第 56 卷 第 10 期 2007 年 10 月
1000-3290/2007/56(10)/5796-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.10,October,2007

基于随机相位编码的确定性量子密钥分配*

林青群 王发强† 米景隆 梁瑞生 刘颂豪

(华南师范大学信息光电子科技学院光子信息技术实验室,广州 510631)

(2007 年 1 月 10 日收到;2007 年 3 月 8 日收到修改稿)

提出一种新的随机相位编码的确定性量子密钥分配(QKD)方案.在该方案中,通信双方不需要公布测量基,就可以共享秘密信息,提高了密钥生成效率.因为传输的量子比特是随机编码的,即便光源非严格为单光子,该方案仍旧是安全的.理论分析显示出,对于光子数分裂攻击,中间人攻击和特洛伊木马等攻击手段,本方案比之前的 QKD 方案具有更强的安全性.

关键词:量子密码,量子密钥分发,安全性

PACC:4250,4230Q,0367

1. 引 言

信息时代的到来,一方面对信息传输速度的要求越来越高,另一方面,对信息安全性的要求也日益增加.量子密码术最引人入胜的魅力,在于具有通过不安全的物理信道能够进行秘密信息传输的可能性.自从 20 世纪 80 年代,Bennett 和 Brassard 提出第一个量子密钥分发协议——BB84 以来[1],量子密码术引起了国际物理学界和密码学界的高度重视,在理论和应用方面都展开了丰富多彩的研究,取得了大量的研究成果.从 2000 年开始,量子密码开始引起商家的重视,量子密码相关的产品已有部分进入市场,具有代表性的公司有美国的 MagiQ 公司,瑞士的 id Quantique 公司等.在国内,量子保密通信也有很大进展,中国科学研究院,华东师范大学等单位相继实现远距离量子密钥分配(QKD)系统[2—5].

以往的 QKD 方案有一个特点:发送的量子比特序列中,那些量子比特将被保留或者丢弃都是完全随机的,要根据传输量子密钥的双方 Alice 和 Bob 公布的测量基是否一致而定.2002 年,Bostrom 和 Felbinger 基于量子比特的纠缠特性,提出一种两路传输的直接安全通信模式的 QKD 方案[6],称之为乒乓协议.该方案中不需要比较 Alice 和 Bob 的测量基,降低了窃听者 Eve 所获得的信息,提高了密钥分配协议的效率,理想情况下该方案的效率为 100%.由于纠缠态制备的困难和认识上存在的不完全性,人们提出一些不使用纠缠态的改进方案[7—10],此类协议的理论和应用等相关研究也广泛开展.

本文提出一种基于随机相位编码的,非纠缠态的,确定性 QKD 协议,并分析该协议的效率和安全性表现,研究表明该协议的效率比传统的协议更高,并能更加有效防范目前对 QKD 实用系统安全性威胁最大的光子数分裂(PNS)攻击[11,12],中间人攻击[13]等几类攻击.

2. 随机相位编码量子密钥分配方案

本文提出的 QKD 方案的具体步骤如下(示意图见图 1,图中 PM 为相位调制器,D_1,D_2 为单光子探测器,Att 为衰减器,M_1,M_2 为反射镜):

1) Bob 随机选择 θ 对量子比特 $|\psi_0\rangle$ 进行相位调制,将 $|\psi_1\rangle = U(\theta)|\psi_0\rangle$ 发送给 Alice.

2) Alice 收到 Bob 发送过来的量子比特,使其通过不等臂的 M-Z 干涉仪,并在长臂随机对其进行相位编码,调相 π 代表发送比特 1,调相 0 代表发送比特 0,也即 $|\psi_2\rangle = U(\pi/0)|\psi_1\rangle = U(\pi+\theta/\theta)|\psi_0\rangle$,并将其发送回给 Bob.

3) Bob 同样在自己的不等臂 M-Z 干涉仪,对返回的量子比特进行 $-\theta$ 的相位调制,其结果为

* 国家自然科学基金(批准号:10404007)资助的课题.

† 通讯联系人. E-mail:fqwang98@sina.com

$|\psi_3\rangle = U(-\theta)|\psi_2\rangle = U(\pi/0)|\psi_0\rangle$，根据不等臂M-Z干涉仪的特点，在理想情况下，两个探测器会得到确定的响应，Alice 调相 0，探测器件 1 响应，代表比特 0，反之，探测器 2 响应，代表比特 1.

