结合高效 BB84 协议的差分密钥分发系统*

陈霞，王发强**，路轶群，赵峰，李明明，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广东省高校重点实验室，广州 510631）

摘 要：提出一种新的相位编码方案，使用差分和高效 BB84 协议实现量子密钥分发. 在保留差分编码优势的同时，此方案进一步增加系统的安全性. Alice 端随机选择{0，π/2，π，3π/2}中的相位对信号脉冲进行调制，Bob 端随机选择{0，π/2}中的相位对信号脉冲进行调制. 为了提高成码率和简化系统，以 $\eta(\eta\to1)$ 的概率选取{0，π} 基对相位进行调制，此时系统运行差分编码，用于生成密钥；以$(1-\eta)$的概率选取{π/2，3π/2}基中的相位对脉冲信号进行调制. {π/2，3π/2}基的选用是为了增加系统维度和进行安全性评估，不用于生成密钥. 设计相应的系统，利用微弱相干光脉冲在该新协议下进行编码，在接收端采用法拉第－迈克尔逊方式进行解码，在实验上实现了长期稳定的密钥分发，误码率＜5%，传输距离达 85 km.

关键词：量子密码；量子密钥分发；相位编码；差分；高效 BB84
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1004-4213(2008)05-1052-5

0 引言

量子密码学作为量子力学与密码学相结合的产物，量子力学的基本原理保证了窃听的可检测性，具有经典密码学无法比拟的优势. 现阶段量子密钥分发的实现主要依靠光纤作为载体，相对于偏振编码，相位编码方式具有一定优势[1]. 在已经提出的多种密钥分发方案中[2-4]，最著名的为 BB84 方案[5]，它具有稳定、安全的特点[6-8]，但是成码率较低. 另一种广为人知的方案为差分密钥传输方案（DPS-QKD）[9]. 此方案中，信息是由两个连续光脉冲间的相位差携带的，连续光脉冲的时间差为 10 ns 量级. 因此虽然在光纤传输过程中，偏振模式会发生改变，但是由于连续光脉冲所经历的温度、压力等环境影响几乎相同，所以产生的偏振模式变换也几乎相同，从而不会影响出射端的干涉对比度. 相对于其他密钥分发协议，此协议的安全性、稳定性和成码率都得到了提高[10,11]. 但由于其空间维度只有一维（只用{0，π}一组基进行调相），在抵御截获－重发攻击时安全性存在隐患[12].

本文在 DPS-QKD 基础上，结合高效 BB84 协议[13]，用两维基{0，π}和{π/2，3π/2}调制相位，提出一种新的相位编码协议. Alice 和 Bob 分别以 $\eta(\eta\to1)$ 的概率选取{0，π}基中的相位，以$(1-\eta)$的概率选取{π/2，3π/2}基中的相位对脉冲信号进行调制. 两维基的使用，加强了系统的安全性. 以 $\eta(\eta\to1)$ 的概率选取{0，π}基中的相位对系统进行调制，相当于用差分协议进行编码，提高了系统的成码率.

本文设计了相应的试验系统运行该协议. 在 Alice 端，采用强度调制器产生连续的微弱相干光脉冲；由于差分系统的稳定性很大程度上决定于干涉仪的稳定性[10,14]，所以在 Bob 端，采用双法拉第旋转镜（FM）技术，完全补偿了 Bob 端的双折射现象和环境引起的偏振抖动，加强了系统的稳定性.

1 密钥分发协议

如图 1，在 Alice 端产生时间差为 Δt 的连续相干脉冲串，被 PM_a 调制相位，经过光纤 T 传输后到达 Bob 端，再通过干涉仪的两臂，在输出端口干涉，光子根据不同的结果到达不同的探测器. 设发生干涉的两个脉冲为 P_1、P_2，这两个脉冲经历的路径可以分别表示为：P_1：PM_a→T→干涉仪短臂，P_2：PM_a→T→干涉仪长臂（含PM_b）. 分别设这两个脉冲离

