第 57 卷 第 8 期 2008 年 8 月
1000-3290/2008/57(08)/4941-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.8,August,2008

时间和相位混合编码的量子密钥分发方案*

张 静 王发强 赵 峰 路轶群† 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 510006)

(2007 年 10 月 19 日收到,2008 年 2 月 20 日收到修改稿)

提出了一种在双马赫-曾德尔干涉仪量子保密通信系统上同时实现时间编码和相位编码的混合量子密钥分发方案.提出的方案将原来相位编码方案中丢弃的脉冲进行时间编码,因此成码率是原方案的二倍.系统同时获得时间编码密钥和相位编码密钥,既可以一组用于通信,另一组用于监视窃听,又可以将两组密钥组合成新密钥.系统具有良好的应用前景.

关键词:量子保密通信,量子密钥分发,相位编码,时间编码

PACC:4250,4230Q,4210J,0365

1. 引 言

量子保密通信最关键的部分是量子密钥分发(QKD)的实现.自 1984 年 Bennett 等[1]提出第一个 QKD 协议之后,量子保密通信引起了人们极大的关注,并逐步从实验走向应用[2—5].在实际的系统中,QKD 的编码方式主要有偏振编码[6]、相位编码[7]、时间编码[8,9]和频率编码[10]等.目前,QKD 系统的传输介质主要是光纤及自由空间.用光子的偏振态作为信息载体简单易控,但由于光纤本身存在随机双折射以及由双折射引起的偏振模色散效应,会导致偏振态在长距离传输后发生随机变化,所以偏振编码常被用在自由空间 QKD 系统中[6,11].用光子的相位进行信息编码在光纤中传输抗干扰能力较强,目前已得到了广泛的应用.

为了提高成码率并确保系统的安全性和稳定性,我们提出了一种新的混合 QKD 方案.在以相位编码的 BB84 协议的基础上,充分利用了系统中舍弃的一半脉冲进行稳定性较强的时间编码,实现了对脉冲的两次编码,因此,这种混合方案成码率是原方案的二倍.通信结束后,系统将生成两组不同类型的密钥,我们可根据环境条件,对密钥进行合理利用.该系统具有较大的实用价值.

2. 混合编码 QKD 方案

图 1 为混合编码 QKD 系统原理示意图,其中 PBS 为偏振分束器,BS 为 50∶50 的分束器,PM1 和 PM2 为相位调制器,D_0 和 D_1 为光子探测器.如图 1 所示,一般的双马赫-曾德尔(M-Z)相位编码 QKD 方案中,Alice 发出的脉冲经两个 M-Z 干涉仪后,有(l_2,l_4),(l_1,l_4),(l_2,l_3)和(l_1,l_3)四条可能的路径到达 Bob 端.四条路径中经过(l_2,l_4)的脉冲路径最短,最早到达探测器,经过(l_1,l_3)的脉冲最后到达探测器,这两种情形都没有干涉现象.经过(l_1,l_4)和(l_2,l_3)两条不同路径的脉冲同时到达探测器,因此会发生干涉现象.Alice 和 Bob 分别调制相位调制器 PM1 和 PM2 的相位,使脉冲 B 的强度随相位差的不同而发生变化,从而实现相位编码.相位编码只利用发生干涉的脉冲 B 成码,在光子进入单光子探测器前,我们往往用门控过滤掉没发生干涉的脉冲 A 和脉冲 C,探测器只探测脉冲 B,完成密钥分配.

我们提出的混合编码方案仍采用脉冲 B 进行相位编码,而原来相位编码方案中舍弃的脉冲 A 和脉冲 C 则进行时间编码.通信结束后,系统将同时获得时间编码密钥和相位编码密钥,成码率是原方案的二倍.

* 国家重点基础研究发展规划(批准号:2007CB307001)资助的课题.

