04)/1924-04

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.4,April,2007

基于超纠缠交换的量子密钥分发*

冯发勇† 张 强

(中国科学技术大学近代物理系,合肥 230026)

(2006 年 8 月 9 日收到;2006 年 11 月 30 日收到修改稿)

给出一种基于超纠缠交换的量子密钥分发方案,这个方案可以同时产生确定密钥和随机密钥,并且它的安全性不受任何损害.这个方案只需要一对在空间(路径)模式和极化模式上超纠缠的光子就能获得 4 bit 的密钥(2 bit 随机密钥和 2 bit 确定密钥).在目前的实验条件下,这个方案可以通过线性光学来实现.

关键词:量子密钥分发,超纠缠,线性光学

PACC:0367,4250

1. 引 言

量子物理的随机特性和纠缠特性为我们带来了一种新的、安全的信息加密技术——量子密码术.这种密码术不同于经典的密码术,它利用的是物理规律而不是数学理论,可以从根本上保证密码的安全性.

最早的量子密钥分发方案是 BB84 方案[1],这种方案在通信的一方进行编码,在另一方进行测量,利用量子测量的随机性来产生密钥对.B92 方案[2]的原理和 BB84 是一样的,不过它采用更少的态来进行编码.基于 Einstein-Podolsky-Rosen(EPR)纠缠对的方案[3]和上面两种方案不同,通信的两端共享一对纠缠粒子,并且都进行随机测量,然后按照一定规则进行符合.从一定意义上,上述三种方案都不是通信的双方将事先编码的密钥进行交换,而是通过量子测量来‘制造’密钥,通信的双方都不能预先按照自己的意愿定义一组密码[4],并且这些方案都要丢弃那些双方不能符合的测量结果,密钥分发的效率理论上都不能达到 100%.

基于纠缠交换的量子密钥分发方案[5,6]可以较大地提高分发效率.最近,提出了一种新的方案[7],使用这种方案,可以在获得 2 bit 随机密钥的同时,按照意愿发送 2 bit 确定密钥,理论上,这种方案可以使得量子比特的利用率达到 100%,这个方案使用了基于四粒子的纠缠交换.我们给出这种方案的另一种实现方法,这种方法基于光子的路径-极化超纠缠交换,只需要使用一对光子.并且,我们也给出这种方法在现有实验条件下的具体实现.

2. 超纠缠态的产生

纠缠交换的概念是由 Zukowski 等[8]首先引入的,并且于 1998 年,由潘建伟等[9]在实验中加以实现.光子对 AB 与光子对 CD 分别处于纠缠态(设为 Bell 态),对光子 B 和光子 C 作 Bell 基测量,结果会使光子 A 和光子 D 这两个没有发生相互作用的光子产生纠缠,这就是纠缠交换的过程.超纠缠[10]是多粒子多维度的纠缠,例如下面我们用到的路径-极化纠缠光子对,它们的空间(路径)自由度处于纠缠状态的同时,极化自由度也处于纠缠状态,这时对一个光子的路径和极化自由度进行 Bell 基测量,会使得另一光子的路径-极化状态发生改变,这就是超纠缠交换的含义.

在我们的实现方法中,使用基于两光子的路径-极化超纠缠,这种态已经在实验中实现[11,12],这是一个($2\times2\times2\times2$)维的态,其产生的装置如图 1 中阴影部分所示.一束紫外光入射到 BBO (β-barium borate)晶体上,有一定概率产生一对极化纠缠的光子对[13],表示为

$$|\Psi(\varphi)\rangle_{\mathrm{pol}}=\frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}}+\mathrm{e}^{\mathrm{i}\varphi}|V\rangle_{\mathrm{A}}|H\rangle_{\mathrm{B}}),\quad(1)$$

* 国家自然科学基金(批准号:10575093)资助的课题.

