第 56 卷 第 4 期 2007 年 4 月
1000-3290/2007/56(04)/2175-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.4,April,2007

基于微弱相干脉冲稳定差分相位量子密钥分发*

赵 峰[1)2)] 路轶群[1)†] 王发强[1)] 陈 霞[1)]
李明明[1)] 郭邦红[1)] 廖常俊[1)] 刘颂豪[1)]

1)(华南师范大学信息光电子科技学院,广州 510006)
2)(陕西理工学院电信工程系,汉中 723003)

(2006 年 5 月 30 日收到;2006 年 12 月 27 日收到修改稿)

基于差分相位量子密钥分发协议,对微弱相干光脉冲相位差进行编码,在接收端采用 Faraday-Michelson 系统进行解码.这种量子密钥分发系统具有密钥生成效率高、接收端干涉稳定性好、极限传输距离长等优点,同时还具有光路结构简单、易于在现有的技术条件下实现等特点,特别适用于远程光纤量子密钥分发.在实验系统中利用嵌入式微处理系统来控制量子密钥分发过程,进行了 76 km 的稳定光纤量子密钥分发实验,其原始密钥的误码率为 5.3%.

关键词:差分相位,量子密钥分发,安全性,稳定性

PACC:4250,4230Q,4210J,0365

1. 引 言

自从 Bennett 和 Brassard 于 1984 年第一次提出量子密钥分发协议[1],量子密码技术发展日趋完善,光纤量子保密通信技术已经从广泛的实验研究[2—5]发展到正式推出了商用化量子密码机[6].差分相位量子密钥分发原理[7]是基于对相干脉冲的相位差进行编码,利用非等臂 Mach-Zehnder(M-Z)干涉仪来测量其相位差进行解码.基于微弱相干光脉冲的量子密钥分发系统具有结构简单、密钥生成效率高、适用于泊松光源等优点,日本 NTT 公司利用集成非等臂 M-Z 干涉仪完成了 105 km 光纤量子密钥分发[4]实验.但是,这种集成干涉仪制作工艺复杂、价格昂贵,并且与偏振相关,在量子密钥分发过程中需要精密的温度控制来消除相位漂移,因此实用化还存在一定困难.中国科学技术大学郭光灿等利用 Faraday-Michelson 干涉方式进行了长距离、长时间、单向、稳定的量子密钥分发实验[8].该实验系统的特点是:基于 BB84 协议或 B92 协议;要求对脉冲相位调制与偏振无关;传输的距离受到分光子攻击限制.然而,基于微弱相干光脉冲下的差分相位量子密钥分发系统抵御分光子攻击能力较强,当平均光子数为 0.1 时,每脉冲的密钥生成效率接近基于理想单光子源的 BB84 协议下的密钥生成效率[9].同时,这种系统利用现有的技术和光通信设备(激光光源、雪崩光电二极管以及现有的光纤线路)就能够实现安全、长距离的光纤量子密钥分发.我们实验室利用分束器获得 4 个相干脉冲光,进行了稳定的差分相位量子密钥分发的实验[6],但是这种方案在抗干扰方面还存在一些问题,密钥的安全性和生成效率还有待提高.本文中,我们改进了该方案,采用强度调制器产生连续的微弱相干光脉冲进行了量子密钥分发实验,其稳定性、安全性以及密钥生成效率均得到了提高,具有很好的实用价值.

2. 安全性分析

许多文献对差分相位量子密钥分发系统的安全性问题进行了讨论[9—11],然而,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,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[12].这里主要讨论基于连续微弱相干光脉冲下的差分相位量子密钥分发系统中的安全性问题.在差分相位量子密钥分发过程中,Eve 对信息的窃取一般采用下列措施[9]:截获-重发

* 国家重点基础研究发展规划(批准号:2001039302)资助的课题.

† E-mail:qkdscnu@126.com

攻击、分光子攻击、序列攻击.其中对于截获-重发攻击和分光子攻击,我们一般假设 Eve 分别对每个信号进行单独的测量,而且每次测量到的结果之间是相互独立的.下面给出差分相位量子密钥分发系统对 Eve 进行攻击时的抵御过程.