使用随机的相位 θ 调制发送信号，不断重复上述过程，Alice 和 Bob 就会获得一致的秘密比特串.

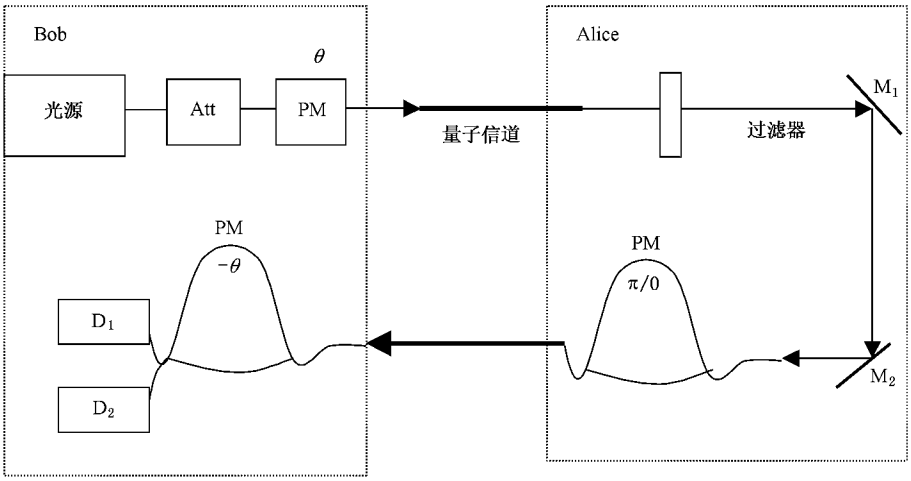

图 1　随机相位编码的确定性 QKD 方案

本文所提出的方案的优势有：1）通信的双方不需要公布测量基的选择，也不需要丢弃测量基不匹配的量子比特，这大大提高了量子密钥分配的效率，为无条件安全的一字一密所需的长密钥提供了应用的前景. 2）在大多数两路的 QKD 方案中[6,7,9,10]，Alice 对量子比特的编码是通过两类 Alice 和 Bob 秘密共享的幺正变换，两种不同的幺正算符成为方案的比特 1 和 0. 这种方案存在的危险是 Eve 可能通过发送特洛伊木马比特从而获得对幺正变换算符的信息[17]. 本方案所有编码都是随机的，即便 Eve 截获量子比特，也无法获得关于相位调制的信息. 3）有些方案是基于随机的偏振编码[8]，由于光纤中存在的双折射及其引起的偏振模色散效应，偏振编码不是光纤量子密码系统的最好选择. 本文方案以光子的相位来编码比特信息，具有抗干扰能力强，极限传输距离远的优点，更适合在光纤中传输. 4）本文所提出的方案结构简单，易于实现.

3. 效率和安全性分析

以文献[18]定义的 QKD 方案的效率 $\varepsilon = b_s/(q_t + b_t)$ 作为参考量，其中 b_s 是 Bob 收到的秘密比特数，q_t 是量子信道中传输的量子比特数，b_t 是公开信道传输的经典比特数（公布测量基的比特，BB84 中 $b_t = 2$）. 本文的方案中没有测量基的比较，所以 $b_t = 0$，故 $b_s = 1$，$q_t = 1$，效率 $\varepsilon = 1$. 假设经过单路方案的传输距离为 L，量子比特传输过程中的能见度为 τ，该方案距离为 $2L$，相应地效率为 τ^2. 简单计算可得，该方案的总效率为 $\xi = \varepsilon\tau^2 = \tau^2$，相比较 BB84 的 $\xi = (1/6)\tau$（$b_s = 0.5$，$q_t = 1$，$b_t = 2$），易见，只要信道传输量子比特的效率 $\tau > 1/6$，该方案是更有效的. 换另一种角度考虑方案的效率性，在同等距离下，本文提出的方案效率是传统的 3 倍，在后面的分析中，还可以看到只要传输脉冲中不包含超过 2 个（传统的协议超过 1 个光子，PNS 攻击就可以成功）的光子，本文的方案仍旧是安全的. 安全性所允许的平均光子数增加一倍，这意味着光源强度可增加，方案安全传输的极限距离也会增加.