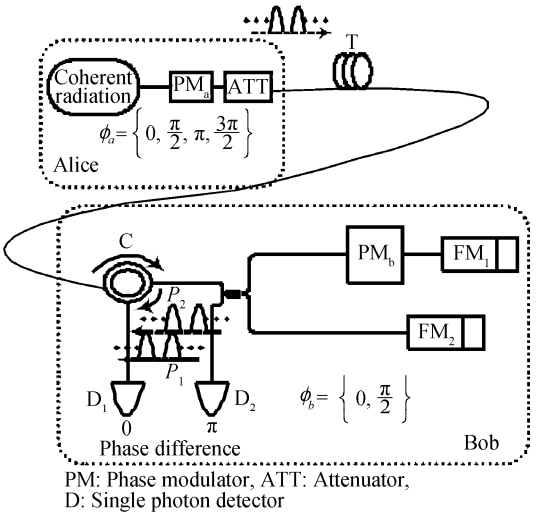


图 1 系统原理图

Fig. 1 Schematic diagram of the proposed scheme

* 国家重点基础研究发展计划 973 项目(2007CB307001)资助
** Tel：020－80597559　　Email：fqwang@scnu.edu.cn
收稿日期：2007-01-25

开 Alice 端时的初态为：$E_1=E_{10}\cdot e^{i\varphi_{a1}}$，$E_2=E_{20}\cdot e^{i\varphi_{a2}}$，其中 φ_{a1} 和 φ_{a2} 表示 Alice 调制的相位，E_{10}、E_{20} 分别为这两个态的振幅，若要在出射端有理想的干涉对比度，要求脉冲的振幅相等，即 $E_{10}=E_{20}=E_0$. T 表示两个脉冲经过光纤 T 的传输矩阵，ϕ 为由传输光纤 T 引起的相位变化，由于这两个脉冲相隔时间很短，经历了相同的传输线（光纤 T），可做相同处理. 这两个脉冲在 Bob 端干涉仪输出端的电场强度表示为

$$P_1:\frac{1}{2}TE_0e^{i\varphi_{a1}}e^{i\varphi},P_2:\frac{1}{2}TE_0e^{i\varphi_{a2}}e^{i\varphi_b}e^{i\varphi}$$

那么到达探测器 D_1 端口的电场强度可表示为

$$E_{out}=\frac{1}{2}TE_0e^{i\varphi}(e^{i(\varphi_{a2}+\varphi_b)}+e^{i\varphi_{a1}}) \tag{1}$$

那么其光强可以表示为

$$P_{out}=E_{out}^{+}\cdot E_{out}=\frac{1}{2}|T|^2\cdot|E_0|^2[1+\cos(\varphi_{a2}+\varphi_b-\varphi_{a1})=A(1+\cos\Delta\varphi)] \tag{2}$$

当 $\Delta\varphi=0$ 时，光子到达 D_1 探测器，当 $\Delta\varphi=\pi$ 时，光子到达 D_2 探测器. 由式(2)可以看出：出射端的光强同时取决于($\varphi_{a2}+\varphi_b-\varphi_{a1}$)，即 Alice 对相邻两个脉冲调制的相位差和 Bob 端对发生干涉的两个脉冲中前一个脉冲调制的相位. 基于此，即可以采用多种方法进行 BB84 编码，增加了系统的灵活性；同时这种不确定性也增加了系统的安全性. 若 $\varphi_b=0$，则出射端的光强完全取决于 $\varphi_{a2}-\varphi_{a1}$，即 Alice 对相邻两个脉冲的调制的相位差，也就是采用了差分编码方式. 基于以上分析，定义以下密钥传输协议.

1.1　相位编码协议

1.1.1　密钥传输过程

1）Alice 对连续的相干脉冲进行调制，以 $\eta(\eta\to1)$ 的概率选取{0，π}基中的相位，以($1-\eta$)的概率选取{π/2，3π/2}基中的相位调制 PM_a，依次对连续相干脉冲进行调制. Alice 记录具体调制相位、调制时间以及选取的是{0，π}基还是{π/2，3π/2}基.

2）Bob 以 $\eta(\eta\to1)$ 的概率选取 0 相位，以($1-\eta$)的概率选取 π/2 相位调制 PM_b. Bob 记录具体调制相位、调制时间以及探测器的响应情况.

