相位漂移对相位编码QKD系统及截获-重发攻击的影响研究

焦海松 王衍波 何 敏 朱 勇 张志永

中国人民解放军理工大学通信工程学院, 江苏 南京 210007

摘要 针对相位编码量子密钥分发(QKD)系统中存在的相位漂移和截获-重发攻击,分析了双马赫-曾德尔干涉仪QKD系统,给出了探测器的输入信号模型,计算了系统量子误码率及窃听信息量,并为提高密钥生成率提供了一种可能的方法。研究表明,相位漂移会使系统误码率增加,稳定性降低;相比理想的截获-重发攻击,窃听信息量有所下降,因此密性放大过程对窃听信息的估计值可以相对减小,最终密钥生成率得以提高。在不考虑传输光纤中的相位相对漂移时,误码率随相位漂移角度呈余弦变化,全部截获-重发攻击时的变化周期是无窃听时的一半,变化频率更加剧烈。55%部分窃听时,若合法通信者选择误码阈值为15%,窃听者可获得25.5%的信息量且不被发现。

关键词 量子光学;量子密钥分发;双马赫-曾德尔干涉仪;相位漂移;量子误码率;窃听信息量

中图分类号 TN918.1 **文献标识码** A

doi: 10.3788/LOP52.042703

Research about Effect of Phase Drift on Phase-Coding QKD System and Intercept-Resend Attack

Jiao Haisong Wang Yanbo He Min Zhu Yong Zhang Zhiyong

Institute of Communications Engineering,PLA University of Science and Technology, Nanjing, Jiangsu 210007, *China*

Abstract In consideration of phase drift and intercept-resend (I-R) attack, the quantum key distribution (QKD) system based on double Mach-Zehnder interferometers is analyzed, the model of detectors′ input signal is built, and the formulas are presented to describe the relationship between the phase drift angle and quantum bit error rate (QBER), as well as the drift angle and eavesdropping information. Meanwhile, a possible method to increase the key generation rate is proposed. Analysis shows that phase drift causes extra errors and damages the system stability. Compared with I-R attack under ideal conditions, eavesdropping information declines, thus the eavesdropping information estimated by privacy amplification could decrease and the final key generation rate would increase. Regardless of the relative phase drift in transmission fiber, QBER varies with phase drift as cosine function, whose period decreases by half under total I-R attack, meaning more sensitive to phase drift. When eavesdropper chooses to attack 55% of all keys, she can gain 25.5% information undiscovered.

Key words quantum optics; quantum key distribution; double Mach-Zehnder interferometers; phase drift; quantum bit error rate; amount of eavesdropping information

OCIS codes 270.5568; 270.5565; 270.5585; 270.2500

1 引 言

量子密钥分发(QKD)因其理论上的无条件安全性[1]倍受人们关注,已成为量子信息领域特别有现实意义的研究方向[2-6]。而实际的QKD系统很难满足理想条件的理论模型假设,为保证实际QKD系统的安全性,必须以牺牲通信距离和降低密钥生成率为代价[7-8]。其安全性证明将所有噪声视为由窃听引起的,因此在密

收稿日期: 2014-12-26; **收到修改稿日期**: 2014-12-29; **网络出版日期**: 2015-03-03

基金项目: 国家自然科学基金(11404407)

作者简介: 焦海松(1990—),男,硕士研究生,主要从事量子通信与信息安全方面的研究。E-mail: jiaohaisong_1990@163.com

导师简介: 王衍波(1961—),男,硕士,教授,主要从事量子通信与信息安全方面的研究。E-mail: foliation@163.com (通信联系人)

性放大环节需舍弃一定数量的生密钥位,导致密钥生成率下降。由于器件、环境的不理想因素的影响,实际QKD系统中存在的相位漂移、偏振模色散等,都会引起量子态的变化,成为系统的噪声。定量地分析某种噪声对QKD及窃听的影响,可以为密性放大环节对窃听信息的估计提供参考,相对地减少牺牲的生密钥位,提高密钥生成效率。

相位编码在光纤中抗干扰能力较强,因此在实际光纤QKD系统中通常采用基于相位编码的量子密钥分发(PC-QKD)方案[9~12]。相位编码方案将信息编码于光子的相位上,但是相位不能通过探测器直接测得,解码一般通过干涉的方法来实现。常用的干涉装置有马赫-曾德尔(M-Z)环[9,12]、法拉第-迈克耳孙环[10]和Sagnac环[11]等,其中基于双不等臂马赫-曾德尔(M-Z)干涉仪的QKD系统广泛应用于远距离通信系统中[12]。而相位、偏振等量子态的漂移在双M-Z干涉仪QKD系统中依然存在,且对系统性能具有极大影响[13]。目前针对PC-QKD系统的攻击方式研究[14-16]大多没有考虑量子态的漂移问题。本文分析了相位漂移对双M-Z干涉仪PC-QKD系统以及针对该系统的截获-重发攻击(I-R攻击)的影响,并对相位漂移与I-R攻击同时存在的双M-Z干涉仪PC-QKD系统进行了研究。

