第 25 卷 第 11 期
2005 年 11 月

光 学 学 报
ACTA OPTICA SINICA

Vol. 25, No. 11
November, 2005

文章编号：0253-2239(2005)11-1568-5

基于六光子量子避错码的量子密钥分发方案*

刘文予 李 宁 王长强 刘 玉

（华中科技大学 电子与信息工程系，武汉 430074）

摘要： 量子信道中不可避免存在的噪声将扭曲被传输的信息，对通信造成危害。目前克服量子信道噪声的较好方案是量子避错码(QEAC)。将量子避错码思想用于量子密钥分发，能有效克服信道中的噪声，且无需复杂的系统。用六光子构造了量子避错码，提出了一种基于六光子避错码的量子密钥分发(QDK)方案。以提高量子密钥分发的量子比特效率和安全性为前提，对六光子避错码的所有可能态进行组合，得到一种六光子避错码的最优组合方法，可将两比特信息编码在一个态中，根据测量结果和分组信息进行解码，得到正确信息的平均概率为 7/16。与最近的基于四光子避错码的克服量子信道噪声的量子密钥分发方案相比，该方案的量子比特效率提高了 16.67%，密钥分发安全性是它的 3.5 倍。

关键词： 量子光学；量子信息；量子密钥分发；量子避错码；量子纠缠

中图分类号：O431.2　　文献标识码：A

Quantum Key Distribution Based on Six-Photon Quantum Error-Avoiding Code

Liu Wenyu　Li Ning　Wang Changqiang　Liu Yu

(*Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan* 430074)

Abstract: Noise that unavoidably exists in the quantum channel will distort transmitted information and destroy the communication. The superior scheme to overcome the noise at present is quantum error-avoiding code (QEAC). The quantum key distribution (QKD) using the QEAC will be robust in the quantum noisy channel without complex system. Six-photon error-avoiding code (SPEAC) is constituted and a robust QKD scheme based on it is proposed. In order to improve the qubit efficiency and the security of QKD, all the possible quantum states in the SPEAC are assembled, and as a result, an optimal scheme is developed, by which two key bits can be encoded in each state and Bob can decode the information successfully with an average probability of 7/16. Compared with the recent QKD scheme based on four-photon QEAC, the qubit efficiency of the authors' scheme increases by 16.67%, and the security is 3.5 times of it.

Key words: quantum optics; quantum information; quantum key distribution; quantum error-avoiding code; quantum entanglement

1 引　　言

无论是经典通信还是量子通信中，光纤信道均是主要的通信信道之一。然而，由于光纤本身的缺陷，光纤信道中存在的偏振效应已成为通信的一大障碍。对经典通信而言，光纤中的偏振效应将导致高速光纤通信系统的脉冲展宽[1]，从而对信号的接收灵敏度及频谱产生影响[2]。对量子通信而言，光纤中的偏振效应将使光子的偏振态发生改变(我们称这种由光纤中的偏振效应引起的噪声为集体噪声)，从而使偏振编码在光纤信道中变得不可用。因此，要实现光纤信道中的量子通信，就必须采取适当措施克服集体噪声。

* 湖北省自然科学基金(2003ABA008)资助课题。

作者简介：刘文予(1963～)，男，湖南人，教授，博士生导师，主要研究方向为多媒体通信与多媒体信息处理、网络安全与数字媒体版权保护、计算机视觉与图形。E-mail：liuwy@hust.edu.cn

收稿日期：2004-12-17；收到修改稿日期：2005-04-05

目前克服量子信道噪声的方案有多种[3~17],其中量子信道编码方案[3~15]是主流方案,而量子避错码(QEAC)方案[8~14]又是量子信道编码方案中较理想者。量子避错码本质上利用了消相干过程中的集体效应即集体消相干,因为在集体消相干情况下,存在能完全保持量子相干性的输入态即相干保持态。量子避错码构造的关键在于找到一组相干保持态,它们构成一个不受外界噪声影响的无噪子空间,将要传输的密钥比特编码在这个子空间中,能有效抵御外界噪声的影响,保护被传输的信息。

结合量子避错码进行密钥分发的方案可参见文献[18~20],基于最近的四光子方案[19],我们构造了六光子避错码,提出了基于六光子避错码的量子密钥分发(QKD)方案。通过对该方案与四光子方案[19]的分析比较,我们证明了该方案的量子比特效率较四光子方案提高了 16.67%,安全性是四光子方案的 3.5 倍。

