相位匹配量子密钥分发协议统计波动分析

周江平，周媛媛*，周学军，聂 宁

(海军工程大学电子工程学院 武汉 430000)

【摘要】相位匹配协议是双场量子密钥分发协议的一种，能突破密钥容量限制且安全性得到了理论和实践的证明。针对实际应用中数据有限长效应产生的不良影响，系统地分析了相位匹配协议统计波动性能；利用高斯分析和切诺夫–霍夫丁界等统计波动分析方法，结合线性规划对相关参数进行估计，分别对不同数据长度情况下三诱骗态及二诱骗态相位匹配协议的性能进行了仿真分析。仿真结果表明：考虑统计波动的相位匹配协议仍能突破线性密钥容量的限制，在数据长度达到 10^{16} 量级时，密钥生成率和最大安全传输距离均接近理想值；在数据长度小于等于 10^{13} 时，增加诱骗态并不能显著提升相位匹配协议性能；随着数据长度的增加，采用切诺夫–霍夫丁界系统性能逐渐趋近采用高斯分析法的系统性能。

关 键 词 诱骗态； 相位匹配协议； 量子密钥分发； 量子光学； 统计波动

中图分类号 O431.2 **文献标志码** A doi:10.12178/1001-0548.2022096

StatisticaL Fluctuation Analysis for Phase Matching Quantum Key Distribution

ZHOU Jiangping, ZHOU Yuanyuan*, ZHOU Xuejun, and NIE Ning

(College of Electronic Engineering, Naval University of Engineering Wuhan 430000)

Abstract The phase matching protocol, which can break through the limitation of key capacity and has been proved by theory and practice, is a kind of twin-field quantum key distribution protocol. Aiming at the adverse effects of the finite data length effect in practical applications, the statistical fluctuation performance of the phase matching protocol is systematically analyzed. Using Gaussian analysis, Chernoff-Hoeffding bounds, and other statistical fluctuation analysis methods, the performances of the three-decoy and two-decoy phase matching protocols under different data lengths were simulated and analyzed combined with linear programming to estimate the relevant parameters. The simulation results show that the phase matching protocol considering statistical fluctuation can still break through the limitation of linear key capacity. When the data length reaches the order of 10^{16}, the key generation rate and the maximum secure transmission distance are both close to ideal values. When the data length is less than or equal to 10^{13}, adding decoy states cannot significantly improve the performance of the phase-matching protocol. As the data length increases, the performance of the system using the Chernoff-Hoeffding bound gradually approaches the performance of the system using the Gaussian analysis method.

Key words decoy state; phase matching protocol; quantum key distribution; quantum optics; statistical fluctuations

量子密钥分发 (quantum key distribution, QKD) 以量子力学原理为基础，使得远距离合法通信双方 (Alice 和 Bob) 能够实现无条件安全密钥共享，是当前量子信息领域最成功的应用之一。在实际环境中，所使用的光源和设备等无法满足 QKD 理想模型的要求，窃听者可对此发动光子数分离攻击和边信道攻击，严重威胁 QKD 系统的安全。随着诱骗态协议[1]、测量设备无关 (measurement-device-independent, MDI) 协议[2]、循环差分相移 (round-robin differential phase shift, RRDPS) 协议[3]等 QKD 协议的提出，QKD 系统的安全性及实用性都得到了保障和改善。然而这些 QKD 协议在不使用可信中继情况下，始终难以突破线性密钥生成率边界 (pirandola-laurenza-ottaviani-banchi bound, PLOB) 的限制[4-5]，即密钥生成率R与信道传输效率η之间的关系为$R \leqslant O(\eta)$。这极大制约了 QKD 协议

收稿日期：2022－03－31；修回日期：2022－05－29

作者简介：周江平 (1989－)，男，博士，主要从事量子通信方面的研究.

*通信作者：周媛媛，E-mail：EPJZYY@aliyun.com

的实际应用。

2018 年，文献 [6] 提出了双场 (twin field, TF) 协议，TF 协议在不使用可信中继情况下，将R与η的关系由线性相关提升至平方根相关，即$R \leqslant O(\sqrt{\eta})$，突破了 PLOB 界，具有里程碑式的意义。TF 协议提出后，其相关的理论与实验都得到了巨大发展[7]，理论上相位匹配 (phase matching, PM)[8]、发送或者不发送 (sending-or-not-sending, SNS)[9] 及无相位后选择 (no phase post-selection, NPP)[10] 等协议从不同方向对 TF 协议进行了扩展；实验上通过对相关协议的参数优化设计、利用超低损耗光纤和单光子检测器等方法，多个实验系统已实现距离超过 500 km 的量子密钥分发[11-12]，其中基于 NPP 协议的实验最远可达 833 km。PM 协议采用相位编码对 TF 协议中的密钥生成进行具体化，信源端对相干态光源进行相位调制，测量端采用相位后补偿技术，具有稳定性好、抗干扰能力强、误比特率低等优势，相较其他 TF 变种协议具有更高的实用性。