2 基于双M-Z干涉仪相位编码系统分析

双M-Z干涉仪相位编码系统结构如图1所示。

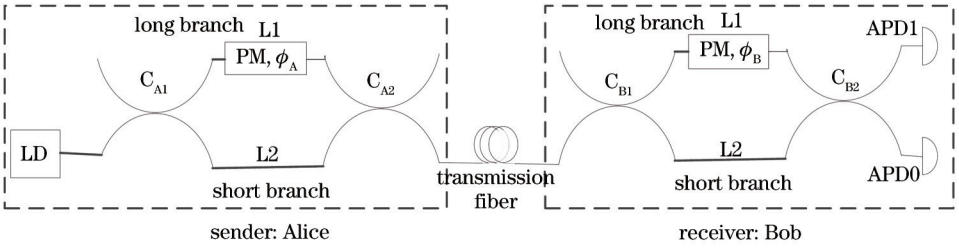

图1 双M-Z干涉仪相位编码系统结构示意图

Fig.1 PC-QKD system based on double Mach-Zehnder interferometers

发送端Alice与接收端Bob使用两个完全相同的M-Z干涉仪,干涉仪由两个3dB耦合器及产生相位差的不等臂波导组成。其中耦合器的传输矩阵[19]为 $M_{\text{coupler}}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & \mathrm{j}\\ \mathrm{j} & 1\end{pmatrix}$。假设长臂相位调制器PM产生相移 $\Delta\phi$,相应的传输矩阵为 $M_{\Delta\phi}=\begin{bmatrix}\exp[\mathrm{j}(\Delta\phi+kl_1)] & 0\\ 0 & \exp(\mathrm{j}kl_2)\end{bmatrix}$,则M-Z干涉仪的传输矩阵为

$$M=M_{\text{coupler}}M_{\Delta\phi}M_{\text{coupler}}=\frac{1}{2}\begin{bmatrix}\exp[\mathrm{j}(\Delta\phi+kl_1)]-\exp(\mathrm{j}kl_2) & \mathrm{j}\{\exp[\mathrm{j}(\Delta\phi+kl_1)]+\exp(\mathrm{j}kl_2)\}\\ j\{\exp[\mathrm{j}(\Delta\phi+kl_1)]+\exp(\mathrm{j}kl_2)\} & \exp(\mathrm{j}kl_2)-\exp[\mathrm{j}(\Delta\phi+kl_1)]\end{bmatrix}. \tag{1}$$

Alice、Bob的干涉仪传输矩阵分别记为 M_A、M_B,分别调相 ϕ_A、ϕ_B,假设光源产生的脉冲为 $E=A\exp(\mathrm{j}\phi_0)$,那么Alice端的输入为 $\begin{pmatrix}0\\E\end{pmatrix}$,输出为 $M_A\begin{pmatrix}0\\E\end{pmatrix}=\frac{1}{2}\begin{bmatrix}\mathrm{j}\{\exp[\mathrm{j}(\phi_A+kl_1)]+\exp(\mathrm{j}kl_2)\}E\\ E\exp(\mathrm{j}kl_2)-E\exp[\mathrm{j}(\phi_A+kl_1)]\end{bmatrix}$。

耦合器 C_{A2} 的输出只有下支路进入传输光纤,因此有一半的能量损失。由于干涉仪长短臂传输距离不同,输出将是两个前后相继的脉冲。不考虑传输光纤中增加的相位,令 $\phi_0=0$,则经过Bob的干涉仪后输出为

$$M_B\begin{bmatrix}0\\ \frac{1}{2}E\exp(\mathrm{j}kl_2)-\frac{1}{2}E\exp[\mathrm{j}(\phi_A+kl_1)]\end{bmatrix}=\frac{1}{4}\begin{bmatrix}\mathrm{j}A\exp(2\mathrm{j}kl_2)\\ A\exp(2\mathrm{j}kl_2)\end{bmatrix}+\frac{1}{4}\begin{bmatrix}\mathrm{j}A\{\exp[\mathrm{j}(\phi_B+kl_1+kl_2)]-\exp[\mathrm{j}(\phi_A+kl_1+kl_2)]\}\\ -A\{\exp[\mathrm{j}(\phi_B+kl_1+kl_2)]+\exp[\mathrm{j}(\phi_A+kl_1+kl_2)]\}\end{bmatrix}+$$
$$\frac{1}{4}\begin{bmatrix}-\mathrm{j}A\exp[\mathrm{j}(\phi_A+\phi_B+2kl_1)]\\ A\exp[\mathrm{j}(\phi_A+\phi_B+2kl_1)]\end{bmatrix}. \tag{2}$$

可见不同路径脉冲经过的路程不同,在 C_{B2} 输出端会有三个前后相继的脉冲到达,只有中间时刻是两个路径的脉冲同时到达,发生干涉。考虑 C_{B2} 下支路的输出,设相干脉冲 $E_1=\frac{1}{4}A\exp[\mathrm{j}(\phi_B+kl_1+kl_2)]$,

