非对称信道相位匹配量子密钥分发

周江平 周媛媛† 周学军

(海军工程大学电子工程学院, 武汉 430033)

(2023 年 4 月 23 日收到; 2023 年 5 月 17 日收到修改稿)

经典相位匹配量子密钥分发要求信道对称, 而实际应用中非对称信道应用场景更加普遍. 为研究信道非对称性对相位匹配协议性能的影响, 基于经典相位匹配协议框架提出非对称相位匹配协议, 建立相关数学仿真模型, 并对信道非对称情况下诱骗态和统计波动等对系统的影响进行仿真分析. 结果表明: 信道非对称性对系统性能影响巨大, 随着信道衰减差异的增大系统性能减小, 且减小速度逐渐加快, 超过 4 dB 时已无法生成密钥; 诱骗态方案不能改变系统对信道衰减差异的容忍度, 但在信道衰减差异较大时, 增加诱骗态可以显著提升系统性能; 随着数据长度的增大, 系统对信道衰减差异的容忍度逐渐提升, 当数据长度大于 10^{12} 时, 这种提升不再明显, 与对称信道相比, 当信道衰减差异为 2 dB 时, 随着数据长度的增大, 系统性能提升更加明显.

关键词: 量子密钥分发, 相位匹配, 非对称信道, 信道衰减差

PACS: 03.67.Dd, 03.67.Ac, 03.67.Hk **DOI:** 10.7498/aps.72.20230652

1 引 言

量子密钥分发 [1] (quantum key distribution, QKD) 基于量子力学基本原理, 可实现远距离双方无条件安全通信, 是应对经典密码体制因依赖计算安全而受量子霸权威胁的有效手段. Bennett 和 Brassard [1] 于 1984 年提出 BB84 协议, 开启了 QKD 研究的新征程. 随后新的 QKD 协议不断被提出, 如诱骗态协议 [2]、测量设备无关协议 [3](measurement device independent, MDI)、循环差分相移协议 [4] 等, 使 QKD 系统在安全性、密钥生成率和安全传输距离等方面的性能得到较大提升. 然而, 这些协议均难以突破线性密钥生成率边界 [5,6] (Pirandola-Laurenza-Ottaviani-Banchi Bound, PLOB). 2018 年, Lucamarini 等 [7] 提出双场 (twin field, TF) 协议, 将密钥生成效率 R 和 η 关系由 $R \leqslant O(\eta)$ 改善为 $R \leqslant O(\sqrt{\eta})$, 突破了 PLOB 界. Ma 等 [8] 将“场”具体化, 提出相位匹配 (phase matching, PM) 协议, 并对其安全性进行严格的证明, 是目前较优的 TF 变种协议之一 [9].

理论上, 针对安全性, Lin 等 [10,11] 从不同的方面再次对 PM 协议的安全性进行分析; 针对编码方式, Shen 等 [12,13] 提出了基于轨道角动量和基于脉冲位置调制两种不同编码方式的 PM 协议; 针对实际应用, Yu 等 [14] 对自由空间中 PM 协议的应用进行了研究, Cui 等 [15] 对基于卫星的 PM 协议进行了研究, Han 等 [16,17] 分别针对 PM 应用中信源问题进行了研究. 实验上, Fang 等 [18] 基于 PM 协议在 302 km 和 402 km 处都突破了 PLOB 界, 最远在 502 km 处密钥生成率仍能达到 0.118 bit/s. Ma 等 [19] 对基于波分多路复用的 PM 协议在量子网络中的应用进行了研究, 讨论了信道噪声对密钥生成率的影响. PM 协议在理论和实际中都得到广泛的研究.

然而, 实际应用中信道非对称情况更加普遍, 量子密钥分发网络中由于各接入节点和中心节点的相对位置不同, 存在信道不对称情况, 移动量子

† 通信作者. E-mail: EPJZYY@aliyun.com

© 2023 中国物理学会 Chinese Physical Society

密钥分发中由于自由空间信道的时变性, 信道难以维持对称. 经典 PM 协议假设密钥分发双方信道具有对称性, 为满足这一要求, 可以给衰减小的信道额外增加衰减, 但是这无疑会减小系统密钥生成率和安全传输距离. Wang 等[20] 基于非对称信道对 MDI 协议进行研究, 提出了性能优化方案, 与 MDI 协议不同, PM 协议通信双方仅在信源强度相同时才能生成密钥, 因而无法通过差异化调整信源强度的方式抵消信道非对称所带来的影响以优化系统性能. Yu 等[21] 对基于自由空间信道的 PM 协议进行研究时, 给出信道非对称情况下, 三诱骗态 PM 协议性能, 但没有研究信道非对称性对 PM 协议性能影响.

本文针对信道非对称问题, 建立非对称 PM 协议仿真模型, 研究信道非对称性对 PM 协议性能的影响. 首先对非对称 PM 协议模型及其安全性进行分析, 随后给出非对称 PM 协议仿真数学模型, 最后对信道非对称性对 PM 协议性能的影响进行仿真分析, 并给出相关结论.

2 非对称 PM 协议模型及安全性分析

非对称 PM 协议模型如图 1(a) 所示. 图中, L 和 R 分别表示 Charlie 端左侧和右侧检测器, A 和 B 分别表示密钥分发两方, A′和 B′分别表示 A、B 双方初始量子比特等效通道. 与经典 PM 协议不同, 非对称 PM 协议模型中, 信道中出现不对称的衰减. 通过对等价纠缠提纯协议的安全性证明, 文献 [8] 中协议Ⅲ(本文简称协议Ⅲ) 的安全性得到证明, 基于协议Ⅲ, 对非对称 PM 协议的安全性进行分析.

基于纠缠的 PM 协议如图 1(b) 所示, 具体流程如下.

1) 态制备. 可信第三方生成态 ρ 并经过分束器生成脉冲分别从 A 和 B 发送至不可信第三方 Charlie, A 和 B 初始化量子比特 $|+i\rangle$ 并利用相位控制门 C_π 对相位进行调制, C_π 表示从量子比特到光模式映射的相位控制门, 其表达式为 $C_\pi = |0\rangle_{\mathrm{A}'}\langle 0| \otimes U_{\mathrm{A}}(0) + |1\rangle_{\mathrm{A}'}\langle 1| \otimes U_{\mathrm{A}}(\pi)$, 其中 $U_{\mathrm{A}}(\phi) = \mathrm{e}^{\mathrm{i}\phi a^\dagger a}$.

2) 测量. Charlie 对接收到的光进行相干检测并记录检测器响应情况.

3) 声明. Charlie 对外声明检测结果.

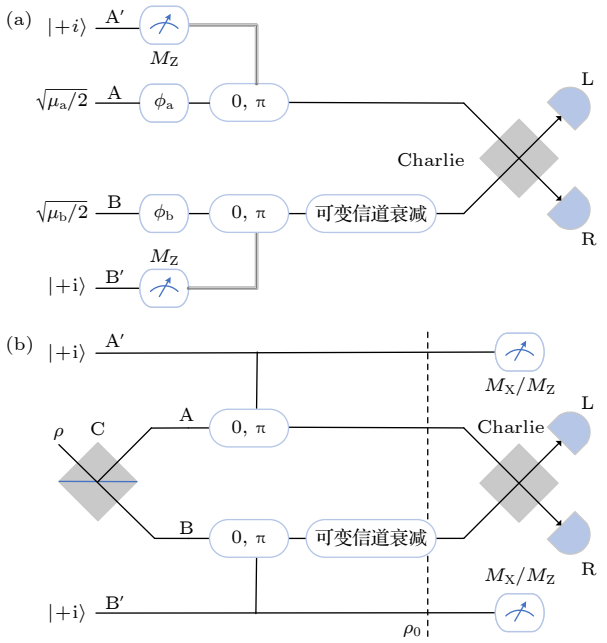

图 1 (a) 非对称 PM 协议模型; (b) 基于纠缠的 PM 协议模型

Fig. 1. (a) Asymmetric PM protocol model; (b) entanglement-based PM protocol model.

