基于多测量算子组合的非线性主动相位补偿攻击

陈俊嘉[1,2] 王金东[1,2] 秦晓娟[3] 赵 峰[4] 魏正军[1,2] 张智明[1,2]

[1]华南师范大学信息光电子科技学院广东省微纳光子功能材料与器件重点实验室，广东 广州 510006

[2]华南师范大学物理与电信工程学院广东省量子调控工程与材料重点实验室，广东 广州 510006

[3]广东理工职业学院工程技术系，广东 广州 510091

[4]陕西理工学院物理与电信工程学院，陕西 汉中 723000

摘要 量子密钥分发采用单光子作为信息载体，结合经典保密通信系统中的一次一密体制，可在理论上实现绝对安全的保密通信。采用拉格朗日乘数法对只选择一种算子的主动相位补偿攻击模型的量子误码率进行了系统分析，得到了量子误码率的分布规律。在此基础上，对结合多种算子进行测量的攻击模型进行了理论模拟，结果显示，在选择不同算子进行攻击时，附加误码率随着比特比值(最终量子密钥中比特0和比特1的比值)的变化而变化，在比特比值接近1的情况下，窃听所引入的附加误码率也不同，这对基于经典交互过程的实际安全性问题的研究有一定的参考价值。

关键词 量子光学；量子密钥分发；主动相位补偿；量子误码率；互信息

中图分类号 TN918.1 **文献标识码** A

doi：10.3788/LOP53.072701

Nonlinear Active Phase Compensation Attack Based on Multiple Operators for Measurement

Chen Junjia[1,2] Wang Jindong[1,2] Qin Xiaojuan[3] Zhao Feng[4] Wei Zhengjun[1,2] Zhang Zhiming[1,2]

[1] *Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou, Guangdong* 510006, *China*

[2] *Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Physics and Telecommunication Engineering, South China Normal University, Guangzhou, Guangdong* 510006, *China*

[3] *Engineering Technology Department, Guangdong Polytechnic Institute, Guangzhou, Guangdong* 510091, *China*

[4] *School of Physics and Telecommunication Engineering, Shaanxi University of Technology, Hanzhong, Shaanxi* 723000, *China*

Abstract Quantum key distribution, with single photon as information carrier, can theoretically provide an absolutely secure way for secret communication through the one time pad scheme of the classical security system. Through a comprehensive analysis with the Lagrange multiplier, the distribution of quantum bit error rate in the way of using only one operator in active phase compensation attack model is obtained. Based on this, the attack model measured by multiple operators is theoretically simulated. The result shows that when different operators are

收稿日期：2016-02-18；**收到修改稿日期**：2016-03-07；**网络出版日期**：2016-06-20

基金项目：国家自然科学基金(61378012，11374107，60978009，61108039，61401176，61401262)、教育部长江学者和创新团队发展计划(IRT1243)、广东省自然科学基金(2014A030310205，2015A030313388)、广东省科技计划项目(2015B010128012，2014B090901016)

作者简介：陈俊嘉(1994—)，男，本科生，主要从事量子密钥分发系统主动相位补偿方面的研究。

E-mail：616198312@qq.com

导师简介：王金东(1974—)，男，博士，副研究员，主要从事量子保密通信及其关键技术方面的研究。

E-mail：wangjd@scnu.edu.cn(通信联系人)

chosen to launch the attack, the relationship between the additional bit error rate and the bit ratio (the ratio of bit 0 and bit 1 in the final quantum key) varies, and the additional quantum bit error rate introduced by hacking is also different when the bit ratio is close to 1. This result has certain reference value to the practical security problems based on the classical mutual process.

Key words quantum optics; quantum key distribution; active phase compensation; quantum bit error rate; mutual information

OCIS codes 270.5568; 270.5565;270.5585

1 引 言

量子密钥分发(QKD)采用单光子作为信息载体,结合经典保密通信系统中的一次一密(OTP)体制,可在理论上实现绝对安全的保密通信。自从 Bennet 等[1]在 1984 年提出 BB84 协议以来,量子密钥分发系统在理论和实验研究上都取得了长足的进展[2-8]。

随着应用研究的不断深入,研究者发现,虽然量子保密通信具备理论上的绝对安全性,但是实际应用的设备却因器件的不理想性而存在安全漏洞。基于不同实现环节的量子黑客攻击方案被不断提出,因此研究现实条件下的量子保密通信系统的无条件安全性成为该领域最被关注的问题之一[9-15]。

