对相位重映射攻击的优化求解

韩保元[1] 孔祥进[2]

[1]中国卫星海上测控部远望六号船, 江苏 江阴 214431

[2]国防科学技术大学理学院, 湖南 长沙 410073

摘要 即插即用(plug-and-play)系统是一种稳定的双向系统,基于相位调制器的不完美性,可以对实际的即插即用系统进行有效的攻击,提出一种改进型的相位重映射攻击方法,从理论上推导出了相位重映射攻击所引起误码率的最小值,并考虑了通信成功率对实际攻击的影响。在这种攻击下,可获得较低的误码率和较高的通信成功率。

关键词 量子光学;相位重映射;误码率;成功率

中图分类号 O431.2; O432.2 **文献标识码** A

doi: 10.31788/AOS201535.0227001

Optimal Solution of Phase-Remapping Attack

Han Baoyuan[1] Kong Xiangjin[2]

[1]*Yuanwang Boat No.Six, China Satellite Maritime Tracking and Controlling Department, Jiangyin, Jiangsu* 214431, *China*

[2]*College of Science, National University of Defense Technology , Changsha, Hunan* 410073, *China*

Abstract The plug-and-play structure is bidirectional and stable system in theory. However, the practical system can be attacked effectively due to the imperfect phase modulator. The modified phase-remapping attack is demonstrated. The minimal value of the bit error rate (BER) is derived, which is caused by the modified phase-remapping attack. The effect of the success rate of communication to the practical system is also considered. Under this attack, the BER can be kept the minimum value and a much better success rate of communication can be achieved.

Key words quantum optics; phase remapping; bit error eate; success rate

OCIS codes 270.5585; 270.5565

1 引 言

量子信息的一个重要实际应用就是量子密钥分发[1-3](QKD)。经过二十几年的发展,QKD在理论和实验上都取得了很大的进展[4-6],并且已经逐步开始走向实用化,目前已经出现了一些商用化的产品,如瑞士Id Quantique公司的Clavis2系统和美国MagiQ公司的QPN5505系统。然而需要指出的是,虽然QKD的无条件安全性已经在理论上得到了证明,但是这些证明要么要求完美的系统设备,要么需要基于一些假设条件来限制窃听者的窃听策略或者窃听能力。在实际的情况下,实现QKD的物理设备总是存在着不同程度的非完美性,这些非完美性就会给系统带来一些安全性漏洞[7-9]。严格的讲,实际QKD系统中任何设备的非完美性都可能给系统带来不同程度的安全性隐患,而窃听者就可以利用这些非完美性来优化自己的攻击行为,从而最大化自己的信息[10-11]。比如理论上要求通信光源为单光子源,而目前的条件下并没有可以实用化的单光子源,所以实际中都是使用衰减后的相干光源来替代,针对这一缺陷,1999年,Dusek等[12]提出了分束攻击,2000年,Brassard等[13]提出光子数分流(PNS)攻击。理论上要求单光子探测器的效率为1,暗记数为0,死时间为0等,然而在实际的情况下,这些条件都无法得到满足。2006年,Makarov等[14]针对单光子探测器效率的不匹配提出了时间移动(time-shift)攻击。2009年,Makarov等[15]利用单光子探测器死时间这一漏洞,提出

收稿日期: 2014-07-29; **收到修改稿日期**: 2014-09-04

作者简介: 韩保元(1988—),男,硕士,助理工程师,主要从事通信方面的研究。E-mail: 814630287@qq.com

可以利用强光来控制探测器的响应，这就是所谓的致盲攻击(blinding attack)。特别一提的是，2010年他们在《自然·光子学》上发文指出，他们在瑞士Id Quantique公司和美国MigiQ公司的商用化QKD系统上实施了该攻击行为，窃取了全部的信息而没有被发现[16]。因此需要充分分析实际QKD系统中各种设备(特别是一些关键设备)的缺陷，寻找其中可能的安全性隐患，并在此基础上考虑可能的攻击方案以及反攻击策略，这对于促进QKD系统的实用化将具有十分重要的作用[17-18]。

即插即用(Plug-and-play)方案是由Muller等提出的第一个双向系统方案[19]，由于其具有良好的稳定性，发展十分迅速，在Id Quantique公司实现的商用化量子系统中采用的就是该方案。本文介绍了对即插即用系统的相位重映射攻击[20]，经过数学建模，第一次给出了仅在相位重映射攻击下系统误码率极小值的解析表达式，并优化了在此误码率下的通信成功率。