在 PM 协议实际应用中，有一个问题急需解决[13-14]：用于提取密钥的数据长度有限，由此带来的统计波动会对系统性能产生较大影响[15-16]。文献 [8] 仅对无穷诱骗态情况进行了分析，没有考虑有限诱骗态情况，也没有考虑数据有限长带来的统计波动影响；文献 [17] 基于弱相干态光源提出了三诱骗态 PM 方案，并用切诺夫界进行了统计波动分析；文献 [18] 针对信源错误提出了四诱骗态 PM 方案，并用高斯分析[19] 进行了统计波动分析；文献 [20-21] 基于不同光源，对比了二诱骗态和三诱骗态 PM 协议性能，并用切诺夫界分别进行了统计波动分析。总的来看，当前对 PM 协议的研究中，大多关注信源的特性及诱骗态方案的设计，统计波动仅仅作为证明其所提出协议有效性的一环，缺少系统性研究。

本文基于光子数信道模型，利用切诺夫–霍夫丁界和高斯分析[22] 对二诱骗态及三诱骗态 PM 协议进行系统性统计波动分析，结合线性规划对相关参数进行估计，最后得出仿真结果并进行对比分析。

1　诱骗态 PM 协议

本文主要关注有限数据长对 PM 协议造成的统计波动影响，对 PM 协议的实际实现方式不作过多讨论。假设 Alice 和 Bob 使用弱相干态光源 (weak coherent state, WCS)，诱骗态 PM 协议可表述如下。

1) Alice 产生随机密钥$\kappa_{\mathrm{a}} \in \{0,1\}$，随机相位$\phi_{\mathrm{a}} \in [0,2\pi)$，随机选取光源脉冲强度$\mu_{\mathrm{a}} \in \{\mu/2, \mu_1/2, \mu_2/2, \cdots\}$，调制后发送至第三方 Eve，相干态脉冲可表示为$\left|\sqrt{\mu_{\mathrm{a}}}\exp(i(\phi_{\mathrm{a}}+\pi\kappa_{\mathrm{a}}))\right\rangle_{\mathrm{A}}$。Bob 产生的相干态脉冲也可类似表示。

2) 光脉冲到达不可信第三方 Eve，Eve 执行相干检测并记录探测器响应的结果，随后将该结果通报给 Alice 和 Bob。Alice 和 Bob 声明脉冲信号强度。

3) Alice 和 Bob 对发送的密钥比特进行筛选。若$\mu_{\mathrm{a}} \neq \mu_{\mathrm{b}}$，直接丢弃该比特，否则根据 Eve 的检测结果再进一步判断；若 Eve 有且仅有一个探测器响应，则保留该比特，若该响应的探测器为右侧探测器时，Bob 还需进行比特翻转操作。

4) 重复执行上述步骤若干次后得到原始密钥序列。对每一个比特，Alice 声明其随机相位的序号j_{a}，同时随机选取一定长度的比特序列公布其真实值，用以估计量子比特误码率 (quantum bit error rate, QBER)。Bob 根据 Alice 的声明对相位进行后补偿，而后筛选出$|j_{\mathrm{b}}-j_{\mathrm{a}}+j_{\mathrm{d}}| \bmod M$($M$为相位分片数) 为 0 或者$M/2$的比特保留 ($j_{\mathrm{d}}$为相位后补偿系数)，并在结果为$M/2$时对比特进行翻转。Bob 向 Alice 声明保留的密钥比特，Alice 同步保留相应比特。

5) Alice 和 Bob 根据信号强度将密钥序列分组，分析不同信号强度时的全局增益Q_{μ_n}和量子比特误码率$E^{\mathrm{Z}}_{\mu_n}$，同时估计相位错误率E^{X}_{μ}。