根据不同的实际漏洞,针对 QKD 系统的攻击方案有很多。根据现有文献,大致可分为针对编解码单元及信道的攻击、针对非理想单光子源的攻击以及针对非理想单光子探测器的攻击等。在针对非理想单光子源方面,有光子数分束攻击[9]、非可信源攻击[10]等攻击方案。在针对编解码单元及信道方面,有大脉冲攻击[11]、相位重映射攻击[12]等攻击方案。在针对非理想单光子探测器方面,有伪态攻击[13]、时移攻击[14]、致盲攻击[15]等攻击方案。此外,文献[16]针对单向相位编码 QKD 系统中的主动相位补偿(APC)过程[17-19]提出一种新的攻击方案。由于在实际的 QKD 网络测试中相位调制器的半波电压会发生不同程度的变化,电压和相位也可能呈非线性关系[18],因此不能再通过单次的扫描测量来确定所有的工作点电压[19],而是需要经过多次扫描得到发送者(Alice)和接收者(Bob)的所有工作点电压以及相位调制器的半波电压,这样 Alice 和 Bob 就需要通过信道来交换经典信息,这就使得 APC 过程中的量子黑客攻击成为可能[16]。

基于单向量子密钥分发系统的 APC 过程的攻击方案采用了相位重映射攻击的理论模型,其特征是窃听者(Eve)只采用一种算子执行半正定算子测量(POVM),该研究结果仅仅说明了攻击的有效性,但并没有系统讨论攻击方案所引入的附加误码的分布特征。本文在第二部分采用拉格朗日乘数法对只选择一种算子的 APC 攻击模型的误码率进行了系统分析,得到了误码率的分布规律。在第三部分对可能的多算子结合的攻击模型进行了理论模拟,得到了每种情况下的附加误码率和比特比值的关系曲线。

2 基于单测量算子的 APC 攻击误码率规律分析

在文献[16]中,当 Eve 只采用一种算子 M_0 执行 POVM 时,得到的结果显示攻击的量子误码率(QBER)可以接近 0,但是会导致 0 和 1 的比特比值不均衡,此文献并未对这种现象进行系统性的分析。当 Eve 选择 M_0、M_1、M_2、M_3 中的某个测量算子进行测量时,攻击过程所引入的量子误码率 Q 分别为[16]

$$Q_0=\frac{1}{2}-\frac{\frac{1}{2}-\frac{1}{2}\cos(\delta_1+\delta_2)}{3-\cos\delta_3-\cos(\delta_1+\delta_2)-\cos\delta_2},\tag{1}$$

$$Q_1=\frac{1}{2}-\frac{\frac{1}{2}-\frac{1}{2}\cos(\delta_2+\delta_3)}{3-\cos\delta_3-\cos(\delta_2+\delta_3)-\cos\delta_1\cos(\delta_2+\delta_3)+\sin\delta_1\sin(\delta_2+\delta_3)},\tag{2}$$

$$Q_2=\frac{1}{2}-\frac{\frac{1}{2}-\frac{1}{2}\cos(\delta_1+\delta_2)}{3-\cos(\delta_1+\delta_2)-\cos\delta_3-\cos\delta_3\cos(\delta_1+\delta_2)+\sin\delta_3\sin(\delta_1+\delta_2)},\tag{3}$$

$$Q_3=\frac{1}{2}-\frac{\frac{1}{2}-\frac{1}{2}\cos(\delta_2+\delta_3)}{3-\cos\delta_1-\cos(\delta_2+\delta_3)-\cos\delta_2},\tag{4}$$