2　基于六光子避错码的量子密钥分发方案

四个 Bell 基中有一个很特殊的态

$$|\psi^-\rangle=1/\sqrt{2}(|01\rangle-|10\rangle),$$

$|0\rangle$和$|1\rangle$分别代表水平偏振态$|H\rangle$和垂直偏振态$|V\rangle$,这个态构成的量子系统总自旋为 0。当它的每一个量子位发生相同的偏振旋转时,整个量子态不发生改变,从而对光纤信道中的集体噪声有较好的鲁棒性,可将信息编码在这个态中使其不受集体噪声影响。基于$|\psi^-\rangle$的这个特殊性质,我们用六光子构造了量子避错码,表 1 中列出了六光子避错码的所有可能形式,其中,$|\psi_1\rangle$,$|\psi_2\rangle$,…,$|\psi_{15}\rangle$ 为六光子避错码的所有可能态;组合方式中的 1,2,…,6 分别表示第一,第二,…,第六个光子。12 表示第一、第二个光子纠缠,依此类推;图示栏中采用图示的排列来描述纠缠态的配对方式,相同符号的小球处于最大纠缠态;$|a\rangle$,$|b\rangle$,…,$|j\rangle$为分量,由分量的表达式可知,不同的分量彼此正交。

表 1　六光子避错码所有可能的态及组合方式

Table 1　Possible assembles of six-photon quantum error-avoiding code (QEAC.)

Encoded states	Pairing ways	Illustrations	Expressions	Remark
$\|\psi_1\rangle$	13　24　56	○⊕○⊕⊗⊗	$1/\sqrt{2}(\|c\rangle+\|h\rangle-\|i\rangle-\|b\rangle)$	$\|a\rangle=1/2(\|000111\rangle-\|111000\rangle)$
$\|\psi_2\rangle$	12　34　56	○○⊕⊕⊗⊗	$1/\sqrt{2}(\|f\rangle+\|h\rangle-\|e\rangle-\|i\rangle)$	$\|b\rangle=1/2(\|001110\rangle-\|110001\rangle)$
$\|\psi_3\rangle$	13　25　46	○⊕○⊗⊕⊗	$1/\sqrt{2}(\|d\rangle+\|h\rangle-\|j\rangle-\|b\rangle)$	$\|b\rangle=1/2(\|001110\rangle-\|110001\rangle)$
$\|\psi_4\rangle$	15　24　36	○⊕⊗⊕○⊗	$1/\sqrt{2}(\|g\rangle-\|a\rangle+\|i\rangle+\|b\rangle)$	$\|c\rangle=1/2(\|001101\rangle-\|110010\rangle)$
$\|\psi_5\rangle$	12　35　46	○○⊕⊗⊕⊗	$1/\sqrt{2}(\|g\rangle+\|h\rangle-\|j\rangle-\|e\rangle)$	$\|d\rangle=1/2(\|001011\rangle-\|110100\rangle)$
$\|\psi_6\rangle$	14　35　26	○⊗⊕○⊕⊗	$1/\sqrt{2}(\|c\rangle-\|a\rangle+\|j\rangle+\|e\rangle)$	$\|d\rangle=1/2(\|001011\rangle-\|110100\rangle)$
$\|\psi_7\rangle$	14　23　56	○⊕⊕○⊗⊗	$1/\sqrt{2}(\|f\rangle+\|b\rangle-\|c\rangle-\|e\rangle)$	$\|e\rangle=1/2(\|010110\rangle-\|101001\rangle)$
$\|\psi_8\rangle$	13　45　26	○⊗○⊕⊕⊗	$1/\sqrt{2}(\|c\rangle-\|d\rangle-\|i\rangle+\|j\rangle)$	$\|f\rangle=1/2(\|010101\rangle-\|101010\rangle)$
$\|\psi_9\rangle$	15　23　46	○⊕⊕⊗○⊗	$1/\sqrt{2}(\|d\rangle+\|e\rangle-\|g\rangle-\|b\rangle)$	$\|f\rangle=1/2(\|010101\rangle-\|101010\rangle)$
$\|\psi_{10}\rangle$	15　34　26	○⊗⊕⊕○⊗	$1/\sqrt{2}(\|d\rangle-\|a\rangle+\|i\rangle+\|e\rangle)$	$\|g\rangle=1/2(\|010011\rangle-\|101100\rangle)$
$\|\psi_{11}\rangle$	25　34　16	⊗○⊕⊕○⊗	$1/\sqrt{2}(\|d\rangle-\|a\rangle+\|f\rangle+\|h\rangle)$	$\|h\rangle=1/2(\|100110\rangle-\|011001\rangle)$
$\|\psi_{12}\rangle$	12　45　36	○○⊗⊕⊕⊗	$1/\sqrt{2}(\|f\rangle+\|j\rangle-\|g\rangle-\|i\rangle)$	$\|h\rangle=1/2(\|100100\rangle-\|011001\rangle)$
$\|\psi_{13}\rangle$	24　35　16	⊗○⊕○⊕⊗	$1/\sqrt{2}(\|c\rangle-\|a\rangle+\|g\rangle+\|h\rangle)$	$\|i\rangle=1/2(\|100101\rangle-\|011010\rangle)$
$\|\psi_{14}\rangle$	23　45　16	⊗○○⊕⊕⊗	$1/\sqrt{2}(\|c\rangle-\|d\rangle-\|f\rangle+\|g\rangle)$	$\|j\rangle=1/2(\|100011\rangle-\|011100\rangle)$
$\|\psi_{15}\rangle$	14　25　36	○⊕⊗○⊕⊗	$1/\sqrt{2}(\|f\rangle-\|a\rangle+\|j\rangle+\|b\rangle)$	$\|j\rangle=1/2(\|100011\rangle-\|011100\rangle)$