4) 筛选. 当仅有 L/R 响应时, 保留相应的量子比特, 如果是 R 响应, 还需对 B 应用 Pauli Y-门.

5) 参数估计. 重复上述过程足够多次数, A 和 B 得到一个 $2n$ 量子比特态 $\rho^n_{\mathrm{A}'\mathrm{B}'}$, 对 $\rho^n_{\mathrm{A}'\mathrm{B}'}$ 随机采样来估计比特错误 E^{Z} 和推导相位错误 E^{X}.

6) 密钥提取. 当错误率低于某一门限值, 基于 $\rho^n_{\mathrm{A}'\mathrm{B}'}$, A 和 B 可以利用标准的纠缠提纯协议来获取密钥.

协议Ⅲ与上述基于纠缠的 PM 协议等价, 而基于纠缠的 PM 协议安全性由 Lo-Chau 安全证明[22] 和 Shor-Preskill 安全证明[23] 共同保证, 因此协议Ⅲ安全性得到证明.

非对称 PM 协议并不改变信源端量子态的制备方式, 保持 $\mu_{\mathrm{a}} = \mu_{\mathrm{b}} = \mu/2$, 因此与协议Ⅲ中具有相同的相干态 $|\sqrt{\mu/2}\mathrm{e}^{\mathrm{i}\phi_{\mathrm{a}}}\rangle$ 和 $|\sqrt{\mu/2}\mathrm{e}^{\mathrm{i}\phi_{\mathrm{b}}}\rangle$ 以及相同的初始化量子比特; 在测量端量子态测量的方式不变, 对经信道传输过来的相干态 A 和 B 进行测量, 与对称信道的差别仅体现在测量结果上, 相较信道对称时的信息损失, 信道的非对称性可能会造成额外的信息损失, 但这种损失本质上仍是信道损失, 并不会造成信息的泄露, 从而产生安全隐患. 在测量结果的声明、密钥的筛选、参数的估计以及最终密钥的提取上, 均与原始 PM 协议保持一致. 因此

仅在信道损失上有所不同的协议, 可以认为两种协议等价, 因此非对称 PM 协议具有与原始 PM 协议相同的安全性.

相较于对称信道, 信道的非对称特性不会引入额外的实际安全性问题. 一方面, 从文献 [8] 中协议Ⅲ的安全性证明可以看出, 其与信道特性无关, 上文中通过协议等价的方式证明了非对称情况下 PM 协议的安全性; 另一方面, 相位匹配协议作为 TF 协议的一个变种, 具有与 TF 协议相同的安全性, Wang 等 [24] 通过理论分析, 给出了 TF 协议在非对称条件下的安全性证明, 也为非对称条件下 PM 协议的安全性奠定了基础.

总体来看, 协议的安全性与信道特性无关. 信道非对称仅会对最终系统性能产生影响, 而不会对系统的安全性产生影响.

3 非对称 PM 协议相关参数

针对非对称信道, 需对经典 PM 协议中相关参数进行调整和适应性改进. 基于原始 PM 协议框架 [8], 对相关参数在非对称信道条件下的形式进行推导.

3.1 检测概率

假设信道为纯损失信道, A, B 与 Charlie 间信道传输率分别为 $\eta_{\rm a}$ 和 $\eta_{\rm b}$, 包括信道、检测器等损失. 不失一般性, 假设 A 和 B 都发送 0, 且相位索引 $j_{\rm a}=j_{\rm b}=0$, 全局相位分别为 $\phi_{\rm a}$ 和 $\phi_{\rm b}$, 且相位差 $\phi_\delta=\phi_{\rm b}-\phi_{\rm a}$.

在 A 和 B 对光脉冲进行编码后, 信源端量子态可以表示为

$$\left(\mathrm{e}^{\mathrm{i}\phi_{\rm a}}a^\dagger+\mathrm{e}^{\mathrm{i}\phi_{\rm b}}b^\dagger\right)|00\rangle_{\rm A0,B0}=\left(a^\dagger+\mathrm{e}^{\mathrm{i}\phi_\delta}b^\dagger\right)|0\rangle, \tag{1}$$

其中, $a^\dagger$ 和 $b^\dagger$ 分别为 A 端和 B 端的生成算符.

信道对生成算符的影响可以表示为

$$\begin{aligned} a^\dagger &\to \sqrt{\eta_{\rm a}}a^\dagger+\sqrt{1-\eta_{\rm a}}s^\dagger,\\ b^\dagger &\to \sqrt{\eta_{\rm b}}b^\dagger+\sqrt{1-\eta_{\rm b}}t^\dagger, \end{aligned} \tag{2}$$

其中, $s^\dagger$ 和 $t^\dagger$ 分别为 A 与 Charlie 之间信道 (后文简称 A 信道) 和 B 与 Charlie 之间信道 (后文简称 B 信道) 的特征算符.

经过信道后, 量子态可以表示为

$$\left(\sqrt{\eta_{\rm a}}a^\dagger+\mathrm{e}^{\mathrm{i}\phi_\delta}\sqrt{\eta_{\rm b}}b^\dagger+\sqrt{1-\eta_{\rm a}}s^\dagger+\mathrm{e}^{\mathrm{i}\phi_\delta}\sqrt{1-\eta_{\rm b}}t^\dagger\right)|0\rangle. \tag{3}$$

在 Charlie 处, 经过干涉后, 量子态可以表示为

$$\left(\frac{\sqrt{\eta_{\rm a}}+\mathrm{e}^{\mathrm{i}\phi_\delta}\sqrt{\eta_{\rm b}}}{\sqrt{2}}l^\dagger+\frac{\sqrt{\eta_{\rm a}}-\mathrm{e}^{\mathrm{i}\phi_\delta}\sqrt{\eta_{\rm b}}}{\sqrt{2}}r^\dagger+\sqrt{1-\eta_{\rm a}}s^\dagger+\mathrm{e}^{\mathrm{i}\phi_\delta}\sqrt{1-\eta_{\rm b}}t^\dagger\right)|0\rangle, \tag{4}$$

其中, $l^\dagger$ 和 $r^\dagger$ 分别为图 1 中 L 检测器和 R 检测器的生成算符.