2 相位重映射攻击

2.1 即插即用原理

图1为最初提出的即插即用量子密钥分发系统的原理图[15]，Bob是密钥发送方，Alice是密钥接收方。Bob端首先发出一个激光脉冲，到达分束器C2，激光被分为P1和P2两部分。P1直接到达Alice端，P2中的一部分通过M2-M1延迟线后到达Alice端。在Alice端，经过分束器C3以后，通过调整时序，Alice将相位信息编码在P2上。随后，P1和P2被反射回Bob端。P1中的一部分经过M1-M2延迟线时，Bob端的相位调制器将相位信息编码在上面，这部分光和P2直接透射到达C2的光发生干涉，干涉结果有一部分可以被探测器D0探测到。探测器DA用来监视通过量子信道的光脉冲强度，使得光脉冲返回Bob端时衰减为平均每个光脉冲中有0.1个光子，此外，DA还可以用来监视是否有木马脉冲进入Alice端。图中laser为激光器；DA,D0为单光子探测器；PM为相位调制器；FR为法拉第镜；C1,C2,C3为分束器；M1,M2,M3为法拉第反射镜。

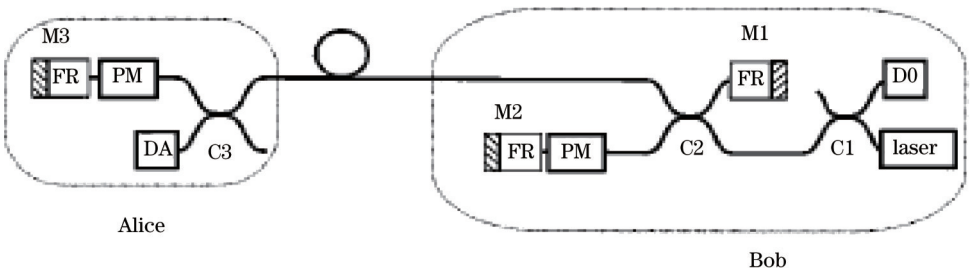

图1 即插即用量子密钥分发系统的原理图

Fig.1 Plug-and-play quantum key distribution system schematic

2.2 相位重映射攻击理论

在即插即用量子密钥分发系统中，信息编码在信号脉冲与参考脉冲的相对相位上。Alice处的相位调制器，只对信号脉冲进行调制，不对参考脉冲进行调制。不幸的是，在当前的量子密钥分发系统中，Alice不能监控两个脉冲的到达时间。相反，Alice只是用其中一个作为触发信号来确定Alice何时应该激活相位调制

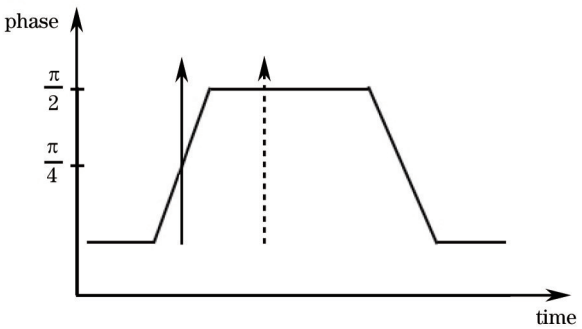

图2 Eve的相位调制器调制

Fig.2 Eve′s modulation of the phase modulator

器。在这种情况下，窃密者(Eve)可以改变信号脉冲，使其在相位调制器调制的上升或下降边缘到达相位调制器[16]，如图2所示(用于当前量子密钥分发系统中的基于波导的铌酸锂相位调制器的上升时间为0.1~1 ns)。

因此，信号脉冲和参考脉冲之间的相对相位会比它原来的更小。原则上，通过仔细控制时间偏移量，Eve可以把编码的相位从 $\left\{0,\frac{\pi}{2},\pi,\frac{3\pi}{2}\right\}$ 变为 $\{0,\sigma,2\sigma,3\sigma\}$，其中 σ 为相位值，$\sigma\in\left[0,\frac{\pi}{2}\right]$。这种控制方式主要针对相位调制器的调制电压随时间变化为线性关系。