2.1.截获-重发攻击

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 Eve 通过无损的信道发送给 Bob.由于 Eve 的介入会破坏脉冲的相干性,从而引入一定的误码,尽管 Eve 可以采取一定的措施来降低误码率,但是误码率降低的同时使得 Eve 获得的信息量减小.因此,在密钥分发结束后 Alice 和 Bob 双方可以通过误码率[10]来判断有无窃听者的介入,以及估计出 Eve 获得的最大信息量.

2.2. 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,Eve 可以从多光子脉冲中分出一部分光子,然后存储在量子存储器中.当 Alice 和 Bob 在经典信道上进行密钥筛选和误码协调后,Eve 根据获得的这些经典信息对存储的光子进行测量.其攻击过程如下:若 Alice 发送 N 个脉冲序列,其平均光子数为 μ,量子信道的传输效率为 T,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 $N\mu(1-T)$部分光子存储在量子存储器中,待 Alice 和 Bob 交换经典信息后再进行测量.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[9],即

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

式中 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(1)式可以看出,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 $2y/N$.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 $2\mu(1-T)$.当每脉冲中平均光子数 $\mu=0.1$,$\lambda=1550$ nm,$\alpha=0.2$ dB/km,量子传输距离为 $l=150$ km 时,$T=10^{-\alpha l/10}=0.001$,Eve 对最终密钥获取的信息接近于 20%.因此,只要平均光子数小于 0.5,那么 Eve 通过分光子攻击无法获得全部的密钥信息.

2.3.序列攻击

差分相位量子密钥分发系统还存在另外一种攻击:序列攻击[9],这种攻击方法不满足单独攻击前提假设.序列攻击过程如下:Eve 利用与 Bob 相同的测量装置对 Alice 发送的光子进行测量,当探测器出现 k 次连续响应时,Eve 可以推出 $k+1$ 个量子态之间的相位关系,然后重新制备出 $k+1$ 个量子态发送给 Bob.然而,序列攻击引入的误码率为 $\frac{1}{2(k+1)}$,Eve 出现 k 个脉冲连续响应的概率 $p(k)$ 与 k 呈指数关系下降,其表达式为[9]

$$p(k)=\mu^{-k},$$

式中 μ 为每个脉冲的平均光子数.当 Eve 为了获得全部密钥的信息时,那么她探测到 k 个光子连续响应的概率应该大于或等于 Bob 的探测概率,即 $\mu^{-k}\geqslant\mu T$.但是,我们可以通过调整平均光子数来限制出现 k 个脉冲连续响应的概率.因此,在相同的条件下,序列攻击的威胁小于单比特攻击给系统带来的威胁.

3. 稳定性分析

图 1 为基于微弱相干脉冲的差分相位量子密钥分发系统光路图,其中 CW 为连续光源,IM 为强度调制器,PM 为相位调制器,FM1,FM2 是 Faraday 旋转镜,D_1,D_2 为单光子探测器.其过程如下:平均光子数小于 1 的两个连续相干脉冲 P_1,P_2 携带着 Alice 加载的信息,通过光纤传输到达 Bob 端,然后分别通过干涉仪的两个臂,经过 Faraday 镜反射后在输出端口干涉,光子根据干涉的结果选择到达不同的探测器 D_1 或 D_2.因此,P_1,P_2 这两个脉冲离开 Alice 端后经历的路径分别可以表示为

$$T\rightarrow L2\rightarrow \mathrm{FM2}\rightarrow L2,$$
$$T\rightarrow L1\rightarrow \mathrm{FM1}\rightarrow L1.$$

脉冲 P_1,P_2 离开 Alice 端时的初态分别为

$$E_1 = E_{10}e^{i\varphi_1},$$
$$E_2 = E_{20}e^{i\varphi_2},$$

其中 φ_1 和 φ_2 表示 Alice 调制的相位,E_{10},E_{20} 分别为这两个态的振幅.