6) Alice 和 Bob 执行纠错和私密放大后得到最终密钥。

2　仿真模型

2.1　光子数信道模型

若 Alice 和 Bob 使用相位随机相干态光源，可用光子数信道模型来描述量子信道[1]。假设信源光子数满足泊松分布，系统全局增益和量子比特误码率可分别表示为：

$$\begin{aligned} Q_{\mu} &= \sum_{k=0}^{\infty}\frac{\mu^k}{k!}\exp(-\mu)Y_k \\ E^{\mathrm{Z}}_{\mu}Q_{\mu} &= \sum_{k=0}^{\infty}\frac{\mu^k}{k!}\exp(-\mu)e^{\mathrm{Z}}_{k}Y_k \end{aligned} \tag{1}$$

式中，μ为信源强度；Y_k为k光子态计数率；e^{Z}_{k}为k光子态计数错误率；Q_{μ}和E^{Z}_{μ}分别是全局增益和量

子比特误码率，可实际观测得到。

2.2 理想情况

为得到系统极限性能，假设无窃听及攻击，数据长度为无穷大，直接引用文献 [8] 附录中相关结论。全局增益、量子比特误码率如下：

$$\begin{aligned} Q_\mu &= 1-\exp(-\eta\mu)+2p_{\mathrm{d}}\exp(-\eta\mu) \\ E_\mu^{\mathrm{Z}}Q_\mu &= (p_{\mathrm{d}}+\eta\mu e_\delta)\exp(-\eta\mu) \end{aligned} \tag{2}$$

式中，η表示 Alice(Bob) 到 Eve 之间信道的传输率(考虑对称信道)；p_{d}表示检测器的暗计数；e_δ表示信号和暗计数同时引起检测器响应的错误概率：

$$e_\delta = \frac{\pi}{M}-\frac{M^2}{\pi^2}\sin^3\left(\frac{\pi}{M}\right) \tag{3}$$

相位错误率如下：

$$\begin{aligned} E_\mu^{\mathrm{X}} = &\sum_{k=0}^{\infty}q_{2k+1}e_{2k+1}^{\mathrm{Z}}+\sum_{k=0}^{\infty}q_{2k}\left(1-e_{2k}^{\mathrm{Z}}\right)\leqslant \\ &q_0e_0^{\mathrm{Z}}+\left(q_1e_1^{\mathrm{Z}}+q_3e_3^{\mathrm{Z}}+q_5e_5^{\mathrm{Z}}\right)+ \\ &(1-q_0-q_1-q_3-q_5) \end{aligned} \tag{4}$$

高阶项对最终结果影响很小，因而式 (4) 中第二步忽略光子数$k\geqslant 6$时的影响。上式中q_k表示k光子态对有效检测的贡献：

$$q_k = P^\mu(k)\frac{Y_k}{Q_\mu} = \frac{\mu^k}{k!}\exp(-\mu)\frac{Y_k}{Q_\mu} \tag{5}$$

此外，为计算系统在理想情况下的密钥生成率，还需要对k光子态计数率、k光子态信号比特误码率进行建模：

$$\begin{aligned} Y_k &= 1-(1-2p_{\mathrm{d}})(1-\eta)^k \\ e_k^{\mathrm{Z}}Y_k &= p_{\mathrm{d}}(1-\eta)^k+e_\delta\left[1-(1-\eta)^k\right] \end{aligned} \tag{6}$$

2.3 密钥生成率及参数估计

密钥生成率的最终公式如下[8]：

$$R_{\mathrm{PM}} = \frac{2}{M}Q_\mu\left[1-fH\left(E_\mu^{\mathrm{Z}}\right)-H\left(E_\mu^{\mathrm{X}}\right)\right] \tag{7}$$

式中，M是相位分片数；f是纠错效率；$H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$，为香农熵函数。

PM 协议后处理包括密钥纠错和私钥放大。密钥纠错依赖于观测值E_μ^{Z}，不需要额外处理；私密放大依赖于E_μ^{X}的估计值，结合式 (4)～式 (5) 可知，需要用诱骗态方法对e_k^{Z}和Y_k进行估计。求解密钥生成率 R 的问题可转化为在一定约束条件下求解E_μ^{X}最大值的问题，可表述为：

$$\max_{Y_k,e_k^{\mathrm{Z}}}(E_\mu^{\mathrm{X}})$$

约束条件为：

$$Q_{\mu_m} = \sum_{k=0}^{\infty}\frac{\mu_m^k}{k!}\exp(-\mu_m)Y_k \tag{8}$$

$$E_{\mu_m}^{\mathrm{Z}}Q_{\mu_m} = \sum_{k=0}^{\infty}\frac{\mu_m^k}{k!}\exp(-\mu_m)e_k^{\mathrm{Z}}Y_k \tag{9}$$