† E-mail:13003005844@ah165.net

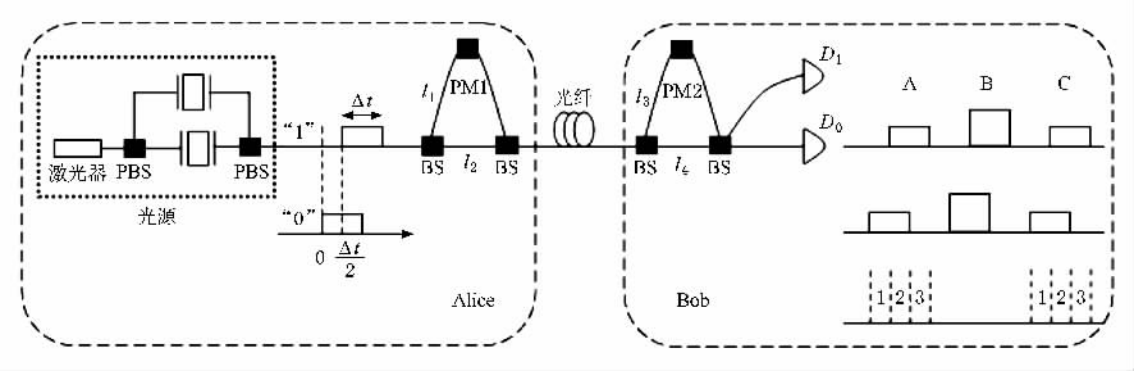

图 1 混合编码 QKD 系统原理示意图

2.1. 时间编码原理及密钥分发过程

图 2 是时间编码原理示意图. 如图 2 所示, Alice 根据参考时间发出持续时间为 Δt 秒的脉冲, 为了编码, 对每个脉冲随机加上一段相对于参考时间的延迟时间 0 或 $\Delta t/2$. 例如, 我们将延迟时间为 0 的脉冲记为比特‘0’, 将延迟时间为 $\Delta t/2$ 的脉冲记为比特‘1’. Alice 发送脉冲时对每个脉冲随机延迟 0 或 $\Delta t/2$, 即 Alice 随机选择发送‘0’或‘1’.

Alice 发出的脉冲可以有两种不同时间的延迟, 所以到达 Bob 端时在时间上有相对位置的重叠. 如果 Bob 在时间 2 窗口探测到光子, 那么他无法判断 Alice 的发送状态. 如果 Bob 在时间 1 或时间 3 窗口探测到光子, 那么他就能推断出 Alice 的发送状态.

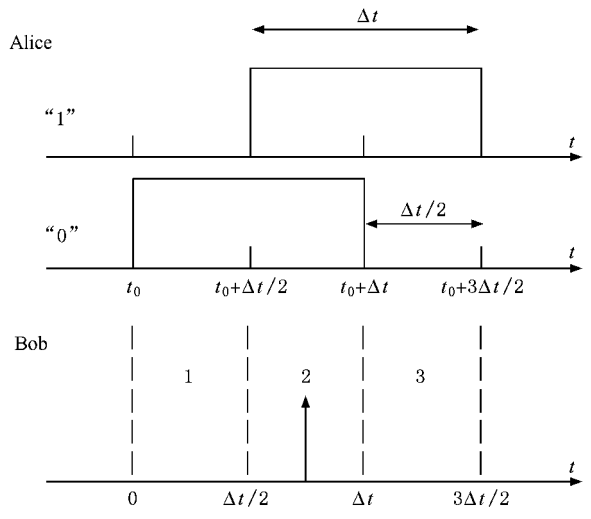

图 2 时间编码原理示意图

下面给出混合编码方案中时间编码密钥分发过程.

1) Alice 发出持续时间为 Δt 的矩形脉冲, 对每个脉冲随机地延迟 0 或 $\Delta t/2$. Alice 记录所发脉冲的时刻和具体的延迟时间.

2) 脉冲经过两个干涉仪后, 没发生干涉的脉冲 A 和脉冲 C 按如下方式生成初始密钥: 在时间 1 窗口探测到光子时记为比特‘0’, 在时间 3 窗口探测到光子时记为比特‘1’.

3) Bob 告知 Alice 他何时探测到光子, 但不公布记录结果. Alice 告诉 Bob 哪些时刻是正确的, 舍弃其他不正确的结果.