† E-mail:fyfeng@mail.ustc.edu.cn

它们的空间(路径)模是 L_A 和 R_B，如果让紫外光束反射，第二次通过 BBO 晶体，又有一定的概率产生空间(路径)模为 R_A 和 L_B 的极化纠缠光子对，调节会聚透镜 F 的焦距和位置，可以使得两次产生光子对的概率相等. 如果模 L_A-R_B 和模 R_A-L_B 在时间上有理想的重叠，则能得到空间模的纠缠态

$$|\Psi^-(\phi)\rangle_{path} = \frac{1}{\sqrt{2}}(|R\rangle_A|L\rangle_B - e^{i\phi}|L\rangle_A|R\rangle_B). \quad (2)$$

总的路径-极化超纠缠可表示为

$$\begin{aligned}|\Psi\rangle_{AB} &= |\Psi^-(\phi)\rangle_{path} \otimes |\Psi(\varphi)\rangle_{pol} \\ &= \frac{1}{\sqrt{2}}(|R\rangle_A|L\rangle_B - e^{i\phi}|L\rangle_A|R\rangle_B) \\ &\otimes \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B + e^{i\varphi}|V\rangle_A|H\rangle_B). \quad (3)\end{aligned}$$

恰当调整实验装置[12,13]，可以使得(3)式中的 ϕ 和 φ 为零，得到态

$$\begin{aligned}|\Psi\rangle_{AB} &= |\Psi^-(0)\rangle_{path} \otimes |\Psi(0)\rangle_{pol} \\ &= \frac{1}{\sqrt{2}}(|R\rangle_A|L\rangle_B - |L\rangle_A|R\rangle_B) \\ &\otimes \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B). \quad (4)\end{aligned}$$

将获得的光子对中的光子命名为光子 A 和光子 B，分别发送给 Alice 和 Bob.

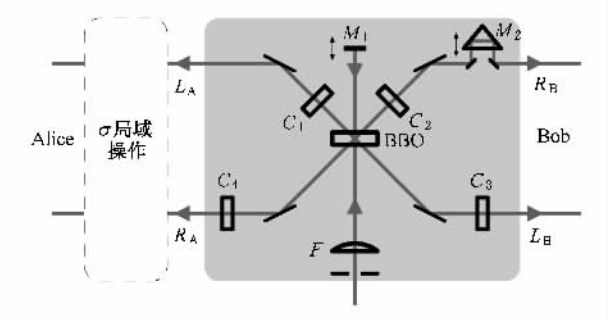

图 1　超纠缠光子对的产生装置和 Alice 的 σ 局域操作　C_1，C_2，C_3，C_4 为补偿器；M_1，M_2 为位置可调节的反射镜；F 为焦距和位置均可调节的会聚透镜

3. 密钥的分发过程

在 Alice 端，Alice 可以对光子 A 的极化进行 σ 局域操作(见图 1)，记路径和极化的 Bell 基分别为

$$\begin{aligned}|\phi^\pm\rangle_{path} &= \frac{1}{\sqrt{2}}(|R\rangle|R\rangle \pm |L\rangle|L\rangle), \\ |\psi^\pm\rangle_{path} &= \frac{1}{\sqrt{2}}(|R\rangle|L\rangle \pm |L\rangle|R\rangle);\end{aligned} \quad (5)$$

$$\begin{aligned}|\phi^\pm\rangle_{pol} &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle \pm |V\rangle|V\rangle), \\ |\psi^\pm\rangle_{pol} &= \frac{1}{\sqrt{2}}(|H\rangle|V\rangle \pm |V\rangle|H\rangle).\end{aligned} \quad (6)$$

在光子通过的两条路径上安放波片(组合)，例如，可以作如下组合：σ_0：(无波片) σ_1：($\lambda/2$,45°) σ_2：($\lambda/2$,45°；$\lambda/2$,0°) σ_3：($\lambda/2$,0°)，其中 $\lambda/2$ 表示二分之一波片，角度为光轴与水平方向的夹角. 记

$$\sigma = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}, \quad (7)$$

则局域操作的结果是

$$\sigma|\psi^+\rangle_{pol} = \{|\psi^+\rangle_{pol}, |\phi^+\rangle_{pol}, |\phi^-\rangle_{pol}, |\psi^-\rangle_{pol}\}. \quad (8)$$