$E_2=\frac{1}{4}A\exp[\mathrm{j}(\phi_A+kl_1+kl_2)]$，则到达探测器APD0的信号强度为

$$I_0=\left|E_1+E_2\right|^2=\frac{1}{4}A^2\cos^2\left(\frac{\phi_A-\phi_B}{2}\right),\tag{3}$$

同理可得，

$$I_1=\frac{1}{4}A^2\sin^2\left(\frac{\phi_A-\phi_B}{2}\right).\tag{4}$$

双M-Z相位编码系统BB84协议[2]实现：Alice随机选择基组$\{0,\pi\}$或$\left\{\frac{\pi}{2},\frac{3\pi}{2}\right\}$调制$\phi_A$，其中$\phi_A=0$或$\frac{\pi}{2}$代表码值0，$\phi_A=\pi$或$\frac{3\pi}{2}$代表码值1；Bob随机调制$\phi_B=0$或$\frac{\pi}{2}$。当AB选择的基组一致时，$\phi_A-\phi_B=0$，$I_0=\frac{1}{4}A^2, I_1=0$，信号全部进入APD0，双方共享比特0；$\phi_A-\phi_B=\pi, I_0=0, I_1=\frac{1}{4}A^2$，信号全部进入APD1，双方共享比特1。当AB选择的基组不同时$\phi_A-\phi_B=\pm\frac{\pi}{2}$，响应不确定。双方通过对比基组，保留相同基对应的比特，舍弃不同基对应的比特。最后进行窃听检测、数据协调和密性放大。

3 相位漂移对双M-Z干涉仪系统误码率与互信息量的影响

在理想情况下相位编码BB84协议是绝对安全的，但实际系统环境并不完美，比如温度变化会导致光纤的热胀冷缩和折射率的变化，环境中的应力变化、震动也会造成光纤长度和折射率的变化，两端干涉系统也很难做到完全对称，这些都会导致脉冲的实际光程发生改变，使得干涉脉冲的相位产生漂移，即使双方的基组是匹配的，接收方也不一定能正确解码。

假设从Alice到Bob的相位漂移为φ_{AB}，调制相位差$\phi_A-\phi_B$记为$\Delta\phi_{AB}$，则由(3)式可得存在漂移时，$I_0=\frac{1}{4}A^2\cos^2\left(\frac{\Delta\phi_{AB}+\varphi_{AB}}{2}\right)$。对比基组之后$\Delta\phi_{AB}=0$或$\pi$，若认为相位漂移$\varphi_{AB}\leqslant\frac{\pi}{2}$，则$I_{0,\max}=\frac{1}{4}A^2\cos^2\frac{\varphi_{AB}}{2}$，$I_{0,\min}=\frac{1}{4}A^2\sin^2\frac{\varphi_{AB}}{2}$，干涉条纹对比度[17]为

$$V=\frac{I_{\max}-I_{\min}}{I_{\max}+I_{\min}}=\cos\varphi_{AB},\tag{5}$$

可以证明对于I_1对比度结果是一样的，这里忽略探测器暗计数，只考虑探测器的效率以及干涉的结果，则仅由于相位漂移造成的量子误码率[17](QBER)为

$$R_{QBE}=R_{QBE,opt}=\frac{1-V}{2}=\sin^2\frac{\varphi_{AB}}{2}.\tag{6}$$

误码率是接收方测量值与发送方值不同的概率，即$P\left(b_i|a_j\right)\left(i\neq j;i,j\in\{0,1\}\right)$，其中$a_j$、$b_i$分别代表Alice发送值为$j$、Bob接收为$i$，则传递概率可表示为

$$P\left(b_i|a_j\right)=\begin{cases}\frac{1-V}{2}, & i\neq j\\ \frac{1+V}{2}, & i=j\end{cases},\tag{7}$$

此时符合二元对称信道模型[18]，Alice与Bob的互信息下降为

$$I(\mathrm{A},\mathrm{B})=1-H\left(R_{QBE}\right)=1-H\left(\sin^2\frac{\varphi_{AB}}{2}\right),\tag{8}$$

其中$H\left(R_{QBE}\right)$是以R_{QBE}为参量的二元熵。

4 存在相位漂移时I-R攻击对PC-QKD系统的影响

在理想情况下，在最简单的I-R攻击中窃听者Eve获得的信息量为$I(\mathrm{A},\mathrm{E})=0.5$，窃听带来的$R_{QBE}=0.25$，$I(\mathrm{A},\mathrm{B})=0.5$，而存在相位漂移时，Eve的截获-重发带来的影响会有所不同。

4.1 存在相位漂移时Eve的窃听信息量与窃听效率

窃听者Eve随机选择测量基，选对或选错基的概率各$\frac{1}{2}$，由于测量塌缩的原因，不可避免地会改变量子态。假设从Alice到Eve的相位漂移是φ_{AE}，对于Eve选对基的部分，测量可能出现的结果及概率与Bob类似，则根据(5)式可得对比度$V=\cos\varphi_{AE}$。然后由(7)式可得AE间的状态传递概率：

$$P\left(\left|e\right\rangle=\left|i\right\rangle\middle\|a\right\rangle=\left|j\right\rangle\right)=\frac{1}{2}\begin{cases}\sin^2\dfrac{\varphi_{AE}}{2}, & i\neq j\\ \cos^2\dfrac{\varphi_{AE}}{2}, & i=j\end{cases}, \tag{9}$$

