第 57 卷 第 2 期 2008 年 2 月
1000-3290/2008/57(02)/0685-04

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.2,February,2008

基于差分相移键控协议的双向量子密钥分配系统研究*

焦荣珍† 冯晨旭

(北京邮电大学理学院,北京 100876)

(2007 年 4 月 23 日收到;2007 年 5 月 23 日收到修改稿)

采用差分相移键控(DPSK)协议分析了双向量子密钥分配(QKD)系统的性能,比较了 BB84 协议、BBM92 协议和 DPSK 协议的安全通信速率与距离的关系,并对协议对抗一些攻击的安全性进行了分析,结果表明 DPSK 协议对长距离 QKD 系统非常实用,具有超过 200 km 的通信距离和较高的通信速率.

关键词:差分相移键控协议,量子效率,通信速率

PACC:0367,4250

1. 引 言

量子保密通信是量子信息科学中的重要分支,量子保密通信以其优越的先天特点有可能改变未来的保密通信方式,近年来已成为国内外的热门研究领域[1—3].而在量子保密通信中不可或缺的一部分是量子密钥分配(QKD),这是保证通信安全性的重要环节,QKD 能让通信双方共享一个无条件安全密钥,因为量子机制就能保证安全,密钥能在之后用来一次性的加密和解密消息.当前,量子密码研究的核心内容,是如何利用量子技术在量子信道上安全可靠地分配密钥,利用各种协议来抵御外界的攻击.从国内外已经公布的文献来看,最常见的量子密钥分配协议有:BB84 协议,BBM92 协议,相关粒子协议[4,5].1992 年,Bennett 等人[6]基于 BB84 协议,以强烈衰减的激光脉冲做单光子源,信息加载在单光子的偏振上,第一次成功地在自由空间完成了演示性实验,从而掀起了量子密钥分发实验研究的高潮.当前,实现光纤中量子密钥分发采用的是相位调制编码,实验方案主要有:由 Bennett 提出的基于双不等臂马赫-曾德耳光子单向传输.该方案有效地制止了木马攻击,在通信双方 Alice 和 Bob 各自的干涉仪内部光脉冲沿不同的路径传播,因此获得较好的实验结果.本文将差分相移键控(DPSK)协议用于双向 QKD 系统,利用其与 BB84 协议和 BBM92 协议的不同,导出基于 DPSK 协议的通信速率与距离的关系式,分析在分光攻击和截断-重发攻击下的 QKD 系统的性能.

2. 理论与计算公式

双向量子密钥分配系统如图 1 所示.

在 BB84 协议中,Alice 给 Bob 发送单光子,随机调制到两种极化基上.Bob 用一个随机选择的极化基来测量接收到的单光子的极化状态.这种对抗任意个体攻击的通信速率由下面的等式给出.

$$R_{\mathrm{BB84}} = \frac{1}{2}\upsilon p_{\mathrm{click}}\{\tau(e,\beta) + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\},$$

其中,因数 1/2 为筛选参数,υ 为传输重复速率,$\tau(e,\beta)$为保密放大阶段的主要衰减因子,其关系式如下:

$$\tau(e,\beta) = -\beta\log_2\left[\frac{1}{2} + 2\frac{e}{\beta} - 2\left(\frac{e}{\beta}\right)^2\right],$$

其中参数这与 BB84 协议相似为

$$\beta = \frac{p_{\mathrm{click}} - p_{\mathrm{m}}}{p_{\mathrm{click}}},$$

其中 p_{m} 为光源发射多光子态的概率,p_{click} 为 Bob 探

* 国家自然科学基金(批准号:60054402)资助的课题.

† E-mail:jiao218@sohu.com

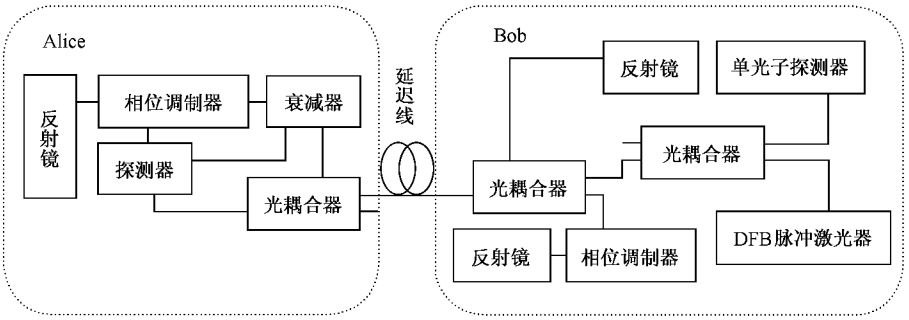

图 1 双向量子密钥分配系统图

测到一个光子的概率,其表达式为

$$p_{\text{click}} = \mu\eta 10^{-(\alpha L + L_r)/10} + 4d,$$

这里 μ 为每脉冲的平均光子数,η 为探测器的量子效率,α 为光纤 dB/km 的损耗因数,L_r 为接收机的损耗,d 为系统每个测量时间窗内的暗记数.