从表 1 中可得知,$\langle\psi_i|\psi_j\rangle=1/2$ 或 1/4,其中 $i\neq j$。因此不可能通过测量完全区分这些态,但可以通过给予接收方辅助信息使其将各态区分开来,得到编码在态中的经典信息。

下面我们给出基于六光子避错码的量子密钥分发方案的具体步骤:

第一步:用六光子避错码构成如下 4 个编码态组合:{$|\psi_1\rangle|\psi_2\rangle|\psi_3\rangle|\psi_4\rangle$}、{$|\psi_5\rangle|\psi_6\rangle|\psi_7\rangle|\psi_8\rangle$}、{$|\psi_6\rangle|\psi_9\rangle|\psi_{10}\rangle|\psi_{11}\rangle$}、{$|\psi_{12}\rangle|\psi_{13}\rangle|\psi_7\rangle|\psi_{14}\rangle$}(这样分组的理由见后文协议分析部分);

第二步:Alice 随机地生成长为 $2n$ bit 的串 A 和长为 n 的序列 B,A 为信息串,取值 0 或 1,B 作为编码辅助串,取值 1,2,3,4,分别与第一步中 4 个组的编号对应。B 中的每一位顺序对应 A 中的两个 bit;

第三步：Alice 根据她已选择的 B 值和 A 值从表 2 中找到对应的态对信息串 A 进行编码；

表 2 由比特串 A 和序列 B 的值确定的编码态

Table 2 Encoded states determined by the values of bit sequence A and sequence B

A	00	01	10	11
$B=1$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_4\rangle$
$B=2$	$\|\psi_5\rangle$	$\|\psi_6\rangle$	$\|\psi_7\rangle$	$\|\psi_8\rangle$
$B=3$	$\|\psi_6\rangle$	$\|\psi_9\rangle$	$\|\psi_{10}\rangle$	$\|\psi_{11}\rangle$
$B=4$	$\|\psi_{12}\rangle$	$\|\psi_{13}\rangle$	$\|\psi_7\rangle$	$\|\psi_{14}\rangle$

第四步：Alice 将编码后的 n 个六光子态发送给 Bob；

第五步：Bob 接收完光子后，通知 Alice 光子接收完毕。对每一个六光子态，Bob 随机从直线偏振基(+)和对角偏振基(×)中选择一个，再用选择的基对这个六光子态中的每一个光子进行单独测量；

第六步：Alice 在经典信道上将序列 B 告诉 Bob。根据 B 值以及测量结果，Bob 判断 Alice 所用的编码态。若测量结果是序列 B 中某态独有的分量，则可得出 Alice 的编码态，得到编码值(测量结果为确定性的)；若无法确定地得出 Alice 的编码态(测量结果为非确定性的)，则此次信息传递失败，丢弃所有信息。