2.3 寻找合适的相位重映射攻击手段

令 $\sigma=\frac{\pi}{2}+\varphi,\varphi\in\left[-\frac{\pi}{2},0\right]$，$\varphi$ 为相位值，则Alice发送的4个态为[16]

$$\left|\tilde{\phi}_k\right\rangle=\frac{1}{\sqrt{2}}\left[\exp\left(\mathrm{i}k\frac{\pi}{2}\right)\exp(\mathrm{i}\varphi)|1\rangle+|2\rangle\right],\ k=0,1,2,3, \tag{1}$$

式中i是虚数单位，$\left|\tilde{\phi}_k\right\rangle$ 为发送的量子态，k 为算子的测量结果。

2.2节已经描述了Eve改变实际量子密钥分发系统相对相位的可能性。需要指出的是Eve的这种能力是不是在任何方式下对Alice和Bob都是有害的，Eve可以使用这个能力在完美单光子源的某些情况下窃取Alice和Bob之间共享的密钥。相位重映射攻击就是针对这种实际情况提出的一种特定截取重发攻击，并对Eve为Alice的态所选择相位偏差 σ 进行了优化。

考虑Eve进行下面的截取重发攻击：Eve截获Alice发送的4个态，并且用一组半正定算子值测量(POVM)算子作用在上面。这一组POVM算子由5个分量组成，$\left\{\boldsymbol{M}_{\mathrm{vac}},\boldsymbol{M}_k:k=0,1,2,3\right\}$，根据POVM算子的完备性则有 $\boldsymbol{M}_{\mathrm{vac}}+\sum_{k=0}^{3}\boldsymbol{M}_k=\boldsymbol{I}$，其中 $\boldsymbol{I}$ 为单位算符。如果输出的和 $\boldsymbol{M}_{\mathrm{vac}}$ 一致，则Eve向Bob发送一个空态，但是如果输出的是 k，k 是算子测量的结果，则Eve向Bob发送标准BB84(一种量子密钥分发)态中的 $\left|\phi_k\right\rangle$ 态。

对于一个固定的相位偏角 σ，Eve应该找一组合适的POVM算子，使得误码率最低。在这种情况下，由于4个态不是线性独立的，明确地区别这4个态是不可能的。故需按照下面的方法找较低的误码率。首先考虑 $\boldsymbol{M}_0$，当 $\boldsymbol{M}_0$ 发生时，Eve向Bob发送 $\left|\phi_0\right\rangle$ 态。如果Alice发送的正好是 $\left|\tilde{\phi}_0\right\rangle$ 态，那么这次的截取重发就不会引进误码。但是，如果Alice实际发送的 $\left|\tilde{\phi}_2\right\rangle$ 态，且Bob用标准基 $\left\{|\phi_0\rangle,|\phi_2\rangle\right\}$ 进行测量(只考虑Bob和Alice采用相同基的情况)，那么Bob将会发现错误，误码率为1；另一方面，如果Alice实际发送的是 $\left|\tilde{\phi}_1\right\rangle$ 或者 $\left|\tilde{\phi}_3\right\rangle$ 态，Bob用标准基 $\left\{|\phi_1\rangle,|\phi_3\rangle\right\}$ 进行测量，那么得到的误码率为0.5。因此，在 $\boldsymbol{M}_0$ 情况下的误码率(没有归一化)为 $\frac{\left[\frac{1}{2}\mathrm{Tr}(\boldsymbol{M}_0\left|\tilde{\phi}_1\right\rangle\left\langle\tilde{\phi}_1\right|)+\mathrm{Tr}(\boldsymbol{M}_0\left|\tilde{\phi}_2\right\rangle\left\langle\tilde{\phi}_2\right|)+\frac{1}{2}\mathrm{Tr}(\boldsymbol{M}_0\left|\tilde{\phi}_3\right\rangle\left\langle\tilde{\phi}_3\right|)\right]}{4}$，其中Tr为求矩阵的迹。当 $\boldsymbol{M}_i(i=0,1,2,3)$ 都没有发生时，Eve向Bob发送一个空态，这种情况意味着这一比特的信息传输是失败的。为了计算最后的误码率，需要把对应于不同 $\boldsymbol{M}_i$ 的没有归一化的误码率相加，归一化相加的和即Eve攻击引起的误码率，为

$$R_{\mathrm{BE}}=\frac{\sum_{i=0}^{3}\mathrm{Tr}(\boldsymbol{M}_i\boldsymbol{L}_i)}{\sum_{i=0}^{3}\mathrm{Tr}(\boldsymbol{M}_i\boldsymbol{\rho})}, \tag{2}$$