1.1.2　密钥传输结束后

1）Bob 通过公共信道通知 Alice：Bob 调相时选择的基，Alice 根据自己的调制记录，通知 Bob 对记录进行不同的处理. 具体处理方法为：首先，在双方共同选用{0，π}基进行相位调制的时间，Alice 通知 Bob 将此部分进行保留，用于生成密钥. 由于 Alice 选取{0，π}基调相的概率为 η，Bob 选取 0 调相的概率为 η，所以选择此种情况的概率 $\eta\cdot\eta=\eta^2$；其次，在双方共同选用{π/2，3π/2}基进行相位调制并且 Alice 对该脉冲前一个脉冲进行0相位调制的时刻进行保留，用于进行安全性分析. 由于Alice选取{π/2，3π/2}基调相的概率为($1-\eta$)，Bob 选取 π/2 调相的概率为($1-\eta$)，并且对于该脉冲的前一个脉冲，选取 0 相位调制的概率为 $\eta/2$，所以选择此种情况的概率为

$$(1-\eta)\cdot(1-\eta)\cdot\frac{\eta}{2}=\frac{\eta(1-\eta)^2}{2}$$

2）生成原始密钥. 在双方共同采用{0，π}基进行相位调制的时间，利用差分编码方式产生原始密钥. 具体操作方法为：在以上时段内，当 Alice 对 PM_a 进行调制，前后两个脉冲差为 0 时，编码为 0；前后两个脉冲差为 π 时，编码为 1. Bob 端探测器 D_1 响应，编码为 0；探测器 D_2 响应，编码为 1.

3）用于安全性分析的采用{π/2，3π/2}基调相的编码生成. 具体操作方法为：在用{π/2，3π/2}基进行相位调制并且 Alice 对该脉冲前一个脉冲进行 0 相位调制的时刻，当 Alice 对此脉冲的调制相位为 π/2 时，编码为 0；对此脉冲的调制相位 3π/2 时，编码为 1. Bob 端探测器 D_1 响应，编码为 0；探测器 D_2 响应，编码为 1.

4）安全性评估. 此部分为本协议的亮点. 安全性评估由两部分组成：第一部分：差分产生的原始码. 随机分别从 Alice 和 Bob 端取出部分由差分产生的原始码进行比对，计算误码率，记为 e_1. 设从两方取出的码数都为 m_1，经公共信道比对得双方的误码数为 r_1，则误码率 $e_1=\frac{r_1}{m_1}$. 第二部分：由步骤 3）产生的编码. 将所有此步骤产生的编码从 Alice 和 Bob 端取出，计算误码率，记为 e_2. 设步骤3）产生的编码码数为 m_2，经公共信道比对得双方的误码数为 r_2，则误码率 $e_2=r_2/m_2$. e_1 和 e_2 是彼此独立的，若都小于 e_{max}，则保留；若 e_1 和 e_2 中有大于 e_{max}，则舍弃密钥，进行重发，这种安全性评估方法比计算 $\bar{e}=(e_1+e_2)/2$，使 $\bar{e}<e_{max}$ 更加严格.

5）若通过步骤 4）的安全性评估，可对生成的密钥进行保密放大[13]，进一步加强它的安全性.

1.2　成码率

该协议的密钥产生于差分编码方式. 差分系统的成码率为$(1-\frac{1}{N})$[9]，其中 N 表示脉冲串中脉冲的个数. 由 1.1.2 节中步骤 1）分析知选择差分编码方式的概率为 η^2. 所以对于本文中的协议，总成码率为 $\left(1-\frac{1}{N}\right)\cdot\eta^2$.

1.3　安全性分析

许多文献对各种攻击方法进行了讨论[7,11]，但

是一些理论上存在的攻击方法在目前技术条件下还无法实现[6]. 即使Eve能够实现这些攻击手段,那么还可以通过保密增强的方法来消除被窃听的信息,所以量子密钥分发形式本身就具有很强的安全性.

对于现有的量子密钥分发系统,在假设 Eve 的能力足够强的情况下,Eve 采取的攻击方法主要有两种,即:截获-重发攻击和分光子攻击. 以下分别讨论本文提出的协议抵御这两种基本攻击的能力.

1)截获-重发攻击. 一般假设 Eve 分别对每个信号进行单独测量,而且每次测量到的结果之间是相互独立的. 具体攻击方法:Eve 利用与 Bob 相同的测量装置,对 Alice 发送的信号进行截获,对截获到的光子进行测量,然后通过无损的信道发送给 Bob. 不难发现,Eve 的介入会破坏脉冲的相干性,从而引入一定的误码. 因此,在密钥分发结束后Alice和Bob双方可以通过误码率来判断有无窃听者的介入.