例如，若测量结果为“001101”($|c\rangle$分量)，又得知编码序列为 $\{|\psi_1\rangle|\psi_2\rangle|\psi_3\rangle|\psi_4\rangle\}$，其中只有 $|\psi_1\rangle$中有 $|c\rangle$分量，则编码态为 $|\psi_1\rangle$，解码得到“00”；若在同一序列下测量结果为“100110”($|h\rangle$分量)，由于序列中 $|\psi_1\rangle$、$|\psi_2\rangle$、$|\psi_3\rangle$中均包含 $|h\rangle$，无法确定编码态，从而无法作确定性解码。

此处，Bob 可以通过测量结果判断信道中是否存在窃听。若测量结果中出现了序列中不可能出现的分量或对每一个六光子态的测量结果中 0 和 1 的数目不相等，则认为信道中存在窃听，立即停止本次通信。否则，进行下一步；

第七步：Bob 丢掉所有非确定性的测量结果，Alice 丢掉所有这些非确定性测量结果对应位上的比特。在无窃听情况下，传送每 3 对纠缠光子对，Bob 能获得的平均信息量为：$7/16\times2=7/8$ bit，其中 7/16 为成功解码得到 2 bit 信息的概率。因此传送 n 个六光子态后 Bob 能获得的平均信息量为：$7/16\times2\times n=(7/8)n$ bit，即信息串 A 中平均有 $(7/8)n$ 个 bit 保留下来；

第八步：为确保密钥的绝对安全性，Alice 和 bob 有必要从剩余结果中随机选择部分比特进行比较，进一步检测是否存在窃听。Alice 从剩余比特中随机选择 x 位，在公共信道上告诉 Bob 哪些比特位被选择了；

第九步：Alice 和 Bob 比较被选择的比特值。如果产生的错误超过了一定的阈值，他们就丢弃所有的数据；如果错误率没有超过阈值，则认为不存在窃听，对剩余比特进行保密加强后作为密钥。

3 六光子避错码方案的分析

下面我们对上述方案进行讨论。为了便于后文讨论，先定义一些参量：

1) 量子比特效率 η

Alice 每发送一个光子，Bob 能从中获得的平均信息量，单位为 bit/qubit；

2) 标志分量

各组中每一个编码态独有的分量；

3) 区分概率

Bob 能根据 Alice 给出的部分信息及测量结果正确判断出编码态的概率。

本文中用六光子构建的相干保持态共有 15 个。由表 1 可知，它们彼此不正交，因此不可能通过对各光子单独的广义量子测量(POVM)的测量结果来明确区分各编码态。如测量结果为 $|a\rangle$，由于 $|\psi_4\rangle|\psi_6\rangle|\psi_{10}\rangle|\psi_{11}\rangle|\psi_{13}\rangle|\psi_{15}\rangle$中均含有分量 $|a\rangle$，则编码态可能为其中任意一个，无法区分。但若将所有态按上述方法分组，并在 Bob 测量后告知编码态所在的分组信息，则 $|a\rangle$可能出现的范围就大大缩小了。原则上讲，可用 15 个态中的少部分态构成编码空间，并保证 Bob 以非零的概率解码。但该方案对于拦截重放攻击抵抗性很差，因为窃听者 Eve 能以非零的概率确定 Alice 的编码态，并重发给 Bob，完成监听操作。为避免上述情况的发生，应尽可能多地利用这 15 个态，在 Bob 完成测量后再公布分组信息。此时即使 Eve 得到测量结果，也无法以非零的概率明确得知发送态，从而防止了重放攻击。

综上所述，要构建一个安全高效无错的六光子协议，将 15 个态进行分组，并在 Bob 测量结束后告知 Bob 分组信息是必须的。虽然态的组合方式并不固定，但须遵循一定的原则，其中包括更多的信息量及更高的区分概率。下面分别以 8 态分组(每组中包含 8 个编码态)和 2 态分组(每组中包含 2 个编码态)为例分析分组大小的选择。

可以证明不存在可行的 8 态分组，使得其中的

任一态均获得非零的区分概率。因为,若要使 8 个态均有非零的区分概率,则至少需要 8 个不同的标志分量,而每个态均由 4 个分量描述,除去各态中的标志分量,各态中还应有 3 个分量,即使这 8 个态中剩余的 3 个分量均相同,一共也需 11 个分量才能表示出这些态,而本文中只有 10 个分量可用。