假设 Bob 发送的量子态为 $|\psi\rangle = \sum_{\theta\in 2\pi}|\theta\rangle$，窃听者 Eve 用一探针逐一与发送的量子比特相互作用，等到 Bob 收到 Alice 的编码信息，再从自己保存的探针的态矢中获得关于密钥的信息. 显然，在双路方案中，Eve 只对其中一路的量子比特进行窃听是无法获得完整信息的，设 Eve 准备的窃听前向信道 E_f 和后向信道 E_b 的两个探针的辅助初态为 $|\varepsilon\rangle$ 和 $|\eta\rangle$，

由于信道噪声，探测器的暗计数等客观因素，以及 Eve 存在的可能性，Alice 和 Bob 各自拥有的两份量子比特序列并不是完全一致的. 为了确保获得可作为密钥所需的一致的安全比特串，后续的步骤为误码调解[14]，秘密放大[15]，又或者应用经典密码学中验证数据完整性的方法，采用单向的 hash 函数[16].

Eve 攻击的过程可表示为

$$\begin{aligned}|\psi\rangle|\varepsilon\rangle|\eta\rangle &\xrightarrow{E_{\mathrm{f}}} \sum_{\theta\in 2\pi}|\theta\rangle|\varepsilon_\theta\rangle|\eta\rangle \\ &\xrightarrow{\text{编码}} \sum_{\theta\in 2\pi}|\theta+\pi/0\rangle|\varepsilon_\theta\rangle|\eta\rangle \\ &\xrightarrow{E_{\mathrm{b}}} \sum_{\theta\in 2\pi}|\theta+\pi/0\rangle|\varepsilon_\theta\rangle|\eta_{\theta+\pi/0}\rangle .\end{aligned} \tag{1}$$

Eve 的探针的态和 Bob，Alice 传送的量子比特组成了复合空间，Bob 接收到 Alice 的编码之后，Eve 探针的辅助态为 $|\varepsilon_\theta,\eta_{\theta+\pi}\rangle$ 或 $|\varepsilon_\theta,\eta_\theta\rangle$，由于没有公布发送基的过程，Eve 只能从这两种态矢情况中辨别出 Alice 的编码行为. 设 $|\psi_1\rangle$ 与 $|\psi_2\rangle$ 是两个态矢量，能正确猜到它们的概率为

$$p=\frac{1}{2}+\frac{1}{2}(1-|\langle\psi_1||\psi_2\rangle|^2)^{\frac{1}{2}}, \tag{2}$$

其中 $|\langle\psi_1||\psi_2\rangle|^2$ 相当于 $|\psi_1\rangle$ 与 $|\psi_2\rangle$ 的夹角的余弦平方 $\cos^2\theta$，注意到辅助态 $|\varepsilon,\eta\rangle$，两个探针的态矢之间的夹角为 π 或 0，所以 Eve 窃听成功概率 $p=\frac{1}{2}$，即 Eve 什么信息也得不到.

量子密码术的安全性在于根据量子力学的基本原理，任何对量子比特的窃听行为都会破坏比特的原始态，因此 Eve 的行为可以被发现和评估. 由于采取的是随机的相位编码，Eve 无法估计 Bob 的调制的相位，同样也无法正确重发量子比特. 由于 M-Z 干涉仪的特点，非 π 或 0 的相位差同样会使探测器有随机响应，称之为非确定结果，所以 Eve 的任何窃听行为不被发现的概率为 1/2，相比较 BB84 协议，该方案安全性更强.

4. PNS 攻击

为了 BB84 协议的无条件安全传输，完美的单光子源是必须的. 实际上，单光子的制备离实际应用还有一段距离，所以在现实的 QKD 系统中，使用的都是经过衰减的激光脉冲控制，每一个激光脉冲中的平均光子数 $\mu<0.1$. 激光脉冲中含有的光子数目是服从泊松分布的，含有 n 个光子的脉冲所占的概率为

$$P(n,\mu)=\frac{\mu^n}{n!}\mathrm{e}^{-\mu}. \tag{3}$$

假如 $\mu=0.04$，每个脉冲有一个以上光子的概率 $P(n>1)\approx 2.0\times10^{-2}$，同样可得 $P(n>2)\approx 5.3\times10^{-4}$. 在 BB84 等单路协议中，只要脉冲中有超过 1 个的光子，PNS 攻击就可以成功，Eve 可以等待 Alice 和 Bob 公布他们的测量基时，才对自己分裂所得的光子进行测量，就可以获得关于编码的确定信息，并可以将自己隐藏在信道噪声之中. PNS 攻击是限制 QKD 系统方案安全传输极限距离的重要因素. 本文的方案由于随机相位编码且不公布任何关于选择基的信息，所以 Eve 无法成功进行上述的窃听. Bob 到 Alice 的前向信道中，量子比特被随机调制，不携带任何关于最终秘密比特的编码，Alice 到 Bob 的后向信道携带了编码信息，但由于随机相位的存在，对于 Eve 同样是随机的，Eve 的 PNS 攻击只能针对双向信道中编码前和编码后的量子比特的不同进行判别 Alice 的编码. 假设脉冲中平均光子数只有 1 个，对本方案安全性的分析，其实是等同于传统的单路协议 BB84 的分析，大量的文章已经证明了此类方案的安全性[1,19].