2.2. 相位编码密钥分发过程

下面给出混合编码方案中相位编码密钥分发过程.

1) 脉冲进入 Alice 端的干涉仪时, Alice 选用两组正交基 $\{0,\pi\}$ 和 $\{\pi/2,3\pi/2\}$ 中的任一相位对脉冲进行调制. Alice 记录调制使用的每组基及具体的调制相位.

2) 脉冲到达 Bob 端干涉仪时, Bob 随机地选择 0 或 $\pi/2$ 调制脉冲. Bob 记录具体的调制相位.

3) 脉冲经过两个干涉仪后, 发生干涉的脉冲 B 按如下方式生成密钥: Bob 端探测器用 D_0 和 D_1 标记. 探测器 D_0 响应而 D_1 不响应, 记为比特‘0’; 探测器 D_1 响应而 D_0 不响应, 记为比特‘1’.

4) Bob 通过公开信道告诉 Alice 他所调制的相位, 但不公布探测器的结果. Alice 告诉 Bob 哪些结果的基相匹配, 舍弃基不匹配时对应的结果.

密钥分发过程完成后, 一般用下面两个步骤处理数据.

第一步, Alice 和 Bob 通过公开信道交换部分数据, 检查误码率的大小. 若误码率未超过允许值, 未公开的数据就可以通过运算生成密码本, 否则, 就表明存在窃听, 本次通信无效.

第二步，通过纠错运算及秘密放大[6]使 Eve 得到的信息量尽可能小.

从以上所述密钥分发过程容易看出，仅运行 BB84 协议时，只有一半脉冲干涉，Bob 有一半概率选对基，成码率只有 $\eta = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. 而混合 QKD 方案中，不干涉的脉冲也携带了信息，有一半信息可以被有效利用，所以成码率是 $\eta' = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}$. 这表明混合协议的效率比经典的 BB84 协议的效率提高了一倍.

3. 混合 QKD 系统中两个关键问题的分析

3.1. 光源的选择

时间编码是利用脉冲之间的重叠来编码的，这就要求脉冲有很好的时间分辨率. 我们选用持续时间 Δt 等于脉冲相干长度的单光子脉冲，并且脉冲各个点都有相同的概率探测密度. 实际系统中，我们通过衰减超高斯脉冲光源可得到接近于单光子水平的矩形脉冲. 超高斯脉冲强度表达式为

$$P(t) = P_0 \exp\left(-\frac{t^{2n}}{2\sigma^{2n}}\right). \tag{1}$$

由(1)式可知，n 越大，脉冲的边沿越陡，就越接近矩形脉冲.

为了实现时间编码，我们设计了如图 3 所示的光源，每个支路上都安装一个偏振光开关. 光开关由起偏器、偏振旋转器和检偏器组成. 激光器发出脉冲后，经过偏振分束器 PBS 分成偏振方向互相垂直的两束线偏振光. 线偏振光通过各自的起偏器后，如果在偏振旋转器上加电压，它将使线偏振光转动 90°，入射的线偏振光就通过检偏器射出 如果不加电压，就没有光射出. 我们使两支路的路程差 Δl 满足 $\frac{\Delta l}{c} = \frac{\Delta t}{2}$，当 Alice 发出一个持续时间为 Δt 的脉冲时，随机控制光开关的开合，就能实现对脉冲随机延迟 0 或 $\Delta t/2$.

3.2. 两种编码之间的干扰

第一种情况，脉冲经过两个干涉仪后，Bob 端产生的三个脉冲之间的时间相对位置取决于干涉仪两臂长差. 如果臂长差较小，脉冲之间的间距就小，可能产生脉冲之间的混乱重叠，无法精确成码. 如图 4(a)所示，若脉冲间距小，脉冲 A 和脉冲 B′以及脉冲 B 和脉冲 C′在时间上就会产生重叠. 这样，我们在脉冲 A 处探测信息时，就可能探测到脉冲 B′的光子，从而无法得到有效信息. 为了避免这种错误交叠，干涉仪的两臂长差需满足如下不等式：