对 σ 操作和 Bell 基作编码

$$\begin{aligned}&\sigma_0 \to 00, \quad \sigma_1 \to 01, \\ &\sigma_2 \to 10, \quad \sigma_3 \to 11; \\ &|\phi^+\rangle_{pol} \to 00, \quad |\psi^+\rangle_{pol} \to 01, \\ &|\psi^-\rangle_{pol} \to 10, \quad |\phi^-\rangle_{pol} \to 11.\end{aligned}$$

把装置产生的初始态 $|\Psi\rangle_{AB}$ 记为

$$|\Psi\rangle_{AB} = |\psi^-\rangle^{AB}_{path} \otimes |\psi^+\rangle^{AB}_{pol}, \quad (9)$$

设 Alice 对她的光子进行的局域操作为 σ_1，将其编码为 01，则 $|\psi^+\rangle^{AB}_{pol}$ 在 σ_1 操作下变为 $|\phi^+\rangle^{AB}_{pol}$.

Alice 进行了光子 A 的 σ_1 局域操作后，两光子的状态变为

$$\begin{aligned}|\Psi'\rangle_{AB} &= |\psi^-\rangle^{AB}_{path} \otimes |\phi^+\rangle^{AB}_{pol} \\ &= \frac{1}{2}\{|\phi'^-\rangle_A|\psi'^+\rangle_B - |\phi'^+\rangle_A|\psi'^-\rangle_B \\ &+ |\psi'^-\rangle_A|\phi'^+\rangle_B - |\psi'^+\rangle_A|\phi'^-\rangle_B\}, \quad (10)\end{aligned}$$

其中

$$\begin{aligned}|\phi'^\pm\rangle &= (|R\rangle|H\rangle \pm |L\rangle|V\rangle)/\sqrt{2}, \\ |\psi'^\pm\rangle &= (|R\rangle|V\rangle \pm |L\rangle|H\rangle)/\sqrt{2}.\end{aligned} \quad (11)$$

这时，Alice 对她手里的光子进行路径-极化纠缠测量，测量的装置如图 2 所示. 图 2 中的阴影部分为 Bell 基变换装置，它是单光子通用 U 门(酉变换门)[14]的一种应用，取垂直方向为波片角度的零方向，设定四分之一波片(右)的角度为 $\pi/4$，四分之一波片(左)的角度为 $-\pi/4$，Bell 基变换装置的作用以算符 S_{Bell} 来表示，则可以得到如下变换：

$$\begin{aligned}&S_{Bell}\{|\phi'^+\rangle, |\phi'^-\rangle, |\psi'^+\rangle, |\psi'^-\rangle\} \\ &= \{|L\rangle|V\rangle, |R\rangle|H\rangle, |L\rangle|H\rangle, |R\rangle|V\rangle\}. \quad (12)\end{aligned}$$

Bell 基经过这样的变换后，入射到极化分束器上，极化分束器的作用是让那些水平极化的光子通过而让垂直极化的光子反射. 例如，$|\phi'^+\rangle$ 通过变换装置之

后,成为$|L\rangle|V\rangle$,经过极化分束器时,被反射进入单光子探测器 D_3,产生响应.这样,就可以将四个单光子探测器的响应分别和四个 Bell 基一一对应起来,对应关系如下:

$$\{|\phi'^{+}\rangle,|\phi'^{-}\rangle,|\psi'^{+}\rangle,|\psi'^{-}\rangle\}\rightarrow\{D_3,D_1,D_4,D_2\},$$

假设 Alice 的测量结果是$|\phi'^{+}\rangle_A$(探测器 D_3 响应),那么她能根据(10)式推断 Bob 的光子处于$|\psi'^{-}\rangle_B$,并将其编码为 10. Alice 通知 Bob 已经进行了 Bell 测量,但不告诉测量结果.