假设脉冲中的平均光子数超过 1 个，不失一般性，Eve 对前向和后向信道的光子分别进行 PNS 攻击，使用受控非门(CNOT)的量子线路表示 Eve 对编码前后的两量子比特进行区分的尝试. 原理图见图 2，图中 PBS 为偏振分束器.

假设输入受控非门的目标比特为 $|t\rangle=a_0|0\rangle+b_0|1\rangle$，Eve 使用 PBS 从前向信道分裂出的编码前量子比特为 $|\psi_1\rangle=a_1|0\rangle+b_1|1\rangle$，该量子信道的运算过程可以表示为

$$\begin{aligned}|\psi\rangle_{\psi_1 t} &= (a_1|0\rangle+b_1|1\rangle)\otimes(a_0|0\rangle+b_0|1\rangle) \\ &= a_0|0\rangle(a_1|0\rangle+b_1|1\rangle) \\ &\quad + b_0|1\rangle(a_1|1\rangle+b_1|0\rangle),\end{aligned} \tag{4}$$

同样地，Eve 从后向信道中获得量子比特为 $|\psi_2\rangle=a_2|0\rangle+b_2|1\rangle$，受控非门的运算结果为

$$\begin{aligned}|\psi\rangle_{\psi_2\psi_1 t} &= (a_2|0\rangle+b_2|1\rangle)\otimes|\psi\rangle_{\psi_1 t} \\ &= (a_2|0\rangle+b_2|1\rangle)\otimes(a_0|0\rangle(a_1|0\rangle \\ &\quad + b_1|1\rangle)+b_0|1\rangle(a_1|1\rangle+b_1|0\rangle)) \\ &= (a_2a_1|0\rangle|0\rangle+b_2b_1|1\rangle|1\rangle)(a_0|0\rangle \\ &\quad + b_0|1\rangle)+(a_2b_1|0\rangle|1\rangle \\ &\quad + b_2a_1|1\rangle|0\rangle)(a_0|1\rangle+b_0|0\rangle),\end{aligned} \tag{5}$$

CNOT 运算的结果显示，Eve 即便获得编码前后的两个光子，它无法辨别编码前后的光子态的区别，也即无法判断出 Bob 随机调制的相位大小，对不超过 2 个光子的脉冲的 PNS 攻击，Eve 无法成功窃听而不被通信双方发觉. 假如脉冲中的平均光子数超

过了 2 个，Eve 当然可以成功获得信息而不引入误码，它只要采取与 Bob 同样的设备，并让截获下来的编码前的量子比特先通过一个量子比特门 Y 门，进行相位翻转，就可以和截获的第二个编码的量子比特进行干涉，获得确定性的信息，脉冲中剩余的比特被 Bob 接收，Alice 和 Bob 无法察觉 Eve 的存在．实际上，脉冲中含有 2 个以上光子的概率是非常小的，Eve 无法获得关于密钥的完整信息．即使它获得了所有超过 3 个光子的脉冲中信息，Alice 和 Bob 可以进行秘密放大的过程消除 Eve 获得的信息．因此，在运用弱激光脉冲做光源的情况下，本文所提出的 QKD 方案依然是安全的．