式中 δ_1、δ_2、δ_3 表示在 Eve 介入的相位漂移参数扫描过程结束后，Alice 根据 BB84 协议选择的用于量子密钥分发的三个相位值，即在扫描过程后，Alice 选择携带 0，δ_1，$\delta_1+\delta_2$ 和 $\delta_1+\delta_2+\delta_3$ 4 个相位值的单光子发送给 Bob。对(1)～(4)式求极值，一般采用拉格朗日乘数法[20-21]。首先，根据极值必要条件对拉格朗日函数求解极值，从组成的方程组中可以求出若干个稳定点。其次，将得到的稳定点代入 Hesse 矩阵中，若矩阵结果正定则稳定点为极小值点，若矩阵结果负定则稳定点为极大值点，若矩阵结果不定则稳定点为非极值点。拉格朗日函数、极值的必要条件和 Hesse 矩阵分别为

$$F(x_1,x_2,x_3,\cdots,\lambda_1,\lambda_2,\lambda_3,\cdots)=f(x_1,x_2,x_3,\cdots)+\lambda_1\Phi(x_1)+\lambda_2\Phi(x_2)+\lambda_3\Phi(x_3)+\cdots, \tag{5}$$

$$\begin{cases}\dfrac{\partial F}{\partial x_i}=0\\ \dfrac{\partial F}{\partial \lambda_i}=0\end{cases}, \tag{6}$$

$$\boldsymbol{H}=\begin{bmatrix}F_{x_1x_1} & F_{x_1x_2} & F_{x_1x_3} & \cdots\\ F_{x_2x_1} & F_{x_2x_2} & F_{x_2x_3} & \cdots\\ F_{x_3x_1} & F_{x_3x_2} & F_{x_3x_3} & \cdots\end{bmatrix}, \tag{7}$$

式中 x_1，x_2，x_3，...为自变量，$f(x_1,x_2,x_3...)$为需要求解的多元函数，$i=1,2,3,\cdots$，$\Phi(x_i)$为与自变量相对应的条件方程，即约束自变量的方程式，λ_i 为与条件方程相对应的常量。将(1)～(4)式代入(5)、(6)式得到以下结果：

1) Eve 单独选择 M_0，得 $\delta_2=\delta_3=0$，$\delta_1\neq0$，误码率恒等于 0；

2) Eve 单独选择 M_1，得 $\delta_1+\delta_2=0$，$\delta_3=0$，误码率恒等于 0；

3) Eve 单独选择 M_2，得 $\delta_2+\delta_3=0$，$\delta_1=0$，误码率恒等于 0；

4) Eve 单独选择 M_3，得 $\delta_1=\delta_2=0$，$\delta_3\neq0$，误码率恒等于 0。

从上述结果可以看出，求解拉格朗日函数所得的结果不存在量子误码率的极值点。为了更进一步探究上述误码率恒等于 0 的情况，绘制了图 1 所示的物理模型，其中 $\psi_k(k=0,1,2,3)$是在 Eve 介入的相位漂移扫描过程结束后，Alice 根据扫描结果选择的满足 BB84 协议的 4 个量子态，这 4 个量子态对应的相位值分别为 0，δ_1，$\delta_1+\delta_2$，$\delta_1+\delta_2+\delta_3$。

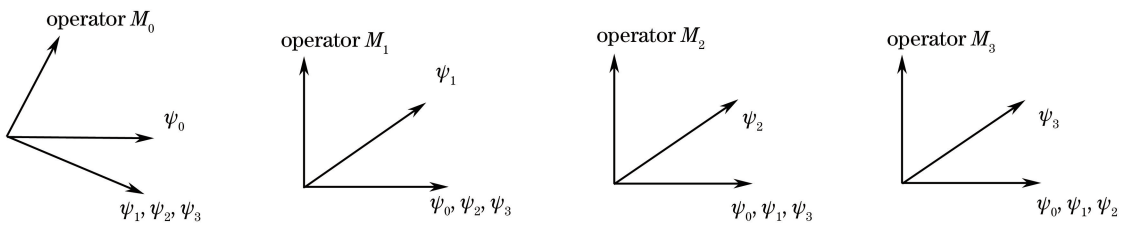

图 1 误码率为 0 时的物理模型。(a) Eve 只选择 M_0；(b) Eve 只选择 M_1；(c) Eve 只选择 M_2；(d) Eve 只选择 M_3

Fig. 1 Physical model when QBER is 0. (a) Eve only chooses M_0; (b) Eve only chooses M_1; (c) Eve only chooses M_2; (d) Eve only chooses M_3