若将 2 个态划分在一组,每次传送 1bit 信息,可以做到解码时以 75%的概率区分。但这样做在量子比特效率上与基于四光子避错码的量子密钥分发协议相同:

基于四光子避错码的量子密钥分发协议量子比特效率:$\eta=(1/4)\times(1/2)=1/8$ (bit/qubit);将六光子避错码分为两个一组进行量子密钥分发的协议量子比特效率:$\eta=(1/6)\times(3/4)=1/8$ (bit/qubit)。

在 8 态分组和 2 态分组不可行情况下,我们通过 4 态分组找到了一种六光子避错码子空间的最优分法(如表 3 所示)。

表 3　六光子避错码子空间的一种最优分法

Table 3　One of the optimal divisions of six-photon QEAC subspace

Group	Encoded states	Distinct weights	Distinguishd probability
1	$\|\psi_1\rangle$	$\|c\rangle$	25%
	$\|\psi_2\rangle$	$\|e\rangle,\|f\rangle$	50%
	$\|\psi_3\rangle$	$\|d\rangle,\|j\rangle$	50%
	$\|\psi_4\rangle$	$\|a\rangle,\|g\rangle$	50%
2	$\|\psi_5\rangle$	$\|g\rangle,\|h\rangle$	50%
	$\|\psi_6\rangle$	$\|a\rangle$	25%
	$\|\psi_7\rangle$	$\|b\rangle,\|f\rangle$	50%
	$\|\psi_8\rangle$	$\|d\rangle,\|i\rangle$	50%
3	$\|\psi_6\rangle$	$\|c\rangle,\|j\rangle$	50%
	$\|\psi_9\rangle$	$\|b\rangle,\|g\rangle$	50%
	$\|\psi_{10}\rangle$	$\|i\rangle$	25%
	$\|\psi_{11}\rangle$	$\|f\rangle,\|h\rangle$	50%
4	$\|\psi_{12}\rangle$	$\|i\rangle,\|j\rangle$	50%
	$\|\psi_{13}\rangle$	$\|a\rangle,\|h\rangle$	50%
	$\|\psi_7\rangle$	$\|b\rangle,\|e\rangle$	50%
	$\|\psi_{14}\rangle$	$\|d\rangle$	50%

值得注意的是,上述最优子空间的划分并不是唯一的,但不同划分导致的效率是一样的,即:Alice 可将 2 bit 信息编码在每个六光子态中,Bob 在解码时能以 50%的概率区分每组中的三个态、以 25%的概率区分其中一个态。

理论上可以证明,我们提出的六光子协议在量子比特效率和通信过程安全性方面均优于原有的四光子方案:

1) 量子比特效率

本文提出的六光子协议,在无窃听情况下量子比特效率为 $\eta=(7/16)\times2\times(1/6)=7/48$ (bit/qubit),其中 7/16 为成功解码得到正确信息的概率;原有的四光子协议,在无窃听情况下的量子比特效率为 $\eta=(1/2)\times1\times(1/4)=1/8$ (bit/qubit),其中 1/2 为成功解码得到正确信息的概率。因此,我们提出的六光子协议的量子比特效率是原四光子协议的 $(7/48)/(1/8)=7/6$,也即提高了 $1/6\approx16.67\%$。

2) 通信过程安全性

在讨论协议的安全性之前需建立窃听者(Eve)的攻击模型。从 Eve 的角度来考虑,他肯定是希望最大可能地获得最大量的信息而以最低的概率被发现。那么,当他截获每六个光子时,为了获得分组信息,必须先保住身份不被揭穿,因此,他必须先获得这个结果所处的正确初始态,然后制备一个与之相同的态发送给 Bob。当 Alice 宣布分组信息后,他再根据获得的编码态和分组信息解码,获得 Alice 传送的正确信息。这种攻击无疑给通信方造成巨大的威胁。因此,下面我们分析协议的安全性时,将 Eve 能获得正确信息且不被发现的概率作为协议安全性的决定性因素。