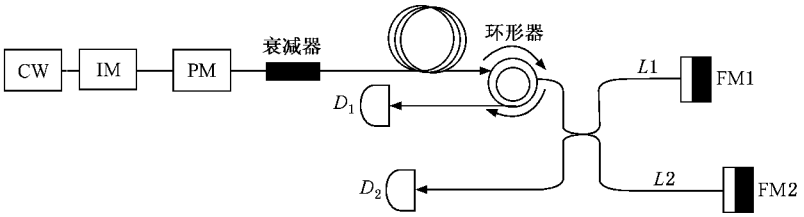

图 1　差分相位量子密钥分发系统光路图

经过光纤传输到达 Bob 端后，这两个脉冲分别表示为

$$L_{2-}\mathrm{e}^{-\mathrm{i}\phi_a}FL_{2+}\mathrm{e}^{\mathrm{i}\phi_a}T\mathrm{e}^{\mathrm{i}\phi_2}\frac{E_1}{2}$$
$$=\frac{1}{2}L_{2-}FL_{2+}TE_1\mathrm{e}^{\mathrm{i}\phi_2}$$
$$=\frac{1}{2}T_1E_{10}\mathrm{e}^{\mathrm{i}\phi_2}\mathrm{e}^{\mathrm{i}\varphi_1}, \quad (2)$$

$$L_{1-}\mathrm{e}^{-\mathrm{i}\phi_b}FL_{1+}\mathrm{e}^{\mathrm{i}\phi_b}T\mathrm{e}^{\mathrm{i}\phi_1}\frac{E_2}{2}$$
$$=\frac{1}{2}L_{1-}FL_{1+}TE_2\mathrm{e}^{\mathrm{i}\phi_1}$$
$$=\frac{1}{2}T_2E_{20}\mathrm{e}^{\mathrm{i}\phi_1}\mathrm{e}^{\mathrm{i}\varphi_2}, \quad (3)$$

式中 L_1，L_2 分别为干涉仪的两个臂的传输矩阵，F 为 Faraday 旋转镜的传输矩阵，T_1，T_2 分别为两个脉冲经过传输光纤的传输矩阵，ϕ_1，ϕ_2 分别为由传输光纤引起的相位变化．若相邻两个脉冲振幅相等，即 $E_{10}=E_{20}=E_0$，两个脉冲时间间隔很短且经历了相同的传输路径，即 $\phi_1=\phi_2=\phi$，$T_1=T_2=T$．因此，当这两个脉冲在 Bob 端发生干涉后，在其中一个端口输出的电场强度可以表示为

$$E_{\mathrm{out}}=\frac{1}{2}TE_0\mathrm{e}^{\mathrm{i}\phi}(\mathrm{e}^{\mathrm{i}\varphi_1}+\mathrm{e}^{\mathrm{i}\varphi_2}), \quad (4)$$

其光强可以表示为

$$P_{\mathrm{out}}=E_{\mathrm{out}}^{+}E_{\mathrm{out}}$$
$$=\frac{1}{2}|T|^2|E_0|^2[1+\cos(\varphi_2-\varphi_1)]. \quad (5)$$

当 Alice 用 $\{0,\pi\}$ 随机调制每个脉冲相位 φ_i，当 $\Delta\varphi=\varphi_2-\varphi_1=0$ 时，光子到达探测器 D_1，而当 $\Delta\varphi=\pi$ 时，光子到达探测器 D_2．在实验系统中为了达到稳定而高的干涉对比度，必须采取以下措施：一是利用相干性、稳定性好的光源；二是经过强度调制器和相位调制器制备出的量子态应具有相等的振幅 $E_{10}=E_{20}$；三是相邻两个脉冲的时间间隔尽可能短，这样可以使得 $T_1=T_2$，$\phi_1=\phi_2$；四是表达式(2)和(3)及(4)的前提条件之一是在恒温下，没有考虑到温度变化对干涉稳定性的影响，所以在实验中需要进行恒温控制．

4. 实验结果

图 2 为实验装置示意图，相干光源(连续半导体激光器)工作在 1550 nm，利用强度调制器 IM 将连续光斩为相干脉冲光，其时间间隔为 Δt，然后经过铌酸锂波导相位调制器进行相位调制，最后衰减至平均光子数 $\mu=0.2$，经过 76 km 的光纤后到达 Bob 方，Bob 利用 Faraday-Michelson 干涉装置测量相位差．根据差分相位量子密钥分发协议，Alice 用 $\{0,\pi\}$ 相位对光脉冲进行随机调制，0 代表经典比特信息“0”，π 代表经典比特信息“1”．这些携带信息的光子经过量子信道到达 Bob 方，由于相邻两个脉冲会发生干涉，光子根据干涉的结果选择不同的路径到达