其中

$$\boldsymbol{L}_0=\frac{1}{2}\boldsymbol{\rho}_0+\boldsymbol{\rho}_2+\frac{1}{2}\boldsymbol{\rho}_3, \tag{3}$$

$$\boldsymbol{L}_1=\frac{1}{2}\boldsymbol{\rho}_0+\frac{1}{2}\boldsymbol{\rho}_2+\boldsymbol{\rho}_3, \tag{4}$$

$$\boldsymbol{L}_2=\boldsymbol{\rho}_0+\frac{1}{2}\boldsymbol{\rho}_1+\frac{1}{2}\boldsymbol{\rho}_3, \tag{5}$$

$$\boldsymbol{L}_3=\frac{1}{2}\boldsymbol{\rho}_0+\boldsymbol{\rho}_1+\frac{1}{2}\boldsymbol{\rho}_2, \tag{6}$$

$$\boldsymbol{\rho}=\boldsymbol{\rho}_0+\boldsymbol{\rho}_1+\boldsymbol{\rho}_2+\boldsymbol{\rho}_3, \tag{7}$$

$$\boldsymbol{\rho}_i=|\phi_i\rangle\langle\phi_i|. \tag{8}$$

在 $\boldsymbol{M}_i$ 为半正定矩阵且 $\boldsymbol{I}-\sum_{i=0}^{3}\boldsymbol{M}_i$ 为半正定矩阵的约束条件下，可以计算误码率 R_{BE} 的最小值。事实上，不用考虑为半正定矩阵这个约束条件，因为一旦找到合适的 $\boldsymbol{M}_i$，然后把 $\boldsymbol{M}_i$ 按相同的比例缩小，就会满足此约束条件，易知上述操作不会影响误码率 R_{BE} 的值。

3 相位重映射攻击最优化

根据以上分析可知，寻找合适的相位重映射攻击手段即为求解一个最优化的数学问题，其中目标函数为 R_{BE} 的最小值，约束条件是 $\boldsymbol{M}_i$ 和 $\boldsymbol{I}-\sum_{i=0}^{3}\boldsymbol{M}_i$ 同时为半正定矩阵。

不妨令 $\boldsymbol{M}_i=\begin{pmatrix}a_i & c_i+id_i\\ c_i-id_i & b_i\end{pmatrix}$，则 $\boldsymbol{M}_i$ 半正定即有 $a_i\geqslant 0;b_i\geqslant 0;c_i^2+d_i^2\leqslant a_ib_i$。

把 a_i,b_i,c_i,d_i 代入误码率的表达式，化简后得到

$$R_{\mathrm{BE}}=\frac{1}{2}-\frac{\cos\varphi}{2}\frac{\cos\varphi(c_0-c_2)+\sin\varphi(d_0-d_2)+\sin 2\varphi(c_3-c_1)+\cos 2\varphi(d_1-d_3)}{2\mu+\lambda_1\left(\sum_{i=0}^{3}c_i\right)+\lambda_2\left(\sum_{i=0}^{3}d_i\right)}, \tag{9}$$

式中 $\lambda_1=\sin 2\varphi+\sin\varphi\cos 2\varphi,\lambda_2=\sin 2\varphi\sin\varphi-\sin\varphi\cos\varphi,\mu=\sum_{i=0}^{3}a_i+\sum_{i=0}^{3}b_i$。

可以采用极坐标变换对(9)式进一步化简，有

$$R_{\mathrm{BE}}=\frac{1}{2}-\frac{\cos\varphi}{2}\frac{r_0\cos(\theta_0-\varphi)+r_2\cos(\theta_2-\varphi)+r_3\cos(\theta_3-2\varphi)+r_1\cos(\theta_1-2\varphi)}{2\mu+\lambda_1(r_0\cos\theta_0-r_1\sin\theta_1-r_2\cos\theta_2+r_3\sin\theta_3)+\lambda_2(r_0\sin\theta_0-r_2\sin\theta_2+r_1\cos\theta_1-r_3\cos\theta_3)}, \tag{10}$$