其中$\frac{1}{2}$是Eve选对基的概率，i、$j\in\{0,\ \pi\}$或$\left\{\frac{\pi}{2},\frac{3\pi}{2}\right\}$。

若Eve选择的测量基与Alice不同，即$\Delta\phi_{AE}=\pm\frac{\pi}{2}$，由(3)式和(4)式可知信号有$\cos^2\left(\frac{\Delta\phi_{AE}+\varphi_{AE}}{2}\right)$的比例到达APD0，有$\sin^2\left(\frac{\Delta\phi_{AE}+\varphi_{AE}}{2}\right)$的比例到达APD1。而对于量子密钥分发系统，信号是经强衰减到单光子水平的量子信号，能量不可再分，信号比例就成为信号到达的概率，即

$$\begin{cases}P_0=\cos^2\left(\dfrac{\Delta\phi_{AE}+\varphi_{AE}}{2}\right)\\ P_1=\sin^2\left(\dfrac{\Delta\phi_{AE}+\varphi_{AE}}{2}\right)\end{cases}. \tag{10}$$

此时，AE间状态传递概率在Alice(或Eve)使用不同基组的情况下是不同的，例如同样是$P(e=0|a=0)$，$P\left(\left|e\right\rangle=\left|\frac{\pi}{2}\right\rangle\middle\|a\right\rangle=\left|0\right\rangle\right)=\frac{1}{2}P_0\big|_{\Delta\phi_{AE}=-\frac{\pi}{2}}=\frac{1}{2}\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$，而$P\left(\left|e\right\rangle=\left|0\right\rangle\middle\|a\right\rangle=\left|\frac{\pi}{2}\right\rangle\right)=\frac{1}{2}\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$。其中$\frac{1}{2}$是Eve选基的概率。

AE间整体的状态传递概率见表1，可以发现Eve选错基时，错误率有可能大于正确率。

表1 Alice-Eve状态传递概率

Table 1 States transfer probabilities between Alice and Eve

$P(e_j\|a_i)$	$e_j=\left\|0\right\rangle$	$\left\|\pi\right\rangle$	$\left\|\frac{\pi}{2}\right\rangle$	$\left\|\frac{3\pi}{2}\right\rangle$
$a_i=\left\|0\right\rangle$	$\frac{1}{2}\cos^2\frac{\varphi_{AE}}{2}$	$\frac{1}{2}\sin^2\frac{\varphi_{AE}}{2}$	$\frac{1}{2}\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$	$\frac{1}{2}\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$
$\left\|\pi\right\rangle$	$\frac{1}{2}\sin^2\frac{\varphi_{AE}}{2}$	$\frac{1}{2}\cos^2\frac{\varphi_{AE}}{2}$	$\frac{1}{2}\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$	$\frac{1}{2}\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$
$\left\|\frac{\pi}{2}\right\rangle$	$\frac{1}{2}\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$	$\frac{1}{2}\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$	$\frac{1}{2}\cos^2\frac{\varphi_{AE}}{2}$	$\frac{1}{2}\sin^2\frac{\varphi_{AE}}{2}$
$\left\|\frac{3\pi}{2}\right\rangle$	$\frac{1}{2}\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$	$\frac{1}{2}\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)$	$\frac{1}{2}\sin^2\frac{\varphi_{AE}}{2}$	$\frac{1}{2}\cos^2\frac{\varphi_{AE}}{2}$

由表1可得，Eve测量结果与Alice发送码值一致的概率是$P_c=\frac{1}{2}P_r+\frac{1}{2}P_w=\frac{1}{2}\cos^2\frac{\varphi_{AE}}{2}+\frac{1}{4}$，其中$P_r=\cos^2\frac{\varphi_{AE}}{2}$、$P_w=\frac{1}{2}$分别是Eve选对基和选错基时解码正确的概率，$P_c$即Eve的窃听效率，则AE间的交互信息量为$I(A,E)=1-\frac{1}{2}H(P_r)-\frac{1}{2}H(P_w)=\frac{1}{2}\left[1-H\left(\cos^2\frac{\varphi_{AE}}{2}\right)\right]$。

4.2 存在相位漂移时AB双方的误码率与互信息量

Eve到Bob的重发过程也有可能产生相位漂移，影响Bob的测量，假设从Eve到Bob的相位漂移为φ_{EB}。对Bob的测量也按照与Eve基组是否匹配分为两部分，对于基组匹配的部分，$\Delta\phi_{EB}=0$或π，测量结果与Eve截获过程相同。由(5)式可得，对比度为$V=\cos\varphi_{EB}$，然后根据(7)式可知Bob与Eve的基一致时状