因此, 对于单光子情况, 不同的检测结果出现的概率如下:

$$\begin{aligned} p_0^1 &= 1-\frac{\eta_{\rm a}+\eta_{\rm b}}{2},\\ p_{\rm l}^1 &= \frac{\eta_{\rm a}+\eta_{\rm b}+2\sqrt{\eta_{\rm a}\eta_{\rm b}}\cos\phi_\delta}{4}\\ &= \left(\frac{\sqrt{\eta_{\rm a}}-\sqrt{\eta_{\rm b}}}{2}\right)^2+\sqrt{\eta_{\rm a}\eta_{\rm b}}\cos^2\frac{\phi_\delta}{2},\\ p_{\rm r}^1 &= \frac{\eta_{\rm a}+\eta_{\rm b}-2\sqrt{\eta_{\rm a}\eta_{\rm b}}\cos\phi_\delta}{4}\\ &= \left(\frac{\sqrt{\eta_{\rm a}}-\sqrt{\eta_{\rm b}}}{2}\right)^2+\sqrt{\eta_{\rm a}\eta_{\rm b}}\sin^2\frac{\phi_\delta}{2},\\ p_{\rm lr}^1 &= 0, \end{aligned} \tag{5}$$

其中 p_0^1 和 $p_{\rm lr}^1$ 分别表示 L 和 R 检测器都不响应和都响应的概率, $p_{\rm l}^1$ 和 $p_{\rm r}^1$ 分别表示只有 L 检测器响应和只有 R 检测器响应的概率.

对于 k 光子情况, 假设 k 个光子相互独立:

$$\begin{aligned} p_0^k &= \left(p_0^1\right)^k,\\ p_{\rm l}^k &= \left(p_0^1+p_{\rm l}^1\right)^k-\left(p_0^1\right)^k,\\ p_{\rm r}^k &= \left(p_0^1+p_{\rm r}^1\right)^k-\left(p_0^1\right)^k,\\ p_{\rm lr}^k &= 1-p_0^k-p_{\rm l}^k-p_{\rm r}^k, \end{aligned} \tag{6}$$

其中 p_0^k 和 $p_{\rm lr}^k$ 分别表示 L 和 R 检测器都不响应和都响应的概率, $p_{\rm l}^k$ 和 $p_{\rm r}^k$ 分别表示只有 L 检测器响应和只有 R 检测器响应的概率.

考虑暗计数的影响, 检测器的响应概率可以表示为

$$\begin{aligned} P_0^k &= (1-p_{\rm d})^2p_0^k,\\ P_{\rm L}^k &= (1-p_{\rm d})^2p_{\rm l}^k+p_{\rm d}(1-p_{\rm d})\left(p_0^k+p_{\rm l}^k\right),\\ P_{\rm R}^k &= (1-p_{\rm d})^2p_{\rm r}^k+p_{\rm d}(1-p_{\rm d})\left(p_0^k+p_{\rm r}^k\right),\\ P_{\rm LR}^k &= (1-p_{\rm d})^2p_{\rm lr}^k+p_{\rm d}(1-p_{\rm d})\left(p_{\rm l}^k+p_{\rm r}^k+2p_{\rm lr}^k\right)+p_{\rm d}^2, \end{aligned} \tag{7}$$

类似地, P_0^k 和 $P_{\rm LR}^k$ 分别表示 L 和 R 检测器都不响应和都响应的概率, $P_{\rm L}^k$ 和 $P_{\rm R}^k$ 分别表示只有 L 检测

器响应和只有 R 检测器响应的概率.

对于输入为相干态时, A 与 B 编码后再经信道传输得到的量子态分别为$\left|\sqrt{\frac{\mu\eta_{\rm a}}{2}}{\rm e}^{{\rm i}\phi_{\rm a}}\right\rangle$和$\left|\sqrt{\frac{\mu\eta_{\rm b}}{2}}{\rm e}^{{\rm i}\phi_{\rm b}}\right\rangle$, 通过 Charlie 端分束器后量子态变为

$$\begin{aligned}|\alpha_{\rm L}\rangle &= \left|\frac{\sqrt{\mu\eta_{\rm a}}}{2}{\rm e}^{{\rm i}\phi_{\rm a}}+\frac{\sqrt{\mu\eta_{\rm b}}}{2}{\rm e}^{{\rm i}\phi_{\rm b}}\right\rangle \\ &= \left|\left(\frac{\sqrt{\mu\eta_{\rm a}}}{2}+\frac{\sqrt{\mu\eta_{\rm b}}}{2}{\rm e}^{{\rm i}\phi_\delta}\right){\rm e}^{{\rm i}\phi_{\rm a}}\right\rangle, \\ |\alpha_{\rm R}\rangle &= \left|\frac{\sqrt{\mu\eta_{\rm a}}}{2}{\rm e}^{{\rm i}\phi_{\rm a}}-\frac{\sqrt{\mu\eta_{\rm b}}}{2}{\rm e}^{{\rm i}\phi_{\rm b}}\right\rangle \\ &= \left|\left(\frac{\sqrt{\mu\eta_{\rm a}}}{2}-\frac{\sqrt{\mu\eta_{\rm b}}}{2}{\rm e}^{{\rm i}\phi_\delta}\right){\rm e}^{{\rm i}\phi_{\rm a}}\right\rangle. \end{aligned} \tag{8}$$

检测器有效响应的概率可以分为以下两种情况:

$$\begin{aligned}&P_\mu(\bar{\rm L}) = (1-p_{\rm d})\exp\left(-|\alpha_{\rm L}|^2\right) = (1-p_{\rm d}) \\ &\times\exp\left[-\left(\frac{\eta_{\rm a}\mu}{4}+\frac{\eta_{\rm b}\mu}{4}+\frac{\sqrt{\eta_{\rm a}\eta_{\rm b}}\mu\cos(\phi_\delta)}{2}\right)\right], \end{aligned} \tag{9}$$

$$\begin{aligned}&P_\mu(\bar{\rm R}) = (1-p_{\rm d})\exp\left(-|\alpha_{\rm R}|^2\right) = (1-p_{\rm d}) \\ &\times\exp\left[-\left(\frac{\eta_{\rm a}\mu}{4}+\frac{\eta_{\rm b}\mu}{4}-\frac{\sqrt{\eta_{\rm a}\eta_{\rm b}}\mu\cos(\phi_\delta)}{2}\right)\right]. \end{aligned} \tag{10}$$

$P_\mu(\bar{\rm L})$表示 L 检测器不响应的概率, L 检测器响应的概率$P_\mu({\rm L}) = 1-P_\mu(\bar{\rm L})$, 类似地, $P_\mu(\bar{\rm R})$表示 R 检测器不响应的概率, R 检测器响应的概率$P_\mu({\rm R}) = 1-P_\mu(\bar{\rm R})$.

ϕ_δ 服从一定的概率分布, 要想得到上述各概率值, 需要对ϕ_δ进行积分. 在相位后补偿过程中, PM 协议会根据参考相位差给出一个补偿系数, 等价于参考相位差ϕ_0服从$[-\pi/M,\pi/M)$的均匀分布, 如果相位索引$j_{\rm a}=j_{\rm b}=0$, 全局相位分别为$\phi_{\rm a}$和$\phi_{\rm b}$, 那么$\phi_{\rm a}$和$\phi_{\rm b}$分别服从$[0,2\pi/M)$和$[\phi_0,2\pi/M+\phi_0)$的均匀分布, 因而$\phi_\delta=\phi_{\rm b}-\phi_{\rm a}$的概率密度函数可表示为

$$f_{\phi_\delta}^{\phi_0}(\phi) = \begin{cases}\left(\frac{M}{2\pi}\right)^2\left[\phi+\frac{2\pi}{M}-\phi_0\right], & \phi\in\left[\phi_0-\frac{2\pi}{M},\phi_0\right), \\ \left(\frac{M}{2\pi}\right)^2\left[-\phi+\frac{2\pi}{M}+\phi_0\right], & \phi\in\left[\phi_0,\phi_0+\frac{2\pi}{M}\right), \\ 0, & \text{otherwise.}\end{cases} \tag{11}$$

3.2 计数率、增益和错误率

首先分析k光子计数率Y_k, 根据定义:

$$\begin{aligned}Y_k &= P_{\rm L}^k+P_{\rm R}^k \\ &\approx (1-p_{\rm d})\left\{\left[1-\frac{\left(\sqrt{\eta_{\rm a}}-\sqrt{\eta_{\rm b}}\right)^2}{4}\right]^k\right. \\ &\quad\left.+\left[1-\frac{\eta_a+\eta_b}{2}+\frac{\left(\sqrt{\eta_{\rm a}}-\sqrt{\eta_{\rm b}}\right)^2}{4}\right]^k\right\} \\ &\quad-2(1-p_{\rm d})^2\left(1-\frac{\eta_{\rm a}+\eta_{\rm b}}{2}\right)^k, \end{aligned} \tag{12}$$

其中, 式中约等于号处忽略了高阶ϕ_δ的影响, 令$\sin^2(\phi_\delta/2)=0$.