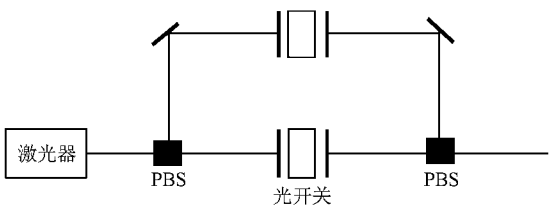

图 3　混合 QKD 系统的光源

$$\frac{l_1 - l_2}{c} = \frac{l_3 - l_4}{c} \geqslant \frac{3\Delta t}{2}, \tag{2}$$

其中 c 是光速.

第二种情况，若 Alice 发射脉冲的频率较高，即两脉冲之间的参考时间较短，则相邻的两个码到达 Bob 端后会在时间上有重叠，同样无法精确成码. 如图 4(b)所示，脉冲 A、脉冲 B 和脉冲 C 是前一个脉冲形成的码，如果参考时间较短，就会引起随后的脉冲 C′与脉冲 A 重叠. Alice 发送脉冲时，选用的参考时间的间隔不小于 $\frac{9\Delta t}{2}$ 就能避免这种情况的发生.

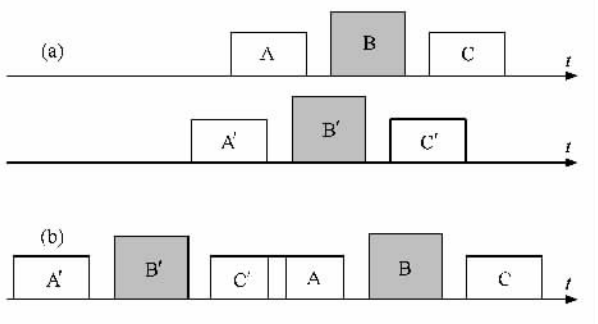

图 4　脉冲之间的干扰　(a)干涉仪臂长差较小引起的脉冲干扰，(b)参考时间较短引起的脉冲干扰

4. 混合 QKD 系统的安全性分析

系统的特点体现在两方面. 首先，混合编码的应用增加了窃听者判断准确信息的难度，窃听者只能进行一次测量，不能同时得到两种密钥信息. 其次，混合方案可形成两组密钥，在通信过程中，我们可以

使用相位编码来监视窃听,用时间编码来成码,实现对系统的实时监控.下面我们以常见的截获—重发攻击为例,具体分析系统的安全性.

假设 Eve 只受量子力学原理的限制,不受任何技术能力的限制.同时假设 Eve 将 Alice 发出的脉冲全部拦截,测量后随机重发给 Bob.

我们通过计算每个脉冲的互信息量来评估系统的安全性.混合方案中同时使用了时间编码和相位编码,两者互不影响,可看作相互独立的事件,分别记为事件 X 和 Y,Alice 发射一个脉冲就记为联合事件(X,Y).两个事件产生的误码率分别记为 Q_1 和 Q_2,系统总误码率记为 Q.根据混合协议的特点,在 Bob 端进行测量就相当于三个事件,每个事件引起的误码率都是均等的.所以,时间编码引起的误码率为 $Q_1=\frac{2}{3}Q$,相位编码引起的误码率为 $Q_2=\frac{1}{3}Q$.我们先计算 Alice 与 Eve 之间的互信息量 $I(A;E)$,

$$\begin{aligned} I(A;E) &= I(X,Y;E) \\ &= I(X;E)+I(Y;E\mid X), \end{aligned} \tag{3}$$

其中 $I(X;E)$是事件 X 与 Eve 之间的互信息量,$I(Y;E\mid X)$是事件 X 发生的条件下 Y 与 Eve 之间的互信息量.我们对 $I(Y;E\mid X)$做进一步化简,

$$\begin{aligned} I(Y;E\mid X) &= \log\frac{P(YE\mid X)}{P(E\mid X)P(Y\mid X)} \\ &= \log\frac{P(YE)}{P(E)P(Y\mid X)}. \end{aligned} \tag{4}$$