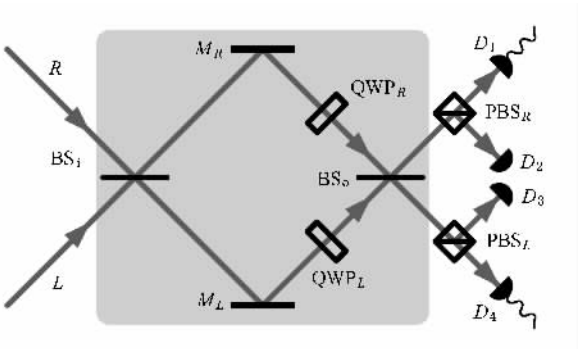

图 2 Bell 基变换和测量装置 BS 为分束器,M 为反射平面镜,QWP 为四分之一波片,PBS 为极化分束器,D 为单光子探测器

Bob 这一端同样也使用图 2 所示的测量装置对他的光子进行 Bell 测量,由(10)式知,Bob 的测量结果应为$|\psi'^{-}\rangle_B$,他将其编码为 10.此时他并不知道光子 A 的实际状态,他只知道制备的光子对的初始态,因为初始态的信息是共享的.由公式

$$\begin{aligned}|\Psi\rangle_{AB}&=|\psi^{-}\rangle_{path}^{AB}\otimes|\psi^{+}\rangle_{pol}^{AB}\\&=\frac{1}{2}\{|\phi'^{-}\rangle_A|\phi'^{+}\rangle_B-|\phi'^{+}\rangle_A|\phi'^{-}\rangle_B\\&\quad+|\psi'^{-}\rangle_A|\psi'^{+}\rangle_B-|\psi'^{+}\rangle_A|\psi'^{-}\rangle_B\},\end{aligned}\tag{13}$$

Bob 推断出光子 A 的状态为$|\psi'^{+}\rangle_A$,然后 Bob 和 Alice 进行经典通信,Alice 将测量结果告诉 Bob.我们假设有一个操作 $\sigma'=\{\sigma'_i,(i=0,\cdots,3)\}$,满足

$$\begin{aligned}\sigma'|\psi'^{+}\rangle&=\{|\psi'^{+}\rangle,|\phi'^{+}\rangle,|\phi'^{-}\rangle,|\psi'^{-}\rangle\},\\\sigma'|\psi'^{-}\rangle&=\{|\psi'^{-}\rangle,|\phi'^{-}\rangle,|\phi'^{+}\rangle,|\psi'^{+}\rangle\},\\\sigma'|\phi'^{+}\rangle&=\{|\phi'^{+}\rangle,|\psi'^{+}\rangle,|\psi'^{-}\rangle,|\phi'^{-}\rangle\},\\\sigma'|\phi'^{-}\rangle&=\{|\phi'^{-}\rangle,|\psi'^{-}\rangle,|\psi'^{+}\rangle,|\phi'^{+}\rangle\}.\end{aligned}\tag{14}$$

那么,假想操作 σ' 和极化操作 σ 之间是一一对应(见(7),(8)式),Bob 将$|\phi'^{+}\rangle_A$与他推断的状态$|\psi'^{+}\rangle_A$进行对比,得到对应关系$|\psi'^{+}\rangle_A\xrightarrow{\sigma'_1}|\phi'^{+}\rangle_A$,Bob 据此推断出 Alice 对光子 A 进行了 σ_1 操作,作如下编码:

$$\sigma'_0\rightarrow 00,\quad \sigma'_1\rightarrow 01,$$
$$\sigma'_2\rightarrow 10,\quad \sigma'_3\rightarrow 11,$$

则 Bob 可以将操作 $\sigma'_1(\sigma_1)$编码为 01.

这样,一方面 Alice 和 Bob 之间可以将 $\sigma_1(\sigma'_1)$操作对应的编码 01 作为他们之间的确定密钥;另一方面 Bob 和 Alice 又秘密共享态$|\psi'^{-}\rangle_B$的信息,并且将它们编码为 10,他们可以将这个测量得到的随机结果作为他们之间的随机密钥.重复上述过程,直至通信双方建立起他们需要的密钥为止.