根据得到的物理模型，以 Eve 选择 M_0 为例解释前文所提到的误码率恒等于 0 的现象，另外三种情况类似。在 APC 阶段，当 Eve 对单光子加载附加相位时，可以使通信双方获得的相位工作点满足 $\delta_2=\delta_3=0$，$\delta_1\neq0$，此时 Alice 的 4 个标准 BB84 量子态分别对应的相位值就由标准的相位值$\left(0,\dfrac{\pi}{2},\pi,\dfrac{3\pi}{2}\right)$变为$(0,\delta_1,\delta_1,\delta_1)$。在下一阶段 QKD 中，Eve 只选择 M_0 对相位为$(0,\delta_1,\delta_1,\delta_1)$的 4 种量子态进行测量，由于 M_0 只能测量到相位为 0 的量子态而无法测量到相位为 δ_1 的量子态，所以 Bob 选择正交基对 Eve 发送的单光子进行测量的结果显示没有误码的产生，此方式导致 Bob 得到的 0 与 1 的比特比值不均衡。在实际应用中并不会单一地追求极低的误码率，而是在比特比值接近 1 的情况下尽可能地降低攻击的附加误码率，这就需要 Eve 窃听所引入的附加误码率随比特比值变化的关系曲线尽可能陡峭。

3 结合多种算子 APC 攻击的误码率及互信息分析

文献[16]给出了其攻击方案的附加误码率随比特比值的变化关系，结果显示，当比特比值等于 1 时，附加误码率为 16.67%，当比特比值大于 1 时，附加误码率会进一步减小。如果窃听所引入的附加误码率随着比特比值的变化曲线越陡峭，那么在比特比值接近 1 的时候，就可以更大程度地降低附加误码率。文献[16]仅提出了单向相位编码系统的相位补偿过程的攻击方案，并没有系统优化不同情况下的附加误码率，也没有涉及到采用不同方式利用多测量算子进行窃听时附加误码率是否不同的情况。本研究对多算子测量的攻击进行理论模拟，并且计算了这个过程中的 Eve 和 Alice 之间的互信息。表 1 为 Eve 选择 M_0 与 M_2 算子进行测量的结果，其余选择方式的测量结果与之类似，其中表 1 中 $|\psi_k\rangle$ 为在 Eve 介入的扫描过程后，Alice 按照 BB84 协议在 QKD 过程中发送的量子态，以上 4 个量子态分别对应于单光子携带的相位信息为 $0,\delta_1,\delta_1+\delta_2,\delta_1+\delta_2+\delta_3$ 的量子态；Tr 为矩阵的迹，即为主对角线上所有元素之和；α,β 为 Eve 执行 POVM 测量时选择测量算子的概率。

表 1 结合 M_0 与 M_2 的攻击误码

Table 1 Attack error when choosing M_0 and M_2

Phase of state that Alice sends	Probability of Eve choosing operators	POVM operator that Eve chooses	Probability of Eve measuring state	Phase of state that Eve resends	Measure basis that Bob chooses	Key that Bob gets	Probability of setting the key	Status of sifting key	Status of quantum bit error
0	α	M_0	$\mathrm{Tr}(M_0\|\psi_0\rangle\langle\psi_0\|)$	0	0	0	1	Keep	√
					$\frac{\pi}{2}$	0	1/2	Discard	
						1	1/2	Discard	
	β	M_2	$\mathrm{Tr}(M_2\|\psi_0\rangle\langle\psi_0\|)$	π	0	1	1	Keep	×
					$\frac{\pi}{2}$	0	1/2	Discard	
						1	1/2	Discard	
δ_1	α	M_0	$\mathrm{Tr}(M_0\|\psi_1\rangle\langle\psi_1\|)$	0	0	0	1	Discard	
					$\frac{\pi}{2}$	0	1/2	Keep	√
						1	1/2	Keep	×
	β	M_2	$\mathrm{Tr}(M_2\|\psi_1\rangle\langle\psi_1\|)$	π	0	1	1	Discard	
					$\frac{\pi}{2}$	0	1/2	Keep	√
						1	1/2	Keep	×
$\delta_1+\delta_2$	α	M_0	$\mathrm{Tr}(M_0\|\psi_2\rangle\langle\psi_2\|)$	0	0	0	1	Keep	×
					$\frac{\pi}{2}$	0	1/2	Discard	
						1	1/2	Discard	
	β	M_2	$\mathrm{Tr}(M_2\|\psi_2\rangle\langle\psi_2\|)$	π	0	1	1	Keep	√
					$\frac{\pi}{2}$	0	1/2	Discard	
						1	1/2	Discard	
$\delta_1+\delta_2+\delta_3$	α	M_0	$\mathrm{Tr}(M_0\|\psi_3\rangle\langle\psi_3\|)$	0	0	0	1	Discard	
					$\frac{\pi}{2}$	0	1/2	Keep	×
						1	1/2	Keep	√
	β	M_2	$\mathrm{Tr}(M_2\|\psi_3\rangle\langle\psi_3\|)$	π	0	1	1	Discard	
					$\frac{\pi}{2}$	0	1/2	Keep	×
						1	1/2	Keep	√