再令 $\theta_0'=\theta_0-\varphi,\theta_2'=\theta_2-\varphi,\theta_1'=-\theta_1+3\varphi,\theta_3'=-\theta_3+3\varphi$，代入(10)式可得

$$R_{\mathrm{BE}}=\frac{1}{2}-\frac{\cos\varphi}{2}\frac{\sum_{j=0}^{3}r_i\cos\theta_i'}{2\mu+\sin\varphi(\omega_0r_0-\omega_2r_2+\omega_3r_3-\omega_1r_1)}, \tag{11}$$

式中有 $\omega_i=\cos(\theta_i'-\varphi)-\sin\theta_i'$。

值得注意的是，在 $\mu=\left(\sum_{i=0}^{3}a_i+\sum_{i=0}^{3}b_i\right)$ 中，a_i,b_i 是对称的，也就是说 a_i,b_i 在(11)式中对称，那么关于 a_i,b_i 求 R_{BE} 偏导数，其函数形式是相同的，因此对(11)式取极值时，必定有 $a_i=b_i$。

由 $a_i\geqslant 0;b_i\geqslant 0;c_i^2+d_i^2\leqslant a_ib_i$ 知，$r_i^2\leqslant a_ib_i$，即得 $r_i\leqslant a_i$。在(11)式中，要求 R_{BE} 最小，则 $\mu=\left(\sum_{i=0}^{3}a_i+\sum_{i=0}^{3}b_i\right)$ 越小越好，即 a_i 越小越好。故而取 $a_i=r_i$ 最佳。

观察(11)式，可以发现 $\theta_0',\theta_2',\theta_1',\theta_3'$ 有一定的对称性，但不是完全的对称，可以尝试着求解(11)式的最小值，不妨令 $\theta_0'=\theta_2'=\theta_1'=\theta_3'=\theta$，代入(11)式得

$$R_{\mathrm{BE}}=\frac{1}{2}-\frac{\cos\varphi}{2}\frac{\cos\theta\sum_{j=0}^{3}r_i}{2\sum_{i=0}^{3}r_i+\sin\varphi[\cos(\theta-\varphi)-\sin\theta](r_0-r_2+r_3-r_1)}, \tag{12}$$

欲求 R_{BE} 的最小值，等价于求

$$\max\left\{\frac{\cos\varphi}{2}\frac{\cos\theta\sum_{j=0}^{3}r_i}{2\sum_{i=0}^{3}r_i+\sin\varphi[\cos(\theta-\varphi)-\sin\theta](r_0-r_2+r_3-r_1)}\right\},$$

即求

$$\min\left\{\frac{2\sum_{i=0}^{3}r_i+\sin\varphi[\cos(\theta-\varphi)-\sin\theta](r_0-r_2+r_3-r_1)}{\cos\theta\sum_{j=0}^{3}r_i}\right\},$$

经计算得，$\sin\varphi[\cos(\theta-\varphi)-\sin\theta]$ 为负数，则要求 $(r_0-r_2+r_3-r_1)$ 越大越好。很明显该式取极小值时，必有 $r_1=r_2=0$，则代入(12)式有

$$R_{\mathrm{BE}}=\frac{1}{2}-\frac{\cos\varphi}{2}\frac{\cos\theta}{2+\sin\varphi[\cos(\theta-\varphi)-\sin\theta]}. \tag{13}$$

由 $\frac{\partial R_{\mathrm{BE}}}{\partial\theta}=0$，推得 $\theta=\arcsin\frac{\sin\varphi-\sin^2\varphi}{2}$。通过上面的分析，得到了一组解，解的形式为

$$\left\{r_i=a_i=b_i,r_1=r_2=0,\theta_1=\varphi+\arcsin\frac{\sin\varphi-\sin^2\varphi}{2},\theta_3=2\varphi+\arcsin\frac{\sin\varphi-\sin^2\varphi}{2}\right\}.$$

为了验证这组解是不是一组极小值解，分别算出了目标函数 R_{BE} 关于每个变量在该组解处的偏导数值，发现所有的偏导数值都为0，且在该处的Hesse矩阵为正定矩阵，所以得出的解是一组极小值点。