态传递概率为 $P\left(\left|b\right\rangle=\left|i\right\rangle\left\|e\right\rangle=\left|j\right\rangle\right)=\begin{cases}\sin^2\dfrac{\varphi_{\mathrm{EB}}}{2}, & i\neq j\\ \cos^2\dfrac{\varphi_{\mathrm{EB}}}{2}, & i=j\end{cases}$，其中 i、$j\in\{0,\ \pi\}$ 或 $\left\{\dfrac{\pi}{2},\dfrac{3\pi}{2}\right\}$。

若 Bob 选择的测量基与 Eve 不同，$\Delta\phi_{\mathrm{EB}}=\pm\dfrac{\pi}{2}$，则根据(10)式得 Bob 端探测器响应的概率为 $\begin{cases}P_0=\cos^2\left(\dfrac{\Delta\phi_{\mathrm{EB}}+\varphi_{\mathrm{EB}}}{2}\right)\\ P_1=\sin^2\left(\dfrac{\Delta\phi_{\mathrm{EB}}+\varphi_{\mathrm{EB}}}{2}\right)\end{cases}$。若以 Eve 调相 $\dfrac{\pi}{2}$，Bob 调相 0 为例，计算得传递概率为 $P\left(\left|b\right\rangle=\left|0\right\rangle\left\|e\right\rangle=\left|\frac{\pi}{2}\right\rangle\right)=P_0\big|_{\Delta\phi_{\mathrm{EB}}=\frac{\pi}{2}}=\sin^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$。

于是，EB 间整体的状态传递概率见表 2，由于经过了对比基组过程，可认为 Bob 的选基概率包含在 Alice 的选基概率中。

表 2 Eve—Bob 状态传递概率

Table 2 States transfer probabilities between Eve and Bob

$P\left(b_j\middle\vert e_i\right)$	$b_j=\left\vert 0\right\rangle$	$\left\vert\pi\right\rangle$	$\left\vert\frac{\pi}{2}\right\rangle$	$\left\vert\frac{3\pi}{2}\right\rangle$
$e_i=\left\vert 0\right\rangle$	$\cos^2\dfrac{\varphi_{\mathrm{EB}}}{2}$	$\sin^2\dfrac{\varphi_{\mathrm{EB}}}{2}$	$\cos^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$	$\sin^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$
$\left\vert\pi\right\rangle$	$\sin^2\dfrac{\varphi_{\mathrm{EB}}}{2}$	$\cos^2\dfrac{\varphi_{\mathrm{EB}}}{2}$	$\sin^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$	$\cos^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$
$\left\vert\frac{\pi}{2}\right\rangle$	$\sin^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$	$\cos^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$	$\cos^2\dfrac{\varphi_{\mathrm{EB}}}{2}$	$\sin^2\dfrac{\varphi_{\mathrm{EB}}}{2}$
$\left\vert\frac{3\pi}{2}\right\rangle$	$\cos^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$	$\sin^2\left(\dfrac{\pi}{4}-\dfrac{\varphi_{\mathrm{EB}}}{2}\right)$	$\sin^2\dfrac{\varphi_{\mathrm{EB}}}{2}$	$\cos^2\dfrac{\varphi_{\mathrm{EB}}}{2}$

下面进行误码率计算，表示为

$$R_{\mathrm{QBE}}=P\left(\left|b\right\rangle=\left|\pi\right\rangle\middle\|\left|a\right\rangle=\left|0\right\rangle\right)P\left(\left|a\right\rangle=\left|0\right\rangle\right)+P\left(\left|b\right\rangle=\left|0\right\rangle\middle\|\left|a\right\rangle=\left|\pi\right\rangle\right)P\left(\left|a\right\rangle=\left|\pi\right\rangle\right)+P\left(\left|b\right\rangle=\left|\frac{3\pi}{2}\right\rangle\middle\|\left|a\right\rangle=\left|\frac{\pi}{2}\right\rangle\right)P\left(\left|a\right\rangle=\left|\frac{\pi}{2}\right\rangle\right)+$$
$$P\left(\left|b\right\rangle=\left|\frac{\pi}{2}\right\rangle\middle\|\left|a\right\rangle=\left|\frac{3\pi}{2}\right\rangle\right)P\left(\left|a\right\rangle=\left|\frac{3\pi}{2}\right\rangle\right),\tag{11}$$

其中 $P\left(\left|b\right\rangle=\left|\pi\right\rangle\middle\|\left|a\right\rangle=\left|0\right\rangle\right)$ 可根据传递概率矩阵表 1 和表 2 计算，具体地

$$P\left(\left|b\right\rangle=\left|\pi\right\rangle\middle\|\left|a\right\rangle=\left|0\right\rangle\right)=\sum_{s=0,\pi,\frac{\pi}{2},\frac{3\pi}{2}}P\left(\left|b\right\rangle=\left|\pi\right\rangle\middle\|\left|e\right\rangle=\left|s\right\rangle\right)P\left(\left|e\right\rangle=\left|s\right\rangle\middle\|\left|a\right\rangle=\left|0\right\rangle\right)=$$
$$\frac{1}{2}\left[\cos^2\frac{\varphi_{\mathrm{AE}}}{2}\sin^2\frac{\varphi_{\mathrm{EB}}}{2}+\sin^2\frac{\varphi_{\mathrm{AE}}}{2}\cos^2\frac{\varphi_{\mathrm{EB}}}{2}+\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{\mathrm{AE}}}{2}\right)\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{\mathrm{EB}}}{2}\right)+\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{\mathrm{AE}}}{2}\right)\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{\mathrm{EB}}}{2}\right)\right],\tag{12}$$