根据表 1 的测量结果，可以计算得到 Eve 选择测量算子 M_0 与 M_2 进行窃听时的误码率，即

$$Q_0=\frac{\alpha(2-\cos\delta_2-\cos\delta_3)+\beta[2-\cos\delta_1-\cos(\delta_1+\delta_2+\delta_3)]}{2\alpha[3-\cos(\delta_1+\delta_2)-\cos\delta_2-\cos\delta_3]+2\beta[3-\cos(\delta_1+\delta_2)-\cos\delta_1-\cos(\delta_1+\delta_2+\delta_3)]},\quad(8)$$

用同样的方法，可以进一步分析 Eve 选择其他可能的两种测量算子进行窃听时引入的误码率，以下用 Q_1 表示 Eve 选择测量算子 M_0 与 M_3 进行窃听时引入的误码率；用 Q_2 表示 Eve 选择测量算子 M_1 与 M_2 进行窃听时引入的误码率；用 Q_3 表示 Eve 选择测量算子 M_1 与 M_3 进行窃听时引入的误码率；用 Q_4 表示 Eve 选

择测量算子 M_0、M_2 与 M_3 进行窃听时引入的误码率。通过类似的数学计算，可以得到上述各种可能的窃听测量方式所引入的误码率分别为：

$$Q_1=\frac{\alpha(2-\cos\delta_2-\cos\delta_3)+\beta(2-\cos\delta_1-\cos\delta_2)}{2\alpha[3-\cos(\delta_1+\delta_2)-\cos\delta_2-\cos\delta_3]+2\beta[3-\cos\delta_2-\cos\delta_1-\cos(\delta_2+\delta_3)]},\tag{9}$$

$$Q_2=\frac{\alpha[2-\cos(\delta_1+\delta_2+\delta_3)-\cos\delta_3]+\beta[2-\cos\delta_1-\cos(\delta_1+\delta_2+\delta_3)]}{2\alpha[3-\cos(\delta_1+\delta_2+\delta_3)-\cos(\delta_2+\delta_3)-\cos\delta_3]+2\beta[3-\cos(\delta_1+\delta_2)-\cos\delta_1-\cos(\delta_1+\delta_2+\delta_3)]},\tag{10}$$

$$Q_3=\frac{\alpha[2-\cos(\delta_1+\delta_2+\delta_3)-\cos\delta_3]+\beta(2-\cos\delta_1-\cos\delta_2)}{2\alpha[3-\cos(\delta_2+\delta_3)-\cos(\delta_1+\delta_2+\delta_3)-\cos\delta_3]+2\beta[3-\cos\delta_2-\cos\delta_1-\cos(\delta_2+\delta_3)]},\tag{11}$$

$$Q_4=\{\alpha(2-\cos\delta_2-\cos\delta_3)+\gamma(2-\cos\delta_1-\cos\delta_2)+\beta[2-\cos\delta_1-\cos(\delta_1+\delta_2+\delta_3)]\}/$$
$$\{2\alpha[3-\cos(\delta_1+\delta_2)-\cos\delta_2-\cos\delta_3]+2\gamma[3-\cos\delta_2-\cos\delta_1-\cos(\delta_2+\delta_3)]+$$
$$2\beta[3-\cos\delta_1-\cos(\delta_1+\delta_2)-\cos(\delta_1+\delta_2+\delta_3)]\}^{-1}。\tag{12}$$