式中，$m=0,1,\cdots,n-1$，线性约束方程总数为 $2n$。

为了得到E_μ^{X}的最大值，可以分别估计Y_k的最小值和e_k^{Z}的最大值。而这两个问题都可以用线性规划来求解。式 (8)～式 (9) 中右侧均有无穷多项，需进一步简化。因为泊松分布中，随着k的增大，高阶项系数呈指数下降，可直接忽略高阶项而不会对最终分析结果产生明显影响。以式 (8) 为例，其右侧$k\geqslant l$所有项的和可表示为：

$$\theta(\mu,l) = 1-\sum_{k=0}^{l-1}\frac{\mu^k}{k!}\exp(-\mu)Y_k \tag{10}$$

令$Y_k=1$，可得$\theta(\mu,l)$的上边界$\theta^{\mathrm{U}}(\mu,l)$。根据经验取常用信号强度值，$\mu\in\{0.02,0.1,0.5,1\}$，在$l=6,\cdots,12$时，$\theta^{\mathrm{U}}(\mu,l)$仿真结果如图 1 所示。

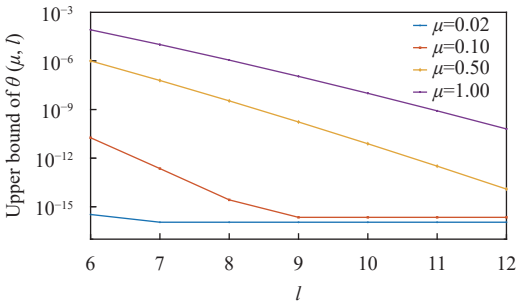

图 1 高阶项和的最大值

当信号强度为 1 和 0.5 时，9 阶以上的高阶项的和分别接近10^{-7}和10^{-10}，影响很小，可以忽略。因此本文对式 (8) 取前 9 项进行仿真计算，即$l=9$。同理，式 (9) 有类似结论。

统计波动会对参数的估计带来影响，分别用文献 [19] 中的高斯分析和文献 [23] 中的切诺夫–霍夫丁界来进行统计波动分析。高斯分析需假设信道统计波动满足正态分布，实际中这一条件难以满足，因此在面对相干攻击等特定威胁时，难以达到无条件安全要求，一般仅作为理论分析工具；切诺夫–霍夫丁界在实际应用中相对具有更高的安全性[22-24]。

1) 高斯分析

根据文献 [19] 结论，约束条件式 (8)、式 (9) 变为不等式组：

$$\hat{Q}_{\mu_m}(1-\beta_{\mathrm{q}}) \leqslant \sum_{k=0}^{8} \frac{\mu_m^k}{k!} \exp(-\mu_m) Y_k \leqslant \hat{Q}_{\mu_m}(1+\beta_{\mathrm{q}})$$
$$\hat{E}^{\mathrm{Z}}_{\mu_m} \hat{Q}_{\mu_m}(1-\beta_{\mathrm{eq}}) \leqslant \sum_{k=0}^{8} \frac{\mu_m^k}{k!} \exp(-\mu_m) e_k^{\mathrm{Z}} Y_k \leqslant \hat{E}^{\mathrm{Z}}_{\mu_m} \hat{Q}_{\mu_m}(1+\beta_{\mathrm{eq}}) \tag{11}$$

式中，$\hat{Q}_{\mu_m}$和$\hat{E}^{\mathrm{Z}}_{\mu_m}$是测量值；$\beta_{\mathrm{q}}$和$\beta_{\mathrm{eq}}$可由下式计算：

$$\beta_{\mathrm{q}} = \frac{n_\alpha}{\sqrt{N_{\mu_m}\hat{Q}_{\mu_m}}};\ \beta_{\mathrm{eq}} = \frac{n_\alpha}{\sqrt{N_{\mu_m}\hat{E}_{\mu_m}\hat{Q}_{\mu_m}}} \tag{12}$$

式中，N_{μ_m}是光源强度为μ_m时脉冲总数；n_α是高斯分析的标准差倍数，与置信度直接相关。

2) 切诺夫–霍夫丁界

根据文献 [22] 附录 D 中的结论，约束条件式 (8)～式 (9) 变为不等式组：

$$\hat{Q}_{\mu_m}\left(1-\delta_{\mathrm{q}}^{\mathrm{L}}\right) \leqslant \sum_{k=0}^{8} \frac{\mu_m^k}{k!} \exp(-\mu_m) Y_k \leqslant \hat{Q}_{\mu_m}\left(1+\delta_{\mathrm{q}}^{\mathrm{U}}\right)$$
$$\hat{E}^{\mathrm{Z}}_{\mu_m} \hat{Q}_{\mu_m}\left(1-\delta_{\mathrm{eq}}^{\mathrm{L}}\right) \leqslant \sum_{k=0}^{8} \frac{\mu_m^k}{k!} \exp(-\mu_m) e_k^{\mathrm{Z}} Y_k \leqslant \hat{E}^{\mathrm{Z}}_{\mu_m} \hat{Q}_{\mu_m}\left(1+\delta_{\mathrm{eq}}^{\mathrm{U}}\right) \tag{13}$$