经计算可知：$P\left(\left|a\right\rangle=\left|0\right\rangle\right)=P\left(\left|a\right\rangle=\left|\pi\right\rangle\right)=P\left(\left|a\right\rangle=\left|\frac{\pi}{2}\right\rangle\right)=P\left(\left|a\right\rangle=\left|\frac{3\pi}{2}\right\rangle\right)=\dfrac{1}{4}$，且 $P\left(\left|b\right\rangle=\left|\frac{3\pi}{2}\right\rangle\middle\|\left|a\right\rangle=\left|\frac{\pi}{2}\right\rangle\right)=P\left(\left|b\right\rangle=\left|\frac{\pi}{2}\right\rangle\middle\|\left|a\right\rangle=\left|\frac{3\pi}{2}\right\rangle\right)=P\left(\left|b\right\rangle=\left|\pi\right\rangle\middle\|\left|a\right\rangle=\left|0\right\rangle\right)=P\left(\left|b\right\rangle=\left|0\right\rangle\middle\|\left|a\right\rangle=\left|\pi\right\rangle\right)$。

因此存在相位漂移时，I-R 攻击造成的误码率为

$$R_{\mathrm{QBE}}=\frac{1}{2}\left[\cos^2\frac{\varphi_{\mathrm{AE}}}{2}\sin^2\frac{\varphi_{\mathrm{EB}}}{2}+\sin^2\frac{\varphi_{\mathrm{AE}}}{2}\cos^2\frac{\varphi_{\mathrm{EB}}}{2}+\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{\mathrm{AE}}}{2}\right)\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{\mathrm{EB}}}{2}\right)+\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{\mathrm{AE}}}{2}\right)\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{\mathrm{EB}}}{2}\right)\right].\tag{13}$$

现计算 AB 的互信息量，在筛选后的数据中 AB 所用的基相同，但 Bob 接收到的都是 Eve 截获-重发的信号，其中一半使用的是 Alice 的基组，这部分 Bob 测得的码值误码率为 $Q_1=\cos^2\dfrac{\varphi_{\mathrm{AE}}}{2}\sin^2\dfrac{\varphi_{\mathrm{EB}}}{2}+\sin^2\dfrac{\varphi_{\mathrm{AE}}}{2}\cos^2\dfrac{\varphi_{\mathrm{EB}}}{2}$，

另一半所用的基组与Alice不同，这部分Bob测得的码值误码率为 $Q_2=\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)\cos^2\left(\frac{\pi}{4}-\frac{\varphi_{EB}}{2}\right)+\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{AE}}{2}\right)\sin^2\left(\frac{\pi}{4}-\frac{\varphi_{EB}}{2}\right)$，则AB间互信息量下降为

$$I(A,B)=1-\frac{1}{2}H(Q_1)-\frac{1}{2}H(Q_2). \tag{14}$$

5 全部、部分截获-重发对PC-QKD的影响

5.1 全部截获-重发

对比理想条件下I-R攻击、相位漂移和相位漂移条件下I-R攻击的系统误码率和交互信息量，分别对(6)、(13)式和(8)、(14)式进行数值计算仿真，如图2所示。

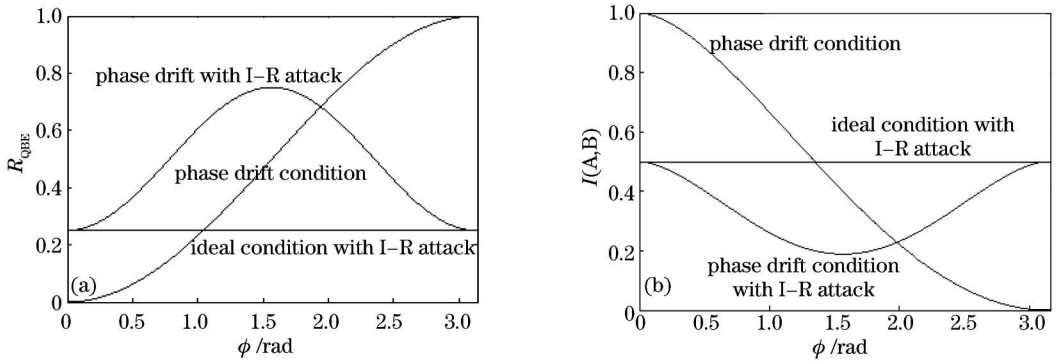

图2 (a)误码率随相位漂移变化曲线;(b)信息量随相位漂移变化曲线

Fig.2 (a) Variation of R_{QBE} with phase drift; (b) variation of information with phase drift