定义 Eve 一次成功的攻击操作为 Eve 伪造出和 Alice 相同的编码态,并被 Bob 解码得到信息。那么,在上述攻击策略中,当 Eve 测量结果为分量 $|r\rangle(r=a,b,\cdots)$ 时,Eve 成功攻击的概率为 $P_{|r\rangle}=\sum_{i=1,2,\cdots,n}P_{\mathrm{cho}}P_{\mathrm{enc}}P_{\mathrm{Eve}}P_{\mathrm{Bob}}$,其中 n 为所有含有测量结果分量的态数量,P_{cho} 为 Eve 选择态 i 的概率,P_{enc} 为态 i 等于 Alice 发送的编码态的概率,P_{Eve} 为 Eve 成功伪造 Alice 的编码态并得到分组信息后,Eve 解码得到信息的概率,P_{Bob} 为 Bob 测量并得到分组信息后,解码得到信息的概率。此处,P_{cho} 与 P_{enc} 的值相同,P_{Eve} 与 P_{Bob} 的值相同。

六光子协议情况下,Eve 测量得到不同分量时能获得正确信息的概率是不完全相同的。

当 Eve 测量结果为 $|a\rangle$ 时,$P_{|a\rangle}=11/192$;当 Eve 测量结果为 $|b\rangle$ 时,$P_{|b\rangle}=5/64$;当 Eve 测量结果为 $|c\rangle$ 时,$P_{|c\rangle}=31/512$;当 Eve 测量结果为 $|d\rangle$ 时,$P_{|d\rangle}=1/32$;当 Eve 测量结果为 $|e\rangle$ 时,$P_{|e\rangle}=65/1024$;当 Eve 测量结果为 $|f\rangle$ 时,$P_{|f\rangle}=5/64$;当 Eve 测量结果为 $|g\rangle$ 时,$P_{|g\rangle}=7/192$;当 Eve 测量结果为 $|h\rangle$ 时,$P_{|h\rangle}=7/192$;当 Eve 测量结果为 $|i\rangle$ 时,$P_{|i\rangle}=1/32$;当 Eve 测量结果为

$|j\rangle$时，$P_{|j\rangle}=1/16$。

那么，对 Eve 得到的任意测量结果$|u\rangle$，Eve 获得正确信息且不被发现的平均概率为

$$\overline{P}_{|u\rangle}=\frac{1}{10}\sum_{i=a,b,\cdots,j}P_{|i\rangle}\approx 0.0535. \quad (1)$$

因此，六光子协议中，Eve 每截获一个光子能以 0.0535 的概率获得 1/3 bit 信息且不被发现。下面将讨论四光子协议的情况。

在原有的四光子协议情况下，Eve 测量得到任意元素$|u\rangle(u=a,b,c)$时，可能获得正确信息且不被发现的概率均相同，即

$$P_{|u\rangle}=\frac{2}{4}\times\frac{2}{4}\times\frac{1}{2}\times\frac{1}{2}+\frac{2}{4}\times\frac{2}{4}\times\frac{1}{2}\times\frac{1}{2}+\frac{2}{4}\times\frac{2}{4}\times\frac{1}{2}\times\frac{1}{2}+\frac{2}{4}\times\frac{2}{4}\times\frac{1}{2}\times\frac{1}{2}=\frac{1}{4}=0.25, \quad (2)$$

因此，Eve 每截获一个光子能以 0.25 的概率获得 1/4 bit 信息且不被发现。由(0.0535×1/3)/(0.25×1/4)=1/3.5可以看出，在不被通信方发现的情况下，四光子方案中泄漏的信息量是六光子方案的 3.5 倍，即六光子方案的安全性是四光子方案的 3.5 倍。

综上所述，与原有的四光子方案相比，六光子协议较大程度上提高了密钥分发的安全性，量子比特效率上也有所提高。

4 结 论

本文中我们提出了基于六光子避错码的量子密钥分发方案，并证明了该方案在量子比特效率和通信过程安全性方面均优于四光子量子密钥分发方案，其中，量子比特效率提高了 16.67%，安全性是四光子方案的 3.5 倍。

需强调的是，本文提出的六光子量子密钥分发方案是针对特定噪声即光纤信道中的集体噪声的，纯态通过该噪声信道仍然为纯态。此外，文中关于安全性的判断也是建立在对于特定攻击方式进行分析的基础上的。

关于该方案的实验实现，由于现在用自变参量下转换(Spontaneous parametric down conversion，SPDC)产生纠缠光子对的效率本来就比较低，而本文中使用了三对两光子纠缠态，因此，量子态的制备将更加复杂和低效。

尽管目前该方案在实验上实现有一定难度，但量子保密通信的主要目的在于保证通信过程的安全性，而该方案能较大程度地提高通信安全性并在一定程度上提高通信效率，因此，该方案仍然具有较大的优越性。