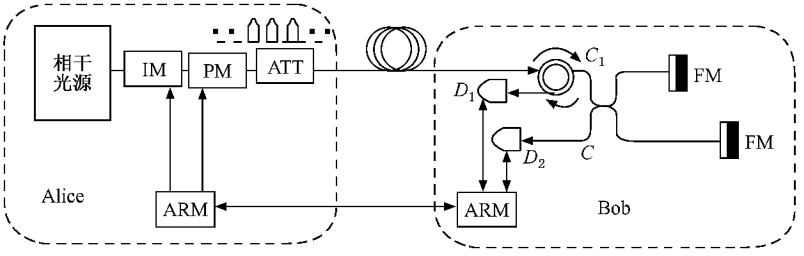

图 2　差分相位量子密钥分发实验装置示意图

探测器.当探测器 D_1 响应、D_2 不响应时,记为经典比特‘0”.反之,当探测器 D_2 响应、D_1 不响应时,记为经典比特‘1”.这样 Alice 和 Bob 双方根据协议建立起秘密的随机二进制序列(原始密钥).

在实验系统中,Alice 和 Bob 的控制系统是基于 ARM (advanced RISC (reduced instruction set computing) machines)芯片的嵌入式微处理系统,这种嵌入式微处理系统具有功能强大、指令简单、功耗低、价格便宜等特点,目前已广泛应用于工控系统.利用微处理系统代替个人计算机进行量子密钥分发,具有体积小、价格便宜、易于控制等优点,因此便于量子密钥分发系统向实用化迈进.由于单光子探测器(id200 型)的响应速率最高为 1 MHz,为了减小暗计数,Alice 和 Bob 双方设定通信速率为 500 kbit/s,单光子探测器门宽 20 ns 的暗计数率为 10^{-4}.Alice 和 Bob 同步信号由 DG535 型时延/脉冲发生器进行精确调整,其最小的时延调整精度为 5 ps.强度调制器 IM 和相位调制器的调制信号由 Alice 方的 ARM 系统发出,控制信号经过 DG535 两路输出分别加载到这两个调制器的控制电路上,得到了脉冲宽度为 5 ns 的稳定相干脉冲,重复频率为 500 kHz.在 Bob 方,由于两个连续相干脉冲的时间间隔为 2 μs,光纤中延时约为 5 ns/m,因此 Faraday-Michelson 干涉仪两臂差为 200 m.三端口光环形器插入损耗为 0.9 dB,2×2 光纤耦合器插入损耗为 0.3 dB, Faraday 旋转镜插入损耗为 0.7 dB.因此,在接收端的插入损耗总共约为 $0.9+2\times0.3+0.7=2.2$ dB,传输线路的插入损耗约为 $0.208\times76=15.8$ dB,因此实际传输线路中的损耗约为 18 dB.我们从一次密钥分发实验的原始密钥中取出 1024 位进行分析,其误码率为 5.3%,因此在安全允许的误码范围内,通过误码协调和保密增强后可以供‘一次一密’方式加密与解密使用.

5. 实验分析

Faraday-Michelson 干涉仪在理论上能够完全抵消光纤随机双折射的影响.但是,如果两个相干的脉冲时间间隔太大,那么在传输过程中受到外部环境的干扰不同,其传输矩阵 $T_1\neq T_2$ 以及 $\phi_1\neq\phi_2$,因此容易导致干涉不稳定.如果缩短连续相干脉冲之间的时间间隔,就可以大大减小影响,那么就必须提高系统的传输速率,然而单光子探测器的响应速率限制了系统传输速率的提高.目前差分相位量子密钥分发系统已经利用一种基于频率上转换的单光子探测器[3],其量子效率和响应速率较高,具有很好的应用前景.其次,使用 Faraday-Michelson 干涉系统时,依然存在一些振动干扰,当我们对两个臂的光纤施加一定扭转应力时可以消除影响,获得稳定的干涉.第三,当干涉仪的两个臂差很大(500 m)时,温度变化会明显影响干涉的稳定性,因此在分发过程中需要对干涉仪进行恒温控制.第四,光子根据干涉结果选择其中一个端口到达单光子探测器(图 2),其中一路经过环形器到达探测器,而另外一路直接到达探测器,由于环形器具有一定的插入损耗,因此在相同的条件下两个探测器的响应速率不同,因此会带来一定的误码以及安全隐患.第五,在实验系统中,我们利用强度调制器来产生相干脉冲光,由于控制电路的缺陷,产生的相干光脉冲宽度为 5 ns 左右,经过 76 km 传输,我们设定单光子探测器的门宽为 20 ns,这样探测器的暗计数较大,从而引起误码率的增加.若使得相干光脉冲的脉冲宽度小于 1 ns 时,可以通过减小探测器的门宽来降低误码率,并且强度调制器和相位调制器都需要进行振动隔离和恒温控制.第六,随着传输距离的增加,同步信号会出现漂移,需要定期进行重新校准.若利用光信号进行同步,那么可以进行更长距离的量子密钥分发.