其中：

$$\delta_{\mathrm{q}}^{\mathrm{L}} = \sqrt{\frac{-3\ln\left(\frac{\varepsilon}{2}\right)}{N_{\mu_m}\hat{Q}_{\mu_m}}};\ \delta_{\mathrm{q}}^{\mathrm{U}} = 2\sqrt{\frac{-2\ln\left(\frac{\varepsilon}{2}\right)+2\ln 2}{N_{\mu_m}\hat{Q}_{\mu_m}}}$$
$$\delta_{\mathrm{eq}}^{\mathrm{L}} = \sqrt{\frac{-3\ln\left(\frac{\varepsilon}{2}\right)}{N_{\mu_m}\hat{E}_{\mu_m}\hat{Q}_{\mu_m}}};\ \delta_{\mathrm{eq}}^{\mathrm{U}} = 2\sqrt{\frac{-2\ln\left(\frac{\varepsilon}{2}\right)+2\ln 2}{N_{\mu_m}\hat{E}_{\mu_m}\hat{Q}_{\mu_m}}} \tag{14}$$

3　仿真及分析

假设 Alice 和 Bob 发送的脉冲数相同，实验中相关参数主要来源于文献 [25]，如表 1 所示。

e_{d}是检测错误概率，主要影响信道传输效率，α为信道损耗，当$n_\alpha = 5$时，可直接计算得失败的概率为$\varepsilon = 5.73\times10^{-7}$，置信度为$1-\varepsilon$。

表 1　仿真中用到的实验参数

e_{d}/%	p_{d}	f	η_{d}/%	M	n_α	α
1.5	8×10^{-8}	1.15	14.5	16	5	0.2

需要说明的是，仿真中所用参数是较为典型的参数，当前实验室中信道损耗、检测效率、暗计数率等均可以做到更优，如最近实现的 833 km 量子密钥分发实验[11]中，$\alpha = 0.158$，$p_{\mathrm{d}} = 1.5\times10^{-11}$，$\eta_{\mathrm{d}} = 83\%$，但在实际应用中成本过高。

仿真中 PM 协议采用最简单的参数设定，主要比较不同统计波动分析方法性能。将理想情况下计算所得的全局增益和 QBER 作为测量值。

3.1　二诱骗态 PM 协议

在二诱骗态 PM 协议下，Alice 和 Bob 选择相同的信源强度，一组典型值为{0,0.05,0.2}，其中信号态强度为 0.2。每种信源强度发送的脉冲数均为$N = 2\times10^{13}$。

Alice 和 Bob 相距 50 km 时，分别利用高斯分析和切诺夫–霍夫丁界对二诱骗态 PM 协议进行统计波动分析，通过线性规划方法估计所得的e_k的最大值和Y_k的最小值列于表 2 中。

从表 2 可以看出，高斯分析对Y_k和e_k的估计更加紧致；由式 (4) 可知，$e_k = 1$的项不会对E_μ^X的结果产生影响，因而两种方法对Y_3和e_3的估计值没有意义。用上述方法计算$k > 3$的项均无法得到有效的估计值。这主要是因为诱骗态数量有限，对系统参数估计的能力有限，无法准确估计高阶参数。结合式 (4) 及式 (7)，将表 2 中的数据代入计算可得，高斯分析与切诺夫–霍夫丁界对应的密钥生成率分别为3.059×10^{-4} bits/脉冲和3.058×10^{-4} bits/脉冲。按照类似的方法计算不同数据长度情况下，不同距离时系统的密钥生成率，可得图 2。

表 2　二诱骗态 PM 协议部分计数率下界及错误率上界的仿真估计值

统计波动分析方法	Y_0	Y_1	Y_3	e_0	e_1	e_3
理想值	$1.600\,0\times10^{-7}$	0.045 853	0.131 35	0.500 00	0.003 755 1	0.001 310 9
高斯分析	$1.595\,5\times10^{-7}$	0.045 614	$3.571\,7\times10^{-33}$	0.503 38	0.003 954 9	1
切诺夫–霍夫丁界	$1.594\,0\times10^{-7}$	0.045 613	$3.914\,8\times10^{-15}$	0.506 32	0.003 957 0	1