本文提出的协议中,密钥是产生于差分编码方式,这种编码方案对于抵御截获-重发攻击已得到了严格的证明[15],但是却有一定的局限性[12]. 这主要是由于对于截获-重发攻击,窃听引起的误码率取决于测量基的空间维度,空间维度的增加会增大误码率,从而易于发现 Eve. 但是传统的差分编码方式都是基于{0,π}基一维调制,所以安全性比较低. 在此协议的1.1.2节中步骤3)产生的编码,相当于用{π/2,3π/2}基对系统增加了一个维度,而二维调制进一步增加了该协议对于截获-重发攻击的安全性.

2)分光子攻击. 相干激光脉冲光源输出的光子数服从泊松分布,因此 Eve 可以从多光子脉冲中分得光子,然后进行存储. 当 Alice 和 Bob 在经典信道上进行密钥筛选和误码协调完成后,Eve 根据获得的这些经典信息然后对获得的光子进行测量. 其攻击过程:Alice 发送 N 个平均光子数为 μ 脉冲序列,量子信道的传输效率为 T,那么当 Eve 利用量子非破坏测量方法,把 $N\mu T$ 部分光子通过无损的信道发送给 Bob ,然后将 $N\mu(1-T)$部分光子存储在她的量子存储器中,当 Alice 和 Bob 交换经典信息后进行测量. 由于 Eve 不知道每个光子的绝对相位 φ_m,只知道相对相位差,并且她获得的是不同的 φ_m 组成的混合态[15],即

$$\rho_e=\frac{1}{N}\left[2\sum_{m\in B}|x_m\rangle\langle x_m|+\sum_{n\in\bar{B}}|n\rangle\langle n|\right] \tag{3}$$

式(3)中 B 表示 Bob 探测到光子的时隙,$\bar{B}$ 表示没有探测到光子的时隙. 从式中可以看出,如果 Bob 探测到 y 个脉冲信号,那么 Eve 通过分光子获取每个脉冲的信息概率为 $\frac{2y}{N}$. 因此,当 Bob 探测到 $N\mu T$ 个脉冲时,Eve 获得每个光子信息的概率为 $2\mu T$,而 Eve 总共窃取了 $N\mu(1-T)$ 个光子,那么她获得的信息为:$2N\mu^2T(1-T)$. 所以,Eve获取信息占密钥信息的比值为$2\mu(1-T)$. 当利用$\mu=0.2$,$\lambda=1\ 551$ nm,$\alpha=0.2$ dB/km,量子传输距离为$l=85$ km时,$T=10^{-\alpha l/10}=0.019\ 95$.(以上参量的取值为试验中所使用的参量) 因此,只要控制平均光子数远远小于 1,那么 Eve 通过分光子攻击无法获得全部的密钥信息.

此外,还通过分别计算不同测量基下的误码率的方法进一步增强了系统的安全性,体现在协议的 1.1.2 节中步骤 4).

以下以偏向选择攻击(Biased Eavesdropping Strategy)方式为例来分析本文采用的安全性分析方法的优势. Eve 以 p_1 的概率选择 0 相位来测量并将测量结果重发给 Bob,以 p_2 的概率选择 π 相位,以 $1-p_1-p_2$ 的概率什么都不做. 根据理论计算,实际信道噪音等测量结果,计算出 $e_{\max}$. 如果 Alice 和 Bob 使用{0,π}基而 Eve 以 p_2 的概率使用 π/2 进行测量,那么Eve的测量结果就是随机的,那么它发送给Bob的错误的可能性为1/2. 根据以上分析,$e_1=p_2/2$,同理可计算出 $e_2=p_1/2$.

那么 $\bar{e}=\frac{(e_1+e_2)}{2}=\frac{(p_1+p_2)}{4}<e_{\max}$,即

$$(p_1+p_2)<4e_{\max} \tag{4}$$

如果分别计算,使 $e_1<e_{\max}$,同时 $e_2<e_{\max}$,则相当于

$$p_1,p_2<e_{\max} \tag{5}$$

很明显这比$(p_1+p_2)<4e_{\max}$更加严格. 如$p_1=0$,$p_2=3e_{\max}$的情况下,满足式(4)而不满足式(5). 这种误码分析方法是源于高效 BB84 方案的,但在本文协议中,对通过{π/2,3π/2}基调相产生的编码,全部用做安全性分析而没有使用到密钥生成中去,这是出于以下考虑:1)通过{π/2,3π/2}基调相产生的编码数目很少,如还用做生成密钥,则能抽取出来进行安全性分析的码数会太少而在概率统计中不能代表误码率;2)只用差分方式产生密钥,可以简化协议,便于实际化应用.

