第 54 卷 第 12 期 2005 年 12 月
1000-3290/2005/54(12)/5544-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.12,December,2005

基于纠缠交换的多方多级量子密钥分配协议*

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 1 月 27 日收到;2005 年 6 月 30 日收到修改稿)

提出了一种基于纠缠交换的多方多级量子密钥分配协议.构造了一种两方三级系统的完备正交归一化基,利用该正交归一化基和纠缠交换可以实现两方量子密钥分配.同时,三级可以推广到多级以及两方推广到多方,即可以实现基于纠缠交换的多方多级量子密钥分配.这样,利用纠缠交换和多级密钥分配可以极大地提高检测窃听的效率、密钥生成率以及信息容量.

关键词:量子密钥分配,纠缠交换,多方,多级

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,诸如 Ekert91[2],BBM92[3],B92[4] 以及其他协议[5].然而这些量子密钥分配协议仅仅包括两方两级系统.近年来,研究人员开始研究包括两方多级系统的量子密钥分配协议[6—10]或者多方两级系统的量子密钥分配协议[11,12].本文提出了一种基于纠缠交换的多方多级量子密钥分配协议.构造了一种两方三级系统的完备正交归一化基,利用该正交归一化基和纠缠交换可以实现两方量子密钥分配.同时,三级可以推广到多级以及两方推广到多方,即可以实现基于纠缠交换的多方多级量子密钥分配.这样,利用纠缠交换和多级密钥分配可以极大地提高检测窃听的效率、密钥生成率以及信息容量.

2. 基于纠缠交换的两方多级量子密钥分配

如果 $H^{(1)}$ 和 $H^{(2)}$ 分别是基为 $\{|i\rangle\}$ 和 $\{|j\rangle\}$ $(i,j=0,1,2)$ 的 Hilbert 空间,那么 3×3 系统 $H=H^{(1)}\otimes H^{(2)}$ 的基为 $\{|i\rangle|j\rangle\}$ $(i,j=0,1,2)$.把方阵 $\{|i\rangle|j\rangle\}$ $(i,j=0,1,2)$ 重新排列,

$$\begin{bmatrix} |0\rangle|0\rangle, & |0\rangle|1\rangle, & |0\rangle|2\rangle \\ |1\rangle|0\rangle, & |1\rangle|1\rangle, & |1\rangle|2\rangle \\ |2\rangle|0\rangle, & |2\rangle|1\rangle, & |2\rangle|2\rangle \end{bmatrix} \longrightarrow \begin{bmatrix} |0\rangle|0\rangle & & \\ |1\rangle|0\rangle & |1\rangle|1\rangle & \\ |2\rangle|0\rangle & |2\rangle|1\rangle & |2\rangle|2\rangle \\ & |1\rangle|2\rangle & |0\rangle|2\rangle \\ & & |0\rangle|1\rangle \end{bmatrix}. \tag{1}$$

现在可以定义一组新的完备正交归一化基 $\{|W_i\rangle, |X_i\rangle, |Y_i\rangle\}$ $(i=0,1,2)$.每次取(1)式中右边方阵中从左上到右下斜对齐的三个输入,把它们适当地组合,即

$$|W_0\rangle=\frac{1}{\sqrt{3}}(|0\rangle|0\rangle+|1\rangle|1\rangle+|2\rangle|2\rangle), \tag{2}$$

* 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

$$|X_0\rangle = \frac{1}{\sqrt{3}}(|0\rangle|0\rangle + e^{i\phi}|1\rangle|1\rangle + e^{-i\phi}|2\rangle|2\rangle), \quad (3)$$

$$|Y_0\rangle = \frac{1}{\sqrt{3}}(|0\rangle|0\rangle + e^{-i\phi}|1\rangle|1\rangle + e^{i\phi}|2\rangle|2\rangle), \quad (4)$$

$$|W_1\rangle = \frac{1}{\sqrt{3}}(|1\rangle|0\rangle + |2\rangle|1\rangle + |0\rangle|2\rangle), \quad (5)$$

$$|X_1\rangle = \frac{1}{\sqrt{3}}(|1\rangle|0\rangle + e^{i\phi}|2\rangle|1\rangle + e^{-i\phi}|0\rangle|2\rangle), \quad (6)$$