与Y_k进行相同的近似操作, 忽略高阶ϕ_δ的影响, 总增益Q_μ可别表示为

$$\begin{aligned}Q_\mu &= P_\mu({\rm L})P_\mu(\bar{\rm R})+P_\mu(\bar{\rm L})P_\mu({\rm R}) \\ &\approx (1-p_{\rm d}){\rm e}^{-\left(\frac{\sqrt{\eta_{\rm a}\mu}-\sqrt{\eta_{\rm b}\mu}}{2}\right)^2} \\ &\quad+(1-p_{\rm d}){\rm e}^{-\left(\frac{\sqrt{\eta_{\rm a}\mu}+\sqrt{\eta_{\rm b}\mu}}{2}\right)^2} \\ &\quad-2(1-p_{\rm d})^2{\rm e}^{-\left(\frac{\eta_{\rm a}\mu+\eta_{\rm b}\mu}{2}\right)}. \end{aligned} \tag{13}$$

k光子错误率$e_k^Z(\phi_\delta)$可以表示为

$$\begin{aligned}e_k^Z(\phi_\delta) &= \frac{P_{\rm R}^k}{Y_k} = \frac{(1-p_{\rm d})p_{\rm r}^k+p_{\rm d}(1-p_{\rm d})p_0^k}{Y_k} = \\ &\frac{(1-p_{\rm d})\left[1-\frac{\eta_{\rm a}+\eta_{\rm b}}{2}+\left(\frac{\sqrt{\eta_{\rm a}}-\sqrt{\eta_{\rm b}}}{2}\right)^2+\sqrt{\eta_{\rm a}\eta_{\rm b}}\sin^2\frac{\phi_\delta}{2}\right]^k}{Y_k} \\ &-\frac{(1-p_{\rm d})^2[1-(\eta_{\rm a}+\eta_{\rm b})/2]^k}{Y_k}. \end{aligned} \tag{14}$$

k光子平均错误率e_k^Z可以表示为

$$e_k^Z = \frac{M}{2\pi}\int_{-\pi/M}^{\pi/M}{\rm d}\phi_0\int_{-3\pi/M}^{3\pi/M}{\rm d}\phi f_{\phi_\delta}^{\phi_0}(\phi)e_k^Z(\phi). \tag{15}$$

联合 (11) 式、(14) 式、(15) 式, 令$k=1$可得:

$$\begin{aligned}e_1^Z &= \frac{M}{2\pi}\int_{-\pi/M}^{\pi/M}{\rm d}\phi_0\int_{-3\pi/M}^{3\pi/M}{\rm d}\phi f_{\phi_\delta}^{\phi_0}(\phi)e_1^Z(\phi) \\ &= \frac{p_{\rm d}\left(1-\frac{\eta_{\rm a}+\eta_{\rm b}}{2}\right)+\frac{\eta_{\rm a}+\eta_{\rm b}}{2}e_\delta}{\frac{\eta_{\rm a}+\eta_{\rm b}}{2}+2p_{\rm d}\left(1-\frac{\eta_{\rm a}+\eta_{\rm b}}{2}\right)}, \end{aligned} \tag{16}$$

其中, e_δ定义如下:

$$e_\delta = \frac{1}{2}-\frac{\sqrt{\eta_{\rm a}\eta_{\rm b}}}{\eta_{\rm a}+\eta_{\rm b}}\frac{M^3}{\pi^3}\sin^3\left(\frac{\pi}{M}\right). \tag{17}$$

采用与经典 PM 协议类似的近似方法, 可得e_k^Z:

$$e_k^Z \approx \frac{1}{Y_k}\left\{p_{\rm d}\left(1-\frac{\eta_{\rm a}+\eta_{\rm b}}{2}\right)^k + e_\delta\left[1-\left(1-\frac{\eta_{\rm a}+\eta_{\rm b}}{2}\right)^k\right]\right\}. \tag{18}$$

量子比特误码率 $E_\mu^Z(\phi_\delta)$ 可表示为

$$E_\mu^Z(\phi_\delta) = \frac{P_\mu(\bar{\rm L})P_\mu({\rm R})}{P_\mu(\bar{\rm L})P_\mu({\rm R})+P_\mu({\rm L})P_\mu(\bar{\rm R})}$$
$$\approx \frac{1}{Q_\mu}\exp\left[-\left(\frac{\eta_{\rm a}\mu+\eta_{\rm b}\mu}{2}\right)\right]$$
$$\times\left\{\left[\frac{\eta_{\rm a}\mu+\eta_{\rm b}\mu}{4}-\frac{\sqrt{\eta_{\rm a}\eta_{\rm b}}\mu\cos(\phi_\delta)}{2}\right]+p_{\rm d}\right\}. \tag{19}$$

进一步对 $E_\mu^Z(\phi_\delta)$ 进行积分, 可以得到平均量子比特误码率 E_μ^Z:

$$E_\mu^Z = \frac{M}{2\pi}\int_{-\pi/M}^{\pi/M}{\rm d}\phi_0\int_{-3\pi/M}^{3\pi/M}E_\mu^Z(\phi_\delta)f_{\phi_\delta}^{\phi_0}(\phi)\,{\rm d}\phi$$
$$= \exp\left[-\left(\frac{\eta_{\rm a}\mu+\eta_{\rm b}\mu}{2}\right)\right]\left[\frac{\eta_{\rm a}\mu+\eta_{\rm b}\mu}{4}\right.$$
$$\left.-\frac{M^3}{\pi^3}\frac{\sqrt{\eta_{\rm a}\eta_{\rm b}}}{2}\mu\sin^3\left(\frac{\pi}{M}\right)+p_{\rm d}\right]. \tag{20}$$

根据文献 [8], 密钥生成率公式如下:

$$R_{\rm PM} \geqslant \frac{2}{M}Q_\mu[1-fH(E_\mu^Z)-H(E_\mu^{\rm X})], \tag{21}$$

其中, M 为相位分片数, 通常情况下 M 一般取 16, $2/M$ 为筛选因子, f 为实际纠错算法效率. $H(x)=-x\log_2 x-(1-x)\log_2(1-x)$ 为香农信息熵函数. $E_\mu^{\rm X}$ 表示相位错误率, 需进行估计, 根据文献 [8] 可得:

$$E_\mu^{\rm X} \leqslant q_0 e_0^z + \sum_{k=0}^{\infty}e_{2k+1}^Z q_{2k+1} + \left(1-q_0-\sum_{k=0}^{\infty}q_{2k+1}\right), \tag{22}$$

其中, q_k 表示检测到的信号中 $|k\rangle$ 光子态信号所占比率, 可以写为

$$q_k = P^\mu(k)(Y_k/Q_\mu), \tag{23}$$

其中 $P^\mu(k)$ 表示信源强度为 μ 时发送 $|k\rangle$ 光子态的概率, 由信源决定.