图 2 中，2DECOY_infinite 表示不考虑统计波动的二诱骗态情况，GS_10、GS_13、GS_16 分别表示$N \in \{2\times10^{10}, 2\times10^{13}, 2\times10^{16}\}$时采用高斯分析的二诱骗态情况，类似的 CH_10、CH_13、CH_16，

分别表示$N\in\{2\times10^{10}, 2\times10^{13}, 2\times10^{16}\}$时采用切诺夫–霍夫丁界的二诱骗态情况。结果表明，考虑统计波动，即便在数据较少的情况下，PM 协议仍可突破 PLOB 界；高斯分析在数据较少的情况下具有明显的性能优势，而数据较少时较难满足正态分布的要求，因而高斯分析的实用性不高；但随着数据量的增加，高斯分析与切诺夫–霍夫丁界分析的结果都趋于无穷数据长度的情况，高斯分析的性能优势不再明显。

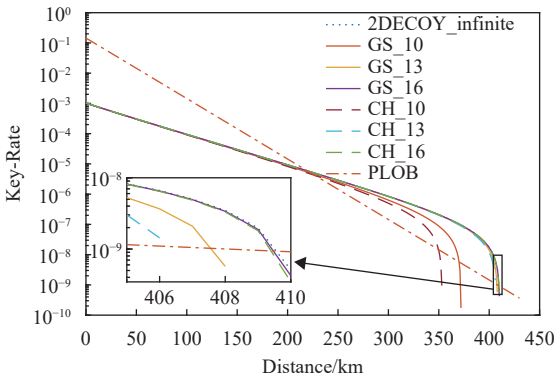

图 2 二诱骗态 PM 协议考虑统计波动时密钥生成率

3.2 三诱骗态 PM 协议

在三诱骗态 PM 协议下，Alice 和 Bob 选择一组典型的信源强度，分别为{0, 0.01, 0.05, 0.2}，其中信号态强度为 0.2。每种信源强度发送的脉冲数为$N=2\times10^{13}$。

与二诱骗态 PM 协议类似，表 3 列举了三诱骗态情况下e_k最大和Y_k最小估计值。

从表 3 中数据可以看出，相比Y_1、e_1的估计值，Y_3、e_3的估计与理论值之间的误差更大，但与二诱骗态 PM 协议不同的是，其估计值对密钥生成率仍具有积极的贡献。结合式 (4) 及式 (7)，将表 3 中的数据代入计算可得，高斯分析与切诺夫–霍夫丁界对应的三诱骗态 PM 协议的密钥生成率分别为3.38×10^{-4}比特/脉冲和3.37×10^{-4}比特/脉冲，比二诱骗态 PM 协议的密钥生成率高，但差异仅有10^{-5}量级。按照类似的方法计算不同数据长度情况下，不同距离时系统的密钥生成率，可得图 3。

图 3 中，3DECOY_infinite 表示不考虑统计波动的三诱骗态情况，GS_10、GS_13、GS_16 分别表示$N\in\{2\times10^{10}, 2\times10^{13}, 2\times10^{16}\}$时采用高斯分析的三诱骗态情况，类似的 CH_10、CH_13、CH_16，分别表示$N\in\{2\times10^{10}, 2\times10^{13}, 2\times10^{16}\}$时采用切诺夫–霍夫丁界的三诱骗态情况。该仿真结果与二诱骗态 PM 协议仿真结果具有相同的趋势，进一步证明了两种统计波动分析方法的通用性。

表 3 三诱骗态部分计数率下界及错误率上界的仿真估计值

统计波动分析方法	Y_0	Y_1	Y_3	e_0	e_1	e_3
理想值	$1.600\,0\times10^{-7}$	0.045 853	0.131 350	0.500 00	0.003 755 1	0.001 310 9
高斯分析	$1.595\,5\times10^{-7}$	0.045 846	0.072 025	0.503 38	0.003 761 5	0.010 097 0
切诺夫–霍夫丁界	$1.594\,0\times10^{-7}$	0.045 844	0.069 886	0.506 34	0.003 767 6	0.013 122 0