BBM92 协议是 BB84 协议双光子派生出来的协议.Alice 和 Bob 每个都共享一个纠缠光子对中的一个光子,因为他们能从两个非正交基中测量出随机选择基的极化状态.平均碰撞概率 p_c 和 BB84 协议时一样,此时 $\beta = 1$,衰减因数 τ 变成

$$\tau(e) = -\log_2\left(\frac{1}{2} + 2e - 2e^2\right),$$

对抗个体攻击的通信速率由下式给出:

$$R_{\text{BBM92}} = \frac{1}{2}\upsilon p_{\text{coin}}\{\tau(e) + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\},$$

其中参数的表达式参见文献[5].

DPSK 协议与 BB84 协议、BBM92 协议不同,它用很多含有脉冲的非正交基,其原理为:所有的脉冲都经过强烈衰减,并在$(0,\pi)$之间随机进行相位调制,其组成图如图 2 所示.在接收端,Bob 通过它的干涉仪随机调制延迟时间 NT,它的干涉仪随机选择一个正整数 N,其中 T 始终是频率的倒数.在穿过 Bob 的干涉仪之后,脉冲在 Bob 输出端的分光器上进行干涉,探测器是否反映取决于分隔时间 NT 的两个脉冲的相位差.Bob 在探测到光子并随机选择正整数 N 的时候进行公共广播.从他的调制信息 Alice 知道哪个探测器记录了信息.这样他们通过分配给探测器一个比特值来形成密钥.

考虑 DPSK 协议的安全性,我们在分析中考虑到了复合攻击. 含有分光和截断-重发攻击的复合攻击时,保密放大衰减参数为

$$\tau(e,\gamma) = \gamma - \frac{e}{N(1-1/2N)},$$

这里

$$\gamma = \begin{cases} 1 - \dfrac{\mu(1-\eta_{\text{BS}})}{N} = 1 - \dfrac{\mu}{N} + \dfrac{p_{\text{signal}}}{N} \\ 1 - 2\mu(1-\eta_{\text{BS}}) = 1 - 2\mu + 2p_{\text{signal}} \end{cases}$$

$$p_{\text{signal}} = \mu\eta 10^{-(\alpha L + L_r)/10}$$

传输效率为

$$\eta_{\text{BS}} = \eta 10^{-(\alpha L + L_r)/10}$$

DPSK 协议对抗多种复合攻击时的通信速率为

$$R_{\text{DPSK}} = \upsilon p_{\text{click}}\{\tau(e,\gamma) + f(e) \times [e\log_2 e + (1-e)\log_2(1-e)]\},$$

其中,υ 为传输的重复速率.p_{click} 为 Bob 探测到光子

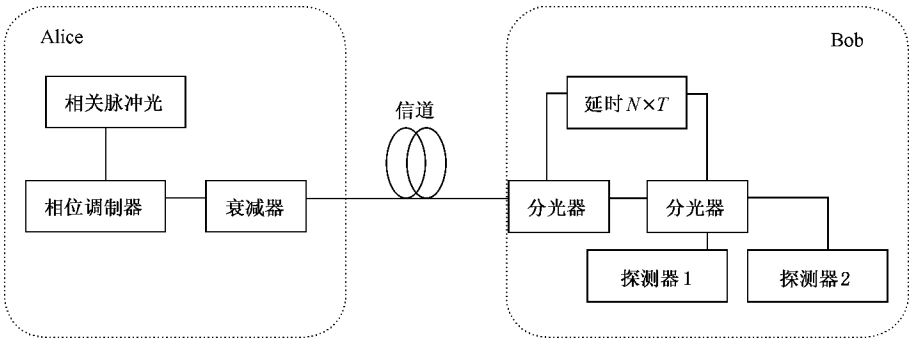

图 2 DPSK 协议组成图

的概率，

$$p_{\text{click}} = \mu\eta 10^{-(\alpha L + L_r)/10} + 2d,$$

其他参数与上文中的相同.

3. 结果与讨论

在 BB84 协议中，考虑分光攻击，在这种攻击中攻击者(Eve)可以在没有产生任何误码的情况下完全获取信息，这种攻击是一个限制 BB84 协议弱脉冲补偿的主要因素.在量子信道中安全通信速率以二次方的速度衰减，$10^{-\alpha L/10}$，这时误码率很小，速率随着光纤传输线性减小.在 BBM92 协议中没有分光攻击，对于小误码率时，与 BB84 协议相似，其通信速率和量子信道的传输线性减小.