1.4 η 的取值范围

对 η 的取值范围进行限制主要是由于需要在两种测量基下产生足够的光子以便计算误码率 e_1,e_2.

假设在一次密钥传输过程中,Alice 发送 N 个光子到 Bob 端. 平均来说,只有 $N(1-\frac{1}{N})\eta^2$ 个光子完全经{0,π}基调制. 为了计算 e_1,必须保证 $N\eta^2$ 足够大以至可以构成为一个能代表统计规律的样本空间,进而可以抽取 m_1 个光子进行误码率分析. 用数

学方式表达为

$$N(1-\frac{1}{N})\eta^2 \geqslant m_1$$

因此

$$\eta \geqslant \sqrt{m_1/(N-1)}$$

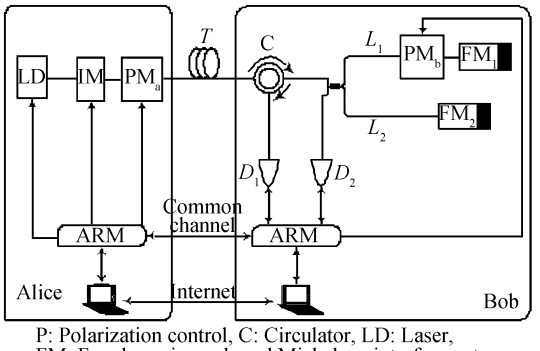
同样要在{π/2，3π/2}基下生成 m_2 个光子进行安全性评估，则要求有 $N\frac{\eta}{2}(1-\eta)^2$ 个光子完全经{π/2，3π/2}基调制. 为了计算e_2，必须保证$N\frac{\eta}{2}(1-\eta)^2 \geqslant m_2$. 所以 η 的取值范围为

$$\eta \geqslant \sqrt{m_1/(N-1)} \quad Y\eta(1-\eta)^2 \geqslant 2m_2/N \qquad (6)$$

在式(6)所述范围内，η 取任意的实数，整个协议都可以成功运作.

2　系统结构及实验

实验装置如图2. Alice端，激光的中心波长是 1 551 nm，脉冲的宽度是5×10^{-12} s，重复率是50 kHz. 利用强度调制器 IM 将连续光斩为连续微弱相干光脉冲，经相位调制器调制后，衰减器将光脉冲能量衰减到平均光子数为 0.2，然后注入到 85 km 的光纤中. 将能量衰减到平均光子数为 0.2，而不是通常意义上的 0.1. 由于在本文的实验条件下当平均光子数为 0.1 时整个实验系统成码率比较低，为了提高成码率，方便实验结果的比对和误码率分析，将平均光子数增加到 0.2 进行实验. Bob 端，用法拉第反射式迈克尔逊干涉仪，自动补偿了环境引起的偏振抖动和光纤双折射引起的相位漂移. 单光子探测器的型号为Id200，它的门宽是5 ns，门脉冲是与光脉冲同步的，量子效率是 8%，暗计数为 2.21×10^{-5}. 根据本文定义的密钥分发协议，以 $\eta=31/32$ 的概率选择{0，π}基调制相位，在 Alice 和 Bob 双方建立密钥. 实验过程中一次产生的原始密钥(raw key)数量约 1 100 Mbits. 为满足式(6)给定的范围和方便在现有条件下进行本文的实验，编程时选择$\eta=31/32$，无特殊意义.



P: Polarization control, C: Circulator, LD: Laser,
FM: Faraday-mirrors-based Michelson interferometers

图 2　系统结构原理图

Fig. 2　The experimental setup

在实验系统中，选用基于 ARM7 的 SOC 芯片 EP7312 的 CPU 做为控制系统核心. 实验产生的密钥通过 RS232 口被送到各自端的计算机，以显示给用户. 从产生的密钥中检测出的误码率小于 5%. 表 1 为从产生的原始码中抽取出来做误码率分析的密钥，为十六进制编码.