$$|Y_1\rangle = \frac{1}{\sqrt{3}}(|1\rangle|0\rangle + e^{-i\phi}|2\rangle|1\rangle + e^{i\phi}|0\rangle|2\rangle), \quad (7)$$

$$|W_2\rangle = \frac{1}{\sqrt{3}}(|2\rangle|0\rangle + |1\rangle|2\rangle + |0\rangle|1\rangle), \quad (8)$$

$$|X_2\rangle = \frac{1}{\sqrt{3}}(|2\rangle|0\rangle + e^{i\phi}|1\rangle|2\rangle + e^{-i\phi}|0\rangle|1\rangle), \quad (9)$$

$$|Y_2\rangle = \frac{1}{\sqrt{3}}(|2\rangle|0\rangle + e^{-i\phi}|1\rangle|2\rangle + e^{i\phi}|0\rangle|1\rangle), \quad (10)$$

式中 $\phi = \frac{2\pi}{3}$.显然,$\{|W_i\rangle, |X_i\rangle, |Y_i\rangle\}(i = 0,1,2)$是 9 个纠缠态.

2.1. 基于纠缠交换的两方多级量子密钥分配协议

我们给出基于纠缠交换的两方三级量子密钥分配协议.协议中的 Alice 和 Bob 表示合法通信用户,Eve 表示窃听者.

(1) Alice 有 4 个三级粒子.粒子 1 和粒子 2 处于基(2)—(10)式中一个公开的基态,粒子 3 和粒子 5 处于基(2)—(10)式中一个公开的基态.相距遥远的 Bob 拥有处于基(2)—(10)式中的一个公开的基态的粒子 4 和粒子 6.例如 6 个粒子的初始态为

$$|\psi_{\mathrm{I}}\rangle = |W_0\rangle_{12} \otimes |W_0\rangle_{35} \otimes |W_0\rangle_{46}. \quad (11)$$

Alice 通过一个不安全的量子信道把粒子 2 发送给 Bob(Eve 可以操纵粒子 2).

(2) Bob 通过一个不安全的量子信道把粒子 6 发送给 Alice(Eve 可以操纵粒子 6).

(3) Alice 在确定双方均收到一个粒子之后随机地选择实施以下两个步骤.

(ⅰ) Alice 对粒子 1 和粒子 3 作一个基(2)—(10)式上的测量(在此称为 Alice 的秘密测量,且作为密钥),并且对粒子 5 和粒子 6 作一个基(2)—(10)式上的测量(在此称为 Alice 的公开测量)并把粒子 5 和粒子 6 的测量结果公开.Bob 对粒子 2 和粒子 4 作一个基(2)—(10)式上的测量(在此称为 Bob 的秘密测量).如果没有 Eve 存在,Bob 根据自己的秘密测量结果和 Alice 的公开测量结果可以推断密钥.总的态变化为

$$|\psi_{\mathrm{II}}\rangle = |\mathrm{AS}\rangle_{13} \otimes |\mathrm{BS}\rangle_{24} \otimes |\mathrm{AP}\rangle_{56}. \quad (12)$$

(ⅱ) Alice 对粒子 3 作了三级的 Hadamard 变换,然后 Alice 对粒子 1 和粒子 3 作一个基(2)—(10)式上的测量(在此称为 Alice 的秘密测量,且作为密钥),并且对粒子 5 和粒子 6 作一个基(2)—(10)式上的测量(在此称为 Alice 的公开测量)并把粒子 5 和粒子 6 的测量结果公开.另外,Alice 公开她已对粒子 3 作了三级的 Hadamard 变换.Bob 对粒子 4 作三级的 Hadamard 变换并对粒子 2 和粒子 4 作一个基(2)—(10)式上测量.如果没有 Eve 存在,Bob 根据自己的秘密测量结果和 Alice 的公开测量结果可以推断密钥.

(4) Alice 和 Bob 随机地选取一个足够大的秘密测量结果子集,利用 Alice 的秘密测量结果、Bob 的秘密测量结果和 Alice 的公开测量结果的相关性检测窃听.如果错误率低于某一门限值,Alice 和 Bob 利用经典的错误纠正和秘密放大方法获得最终密钥,否则放弃所获得的随机比特.