由于相干脉冲的时间间隔较小，在传输光纤里经历的环境相似，而在系统两端经过的光路不同，因此不考虑传输光纤中相干脉冲相位的相对漂移，而认为相位漂移主要来自于两端不等臂干涉仪，图2认为 $\phi=\varphi_{AE}=\varphi_{EB}=\varphi_{AB}$，从中可以看出：

1)当相位漂移量较小时，与只存在相位漂移或I-R攻击相比，相位漂移与I-R攻击同时存在时误码率更大，通信双方的互信息量更小；

2)误码率随相位漂移角度呈余弦形式变化，而交互信息量随漂移角度周期变化，其变化趋势也类似余弦函数曲线，并且由于截获-重发过程，I-R攻击下的误码率和互信息量的变化周期减小了一半，且对漂移角度更加敏感，变化频率更高；

3)存在相位漂移时的I-R攻击造成 $R_{QBE}\geqslant 0.25$，可见在全部截获-重发情况下，系统误码率过大，Eve的窃听会被发现。

另一方面，Eve的窃听效率 $P_c\leqslant\frac{3}{4}$，窃听信息量 $I(A,E)\leqslant 0.5$，相比理想条件下的I-R攻击都有所降低。这说明对于存在相位漂移的I-R攻击，通信双方的密性放大过程对Eve窃听信息的估计值可以有所减小，因此最终的密钥生成率可以得到相对提高。

为减小相位漂移对QKD的影响，需采取必要的措施加以控制与补偿。一般的方法包括：改变干涉系统结构，如使用plug and play系统；采取被动补偿措施，对干涉装置进行恒温与减震控制；跟踪相位漂移参数，进行主动补偿。通过减小或消除漂移对窃听的影响，可以更准确地估计Eve窃听的信息量，提高密性放大效率。

5.2 部分截获-重发

假设Eve进行部分I-R攻击，设窃听比例为 k，则Eve部分窃听的信息量

$$I_P(A,E)=k\cdot I(A,E)=\frac{k}{2}\left[1-H\left(\cos^2\frac{\varphi_{AE}}{2}\right)\right], \tag{15}$$

系统误码率为

$$R_{QBE,P}=kQ_1'+(1-k)Q_2', \tag{16}$$

其中 Q_1' 是存在Eve窃听攻击时的误码率，即(13)式；Q_2' 是不存在窃听时的误码率，即(6)式。

Alice与Bob的互信息为

$$I_P(A,B)=k\cdot I_1(A,B)+(1-k)I_2(A,B), \tag{17}$$

其中 $I_1(A,B)$ 是存在Eve窃听攻击时的互信息，即(14)式；$I_2(A,B)$ 是不存在窃听时的互信息，即(8)式。

假设通信双方采用非相干攻击误码阈值[18]为15%进行窃听检测，则须 $R_{QBE,P}<15\%$，令相位漂移角为0，得最大窃听比例 k=0.6。为增大误码率对相位漂移的容忍程度，k 值应越小越好；而为增加Eve的窃听信息 $I_P(A,B)$，应尽量增大 k 值。综合考虑这两方面的因素 k 可取在0.55附近，如图3($\phi=\varphi_{AE}=\varphi_{EB}=\varphi_{AB}$)所示。

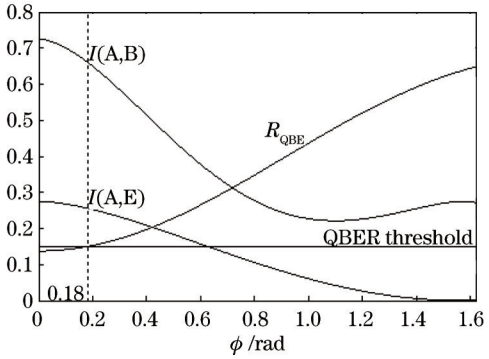

图3 误码率与互信息随相位漂移的变化曲线(部分窃听)

Fig.3 Variation of R_{QBE} and information with phase drift(partial eavesdropping)

从图中可以看出，误码率达到阈值时漂移角约为0.18 rad(即10.31°)。$I(A,E)=0.255$，即为使窃听不被发现Eve在窃听比例为55%时，对相位漂移有10.31°的容忍限度，能获得0.255的信息。然而，$I(A,E)\leqslant I(A,B)$，符合安全判据[18]，即虽然Eve通过部分窃听获得部分信息而不被发现，但是AB仍可以通过纠错和密性放大过程保证量子密钥的安全性，采用15%的阈值进行窃听检测仍是可行的。

6 结 论

分析了相位漂移对基于双M-Z干涉仪相位编码QKD系统稳定性的影响以及对该系统下的I-R攻击的影响。相位漂移会引起额外的误码，且与只存在相位漂移或I-R攻击相比，相位漂移和I-R攻击都存在时，误码率更大，$I(A,B)$ 更小。I-R攻击使误码率随相位漂移角度的变化频率更高，相位漂移则使I-R攻击的窃听信息量减小，表明可通过减小密性放大过程中对Eve窃听信息的估计值，相对提高密钥生成率。基于相位漂移的影响，阐述了相位补偿的一般解决方法。