根据表 1～表 4 的内容，计算得 $e_1=23/512=4.492\%$，$e_2=21/512=4.102\%$.

表 1　Alice 端码{0，π}基下产生的密钥

密钥(512 bits)										
C6	A2	BA	3A	FE	CE	D6	0A	6A	8E	EA
AA	CE	4E	22	92	42	9A	76	7E	EA	56
DE	FE	22	72	92	52	22	C2	7E	92	EA
DE	0E	B2	AE	E2	2E	82	4E	26	72	C6
A2	56	9A	22	6E	C6	7E	62	F2	76	3A
A6	6A	5E	4A	66	2A	DE	FE	2A		

表 2　Alice 端用{π/2，3π/2}基进行相位调制产生的编码

密钥(512 bits)										
82	2E	0A	AE	6A	D2	D6	D6	92	DE	C6
06	C2	F6	EE	8A	72	4A	22	16	06	46
8A	FE	46	0E	2A	2E	1A	DA	OE	56	9E
FE	66	E2	96	52	36	FE	8A	DA	0E	F2
8A	82	1A	C2	4E	56	9A	CA	FA	66	16
7E	B6	BE	96	0A	3A	CA	96	72		

表 3　Bob 端 0 相位调制下产生的密钥

密钥(512 bits)										
C6	E2	BA	3A	FE	8E	96	0A	2A	8E	EA
AA	CA	4F	22	D2	42	9A	36	7E	EA	56
DA	FF	27	77	92	57	22	C2	7E	92	EA
DF	0E	B2	AE	E2	2E	82	4F	26	72	C6
E2	52	9A	22	6E	C2	7F	62	F2	76	3A
A6	2A	5A	0A	66	2A	DE	FE	2A		

表 4　Bob 端 π/2 相位调制下产生的编码

密钥(512 bits)										
82	2E	0A	AF	6A	D2	D7	D6	92	DE	C2
06	C2	B6	EF	8A	72	4A	62	16	06	46
8A	FE	06	0E	2A	2E	5A	9A	OA	56	9E
FA	66	E7	96	52	36	FE	8A	DF	0E	F2
CA	82	1A	C2	4E	16	DA	CA	FA	66	16
7E	F6	BE	5A	0A	7A	CA	96	72		

随后将通过安全性分析差分编码产生的密钥用于加密图像，效果良好. 此实验为协议方案的验证性实验，至于实验数据的优化等，将留待后续工作.

3　结论

提出了一种新的相位调制量子密钥编码协议，并设计相应的系统，实验论证了其正确性和可操作性. 此系统具有以下特点：1)安全，二维测量基({0，π}和{π/2，3π/2})的使用增加了系统自由度，从而可以有效抵御截获－重复攻击，差分编码方式可以

有效抵御光子束分束攻击，差分协议和高效 BB84 协议的联合使用可以有效的迷惑窃听者，这些措施都增加了系统的安全性. 2)稳定，相位编码适合于光纤传输系统，差分编码方式自身稳定性就很高，同时又在 Bob 端使用双 FM 反射式干涉仪，自动补偿了环境引起的偏振抖动和光纤双折射引起的相位漂移，进一步提高了系统稳定性. 3)高效，差分编码方式的优势之一是高成码率，同时采用高的脉冲重复率(本系统中为50 KHz)，可进一步提高密钥生成率.

参考文献

[1] HONJO T, INOUE K. Differential-pahse-shift quantum key distribution[J]. *NTT Technical Review*, 2004, **2**(12): 26-33.

[2] BENNETT C H. Quantum cryptography using any two nonorthogonal states [J]. *Physics Review Letter*, 1992, **68**(21): 3121-3124.

[3] EKERT A K. Quantum cryptography based on Bell's theorem [J]. *Physical Review Letter*, 1991, **67**(6): 661-663.

[4] BENNETT C H, BRASSARD G, MERMIN N D. Quantum cryptography without Bell's theorem [J]. *Physical Review Letter*, 1992, **68**(5): 557-559.

[5] BENNETT C H, BRASSARD G. Quantum cryptography: public key and coin tossing[C]. *Proceedings of the IEEE International Conference on Computer Systems and Signal Processing*, New York, 1984: 175-179.