6. 结 论

在目前的技术条件下,基于微弱相干脉冲下的差分相位量子密钥分发系统能够有效地抵御窃听者的攻击,若平均光子数远小于 1 时,其传输距离不会受到分光子攻击的限制.本文基于微弱光脉冲下利用差分相位量子密钥分发协议成功进行了 76 km 光纤量子密钥分发实验,原始密钥误码率为 5.3%.从理论和实验上证明了基于微弱相干脉冲下的差分相位量子密钥分发方式具有安全性好、脉冲密钥生成效率高、干涉稳定性好、传输距离长等特点.这种量子密钥分发系统无论在点到点量子密钥分发系统,还是在量子密钥分发局域网络系统都具有很好的实用开发前景.

[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 *et al* 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁　创、符东浩、梁　冰等 2001 物理学报 **50** 1429]
[3] Kimura T, Nambu Y, Hatanaka T A *et al* 2004 *Jpn. J. Appl. Phys.* **43** 1217
[4] Takesue H, Diamanti E, Honjo T *et al* 2005 *New J. Phys.* **7** 232
[5] Wu G, Zhou C Y, Chen X L *et al* 2005 *Acta Phys. Sin.* **54** 3622 (in Chinese) [吴　光、周春源、陈修亮等 2005 物理学报 **54** 3622]
[6] Li M M, Wang F Q, Lu Y Q *et al* 2006 *Acta Phys. Sin.* **55** 4642 (in Chinese) [李明明、王发强、路轶群等 2006 物理学报 **55** 4642]
[7] Inoue K, Waks E, Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[8] Mo X F, Zhu B, Han Z F *et al* 2005 *Opt. Lett.* **30** 2632
[9] Waks E, Takesue H, Yamamoto Y 2006 *Phys. Rev.* A **73** 012344
[10] Inoue K, Waks E, Yamamoto Y 2003 *Phys. Rev.* A **68** 022317
[11] Inoue K, Honjo T 2005 *Phys. Rev.* A **71** 042305
[12] Lütkenhaus N 1999 *Phys. Rev.* A **59** 3305

Stable differential-phase-shift quantum key distribution based on weak coherent pulses *

Zhao Feng[1)2)]　Lu Yi-Qun[1)†]　Wang Fa-Qiang[1)]　Chen Xia[1)]　Li Ming-Ming[1)]
Guo Bang-Hong[1)]　Liao Chang-Jun[1)]　Liu Song-Hao[1)]
1) (*School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)
2) (*Department of Electronic and Information Engineering, Shaanxi University of Technology, Hanzhong* 723003, *China*)
(Received 30 May 2006; revised manuscript received 27 December 2006)

Abstract

Differential phase shift quantum key distribution (DPSQKD) experiment based on weak coherent pulses have been performed in the laboratory. We encoded the bit information between the consecutive pulses. The bit information was decoded at Bob's side by Michelson-Faraday interferometer and single photon detector. This kind of quantum key distribution system can provide stable key distribution process, high efficiency of key creation, and high security key. So it is easily implemented in optical fibers using readily available optical telecommunication tools. We experimented DPSQKD over 76 km on fiber, the error rate of the sifted key is 5.3%. The quantum key distribution process is controlled by micro-computer based on ARM (advanced RISC (reduced instruction set computing) machines) processor.

Keywords: differential phase, quantum key distribution, security, stability
PACC: 4250, 4230Q, 4210J, 0365

* Project supported by the State Key Development Programe for Basic Research of China (Grant No. 2001039302).
† E-mail: qkdscnu@126.com