图3是最小误码率随相位偏角 φ 变化的曲线图，从图中可以看出最小误码率随着 φ 的增大而增大，在 $\varphi=-\frac{\pi}{2}$ 即 $\sigma=0$ 处，有一个奇点。可以从物理上对这个奇点的存在进行解释：当 $\sigma=0$ 时，Alice处的相位调制器没有对态进行相位调制，Alice将会向Bob发送相同的态，如果Eve采取文中所说的攻击，那么为了寻求误码率的最低，Eve会对态进行拦截，然后给Bob发送一个空态，此时的误码率最小为0，但同时通信的成功率为0，相当于Alice和Bob之间无法进行通信，这种情况显然是不行的，对应于图中的奇点。

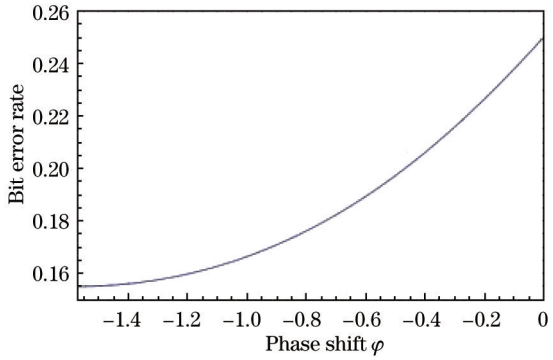

图3 误码率随偏角的变化

Fig.3 Bit error rate changing with phase shift

可以算出当 $\varphi\to-\frac{\pi^+}{2}$ 时，R_{BE} 的极值结果如下：

$$\lim_{\varphi\to-\frac{\pi^+}{2}}R_{\mathrm{BE}}=\lim_{\varphi\to-\frac{\pi^+}{2}}\left\{\frac{1}{2}-\frac{\cos\varphi}{2}\frac{\cos\theta}{2+\sin\varphi[\cos(\theta-\varphi)-\sin\theta]}\right\}, \tag{14}$$

式中 $\theta=\arcsin\frac{\sin\varphi-\sin^2\varphi}{2}$，则具体计算得到

$$\lim_{\varphi\to-\frac{\pi^+}{2}}R_{\mathrm{BE}}=\lim_{\varphi\to-\frac{\pi^+}{2}}\left\{\frac{1}{2}-\frac{\cos\varphi}{2}\frac{\cos\theta}{2+\sin\varphi[\cos(\theta-\varphi)-\sin\theta]}\right\}=\frac{3-\sqrt{6}}{6-\sqrt{6}}\approx15.51\%, \tag{15}$$

(15)式表明单采用文中的方法对QKD系统进行攻击，误码率不会低于15.51%。这与文献[16]中给出的结果相一致。

在上述推导过程中，并没有对 a_0,a_3 即 r_0,r_3 进行具体的限制，这就表明只要 r_0,r_3 满足约束条件，它们具体的值不会影响当 φ 一定时，系统的最低误码率。

不过虽然 r_0,r_3 的具体值虽然不会影响当 φ 一定时系统的最低误码率，但会影响此时系统通信的成功率。

定义系统通信的成功率 P_{succ} 为

$$P_{\mathrm{succ}}=\frac{1}{4}\sum_{i=0}^{3}\mathrm{Tr}(\boldsymbol{M}_i\boldsymbol{\rho}),\tag{16}$$

代入 $\boldsymbol{M}_i$，$\boldsymbol{\rho}$ 的表达式有

$$P_{\mathrm{succ}}=\frac{1}{2}\{2+\sin\varphi[\cos(\theta-\varphi)-\sin\theta]\}(r_0+r_3),\tag{17}$$

式中 $r_0+r_3\leqslant 1$；$1+2r_0r_3[1+\sin(2\theta-\varphi)]-2(r_0+r_3)\geqslant 0$。

根据约束条件，求得

$$P_{\mathrm{succ}}^{\max}=\frac{2-\sqrt{4-2[1+\sin(2\theta-\varphi)]}}{2[1+\sin(2\theta-\varphi)]}\{2+\sin\varphi[\cos(\theta-\varphi)-\sin\theta]\}.\tag{16}$$