在(8)～(11)式中 $\alpha+\beta=1$，在(12)式中 $\alpha+\beta+\gamma=1$，α、β、γ 为 Eve 执行 POVM 测量时选择测量算子的概率，而 0 与 1 的比特比值

$$r=\frac{\alpha+1}{2-\alpha}。\tag{13}$$

根据(8)～(11)式，模拟出当比特比值在[1,2]区间变化时误码率及互信息的计算结果，如图 2 所示。

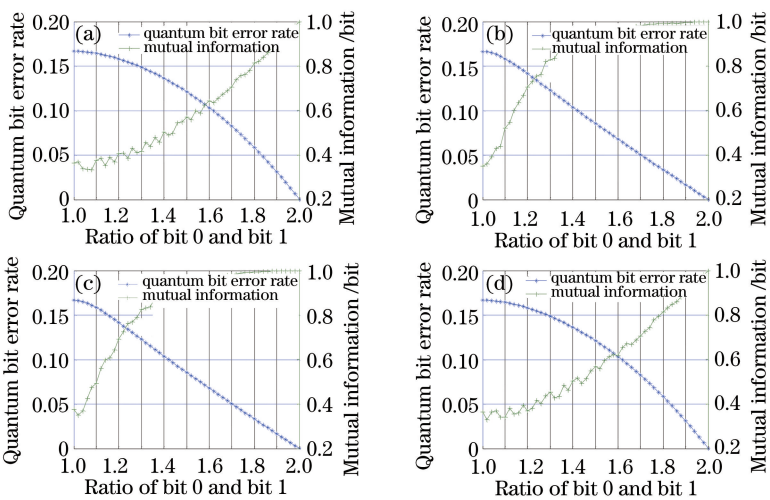

图 2 Eve 选择不同测量算子组合时量子误码率和互信息与比特比值的关系。(a)Eve 选择 M_0 与 M_2；(b) Eve 选择 M_0 与 M_3；(c) Eve 选择 M_1 与 M_2；(d) Eve 选择 M_1 与 M_3

Fig. 2 QBER and mutual information versus quantum bit ratio when Eve chooses different operators. (a) Eve chooses M_0 and M_2; (b) Eve chooses M_0 and M_3; (c) Eve chooses M_1 and M_2; (d) Eve chooses M_1 and M_3

通过对图 2 和图 3 的模拟结果进行分析，可以得到以下结果：1)在比特比值为 1 时，无论 Eve 采用哪种测量算子组合的方式，其附加误码率都为 16.67%，而对于每一个量子比特，Eve 都可以获取其中 0.35 比特的信息；2)为了进一步分析该窃听方式在实际应用中的有效性，需要考虑在比特比值接近 1 的情况下，能否通过窃听方式的优化使得误码率在原有 16.67%的基础上迅速降低，所以需要关注误码率曲线和互信息曲线的斜率问题。通过图 2 与图 3 的对比，可得出在比特比值接近 1 的情况下，Eve 选择两种测量算子组合的方式得到的误码率曲线和互信息曲线的斜率比选择三种测量算子的组合更大。对于选择两种测量算子的情况，图 2(b)与图 2(c)的误码率曲线和互信息曲线的斜率更大，因此 Eve 在采用两种算子组合的方式对窃听行为进行优化时，应当选择测量算子 M_0 与 M_3 或者 M_1 与 M_2 的组合方式。

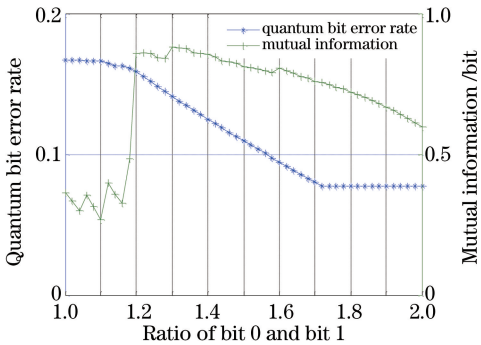

图 3 Eve 选择 M_0、M_2 和 M_3 时误码率和互信息与比特比值的关系

Fig. 3 QBER and mutual information versus bit ratio when Eve chooses M_0, M_2, and M_3

4 结 论

分析了结合多种算子进行窃听的情况下，附加误码率和比特比值之间的关系，发现其变化关系随算子组合的不同而不同，误码率曲线具有不同的斜率和变化特征。因此，当比特比值约为 1 时，不同算子组合引入的附加误码率不同，这对优化针对单向相位编码系统主动相位补偿过程的攻击具有明显的实际应用价值。

参 考 文 献

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[C]. International Conference on Computers Systems and Signal Processing, IEEE, 1984: 175-179.