上述的密钥分发过程中,为了检查密钥分发的安全性,Bob 可以通过经典信道传递给 Alice 一些他自己获得的量子比特,Alice 可以使用量子测量的随机性原理判断是否有窃听者存在,在文献[5,7]中有详细的讨论.如果用于检查安全性的光子对数目一定,那么当密钥分发的整个过程中使用的总光子对数目非常大时,可以使得光子对的利用率趋近 100%.

需要指出的是,因为环境的影响,路径-极化纠缠在实际中很容易退相干而难以远距离分发.这一问题可以通过文献[15]中提出的办法加以解决,将分发的纠缠对换成时间-极化纠缠就可以克服路径-极化纠缠的这个缺点.再利用文献[15]中提出的时间-路径转换器,可以把对时间-极化的测量转换成对路径-极化的测量.经过这些改进以后,本文的讨论仍然适用,并克服了路径-极化纠缠的弱点,从而更加有利于实验实现.

4. 结 论

本文给出了一种基于光子路径-极化超纠缠交换的高效量子密钥分发方法.本文的方法只利用一对光子就可以产生 2 bit 确定密钥和 2 bit 随机密钥,这种方法相对于基于双纠缠对的分发方法,效率大大提高,并且本文的方案在实验上是容易实现的.

感谢陈增兵教授的指导,同时感谢张军、周晓琪、陆朝阳等同学的讨论和建议.

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Proceeding* (New York: IEEE) p175
[2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[4] Nielsen M A, Chuang I L 2003 *Quantum Computation and Quantum Information* (Beijing: Higher Education Press) p591
[5] Li C, Song H S, Zhou L *et al* 2003 *J. Opt.* B **5** 155
[6] Yang Y G, Wen Q Y, Zhu F C 2005 *Acta Phys. Sin.* **54** 5544 (in Chinese) [杨宇光、温巧燕、朱甫臣 2005 物理学报 **54** 5544]
[7] Li C, Wang Z, Wu C F *et al* 2006 *Int. J. Quantum Inform.* **4** 1
[8] Zukowski M, Zeilinger A, Horne M A *et al* 1993 *Phys. Rev. Lett.* **71** 4287
[9] Pan J W, Bouwmeester D, Weinfurter H *et al* 1998 *Phys. Rev. Lett.* **80** 3891
[10] Kwiat P G 1997 *J. Mod. Opt.* **44** 2173
[11] Chen Z B, Pan J W, Zhang Y D *et al* 2003 *Phys. Rev. Lett.* **90** 160408
[12] Yang T, Zhang Q, Zhang J *et al* 2005 *Phys. Rev. Lett.* **95** 240406
[13] Kwiat P G, Mattle K, Weinfurter H *et al* 1995 *Phys. Rev. Lett.* **75** 4337
[14] Englert B G, Kurtsiefer C, Weinfurter H 2001 *Phys. Rev.* A **63** 032303
[15] Chen Z B, Zhang Q, Bao X H *et al* 2006 *Phys. Rev.* A **73** 050302(R)

Quantum key distribution based on hyperentanglement swapping*

Feng Fa-Yong† Zhang Qiang
(*Department of Modern Physics, University of Science and Technology of China, Hefei* 230026, *China*)
(Received 9 August 2006; revised manuscript received 30 November 2006)

Abstract

We present a quantum key distribution scheme based on hyperentanglement swapping, which can simultaneously generate deterministic and random keys without the loss of security. The scheme only requires two-photon states entangled both in spatial (path) and polarization modes, and such a photon pair can create 4 bit of secure keys (2 bit of random keys and 2 bit of deterministic keys). Our protocol can be implemented with linear optics under current technology.

Keywords: quantum key distribution, hyperentanglement, linear optics
PACC: 0367, 4250

* Project supported by the National Natural Science Foundation of China (Grant No. 10575093).
† E-mail: fyfeng@mail.ustc.edu.cn