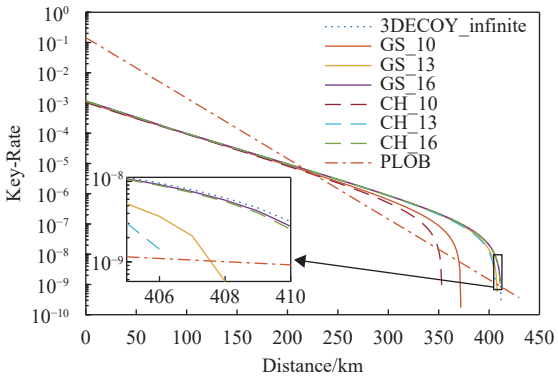

图 3 三诱骗态 PM 协议考虑统计波动时密钥生成率

3.3 二诱骗态与三诱骗态 PM 协议对比

对比表 2 与表 3 数据可知，在统计波动分析方法相同的条件下，对Y_0, Y_1, e_0, e_1的估计，三诱骗态 PM 协议略优于二诱骗态 PM 协议，但两种协议相差很小；对Y_3, e_3的估计，三诱骗态 PM 协议提升明显。能对更多参数进行有效估计是三诱骗态相对二诱骗态性能更好的原因之一。

基于切诺夫–霍夫丁界更高的实用价值，进一步对比三诱骗态和二诱骗态 PM 协议利用该方法进行统计波动分析时的性能，如图 4 所示。

图 4 中，2DECOY_infinite、2DECOY_10、2DECOY_13、2DECOY_16 分别表示$N\in\{\infty, 2\times10^{10}, 2\times10^{13}, 2\times10^{16}\}$时采用切诺夫–霍夫丁界的二诱骗态情况，类似地，3DECOY_infinite、3DECOY_10、3DECOY_13、3DECOY_16 表示相应数据长度下三诱骗态情况。图中结果显示，在数据长度较短(N取2×10^{10},2×10^{13}) 时，二诱骗态与三诱骗态 PM 协议密钥生成率曲线基本重合，性能差异极

小；当N取2×10^{16}时，二诱骗态与三诱骗态 PM 协议性能分别趋近于对应的无限数据长时性能，性能差异在实际应用中仍可忽略。三诱骗态 PM 协议通过增加诱骗态数量，为参数估计提供更多的约束条件，以此提升参数估计的精确度，对比表 2 与表 3 中的数据，可以看出这种提升，但图 4 也反应出这种提升无法在密钥生成率及最大安全传输距离上体现出来。综合来看，三诱骗态 PM 协议利用了更多的数据，其所消耗的时间及存储空间较二诱骗态 PM 协议多 33%，但是并不能得到较好的性能提升，因而二诱骗态 PM 协议具有更高的实用价值。

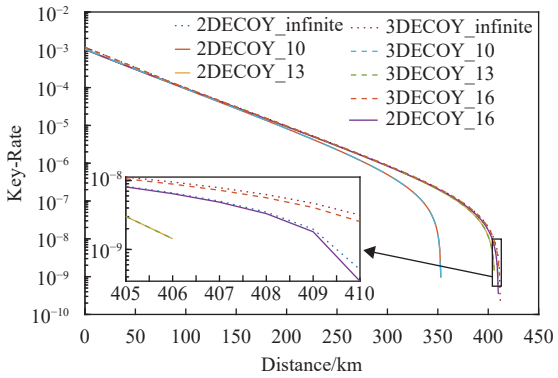

图 4　基于切诺夫-霍夫丁界统计波动分析的诱骗态 PM 协议密钥生成率

4　结 束 语

考虑统计波动后，PM 协议仍能突破 PLOB 界实现无条件安全密钥分发。在信道损失较小 (距离小于 200 km) 且数据长度大于10^{10}时，二诱骗态和三诱骗态 PM 协议性能都接近无穷数据长情况；反之，当信道损失较大时，数据长度对 PM 协议性能影响较大，随着数据长度增大，PM 协议性能增强，当数据长度大于10^{13}时，系统性能提升不再明显。

采用切诺夫–霍夫丁界进行统计波动分析，可以保证 PM 协议的安全性，但是在数据量较小时，其性能与利用高斯分析进行统计波动分析的 PM 协议有一定差距，数据量增大可以逐渐缩小这种差距。

增加诱骗态无法显著提高考虑统计波动的 PM 协议性能，特别是在数据量较小时，增加诱骗态只能增大系统开销，系统性能提升可以忽略。

综合来看，采用二诱骗态 PM 协议、切诺夫–霍夫丁界统计波动分析方法，取数据长度为10^{13}量级，是一种较实用的量子密钥分发方案。

参 考 文 献

[1] LO H K, MA X F, CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94: 230504.