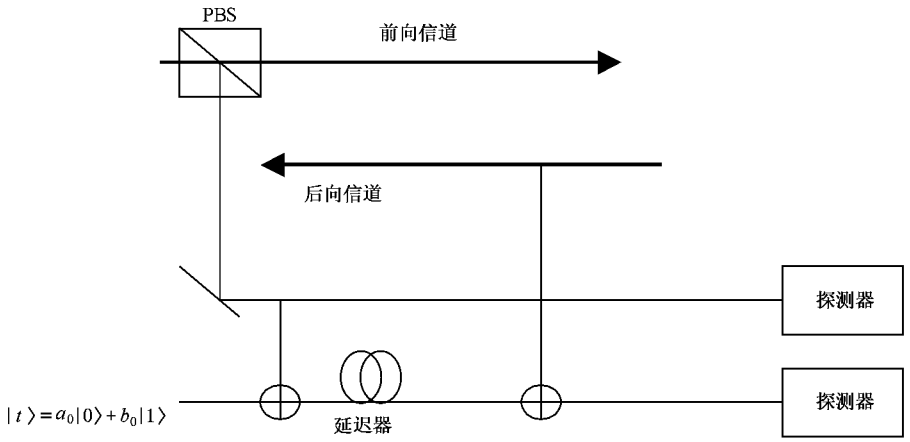

图 2　CNOT 门窃听线路原理图

5. 中间人攻击

传统的 QKD 系统方案的安全性对于 Eve 采取的中间人攻击(Impersonation attack)是脆弱的．Eve 在量子信道截获 Bob 发送来的脉冲，它假扮 Bob 发送给 Alice 自己随机相位调制 θ_E 的信号，Alice 误以为是 Bob 发来的前向信号，相位编码后再发送回给 Eve，Eve 根据自己的调制信息获得正确的 Alice 编码信息，再假扮 Alice 相位编码刚才截获的 Bob 的信号，发送给 Bob，Eve 可以做到完美的窃听而不被发觉．因此，传输密钥的双方事先进行量子信道和公共信道的认证过程是密钥分配安全性的保证．双路的 QKD 方案没有公共信道，所以需要对量子信道进行量子认证过程[13]．实际上，只需要对前面所叙述的随机相位编码的方案进行轻微的修正，就可以对抗中间人攻击，而不需要额外的量子认证过程．

只需让 Bob 不再只是单一的对脉冲调制 θ，而是以 $1-c$ 的概率调制 θ，以 c 的概率调制相位 $\theta+\frac{\pi}{2}$，Alice 接收到前向信道的脉冲，也不再是单一的以 π 或 0 进行相位编码，而是以 $1-b$ 的概率进行原来的编码，以 b 的概率调相为 $\frac{\pi}{2}$．量子比特发送完毕后，Alice 和 Bob 公布各自调制 $\frac{\pi}{2}$ 相位的比特位置，并丢弃这些位置的比特，通过比较 Alice 用 $\frac{\pi}{2}$ 编码和 Bob 用 $\theta+\frac{\pi}{2}$ 调制的位置的比特情况，就可以以 $\frac{bc}{2}$ 的概率发现 Eve 作为中间人的存在与否．由于公布的位置都是非最终密钥比特的信息，所以前面对双路确定性 QKD 方案的分析依然成立．显而易见，修正方案的效率由原先理想情况下的 1 变成了 $(1-c)(1-b)$．修正方案的效率与 b 和 c 成线性关系，调高 b 和 c 的数值，方案对抗中间人攻击的能力增强，但密钥分发效率降低，在实际应用中，要根据信道情况妥善调整 b 和 c 的大小．当然 Eve 也可以调整自己的策略，不只是对自己的伪装信号单一调整 π 或 0，也以一定比率调制信号相位为 $\frac{\pi}{2}$，但显然，Eve 会减少了自己正确获得信息的概率．虽然 Eve 可以减小了自己被发现的概率，但还是存在被发现的可能性，这比以前的 QKD 方案对中间人攻击无可奈何的情况，本修正方案是更优秀的．

6. 特洛伊木马攻击

为了窃听密钥信息，Eve 可以调节一种辅助源(auxiliary source)信号发射入量子信道，通过分析反向散射光，可以获得 Alice 或 Bob 设备的信息，从而

获得双方之间传输的信息.以目前的技术,探测相位调节器的技术还没成熟[20],而且本文提出的方案中,信号在传输过程中一直是随机相位编码的,因此 Eve 即便获得特洛伊木马辅助态 $|\eta\rangle_{\otimes}|\theta\rangle$,他也无法得到 Alice 随机编码的相位,通用特洛伊木马攻击[20]对本方案不适用.进一步地说,只要认真设计好系统与量子信道连结的这一环节,就可以把特洛伊木马攻击成功的可能性降得更低.

1)在系统中加入设计精良的滤波器,只允许规定的波长的信号进入设备,可以防止 Eve 的特洛伊木马信号侵入.

2)采用门控技术,只在信号光到来的时刻,开启设备进行接收,相位调节器等器材仅在合法的信号光到来的极短时间内有效.