因为 X,Y 相互独立,所以 $P(Y\mid X)=P(Y)$,代入(4)式有

$$\begin{aligned} I(Y;E\mid X) &= \log\frac{P(YE)}{P(E)P(Y)} \\ &= \log\frac{P(E\mid Y)}{P(E)} \\ &= I(Y;E). \end{aligned} \tag{5}$$

将(5)式代入(3)式后得

$$I(A;E)=I(X;E)+I(Y;E). \tag{6}$$

时间编码的安全性依赖于系统的干涉对比度[8].为了计算 $I(X;E)$,我们在时间编码系统中定义干涉对比度 C 和对比度衰减 Δ 两个参数.由文献[8]可知,时间编码在没有窃听情况下的理想干涉对比度为 1/2,如果存在对比度衰减,则有如下关系式:

$$C=\frac{1}{2}(1-\Delta). \tag{7}$$

同时,对比度也可表示成误码率 Q_1 和互信息量 $I(X;E)$的函数[8],

$$\begin{aligned} C=\frac{1}{2}\Big[&\sqrt{2Q_1+\frac{1-\eta}{\eta}}\sqrt{I_{XE}} \\ &+\sqrt{2Q_1}\sqrt{I_{XE}-\frac{1-\eta}{\eta}}+1-I_{XE}-2Q_1\Big], \end{aligned} \tag{8}$$

其中 η 是信道的传输效率.由于传输信道本身的不完善,传输效率往往比 1 小得多,这里我们考虑理想的情况,即 $\eta=1$.于是,从(7),(8)式中我们得到 $I(X;E)$的表达式

$$I(X;E)=2Q_1+2\sqrt{2Q_1\Delta}+\Delta. \tag{9}$$

对于 $I(Y;E)$的计算,满足相位编码互信息量关系式,由文献[6]可得

$$\begin{aligned} I(Y;E) &= \frac{2}{\ln 2}Q_2+O(Q_2)^2 \\ &\approx 2.9Q_2. \end{aligned} \tag{10}$$

将 $Q_1=\frac{2}{3}Q$,$Q_2=\frac{1}{3}Q$ 以及(9)和(10)式代入到(6)式中,得到 Alice 与 Eve 之间的互信息量为

$$I(A;E)=2.3Q+\sqrt{\frac{16Q\Delta}{3}}+\Delta. \tag{11}$$

Alice 与 Bob 之间的互信息量表达式如下:

$$\begin{aligned} I(A;B) &= 1+(1-Q)\log_2(1-Q) \\ &\quad +Q\log_2(Q). \end{aligned} \tag{12}$$

由安全判据[12] $I(A;B)\geqslant I(A;E)$,我们可以评估系统的安全性.图 5 为 $I(A;B)$和 $I(A;E)$与 Q 的关系.从图 5 可以看出,对比度衰减为 10% 时,系统允许的最大误码率为 9.6%,只要误码率大于 9.6% 就说明有窃听;对比度衰减为 5% 时,允许的最大误码率为 11.4%.BB84 方案允许的最大误码率为 15%.从安全判据 $I(A;B)\geqslant I(A;E)$可以看出,不管对比度衰减多少,Q 值越小,$I(A;B)$与 $I(A;E)$的差异就越大,Bob 将获得比 Eve 更多的信息量,

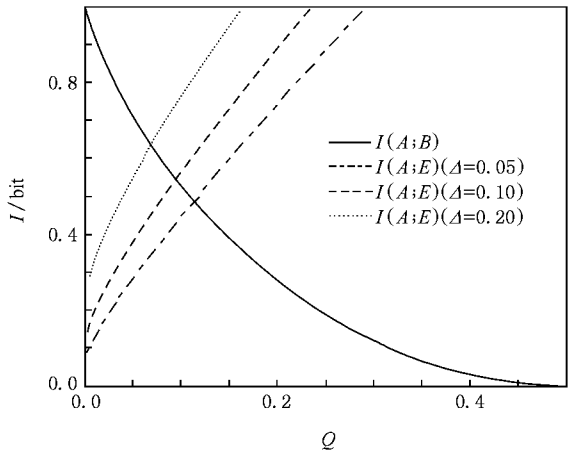

图 5 互信息量 I 与误码率 Q 之间的关系

说明通信更为安全.由此可知,为了达到更高的安全性,在对比度损耗允许的范围内,应尽量降低最大误码率.