2.2. 基于纠缠交换的两方多级量子密钥分配协议的安全性分析

所提出的基于纠缠交换的两方多级量子密钥分配协议具有以下特点.

(1)具有更高的密钥生成率.在 BB84 以及 B92 协议中,Bob 和 Alice 必须随机选择两种测量基来保证安全性.这意味着 Alice 和 Bob 通过所传送的量子比特所共享的、有用的随机比特数在检测窃听之前每一传送的量子比特共享 0.5 个比特,在 E91 协议中为 0.25 个比特.在我们提出的方案中达到 $\log_2 3$ 个比特,这是因为 Alice 和 Bob 总是实施相同基的测量,所以在协议的过程中都获得了 $2\log_2 3$ 个相关的比特.如果级数为 d,则每个传送的粒子所获得的共享密钥为 $\log_2 d$,所以级数越高密钥率越高.

(2)仅仅需要一个单一量子系统而不是一系列的量子系统来生成任意长度的密钥.相同的两个粒子(粒子 2 和粒子 6)在 Alice 和 Bob 之间反复传送.

(3)基于纠缠交换的协议具有更高的窃听检测率,并且为获得相同的检测率只需测试更少的随机比特.所传送的粒子本身不携带任何信息,仅仅由 Alice 和 Bob 之间测量结果的相关性确定密钥.所以截取和复制它们不能使 Eve 获得任何关于密钥的信息.根据 Alice 和 Bob 的测量结果以及 Alice 公开的测量结果的相关性,Alice 和 Bob 通过公开比较他们所获得的随机比特一个足够大的子集来检测窃听.如果他们发现所测试的子集相同,可以推断没有窃听存在且剩下的未测试的随机比特也是相同的,就形成一个密钥.在 BB84 协议中,对于每一被测试的比特,揭示 Eve 存在的检测概率为$\frac{1}{4}$(假设 Eve 确实存在).这样,如果测试了 N 个比特,则揭示 Eve 存在的检测概率为 $1-(\frac{3}{4})^N$.在本方案中,如果 Alice 和 Bob 测试了 N 个比特,则揭示 Eve 存在的检测概率为 $1-(\frac{1}{9})^{\frac{N}{2\log_2 3}}$.

对于级数 $d>3$ 的情形,类似于级数为 3 的情形.首先定义一个新的包括 d^2 个基矢量的完备正交归一化基 $\{|W_i\rangle,|X_i\rangle,|Y_i\rangle,\cdots,|Z_i\rangle\}$($i=0,1,2,3,\cdots,d-1$),具体构造方法类似于级数为 3 的情形.协议也类似于级数为 3 的情形.对于级数为 d 的情形,检测窃听的效率、密钥生成率分别为 $1-\left(\frac{1}{d^2}\right)^{\frac{N}{2\log_2 d}}$ 和 $\log_2 d$.

3. 基于纠缠交换的多方多级量子密钥分配协议

将上述两方多级量子密钥分配协议推广到多方多级量子密钥分配协议.对于三方三级的情况,类似于两方三级的情况,首先构造一组新的正交归一化基.

$$|W_0\rangle=\frac{1}{\sqrt{3}}(|0\rangle|0\rangle|0\rangle+|1\rangle|1\rangle|1\rangle+|2\rangle|2\rangle|2\rangle),\tag{13}$$

$$|X_0\rangle=\frac{1}{\sqrt{3}}(|0\rangle|0\rangle|0\rangle+e^{i\phi}|1\rangle|1\rangle|1\rangle+e^{-i\phi}|2\rangle|2\rangle|2\rangle),\tag{14}$$

$$|Y_0\rangle=\frac{1}{\sqrt{3}}(|0\rangle|0\rangle|0\rangle+e^{-i\phi}|1\rangle|1\rangle|1\rangle+e^{i\phi}|2\rangle|2\rangle|2\rangle),\tag{15}$$

$$|W_1\rangle=\frac{1}{\sqrt{3}}(|1\rangle|0\rangle|0\rangle+|2\rangle|1\rangle|1\rangle+|0\rangle|2\rangle|2\rangle),\tag{16}$$