7. 结 论

传统的单路 QKD 方案已经成功地应用了很多年,新颖的非纠缠态的双路量子密钥分发方案,结合了量子超密编码和 BB84 协议的特点,提高了量子信道的容量,增强了量子密钥分发的安全性.窃听者 Eve 对前向或后向信道的干扰导致的编码前和编码后量子比特之间的任何不相关性都将暴露他的行为.当系统使用衰减激光脉冲作为光源,BB84 的 QKD 协议不是无条件安全的,因为 Eve 可以采取 PNS 攻击获得正确信息.双路 QKD 方案不需要公布基的选择,通信双方就可以获得确定性的秘密信息传输,只要脉冲中的平均光子数不超过 2 个,方案依然是安全的.运用秘密放大技术,双路方案的系统完全可以采用弱激光光源,获得更远的传输距离.

本文提出一种基于随机相位编码的确定性双路 QKD 方案,不但具有上述优势,而且采取随机相位编码,大大提高了 Eve 窃听的难度,增强方案的安全性.修正的方案还能有效的对抗中间人攻击,一定程度上改善了 QKD 方案本身对中间人攻击的缺陷.系统结构简单,易于实现,相位编码比大多数偏振编码的双路方案受信道双折射现象的影响小,更适合于光纤的长距离传输,可能是未来一种实用的长距离量子光通信系统.

[1] Bennett C H, Brassard G 1984 *In Proceedings of IEEE International Conference on Computers, Systems and Singal Processing, Bangalore, India* (IEEE, New York) p175—179

[2] Liang C, Fu D H, Liang B 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁 创、符东浩、梁 冰 2001 物理学报 **50** 1429]

[3] Zhou C Y, Wu G, Chen X L 2003 *Appl. Phys. Lett.* **83** 1692

[4] Chen X L, Zhou C Y, Wu G 2004 *Appl. Phys. Lett.* **85** 1648

[5] Wu G, Zhou C Y, Chen X L 2005 *Acta Phys. Sin.* **54** 3626 (in Chinese) [吴 光、周春源、陈修亮 2005 物理学报 **54** 3626]

[6] Bostrom K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[7] Cai Q Y, Li B W 2004 *Chin. Phys. Lett.* **21** 601

[8] Deng F G, Long G L 2004 *Phys. Rev.* A **70** 012311

[9] Kye W H, Kim C M, Kim M S, Park Y J 2005 *Phys. Rev. Lett.* **95** 40501

[10] Lucamarini M, Mancini S 2005 *Phys. Rev. Lett.* **94** 140501

[11] Brassard G, Lutkenhau N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330

[12] Lutkenhaus N 2000 *Phys. Rev.* A **61** 052304

[13] Dusek M, Haderka O, Hendrych M, Myska R 1999 *Phys. Rev.* A **60** 149

[14] Brasard G, Salvail L 1994 *Advances in Cryptology* 1994 *Proceedings of Eurocrypt* '93, *Lecture Notes in Computer Science* **765** 410—423

[15] Bennett C H, Brassard G, Crepeau C 1995 *IEEE transaction Information Theroy* **41** No 6

[16] Carter J L, Wegman M N 1979 *J. Comput. Syst. Sci.* **18** 143

[17] Boileau J C, Laflamme R, Laforest M, Myers C R 2000 *Phys. Rev. Lett.* **93** 220501

[18] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635

[19] Bennett C H, Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881

[20] Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G 2005 *quant-ph*/0507063

Deterministic quantum key distribution based on random phase coding*

Lin Qing-Qun Wang Fa-Qiang† Mi Jing-Long Liang Rui-Sheng Liu Song-Hao

(*Lab of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510631, *China*)

(Received 10 January 2007; revised manuscript received 8 March 2007)

Abstract

We propose a new quantum key distribution scheme based on random phase coding. In this scheme, the sender and the receiver can share the secret information without basis reconciliation, and besides, this scheme is more efficient. As the phase of the qubit is coded randomly, this protocol is robust even when the source is not a prefect single photon. We show theoretically that it has higher security against the attacks, such as the photon-number-splitting, the impersonation attack, and the Trojan attack, etc., than the previous QKD scheme.

Keywords: quantum cryptography, quantum key distribution, security

PACC: 4250, 4230Q, 0367

* Project supported by the National Natural Science Foundation of China (Grant No. 10404007).

† Corresponding author. E-mail: fqwang98@sina.com