4 仿真分析

假设光源为弱相干态光源, 光子数服从泊松分布, 仿真参数见表 1[8] .

表 1 主要仿真参数

Table 1. The Main parameters in numerical simulations.

参数	暗记数 $p_{\rm d}$	纠错效率 f	相位分片数 M	置信度 $1-\theta$
取值	8×10^{-8}	1.15	16	$1-5.73\times10^{-7}$

4.1 信道非对称性对系统的影响

4.1.1 信道非对称性对相关参数的影响

假设 A 和 B 之间信道的总衰减为 10 dB, 即 $-10\lg(\eta_{\rm a}\eta_{\rm b})=10$, 并以其信道衰减的差值 $\alpha_\delta=-10\lg(\eta_{\rm a}/\eta_{\rm b})$ 来衡量信道的不对称程度.

单光子计数率 Y_1 和全局增益 Q_μ 随 α_δ 变化的曲线如图 2 所示. 图 2 中, A 和 B 信道衰减相同时, 即横坐标为 0 处, Y_1 和 Q_μ 均取最小值, 随着 α_δ 绝对值的增大, Y_1 和 Q_μ 也会增大. 这是因为, 信道总衰减不变时, 信道差异越大, 其中一方必然与 Charlie 之间衰减更小, 从而使得一方光子到达 Charlie 端的概率更大, 使得 Y_1 和 Q_μ 增大. 从这两个参数看, 信道的非对称有利于提高接收端的有效检测数量, 对提高密钥生成率具有积极贡献. 但是这不能抵消信道非对称导致错误率升高所带来的影响.

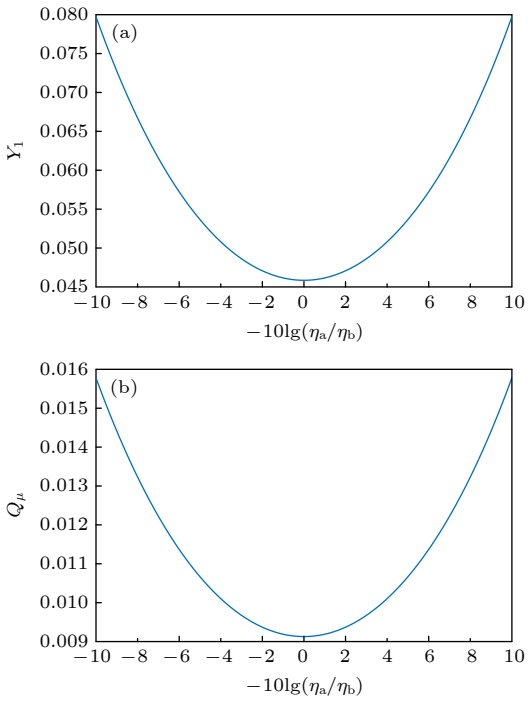

图 2 单光子计数率和全局增益随信道衰减差变化情况 (a) 单光子计数率 Y_1; (b) 全局增益 Q_μ

Fig. 2. Variation of the single-photon yield and total gain with channel attenuation difference: (a) Single photon counting rate Y_1; (b) global gain Q_μ.

量子比特误码率 E_μ^Z 和相位错误率 $E_\mu^{\rm X}$ 随 α_δ 变化情况如图 3 所示. E_μ^Z 和 $E_\mu^{\rm X}$ 均在信道完全对称时取得最小值, 随着信道差异增大, E_μ^Z 和 $E_\mu^{\rm X}$ 逐渐增

大, 对最终密钥生成率产生不利影响. 信道的非对称性使得系统非对准错误激增, 这也导致 A 和 B 信道差最大时, E_μ^Z 的值上升了 200 倍以上. 信道的非对称性同样会对系统相位错误产生影响, 但是基于 PM 协议相位后补偿策略, 这种影响被减弱, 相比于对称情况, 最坏情况下, E_μ^{X} 增大 1 倍左右.

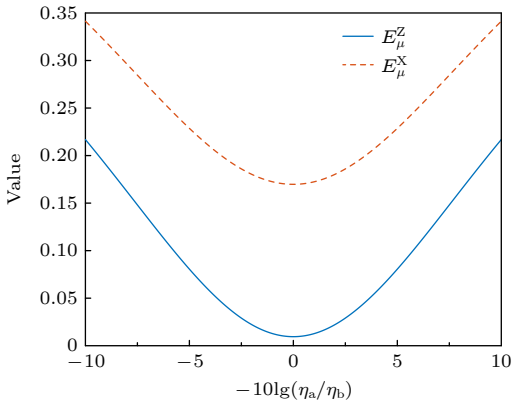

图 3 量子比特误码率和相位错误率随信道衰减差的变化

Fig. 3. Variation of QBER and phase error rate with channel attenuation difference.

Q_μ, E_μ^Z 和 E_μ^{X} 直接对密钥生成率产生影响, 在其综合作用下, 密钥随信道差异 α_δ 变化情况如图 4 所示.

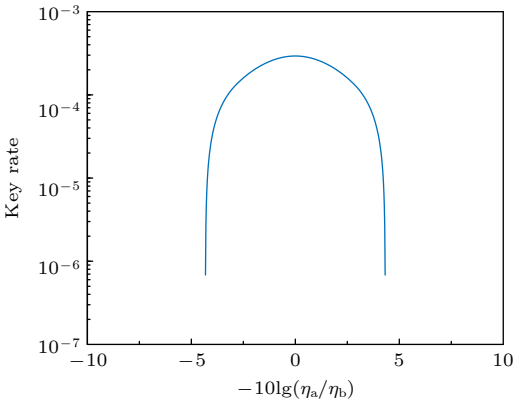

图 4 PM 协议密钥生成率随信道衰减差的变化

Fig. 4. Variation of PM protocol key generation rate with channel attenuation difference.

可以看出, 在 A 和 B 信道总衰减一定的情况下, 密钥生成率会随着 α_δ 的绝对值增大而减小, 且下降速度越来越快. 在 α_δ 绝对值大于 4 dB 时, 系统无法再生成密钥. 这说明, 虽然信道的非对称增加了有效响应, 但是误码率也随之增大, 最终系统密钥生成率还是会因信道的不对称而下降. 需要说明的是, 并不能通过增大信道衰减较大一端的发送信号光强来补偿信道的衰减, 这样会破坏信源端量子态制备的约束, 导致系统存在安全隐患.

4.1.2 信道非对称对密钥生成率的影响

假设 A 和 B 到 Charlie 的信道衰减差 α_δ 分别为 0, 3, 4, 6 dB 时, 密钥生成率随 A 和 B 信道总衰减的变化情况如图 5 所示.