2 Bennett C H, Bessette F, Brassard G, *et al*.. Experiment quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3-28.

3 Stucki D, Gisin N, Guinnard O, *et al*.. Quantum key distribution over 67 km with a plug & play system[J]. New Journal of Physics, 2002, 4(1): 41.

4 Gobby C, Yuan Z L, Shields A J. Quantum key distribution over 122 km of standard telecom fiber[J]. Applied Physics Letters, 2004, 84(19): 3762-3764.

5 Mo X F, Zhu B, Han Z F, *et al*.. Faraday-Michelson system for quantum cryptography[J]. Optics Letters, 2005, 30(19): 2632-2634.

6 Chen Yan, Shen Yong, Zou Hongxin. An all-fiber continuous variable quantum key distribution based on multi-bits coding of single pulse[J]. Acta Optica Sinica, 2015, 35(7): 0727001.
陈 岩, 沈 咏, 邹宏新. 基于单脉冲多位编码的全光纤连续变量量子密钥分发[J]. 光学学报, 2015, 35(7): 0727001.

7 Liu Youming, Wang Chao, Huang Duan, *et al*.. Study of synchronous technology in high-speed continuous variable quantum key distribution system[J]. Acta Optica Sinica, 2015, 35(1): 0106006.
刘友明, 汪 超, 黄 端, 等. 高速连续变量量子密钥分发系统同步技术研究[J]. 光学学报, 2015, 35(1): 0106006.

8 Guo Dabo, Zhang Yanhuang, Wang Yunyan. Performance optimization for the reconciliation of Gaussian quantum key distribution[J]. Acta Optica Sinica, 2014, 34(1): 0127001.
郭大波, 张彦煌, 王云艳. 高斯量子密钥分发数据协调的性能优化[J]. 光学学报, 2014, 34(1): 0127001.

9 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography[J]. Physical Review Letters, 2005, 94(23): 230503.

10 Brassard G, Lütkenhaus N, Mor T, *et al*.. Limitations on practical quantum cryptography[J]. Physical Review Letters, 2000, 85(6): 1330-1333.

11 Vakhitov A, Makarov V, Hjelme D R. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography[J]. Journal of Modern Optics, 2001, 48(13): 2023-2038.

12 Fung C H F, Qi B, Tamaki K, *et al*.. Phase-remapping attack in practical quantum-key-distribution systems[J]. Physical Review A, 2007, 75(3): 032314.

13 Makarov V, Anisimov A, Skaar J. Effects of detector efficiency mismatch on security of quantum cryptosystems[J]. Physical Review A, 2005, 74(2): 022313.

14 Qi B, Fung C H F, Lo H K, *et al*.. Time-shift attack in practical quantum cryptosystems[J]. Quantum Information & Computation, 2005, 7(1): 73-82.

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

16 Dong Z Y, Yu N N, Wei Z J, *et al*.. An attack aimed at active phase compensation in one-way phase-encoded QKD systems[J]. The European Physical Journal D, 2014, 68(8): 1-6.

17 Makarov V, Brylevski A, Hjelme D R. Real-time phase tracking in single-photon interferometers[J]. Applied Optics, 2004, 43(22): 4385-4392.

18 Zhang L J, Wang Y G, Yin Z Q, *et al*.. Real-time compensation of phase drift for phase-encoded quantum key distribution systems[J]. Chinese Science Bulletin, 2011, 56(22): 2305-2311.

19 Chen W, Hang Z F, Mo X F, *et al*.. Active phase compensation of quantum key distribution system[J]. Chinese Science Bulletin, 2008, 53(9): 1310-1314.

20 Yue Yuying, Du Guangbin, Liu Xingxiang. Eigenvalues and eigenvectors of the weak adjoint matrix and m-weak adjoint matrix[J]. Journal of Yanan University (Natural Science Edition), 2011, 30(3): 39-41.
岳育英, 杜光斌, 刘兴祥. 多元函数条件极值计算的一种方法[J]. 延安大学学报(自然科学版)2011, 30(3): 39-41.

21 Chen Huiru. The discriminances and applications of the infinitesimal and infinitely sequence of number[J]. Journal of Chaohu College, 2010, 12(6): 116-118.
陈惠汝. 多元函数极值求法探讨[J]. 巢湖学院学报, 2010, 12(6): 116-118.