全部I-R攻击误码率过大，Eve会被通信双方发现，为使窃听不被发现需选择部分窃听，本文给出了一个合理的窃听比例。结果表明，若通信双方选择误码阈值为15%，在进行55%部分窃听时，Eve可获得25.5%的信息量且不被发现。但是 $I(A,E)\leqslant I(A,B)$，仍然满足安全判据，通信双方可以通过纠错和密性放大过程保证量子密钥的安全性。本文主要研究了相位漂移对I-R攻击的影响，下一步应考虑通过密性放大过程准确估计在漂移条件下的窃听信息，对提高密钥生成率做定量研究。

参 考 文 献

1 H K Lo, H F Chau. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050-2056.

2 C H Bennett, G Brassard. Quantum cryptography: public key distribution and coin tossing [C]. Proceeding of IEEE International Conference on Computers, Systems and signal Processing, 1984: 175-179.

3 Shen Zeyuan, Fang Jian, He Guangqiang, *et al*.. Synchronous scheme and experimental realization in continuous variable quantum 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.

4 Zhao Guhao, Zhao Shanghong, Yao Zhoushi, *et al*.. Quantum key distribution analysis for filtering scheme based on double fiber Bragg gating [J].Chinese J Lasers, 2013, 40(9): 0918001.

赵顾颢, 赵尚弘, 幺周石, 等. 基于双光纤布拉格光栅滤波的量子密钥分发误码率分析[J]. 中国激光, 2013, 40(9): 0918001.

5 Zhu Feng, Wang Qin. Quantum key distribution protocol based on heralded single photon source [J].Acta Optica Sinica, 2014, 34(6): 0627002.
朱 峰, 王 琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014, 34(6): 0627002.

6 Dong Chen, Zhao Shanghong, Dong Yi, *et al*.. Analysis of quantum key distribution protocols in hybrid quantum-classical optical network [J]. Laser & Optoelectronics Progress, 2014, 51(11): 112701.
东 晨, 赵尚弘, 董 毅, 等. 量子-经典混合光网络的密钥分配协议研究[J].激光与光电子学进展, 2014, 51(11): 112701.

7 D Gottesman, H K Lo, N Lukenhaus, *et al*.. Security of quantum key distribution with imperfect devices [J]. Quantum Information and Computation, 2004, 4(5): 325-360.

8 Scarani V, Bechmann-Pasquinucci H, Cerf NJ, *et al*.. The security of practical quantum key distribution [J]. Rev Mod Phys, 2009, 81(3): 1301-1350.

9 Hughes R J, Mongan G L, Peterso C G. Quantum key distribution over a 48 km optical fibre network [J]. J Mod Opt, 2000, 47(2-3): 533-547.

10 Mo Xiaofan, Zhu Bing, Han Zhengfu, *et al*.. Faraday-michelson system for quantum cryptography [J]. Opt Lett, 2005, 30 (19): 2632-2634.

11 Wu Guang, Zhou Chunyuan, Zeng Heping. Single-photon interference and router-control in an optic fiber Sagnac interferometer [J]. Acta Physica Sinica, 2004, 53(3): 698-702.
吴 光, 周春源, 曾和平. 光纤Sagnac干涉仪中单光子干涉及路由控制[J].物理学报, 2004, 53(3): 698-702.

12 Dixon A R, Yuan Z L, Dynes J F, *et al*.. Continuous operation of high bit rate quantum key distribution [J]. Appl Phys lett, 2010, 96(16): 161102.

13 Chen Shuai, Wang Jindong, Zhong Pingping, *et al*.. Influence of time jitter on quantum Bit error rate of phase-coding quantumkey distribution system [J]. Acta Optica Sinica, 2011, 31(7): 0727001.
陈 帅, 王金东, 钟平平, 等. 时间抖动对相位编码量子密钥分发系统量子误码率的影响[J].光学学报, 2011, 31(7): 0727001.

14 Feihu Xu, Bing Qi, Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system [J]. New J Phys, 2010, 12(11):113026.

15 S H Sun, M S Jiang, L M Liang. Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system [J]. Phys Rev A, 2011, 83(6): 062331.

16 S H Sun, M S Jiang, L M Liang. Single-photon-detection attack on the phase-coding continuous-variable quantum cryptography [J]. Phys Rev A, 2012, 86(1): 012305.

17 Gisin N, Ribordy G, Tittle W, *et al*.. Quantum cryptography [J]. Rev Mod Phys, 2002, 74(1): 145-195.

18 Ma RuiLin. Quantum Cryptography Communication [M]. Beijing: Science Press, 2006, 74: 88-89.
马瑞霖. 量子密码通信[M]. 北京: 科学出版社, 2006, 74: 88-89.

19 Gerd Keiser. Optical Fiber Communications [M]. Beijing: Publishing House of Electronics Industry, 2012: 304-308.
凯 泽. 光纤通信 [M]. 北京: 电子工业出版社, 2012: 304-308.

栏目编辑: 刘丰瑞