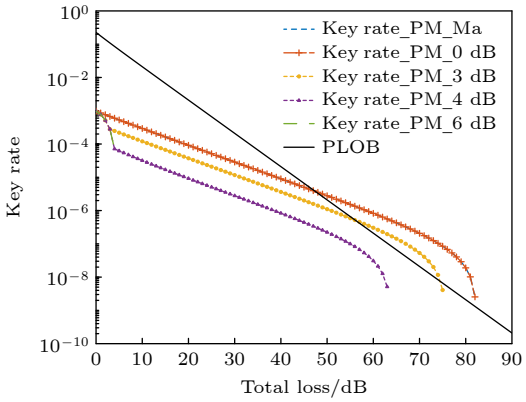

图 5 不同信道差异时密钥生成率随信道总衰减的变化

Fig. 5. Variation of key generation rate with total channel attenuation for different channel differences.

图 5 给出了 5 种不同的情况下密钥生成率的图像, 粗的虚线表示原始 PM 协议, 带“+”标记的点划线表示基于非对称 PM 协议且 $\alpha_\delta = 0$ dB 的情况, 带“圆圈”标记的点线表示 $\alpha_\delta = 3$ dB 时情况, 带“三角形”标记的点线表示 $\alpha_\delta = 4$ dB 时情况, 细虚线表示 $\alpha_\delta = 6$dB 时情况, 实线表示 PLOB 界.

从图 5 可以看出, 经典 PM 协议与 α_δ 为 0 dB 时非对称 PM 协议密钥生成率曲线重合, 这说明本章提出的非对称 PM 协议在信道对称时可以退化到原始 PM 协议, 进一步说明了非对称 PM 协议的合理性. 相对于对称情况, 当 α_δ 为 3 dB 时, 信道总衰减小于 70 dB 时, 密钥生成率下降约 4 dB, 能生成密钥的最大信道总衰减减小 7 dB, 且只有在信道总衰减为 56—74 dB 这一较小范围时才能突破 PLOB 界; 当 α_δ 为 4 dB 时, 系统已无法突破 PLOB 界, 密钥生成率下降约 10 dB, 能生成密钥的最大信道总衰减减小 20 dB; 当 α_δ 为 6 dB 时, 其图像在信道总衰减大于 4 dB 时截断, 尽管系统信道总衰减较小, 但由于信道的非对称性导致无法生成密钥; 图中 α_δ 取 3, 4, 6 dB 时的图像在信道总衰减为 0—4 dB 时有重叠部分, 这是因为当信道总衰减没有达到信道衰减差时, 仅增大 A 信道衰减,

保持 B 信道衰减为 0 dB 不变, 因此α_δ不同时的图像在起始段处理相同, 图像会有重叠.

总体来看, 信道的非对称性对密钥生成率影响较大, 两条信道差异过大时, 这种差异取代信道衰减成为制约系统性能的主要因素, 甚至使系统在信道总衰减较小的情况下也无法生成密钥.

4.2 实际应用中非对称 PM 协议

4.2.1 诱骗态数量非对称 PM 协议性能的影响

图 6(a), (b) 分别所示为二诱骗态和三诱骗态非对称 PM 协议在不同信道传输率时密钥生成率的等高线图, 密钥生成率从中间向两边逐渐减小, 最终形成两条明显的边界, 表明随着信道之间差异的增大, 密钥生成率逐渐减小直至无法生成密钥,

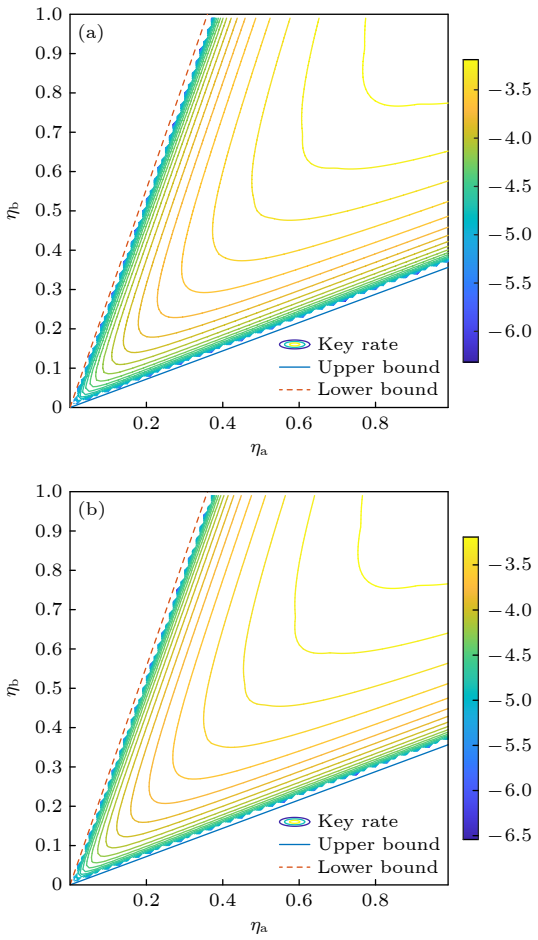

图 6 不同诱骗态数量时密钥生成率随信道传输效率变化等高线图 (a) 二诱骗态; (b) 三诱骗态

Fig. 6. The contour plot of key generation rate as a function of channel transmission efficiency for different numbers of decoy states: (a) Two-decoy-state; (b) three-decoy-state.

与图 4 和图 5 的结论可相互印证. 同样, 理想情况下非对称 PM 协议密钥生成率的等高线图也具有明显的边界, 图中用虚线和实线分别表示其上下边界 (后文简称为理想密钥生成率边界). 对比可知, 二、三诱骗态方案的密钥生成率边界都十分接近理想情况, 没有使得相应的边界显著收缩, 这说明诱骗态方案对非对称 PM 协议仍然有效; 此外, 还可说明诱骗态的数量对系统容忍信道非对称的程度并无明显影响. 因此在选择诱骗态方案时, 可以不考虑信道非对称度的约束.

图 7 所示为α_δ分别为 0 dB 和 4 dB 时, 二诱骗态和三诱骗态非对称 PM 协议密钥生成率随信道总衰减的变化情况. 虚线表示理想对称情况下非对称 PM 协议密钥生成率. 在$\alpha_\delta = 0$ dB时, 二诱骗态和三诱骗态非对称 PM 协议密钥生成率差异极小, 且都十分接近极限值, 但是当$\alpha_\delta = 4$ dB时, 三诱骗态 PM 协议明显优于二诱骗态 PM 协议, 特别是在信道总衰减超过 50 dB 时, 密钥生成率提高 65% 以上, 且能生成密钥的最大信道总衰减提升 3 dB. 对于非对称信道情况下, 采用三诱骗态可以有效提升系统的性能.

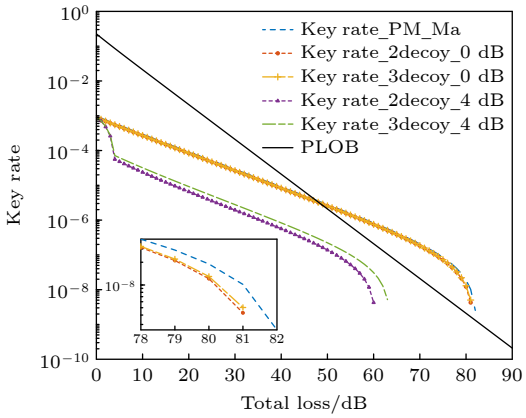

图 7 不同诱骗态数量时密钥生成率随信道总衰减变化情况

Fig. 7. Variation of key generation rate with total channel attenuation for different decoy states.