$$|X_1\rangle=\frac{1}{\sqrt{3}}(|1\rangle|0\rangle|0\rangle+e^{i\phi}|2\rangle|1\rangle|1\rangle+e^{-i\phi}|0\rangle|2\rangle|2\rangle),\tag{17}$$

$$|Y_1\rangle=\frac{1}{\sqrt{3}}(|1\rangle|0\rangle|0\rangle+e^{-i\phi}|2\rangle|1\rangle|1\rangle+e^{i\phi}|0\rangle|2\rangle|2\rangle),\tag{18}$$

$$|W_2\rangle=\frac{1}{\sqrt{3}}(|2\rangle|0\rangle|0\rangle+|1\rangle|2\rangle|2\rangle+|0\rangle|1\rangle|1\rangle),\tag{19}$$

$$|X_2\rangle=\frac{1}{\sqrt{3}}(|2\rangle|0\rangle|0\rangle+e^{i\phi}|1\rangle|2\rangle|2\rangle+e^{-i\phi}|0\rangle|1\rangle|1\rangle),\tag{20}$$

$$|Y_2\rangle=\frac{1}{\sqrt{3}}(|2\rangle|0\rangle|0\rangle+e^{-i\phi}|1\rangle|2\rangle|2\rangle+e^{i\phi}|0\rangle|1\rangle|1\rangle),\tag{21}$$

$$|W_3\rangle=\frac{1}{\sqrt{3}}(|0\rangle|0\rangle|1\rangle+|1\rangle|1\rangle|2\rangle+|2\rangle|2\rangle|0\rangle),\tag{22}$$

$$|X_3\rangle=\frac{1}{\sqrt{3}}(|0\rangle|0\rangle|1\rangle+e^{i\phi}|1\rangle|1\rangle|2\rangle+e^{-i\phi}|2\rangle|2\rangle|0\rangle),\tag{23}$$

$$|Y_3\rangle=\frac{1}{\sqrt{3}}(|0\rangle|0\rangle|1\rangle+e^{-i\phi}|1\rangle|1\rangle|2\rangle+e^{i\phi}|2\rangle|2\rangle|0\rangle),\tag{24}$$

$$|W_4\rangle=\frac{1}{\sqrt{3}}(|1\rangle|0\rangle|1\rangle+|2\rangle|1\rangle|2\rangle+|0\rangle|2\rangle|0\rangle),\tag{25}$$

$$|X_4\rangle=\frac{1}{\sqrt{3}}(|1\rangle|0\rangle|1\rangle+e^{i\phi}|2\rangle|1\rangle|2\rangle+e^{-i\phi}|0\rangle|2\rangle|0\rangle),\tag{26}$$

$$|Y_4\rangle=\frac{1}{\sqrt{3}}(|1\rangle|0\rangle|1\rangle+e^{-i\phi}|2\rangle|1\rangle|2\rangle+e^{i\phi}|0\rangle|2\rangle|0\rangle),\tag{27}$$

$$|W_5\rangle=\frac{1}{\sqrt{3}}(|2\rangle|0\rangle|1\rangle+|1\rangle|2\rangle|0\rangle+|0\rangle|1\rangle|2\rangle),\tag{28}$$

$$|X_5\rangle=\frac{1}{\sqrt{3}}(|2\rangle|0\rangle|1\rangle+e^{i\phi}|1\rangle|2\rangle|0\rangle$$

$$+ e^{-i\phi} |0\rangle |1\rangle |2\rangle), \quad (29)$$

$$|Y_5\rangle = \frac{1}{\sqrt{3}}(|2\rangle |0\rangle |1\rangle + e^{-i\phi} |1\rangle |2\rangle |0\rangle + e^{i\phi} |0\rangle |1\rangle |2\rangle), \quad (30)$$

$$|W_6\rangle = \frac{1}{\sqrt{3}}(|0\rangle |0\rangle |2\rangle + |1\rangle |1\rangle |0\rangle + |2\rangle |2\rangle |1\rangle), \quad (31)$$