参 考 文 献

1 Wang Muguang, Li Tangjun, Jian Shuisheng *et al.*. Analytical theory of pulse broadening due to polarization effects in optical fibers[J]. *Acta Optica Sinica*, 2004, **24**(4): 512～516 (in Chinese)
王目光，李唐军，简水生 等. 光纤偏振效应导致脉冲展宽的解析模型[J]. 光学学报，2004，**24**(4)：512～516

2 Liu Jianfei, Yu Jinlong, Wang Jian *et al.*. Study on effect of PMD-induced pulse broadening on sensitivity and frequency spectrum[J]. *Acta Optica Sinica*, 2003, **23**(2): 188～192 (in Chinese)
刘剑飞，于晋龙，王 剑 等. 偏振模色散引起的脉冲展宽对接收灵敏度及频谱的影响[J]. 光学学报，2003，**23**(2)：188～192

3 A. R. Calderbank, P. W. Shor. Good quantum error-correcting codes exist[J]. *Phys. Rev.* (*A*), 1996, **54**(2): 1098～1105

4 P. W. Shor. Scheme for reducing decoherence in quantum computer memory[J]. *Phys. Rev.* (*A*), 1995, **52**(4): R2493～R2496

5 A. M. Steane. Error correcting codes in quantum theory[J]. *Phys. Rev. Lett.*, 1996, **77**(5): 793～797

6 A. M. Steane. Multiple particle interference and quantum error correction[J]. *Proc. R. Soc.* (*A*), 1996, **452**: 2551～2577

7 A. M. Steane. Simple quantum error-correcting codes[J]. *Phys. Rev.* (*A*), 1996, **54**(6): 4741～4751

8 L. M. Duan, G. C. Guo. Preserving coherence in quantum computation by pairing quantum bits[J]. *Phys. Rev. Lett.*, 1997, **79**(10): 1953～1956

9 D. A. Lidar, I. L. Chuang, K. B. Whaley. Decoherence-free subspaces for quantum computation[J]. *Phys. Rev. Lett.*, 1998, **81**(12): 2594～2597

10 L. M. Duan, G. C. Guo. Optimal quantum codes for preventing collective amplitude damping[J]. *Phys. Rev.* (*A*), 1998, **58**(5): 3491～3495

11 P. Zanardi, M. Rasetti. Noiseless quantum codes[J]. *Phys. Rev. Lett.*, 1997, **79**(17): 3306～3309

12 J. Kempe, D. Bacon, D. A. Lidar *et al.*. Theory of decoherence-free fault-tolerant universal quantum computation [J]. *Phys. Rev.* (*A*), 2001, **63**(4): 042307-1～042307-29

13 D. A. Lidar, D. Bacon, K. B. Whaley. Concatenating decoherence-free subspaces with quantum error correcting codes [J]. *Phys. Rev. Lett.*, 1999, **82**(22): 4556～4559

14 D. A. Lidar, D. Bacon, J. Kempe *et al.*. Protecting quantum information encoded in decoherence-free states against exchange errors[J]. *Phys. Rev.* (*A*), 2000, **61**(5): 052307-1～052307-5

15 S. M. Roy. Quantum zeno and anti-zeno paradoxes[J]. *Indian Academy of Sciences*, 2001, **56**: 169～178

16 H. J. Briegel, W. Dúr, J. I. Cirac *et al.*. Quantum repeaters: the role of imperfect local operations in quantum communication [J]. *Phys. Rev. Lett.*, 1998, **81**(26): 5932～5935

17 M. Martinelli. A universal compensator for polarization changes induced by birefringence on a retracing beam [J]. *Opt. Commun.*, 1989, **72**(6): 341～344

18 Z. D. Walton, A. E. Abouraddy, A. V. Sergienko *et al.*. Decoherence-free subspace in quantum key distribution[J]. *Phys. Rev. Lett.*, 2003, **91**(8): 087901-1～087901-4

19 J. C. Boileau, D. Gottesman, R. Laflamme *et al.*. Robust polarization-based quantum key distribution over collective-noise channel[J]. *Phys. Rev. Lett.*, 2004, **92**(1): 017901-1～017901-4

20 Xiangbin Wang. Quantum key distribution with two-qubit quantum codes[J]. *Phys. Rev. Lett.*, 2004, **92**(7): 077902-1～077902-4