4.2.2 数据有限长对非对称 PM 协议影响

考虑统计波动, 采用高斯分析对基于三诱骗态的非对称 PM 协议进行分析. 数据长度较大时, 不同信源强度发送概率对系统性能影响极小, 不失一般性, 仅对信源强度的取值进行全局搜索优化, 各强度发送概率$p_\mu = p_{v1} = p_{v2} = p_\omega = 0.25$. 不同数

据长度下, 非对称 PM 协议密钥生成率等高线图如图 8 所示.

图 8 分别表示数据长度 $N = 10^8$, 10^{10}, 10^{12}, 10^{16}时, 密钥生成率情况, 子图中直线为理想密钥生成率边界. 对比各子图可以看出, 数据长度小于 10^{10}时, 系统密钥生成率下降明显, 且边界收缩幅度较大, 对信道的非对称性容忍度进一步降低, 在数据长度较短如10^8时, 需额外关注信道非对称性对系统产生的影响. 随着数据长度的增加, 密钥生成率逐渐逼近理想情况的边界.

不同信道衰减差情况下, 数据长度对密钥生成率的影响如图 9 所示. 图 9 中, 分别给出α_δ在 0 dB 和 2 dB, 数据长度 N为10^{10}, 10^{12}, 10^{16}时密钥生成率图像. 总体来看, 信道差一定, 密钥生成率会随着数据长度的减小而减小. 数据长度达到10^{16}时, 密钥生成率接近理想情况. 当α_δ为 0 dB 时, N取 10^{10}系统在信道总衰减为 56 dB 时刚好达到 PLOB 界, 而当α_δ为 2 dB 时, N需取10^{12}, 系统才能在信道总衰减为 62 dB 时达到 PLOB 界, 无法超过 PLOB 界, 没能体现出 PM 协议的优势. 当系统信道总衰减小于 55 dB时, α_δ为 0 dB, N取10^{10}时, 密钥生成率仍然比α_δ为 2 dB, N取10^{16}时要大, 可见在信道总衰减较小时, 信道衰减差对密钥生成率影响较大; 当系统信道总衰减大于 55 dB 时, α_δ为 0 dB, N取10^{10}时的密钥生成率急剧减小, 相对α_δ为 2 dB, N取大于10^{12}的情况无优势, 但相对α_δ为 2 dB, N取10^{10}的情况仍然有较大优势; 当α_δ为 0 dB, N取大于10^{12}时, 密钥生成率已超过α_δ为 2 dB 的极限. 上述情况说明, 信道衰减差导致的性能下降, 只有在数据长度较小、信道总衰减较大时, 才能在一定程度上通过增大数据长度来弥补, 且这种提升上限较低.

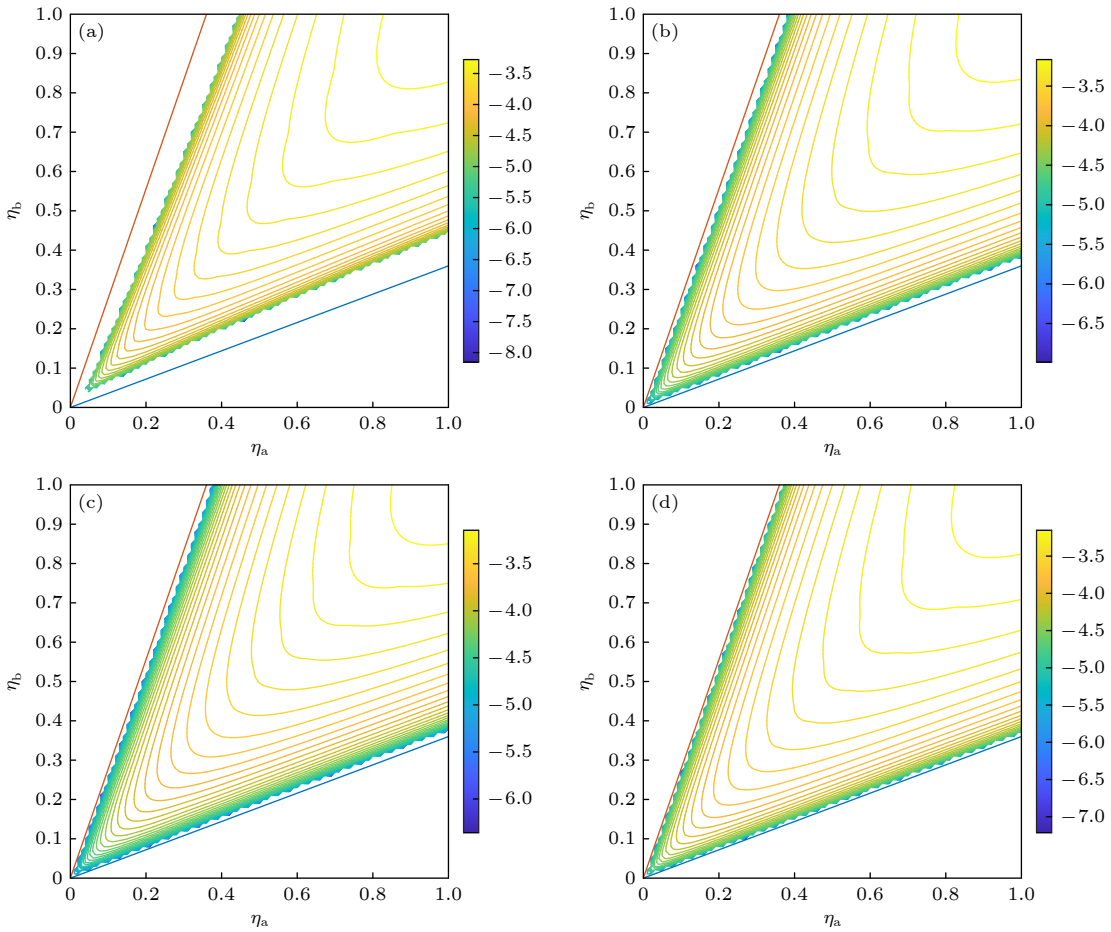

图 8 不同数据长度情况下密钥生成率随信道传输率变化图像 (a) $N = 10^8$; (b) $N = 10^{10}$; (c) $N = 10^{12}$; (d) $N = 10^{16}$

Fig. 8. Image of key generation rate changing with channel transmission rate under different data lengths: (a) $N = 10^8$; (b) $N = 10^{10}$; (c) $N = 10^{12}$; (d) $N = 10^{16}$.

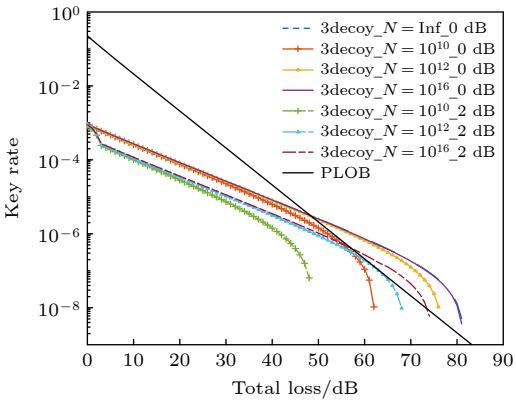

图 9 不同信道衰减差情况下数据长度对密钥生成率的影响

Fig. 9. Effect of data length on key rate under different channel attenuation differences.