[6] LIU Jing- feng, LIANG Riu-sheng, TANG Zhi-lie, *et al*. Eavesdropping of Practical QKD System Based on BB84 Protocol[J]. *Acta Photonica Sinica*, 2004, **33**(11): 1356-1359.
刘景锋，梁瑞生，唐志列等. 基于 BB84 协议的实际 QKD 系统的窃听问题研究[J]. 光子学报，2004，**33**(11)：1356-1359.

[7] CHEN Zhi-xin, TANG Zhi-lie, LIAO Chang-jun, *et al*. Practical security problem of six states QKD protocol[J]. *Acta Photonica Sinica*, 2006, **35**(1): 126-129.
陈志新，唐志列，廖常俊等. 实际量子密钥分配扩展 BB84 协议窃听下的安全性分析[J]. 光子学报，2006，**35**(1)：126-129.

[8] CHEN Zhi-xin, TANG Zhi-lie, WEI Zheng-jun, *et al*. On the breidbart eavesdropping information problem of BB84 QKD protocol[J]. *Acta Photonica Sinica*, 2004, **33**(12): 1469-1472.
陈志新，唐志列，魏正军等. QKD 系统在 Breidbart 基窃听下 BB84 协议的信息量研究 [J]. 光子学报，2004，**33**(12)：1469-1472.

[9] INOUE K, WAKS E, YAMAMOTO Y. Differential phase shift quantum key distribution[L]. *Phys Rev Lett*, 2002, **89**(3): 037902-1-037902-3.

[10] INOUE K, HONJO T. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack [J]. *Phy Rev A*, 2005, **71**(4): 042305-1-042305-4.

[11] LI Ming-ming, Wang Fang-qiang, Lu Yi-qun, *et al*. A highly stable differential phase shift key distribution QKD system [J]. *Acta Physica Sinica*, 2006, **55**(9): 4642-4624.
李明明，王发强，路轶群等. 高稳定的差分相位编码量子密钥分发系统[J]. 物理学报，2006，**55**(9)：4642-4644.

[12] HONJO T, INOUE K. Differential-phase-shift quantum key distribution with an extended degree of freedom[J]. *Opt Lett*, 2006, **31**(4): 522-524.

[13] HOI-KWONG L, CHAU H F, ARDEHALI M. Efficient quantum key distribution scheme and proof of its unconditional Security[J]. *J of Cryptology*, 2005, **18**(2): 133-165.

[14] ZHENG Li-ming, WANG Fa-qiang, LIU Wei-ming, *et al*. Interference stability analysis of quantum key distribution system based on single photon[J]. *Acta Photonica Sinica*, 2005, **34**(5): 797-800.
郑力明，王发强，刘伟平，等. 单光子量子密钥分发系统中干涉稳定性分析[J]. 光子学报，2005，**34**(5)：797-800.

[15] WAKS E, TAKESUE, YAMAMOTO Y. Security of differential-phase-shift quantum key distribution against individual attacks[J]. *Phys Rev A*, 2006, **73**(1): 012344-1—012344-9.

A Differential Phase Shift Key Distribution QKD System Combing with Efficient BB84 Scheme

CHEN Xia, WANG Fa-qiang, LU Yi-qun, ZHAO Feng, LI Ming-ming, LIANG Rui-sheng, LIU Song-hao

(*Lab of Photonic Information Technology, South China Normal University, Guangzhou* 510006, *China*)

Received date: 2006-10-27

Abstract: A novel phase modulated quantum key distribution scheme with high security, which is combined differential phase shift quantum key distribution (DPS-QKD) with efficient BB84 scheme, is proposed. Alice chooses phase in $\{0, \pi/2, \pi, 3\pi/2\}$ randomly to modulate the phase of signal pulses and Bob do it in $\{0, \pi/2\}$. The system is designed to demonstrate its feasibility, which features perfect stability with a QBER less than 5% during 85-km fiber transmission.

Key words: Quantum cryptography; Quantum key distribution; Phase coding; Quantum key distribution; Efficient BB84 scheme

CHEN Xia was born in 1982. She graduated from Tianjin University in 2004. Now as a postgraduate student, she is engaged in the study of quantum cryptographic communication and optics information at South China Normal University.