图4是 $P_{\mathrm{succ}}^{\max}$ 随相位偏角 φ 变化的曲线图，从图中可以看出在误码率最低的前提下，随着偏角的增大，最大通信成功率逐渐增大。本文攻击策略就是保证误码率最低，尽量增大通信成功率，所以对于确定的 φ 值，Eve所采取的一组POVM算子为

$$\boldsymbol{M}_0=r_0\begin{bmatrix}1 & \exp[\mathrm{i}(\theta+\varphi)]\\ \exp[-\mathrm{i}(\theta+\varphi)] & 1\end{bmatrix},\ \boldsymbol{M}_1=\boldsymbol{M}_2=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix},$$

$$\boldsymbol{M}_3=r_3\begin{bmatrix}1 & \exp[-\mathrm{i}(-\theta+3\varphi)]\\ \exp[-\mathrm{i}(-\theta+3\varphi)] & 1\end{bmatrix},\ \boldsymbol{M}_{\mathrm{vac}}=\boldsymbol{I}-\sum_{i=0}^{3}\boldsymbol{M}_i.$$

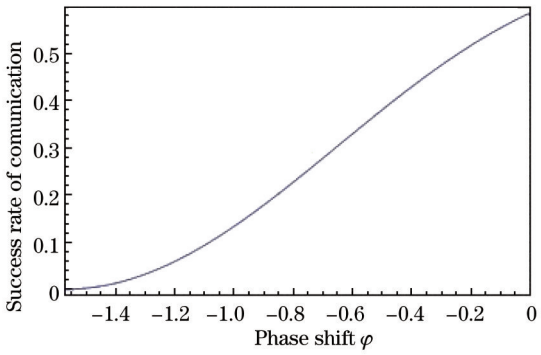

图4 最大通信成功率与偏角的关系图

Fig.4 Best success rate of communication changing with phase shift

在这种攻击下，通信误码率和成功率分别为

$$R_{\mathrm{BE}}=\frac{1}{2}-\frac{\cos\varphi}{2}\frac{\cos\theta}{2+\sin\varphi[\cos(\theta-\varphi)-\sin\theta]},\quad P_{\mathrm{succ}}^{\max}=\frac{2-\sqrt{4-2[1+\sin(2\theta-\varphi)]}}{2[1+\sin(2\theta-\varphi)]}\{2+\sin\varphi[\cos(\theta-\varphi)-\sin\theta]\},$$

式中 $r_0=r_3=\dfrac{2-\sqrt{4-2[1+\sin(2\theta-\varphi)]}}{2[1+\sin(2\theta-\varphi)]}$，$\theta=\arcsin\dfrac{\sin\varphi-\sin 2\varphi}{2}$。

以上提出的攻击方法的成功率要远远优于文献[16]中的成功率，从上面的结论中可以看出随着 σ 的减小，相位重映射攻击所引起的系统最低误码率会降低，但通信的成功率也会随之减小，换句话说，可认为是通过牺牲系统的通信成功率来降低系统的误码率。在实际系统中，系统的通信成功率是一定的，在该成功率下相位重映射所带来的最小误码率也是确定的，在误码率一定的情况下优化了成功率，其实就是在成功率一定的情况下降低了误码率，这将会对实验起着指导意义。

4 结 论

在文献[16]的基础上针对相位重映射攻击进行了解析求解，给出了误码率极小值的解析表达式，并在误码率取极小值的时候优化了系统的通信成功率，给出了最佳的攻击方法。重点考虑了相位重映射攻击所带来的误码率在理论上能达到的最小值，理论推导出了该最小值，证明了任何一种相位重映射攻击所引起的误码率

都不会小于该最小值(15.51%)。本文的攻击方法与文献[16]中的方法相比,在误码率相同的情况下,提高了系统的通信成功率。在实际的实验系统中,系统的通信成功率是给定的,在这个约束条件下,采用本文中的攻击方法所带来的误码率会低于文献[16]的攻击方法,这对实际的实验系统有着重要的意义。

参 考 文 献

1 Shen Zeyuan, Fang Jian, He Guangqiang, *et al*.. Synchronous scheme and experimental realization in continuous variable quautum key distribution system [J]. Chinese J Lasers, 2013, 40(3): 0305004.
申泽源, 房 坚, 何广强, 等. 连续变量量子密钥分发系统中同步方案及实验实现[J]. 中国激光, 2013, 40(3): 0305004.