5 结 论

本文针对实际中密钥分发双方信道常处于非对称状态这一现象, 提出了非对称 PM 协议, 建立了相关参数仿真模型, 推导了非对称 PM 协议总增益和量子比特误码率公式, 从诱骗态方案、统计波动分析等两方面对非对称 PM 协议进行了分析. 仿真结果表明: 信道的非对称性会对密钥生成率产生较大影响, 信道差异越大, 密钥生成率越小, 通过光衰减器调节信道衰减, 保持信道之间的对称, 对提升系统密钥生成率具有积极作用; 对于信道差异较大的情况, 三诱骗态比二诱骗态性能更优; 数据有限长对非对称 PM 协议同样有不利影响, 数据长度越小, 密钥生成率越小, 且密钥生成率边界会收缩, 当数据长度大于 10^{12} 时, 继续增大数据长度并不会对系统的性能有明显提升. 在 PM 协议的实际应用中, 充分考虑非对称信道的影响具有重要意义.

参考文献

[1] Bennett C H, Brassard G 1984 *Process IEEE International Conference Computer System Signal Processing* Bangalore, India, December 9–12, 1984 pp175–179
[2] Lo H K, Ma X, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[3] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[4] Sasaki T, Yamamoto Y, Koashi M 2014 *Nature* **509** 475
[5] Takeoka M, Guha S, Wilde M M 2014 *Nat. Commun.* **5** 5235
[6] Pirandola S, Laurenza R, Ottaviani C, Banchi L 2017 *Nat. Commun.* **8** 15043
[7] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400
[8] Ma X F, Zeng P, Zhou H Y 2018 *Phys. Rev. X* **8** 031043
[9] Xu F, Ma X, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[10] Lin J, Lütkenhaus N 2018 *Phys. Rev. A* **98** 042332
[11] Zeng P, Wu W, Ma X 2020 *Phys. Rev. Appl.* **13** 064013
[12] Shen Z, Chen G, Wang L, Li W, Mao Q, Zhao S 2022 *Laser Phys. Lett.* **19** 095202
[13] Yu B, Mao Q P, Zhu X M, Yu Y, Zhao S M 2021 *Phys. Lett. A* **418** 127702
[14] Yu Y, Wang L, Zhao S, Mao Q 2022 *Europhys. Lett.* **138** 28001
[15] Cui W, Song Z, Huang G, Jiao R 2022 *Quantum Inf. Process.* **21** 313
[16] Han L, Yu Y, Lu W, Xue K, Li W, Zhao S 2022 *Quantum Inf. Process.* **22** 37
[17] Li W T, Wang L, Li W, Zhao S M 2022 *Chin. Phys. B* **31** 050310
[18] Fang X T, Zeng P, Liu H, Zou M, Wu W, Tang Y L, Sheng Y J, Xiang Y, Zhang W, Li H, Wang Z, You L, Li M J, Chen H, Chen Y A, Zhang Q, Peng C Z, Ma X, Chen T Y, Pan J W 2020 *Nat. Photonics* **14** 422
[19] Ma H Q, Han Y, Dou T, Li P 2023 *Chin. Phys. B* **32** 020304
[20] Wang W, Xu F, Lo H K 2019 *Phys. Rev. X* **9** 041012
[21] Yu Y, Wang L, Zhao S, Mao Q 2021 *13 th* International Conference on Wireless Communications and *Signal Processing* Changsha, China, October 20, 2021 pp1–4
[22] Lo H K, Chau H F 1999 *Science* **283** 2050
[23] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[24] Wang W, Lo H K 2020 *New J. Phys.* **22** 013020

Asymmetric channel phase matching quantum key distribution

Zhou Jiang-Ping Zhou Yuan-Yuan † Zhou Xue-Jun

(*College of Electronic Engineering, Naval University of Engineering, Wuhan* 430033, *China*)

(Received 23 April 2023; revised manuscript received 17 May 2023)

Abstract

The phase-matching protocol is a practical and promising protocol that can surpass the linear key generation rate boundary. However, classical phase-matching quantum key distribution requires the channel attenuation between communicating parties to be symmetric. In practice, channels used are often asymmetric, owing to geographical reasons in a quantum key distribution network. To enhance the practicality of phase-matching, this paper proposes an asymmetric phase-matching protocol based on the classical framework and establishes a relevant mathematical simulation model to study the influence of channel asymmetry on its performance. The simulation results show that channel asymmetry significantly affects the count rate, error rate, gain, and quantum bit error rate (QBER), ultimately, system performance. As the channel attenuation difference increases, the system performance decreases and the rate of decrease accelerates. Key generation becomes impossible when the channel attenuation difference exceeds 4 dB. Although the decoy-state scheme cannot change the system's tolerance to channel attenuation difference, when the channel attenuation difference is large, the increasing of the number of decoy states significantly can improve system performance, with a three-decoy-state phase-matching protocol outperforming a two-decoy-state protocol. Considering the limited data length, the system performance is improved as the data length increases, and the tolerance to channel attenuation differences gradually increases. When the data length exceeds 10^{12}, this improvement does not continue any more. The system cannot break through the boundary of linear key generation rate when the channel attenuation difference is 2 dB and the data length is less than 10^{12}. Comparing with symmetric channels, the system performance improvement is very significant under asymmetric channel conditions as the data length increases.

Keywords: quantum key distribution, phase matching, asymmetric channel, channel attenuation difference

PACS: 03.67.Dd, 03.67.Ac, 03.67.Hk **DOI:** 10.7498/aps.72.20230652

† Corresponding author. E-mail: EPJZYY@aliyun.com

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

非对称信道相位匹配量子密钥分发

周江平　周媛媛　周学军

Asymmetric channel phase matching quantum key distribution

Zhou Jiang-Ping　Zhou Yuan-Yuan　Zhou Xue-Jun

引用信息 Citation: Acta Physica Sinica, 72, 140302 (2023)　DOI: 10.7498/aps.72.20230652
在线阅读 View online: https://doi.org/10.7498/aps.72.20230652
当期内容 View table of contents: http://wulixb.iphy.ac.cn

您可能感兴趣的其他文章
Articles you may be interested in

光纤偏振编码量子密钥分发系统荧光边信道攻击与防御
Eavesdropping and countermeasures for backflash side channel in fiber polarization-coded quantum key distribution
物理学报. 2019, 68(13): 130301　https://doi.org/10.7498/aps.68.20190464

标记单光子源在量子密钥分发中的应用
Overview of applications of heralded single photon source in quantum key distribution
物理学报. 2022, 71(17): 170304　https://doi.org/10.7498/aps.71.20220344

基于混合编码的测量设备无关量子密钥分发的简单协议
A simple protocol for measuring device independent quantum key distribution based on hybrid encoding
物理学报. 2020, 69(19): 190301　https://doi.org/10.7498/aps.69.20200162

基于峰值补偿的连续变量量子密钥分发方案
Continuous-variable quantum key distribution based on peak-compensation
物理学报. 2021, 70(11): 110302　https://doi.org/10.7498/aps.70.20202073

基于量子催化的离散调制连续变量量子密钥分发
Discrete modulation continuous-variable quantum key distribution based on quantum catalysis
物理学报. 2020, 69(6): 060301　https://doi.org/10.7498/aps.69.20191689

参考系波动下的参考系无关测量设备无关量子密钥分发协议
Reference-frame-independent measurement-device-independent quantum key distribution under reference frame fluctuation
物理学报. 2019, 68(24): 240301　https://doi.org/10.7498/aps.68.20191364