5. 结　论

本文提出了一种新的混合 QKD 方案,即在双 M-Z 系统上同时实现时间编码和相位编码的混合编码方案,脉冲同时携带两种信息,加大了窃听的难度,并且成码率是原相位编码方案的二倍.由于系统编码时使用了时间信息,受环境变化的影响较小,稳定性较强.同时,系统在通信双方使用精确的时间同步,降低了暗计数的影响.从生成密钥的角度考虑,有几种方案可以灵活选用:当相位编码不稳定或系统暗计数影响很大时,只使用时间编码信息成码,相位编码信息只用于检测安全性;也可以在相位编码有优势时,用时间编码信息来检测安全性;同时,生成的两部分密钥也可以直接组合成新密钥.混合编码 QKD 系统有很好的应用前景.

[1] Bennett C H, Brassard G 1984 *Int. Conf. Computers Systems and Signal Processing* (New York: IEEE) p175

[2] Liang C, Fu D H, Liang B, Liao J, Wu L A, Yao D C, Lü S W 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁　创、符东浩、梁　冰、廖　静、吴令安、姚德成、吕述望 2001 物理学报 **50** 1429]

[3] Wu G, Zhou C Y, Chen X L, Han X H, Zeng H P 2005 *Acta Phys. Sin.* **54** 3622 (in Chinese) [吴　光、周春源、陈修亮、韩晓红、曾和平 2005 物理学报 **54** 3622]

[4] Li M M, Wang F Q, Lu Y Q, Zhao F, Chen X, Liang R S, Liu S H 2006 *Acta Phys. Sin.* **55** 4642 (in Chinese) [李明明、王发强、路轶群、赵　峰、陈　霞、梁瑞生、刘颂豪 2006 物理学报 **55** 4642]

[5] Zhao F, Lu Y Q, Wang F Q, Chen X, Li M M, Guo B H, Liao C J, Liu S H 2007 *Acta Phys. Sin.* **56** 2175 (in Chinese) [赵　峰、路轶群、王发强、陈　霞、李明明、郭邦红、廖长俊、刘颂豪 2007 物理学报 **56** 2175]

[6] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[7] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

[8] Debuisschert T, Boucher W 2004 *Phys. Rev.* A **70** 042306

[9] Debuisschert T, Boucher W 2005 *Phys. Rev.* A **72** 062325

[10] Merolla J M, Mazurenko Y, Goedgebuer J P, Rhodes W T 1999 *Phys. Rev. Lett.* **82** 1656

[11] Miao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2123 (in Chinese) [苗二龙、莫小范、桂有珍、韩正甫、郭光灿 2004 物理学报 **53** 2123]

[12] Csiszar I, Körner J 1978 *IEEE Trans. Inform. Theory* **24** 339

Quantum key distribution based on time coding and phase coding*

Zhang Jing Wang Fa-Qiang Zhao Feng Lu Yi-Qun† Liu Song-Hao

(*Laboratory of Photonic Information Technology, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

(Received 19 October 2007; revised manuscript received 20 February 2008)

Abstract

A new quantum key distribution scheme is proposed to realize both phase coding and time coding based on two unbalanced Mach-Zehnder interferometers. The pulses which are discarded in the phase coding scheme can be coded in time coding, so the useful bit rate in the present scheme can be doubled. At the same time, the phase coding keys and the time coding keys are obtained. We can use one group of keys to communicate and the other one to guard against eavesdropping, or combine both of them to form new keys. This scheme has favorable application prospect.

Keywords: quantum secure communication, quantum key distribution, phase coding, time coding

PACC: 4250, 4230Q, 4210J, 0365

* Project supported by the State Key Development Program for Basic Research of China (Grant No. 2007CB307001).

† E-mail: 13003005844@ah165.net