$$|X_6\rangle = \frac{1}{\sqrt{3}}(|0\rangle |0\rangle |2\rangle + e^{i\phi} |1\rangle |1\rangle |0\rangle + e^{-i\phi} |2\rangle |2\rangle |1\rangle), \quad (32)$$

$$|Y_6\rangle = \frac{1}{\sqrt{3}}(|0\rangle |0\rangle |2\rangle + e^{-i\phi} |1\rangle |1\rangle |0\rangle + e^{i\phi} |2\rangle |2\rangle |1\rangle), \quad (33)$$

$$|W_7\rangle = \frac{1}{\sqrt{3}}(|1\rangle |0\rangle |2\rangle + |2\rangle |1\rangle |0\rangle + |0\rangle |2\rangle |1\rangle), \quad (34)$$

$$|X_7\rangle = \frac{1}{\sqrt{3}}(|1\rangle |0\rangle |2\rangle + e^{i\phi} |2\rangle |1\rangle |0\rangle + e^{-i\phi} |0\rangle |2\rangle |1\rangle), \quad (35)$$

$$|Y_7\rangle = \frac{1}{\sqrt{3}}(|1\rangle |0\rangle |2\rangle + e^{-i\phi} |2\rangle |1\rangle |0\rangle + e^{i\phi} |0\rangle |2\rangle |1\rangle), \quad (36)$$

$$|W_8\rangle = \frac{1}{\sqrt{3}}(|2\rangle |0\rangle |2\rangle + |1\rangle |2\rangle |1\rangle + |0\rangle |1\rangle |0\rangle), \quad (37)$$

$$|X_8\rangle = \frac{1}{\sqrt{3}}(|2\rangle |0\rangle |2\rangle + e^{i\phi} |1\rangle |2\rangle |1\rangle + e^{-i\phi} |0\rangle |1\rangle |0\rangle), \quad (38)$$

$$|Y_8\rangle = \frac{1}{\sqrt{3}}(|2\rangle |0\rangle |2\rangle + e^{-i\phi} |1\rangle |2\rangle |1\rangle + e^{i\phi} |0\rangle |1\rangle |0\rangle), \quad (39)$$

式中 $\phi = \frac{2\pi}{3}$. 显然 $\{|W_i\rangle, |X_i\rangle, |Y_i\rangle\}$ $(i = 0,1,2,\cdots,8)$ 是 27 个纠缠态.

我们给出了基于纠缠交换的三方三级量子密钥分配协议. 协议中的 Alice, Bob 和 Carol 表示合法通信用户, Eve 表示窃听者.

(1) 初始阶段, Alice 拥有粒子 1、粒子 2、粒子 3、粒子 A 和粒子 B. 粒子 1 和粒子 2 处于基(2)—(10)式中的一个公开的基态. 粒子 3、粒子 A 和粒子 B 制备在基(13)—(39)式的一个公开的基态. Bob(Carol)拥有粒子 5 和粒子 D(粒子 4 和粒子 C). 粒子 5 和粒子 D(粒子 4 和粒子 C)制备在基(2)—(10)式中的一个公开的基态. 例如,初始 9 个粒子的态为

$$|\psi_{\mathrm{I}}\rangle = |W_0\rangle_{3AB} \otimes |W_0\rangle_{12} \otimes |W_0\rangle_{5D} \otimes |W_0\rangle_{4C}. \quad (40)$$

Alice 通过一个不安全的量子信道把粒子 A(B)发送给 Bob(Carol)(Eve 可以操纵粒子 A 和粒子 B).

(2) Bob(Carol)通过一个不安全的量子信道把粒子 D(C)发送给 Alice(Eve 可以操纵粒子 D 和粒子 C).

(3) Alice 在确定三方均收到一个粒子之后随机地选择实施以下两个步骤.