2 Haibin Du, Yan Liang, Shengxiang Zhang, *et al*.. Practical high-speed light source for decoy-state quantum key distribution [J]. Chin Opt Lett, 2014, 12(7): 072702.

3 Wang Yunyan, Guo Dabo, Zhang Yanhuang, *et al*.. Algorithm of multidimensional reconciliation for continuous-variable quantum key distribution [J]. Acta Optica Sinica, 2014, 34(8): 0827002.
王云艳, 郭大波, 张彦煌, 等. 连续变量量子密钥分发多维数据协调算法[J]. 光学学报, 2014, 34(8): 0827002.

4 Michel Boyer, Ran Gelles, Tal Mor. Attacks on fixed-apparatus quantum-key-distribution schemes [J]. Phys Rev A, 2014, 90(1): 012329.

5 W T Buttler, R J Hughes, S K Lamoreaux, *et al*.. Daylight quantum key distribution over 1.6 km [J]. Phys Rev Lett, 2000, 84(24): 5652-5655.

6 C Kuresiefer, P Zarda, M Halder, *et al*.. A step towards global key distribution [J]. Nature, 2002, 419: 450.

7 Huang Jianhua, Wu Guang, Zeng Heping. Study of 1.5 GHz harmonics ultrashort pulse gated InGaAs/InP avalanche photodiode single-photon detection [J]. Acta Optica Sinica, 2014, 34(2): 0204001.
黄建华, 吴 光, 曾和平. 基于1.5 GHz多次谐波超短脉冲门控InGaAs/InP雪崩光电二极管的近红外单光子探测技术研究[J]. 光学学报, 2014, 34(2): 0204001.

8 Guo Xueshi, Gao Kang, Liu Nannan, *et al*.. Differential detection system for measuring the quantum noise of pulsed light [J]. Acta Optica Sinica, 2013, 33(9): 0927002.
郭学石, 高 亢, 刘楠楠, 等. 适用于测量脉冲光量子噪声的差分探测系统[J]. 光学学报, 2013, 33(9): 0927002.

9 Feng Tang, Bing Zhu. Scintillation discriminator improves free-space quantum key distribution [J]. Chin Opt Lett, 2013, 11(9): 090101.

10 A Rubenok, J A Slater, P Chan, *et al*.. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks [J]. Phys Rev Lett, 2013, 111(13): 130501.

11 Normand J Beaudry, Marco Lucamarini, Stefano Mancini, et al.. Security of two-way quantum key distribution [J]. Phys Rev A, 2013, 88(6): 062302.

12 Miloslav Dusek, Ondrej Haderka, Martin Hendrych, et al.. Quantum identification system [J]. Phys Rev A, 1999, 60(1): 149-156.

13 Gilles Brassard, Norbert Lütkenhaus, Tal Mor, et al.. Limitations on practical quantum cryptography [J]. Phys Rev Lett, 2000, 85(6): 1330-1333.

14 Vadim Makarov, Andrey Anisimov, Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems [J]. Phys Rev A , 2006, 74(2): 022313.

15 Vadim Makarov. Controlling passively quenched single photon detectors by bright light [J]. New J Phys, 2009, 11(6): 065003.

16 L Lydersen, C Wiechers, C Wittmann, et al.. Hacking commercial quantum cryptography systems by tailored bright illumination [J]. Nat Photonics , 2010, 4(10): 686-689.

17 Francesco Buscemi, Michael J W Hall, Masanao Ozawa, *et al*.. Noise and disturbance in quantum measurements: An information-theoretic approach [J]. Phys Rev Lett, 2014, 112(5): 050401.

18 Fabio Grazioso, Frédéric Grosshans. Quantum-key-distribution protocols without sifting that are resistant to photon-number-splitting attacks [J]. Phys Rev A, 2013, 88(5): 052302.

19 A Muller, T Herzog, B Huttner, *et al*.. "Plug and play" systems for quantum cryptography [J]. Appl Phys Lett, 1997, 70(7): 793-795.

20 Chi-Hang Fred Fung, Bing Qi, Kiyoshi Tamaki, *et al*.. Phase-remapping attack in practical quantum-key-distribution systems [J]. Phys Rev A, 2007, 75(3): 032314.

栏目编辑: 王晓琰