在 DPSK 协议中，分光攻击时，Eve 用一个传输率为 η_{BS} 分光器来来获得多个脉冲的相关量子态的副本.当 Eve 用干涉仪选择测量一个和 Bob 无关的延迟时间 $M\tau$ 时得到的脉冲时，它的信息增益可作如下分析：Eve 和 Bob 在一个时隙内的测量单光子概率分别为 $\mu(1-\eta_{\text{BS}})$ 和 $\mu\eta_{\text{BS}}$，在一段时间内探测的概率为 $\mu^2\eta_{\text{BS}}(1-\eta_{\text{BS}})$.所以 Eve 在 Bob 在特定时间内探测到一个光子的比特值的概率可表示为 $\mu^2\eta_{\text{BS}}(1-\eta_{\text{BS}})/\mu\eta_{\text{BS}} = \mu(1-\eta_{\text{BS}})$.另一方面，Eve 随机选择的 M 和 Bob 的 N 匹配的概率为 $1/N$.如假设 Eve 没有一个有着有限的足够长的相关时间的量子记忆，这样，Eve 获得和 Bob 相关的比特信息的概率为 $\mu(1-\eta_{\text{BS}})/N$.如考虑 Eve 有量子记忆，此时 Eve 获得信息的概率增加到 $2\mu(1-\eta_{\text{BS}})$.

截断-重发攻击时，Eve 截断了相隔时间为 MT 的两个脉冲，然后让它们穿过一个干涉仪，干涉仪的延迟为 MT，测量差分相位，按照它的测量结果可得出 Bob 发送相应的相位信息.设在不确定的情况下或者真空条件的情况下，它发送的是真空态，而当它测量到单光子时它发送一个有正确相位差的光子插入两个脉冲中.此时，当 Bob 采用一个已知的延迟时，$N = M$，然后测量中心时隙，他没有探测到监听者，因为他得到了正确的回答.然而，如果以概率 $1-1/2N$ 他选择了另一种延迟，N 和 M 不等，或者测量的边时隙，这就会产生随机的，非相关的结果，这就会有概率 1/2 产生误码.因此，这种攻击产生误码率为 $\frac{1}{2}(1-1/2N)$.如果系统的误码率为 e，Eve 就对所有脉冲中的 $2e(1-1/2N)$ 进行攻击，就不会超过系统的误码率.则能够以概率 $1/2N$ 得到这些截断脉冲的信息.

在计算安全通信速率随传输距离变化时，将信道衰减在 1.55 μm 时定为 $\alpha = 0.2$ dB/km，附加的损耗 $L_r = 1$ dB.计算表明简单有效的 DPSK 协议能具有超过 200 km 的通信距离并且有较高的通信速率，为更好地改进光纤 QKD 系统性能提供参考.

[1] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[2] Miao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2126 (in Chinese) [苗二龙、莫小范、桂有珍、韩正甫、郭光灿 2004 物理学报 **53** 2126]

[3] Ma H Q, Li Y L, Zhao H, Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese) [马海强、李亚玲、赵　环、吴令安 2005 物理学报 **54** 5014]

[4] Bennett C H, Brassard G 1984 *Proc. IEEE Interna. Conf. Computers Systems and Signal Processing* (Bangalore, New York: IEEE)

[5] Diamanti E, Takesue H, Honjo T, Inoue K, Yamamoto Y 2004 *Phys. Rev.* A **72** 52311

[6] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

Analysis of differential-phase-shift keying protocol for a two-way quantum-key-distribution system *

Jiao Rong-Zhen† Feng Chen-Xu

(*Science School, Beijing University of Post and Telecommunication, Beijing* 100876, *China*)

(Received 23 April 2007; revised manuscript received 23 May 2007)

Abstract

The performance of a two-way quantum-key-distribution (QKD) system are analyzed using the differential-phase-shift keying (DPSK) protocol. The comparison is based on the secure communication rate as a function of distance for three QKD protocols: the Bennett-Brassard 1984, the Bennett-Brassard-Mermin 1992, and the coherent differential-phase-shift keying protocols. We discussed the security of DPSK protocol against any type of individual photon splitting attack and concluded that the simple and efficient DPSK protocol allows for more than 200 km of secure communication distance with high communication rates.

Keywords: differential-phase-shift keying protocol, quantum efficiency, communication rate

PACC: 0367, 4250

* Project supported by the National Natural Science Foundation of China (Grant No. 60054402).

† E-mail: jiao128@sohu.com