(ⅰ) Alice 对粒子 2 和粒子 3 作一个基(2)—(10)式上的测量(在此称为 Alice 的秘密测量)并且对粒子 1、粒子 C 和粒子 D 作一个基(13)—(39)式上的测量(在此称为 Alice 的公开测量)并把粒子 1、粒子 C 和粒子 D 的测量结果公开. Bob(Carol)对粒子 5 和粒子 A(粒子 4 和粒子 B)作一个基(2)—(10)式上的测量(在此称为 Bob(Carol)的秘密测量). 如果没有 Eve 存在, Bob(Carol)根据自己的秘密测量结果和 Alice 的公开测量结果可以推断密钥. 最后的态为

$$|\varphi_{\mathrm{III}}\rangle = |\mathrm{AP}\rangle_{1CD} \otimes |\mathrm{AS}\rangle_{23} \otimes |\mathrm{BS}\rangle_{5A} \otimes |\mathrm{CS}\rangle_{4B}. \quad (41)$$

Alice 的公开测量结果 $|\mathrm{AP}\rangle_{1CD}$, Alice 的秘密测量结果 $|\mathrm{AS}\rangle_{23}$, Bob 的秘密测量结果 $|\mathrm{BS}\rangle_{5A}$, Carol 的秘密测量结果 $|\mathrm{CS}\rangle_{4B}$ 的组合一共有 19683 种,但 $|\psi_{\mathrm{III}}\rangle$ 只有 729 种可能的组合出现的概率不为零.

(ⅱ) Alice 对粒子 2 作了三级的 Hadamard 变换,然后 Alice 对粒子 2 和粒子 3 作一个基(2)—(10)式上的测量(在此称为 Alice 的秘密测量)并且对粒子 1、粒子 C 和粒子 D 作一个基(13)—(39)式上的测量(在此称为 Alice 的公开测量)并把粒子 1、粒子 C 和粒子 D 的测量结果公开. 另外, Alice 公开其已对粒子 2 作了三级的 Hadamard 变换. Bob(Carol)对粒子 5(4)作三级的 Hadamard 变换并对粒子 5 和粒子 A(粒子 4 和粒子 B)作一个基(2)—(10)式上的测量. 如果没有 Eve 存在, Bob(Carol)根据自己的秘密测量结果和 Alice 的公开测量结果可以推断密钥.

(4) Alice, Bob 和 Carol 随机地选取一个足够大的秘密测量结果子集,利用 Alice 的秘密测量结果、Bob 的秘密测量结果、Carol 的秘密测量结果和 Alice 的公开测量结果的相关性检测窃听. 如果错误率低于某一门限值, Alice, Bob 和 Carol 利用经典的错误纠正和秘密放大方法获得最终密钥,否则放弃所获得的随机比特.

4. 结 论

本文提出了一种基于纠缠交换的多方多级量子密钥分配协议.该方案实现的可行性取决于基(2)—(10)式上的可靠测量、基(13)—(39)式上的可靠测量以及制备具有多个能量级的粒子处于某一规定的态并将之发送给多个接收者的可行性.另外,态的消相干时间也是实现该方案可行性需要考虑的一个重要因素.

[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] Durt T, Cerf N J, Gisin N *et al* 2003 *Phys. Rev.* A **67** 012311

[7] Bechmann-Pasquinucci H, Tittel W 2000 *Phys. Rev.* A **61** 062308

[8] Bourennane M, Karlsson A, Björk G *et al* 2002 *J. Phys. A* **35** 10065

[9] Bourennane M, Karlsson A, Björk G 2001 *Phys. Rev.* A **64** 012306

[10] Cerf N J, Bourennane M, Karlsson A *et al* 2002 *Phys. Rev. Lett.* **88** 127902

[11] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[12] Scarani V, Gisin N 2001 *Phys. Rev.* A **65** 012311

Multi-party multi-level quantum key distribution protocol based on entanglement swapping*

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 27 January 2005; revised manuscript received 30 June 2005)

Abstract

A multi-party multi-level quantum key distribution protocol based on entanglement swapping is proposed. A perfect complete orthonormal basis of the bi-party three-level systems is first constructed. By using this basis and swapping the entanglement, bi-party quantum key distribution is realized. In addition, three-level can be generalized to multi-level and bi-party to multi-party, i.e., multi-party multi-level quantum key distribution based on entanglement swapping can be achieved. Using entanglement swapping and multi-level key distribution can significantly increase the efficiency of the detection of eavesdropping, the key generation rate and the information flux.

Keywords: quantum key distribution, entanglement swapping, multi-party, multi-level

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