[2] LO H K, CURTY M, QI B. Measurement-Device-Independent quantum key distribution[J]. Physical Review Letters, 2012, 108: 130503.

[3] ZHANG Y Y, BAO W S, ZHOU C, et al. Round-Robin differential phase shift with heralded single-photon source[J]. Chinese Physics Letters, 2017, 34(4): 040301.

[4] TAKEOKA M, GUHA S, WILDE M M. Fundamental rate-loss tradeoff for optical quantum key distribution[J]. Nature Communications, 2014, 5: 5235.

[5] PIRANDOLA S, LAURENZA R, OTTAVIANI C, et al. Fundamental limits of repeaterless quantum communications[J]. Nature Communications, 2017, 8: 15043.

[6] LUCAMARINI M, YUAN Z L, DYNES J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557: 400-403.

[7] GRASSELLI F, CURTY M. Practical decoy-state method for twin-field quantum key distribution[J]. New Journal of Physics, 2019, 21: 073001.

[8] MA X F, ZENG P, ZHOU H Y. Phase-Matching quantum key distribution[J]. Physical Review X, 2018, 8: 031043.

[9] WANG X B, YU Z W, HU X L. Twin-Field quantum key distribution with large misalignment error[J]. Physical Review A, 2018, 98(6): 1-12.

[10] CUI C H, YIN Z Q, WANG R, et al. Twin-Field quantum key distribution without phase postselection[J]. Physical Review Applied, 2019, 11(3): 1.

[11] WANG S, YIN Z Q, HE D Y, et al. Twin-Field quantum key distribution over 830 km fibre[J]. Nature Photonics, 2022, 16(2): 154-161.

[12] CHEN J P, ZHANG C, LIU Y, et al. Twin-Field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas[J]. Nature Photonics, 2021, 15(8): 570-575.

[13] CHEN G, WANG L, LI W, et al. Multiple-Pulse phase-matching quantum key distribution[J]. Quantum Information Processing, 2020, 19: 416.

[14] LI W, WANG L, ZHAO S M. Phase matching quantum key distribution based on single-photon entanglement[J]. Scientific Reports, 2019, 9: 15466.

[15] BUNANDAR D, GOVIA L C G, KROVI H, et al. Numerical finite-key analysis of quantum key distribution[J]. NPJ Quantum Information, 2020, 6: 104.

[16] CURRÁS-LORENZO G, NAVARRETE Á, AZUMA K, et al. Tight finite-key security for twin-field quantum key distribution[J]. NPJ Quantum Information, 2021, 7: 22.

[17] 虞味, 周媛媛, 周学军. 基于弱相干态光源的相位匹配诱骗态量子密钥分配方案[J]. 量子电子学报, 2021, 38(1): 37-44.
YU W, ZHOU Y Y, ZHOU X J. Phase-Matching decoystate quantum key distribution scheme with weak coherent source[J]. Chinese Journal of Quantum Electronics, 2021, 38(1): 37-44.

[18] YU Y, WANG L, ZHAO S M, et al. Decoy-State phase-matching quantum key distribution with source errors[J]. Optics Express, 2021, 29(2): 2227.

[19] MA X F, QI B, ZHAO Y, et al. Practical decoy state for quantum key distribution[J]. Physical Review A: Atomic, Molecular, and Optical Physics, 2005, 72: 012326.

[20] 周江平, 周媛媛, 周学军, 等. 二诱骗态相位匹配量子密钥分发方案[J]. 电子科技大学学报, 2021, 50(5): 650-655.
ZHOU J P, ZHOU Y Y, ZHOU X J, et al. Two-Decoystate phase matching quantum key distribution method[J]. Journal of University of Electronic Science and Technology of China, 2021, 50(5): 650-655.

[21] ZHOU J P, ZHOU Y Y, GU R W, et al. Passive decoy state phase matching quantum key distribution[J]. International Journal of Quantum Information, 2022, 20(4): 2250005.

[22] ZHANG Z, ZHAO Q, RAZAVI M, et al. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems[J]. Physical Review A, 2017, 95: 012333.

[23] CURTY M, XU F H, CUI W, et al. Finite-Key analysis for measurement-device-independent quantum key distribution[J]. Nature Communications, 2014, 5: 3732.

[24] DING H J, MAO C C, ZHANG C M, et al. Improved statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Quantum Information Processing, 2018, 17: 332.

[25] MA X F, FUNG C H F, RAZAVI M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Physical Review A: Atomic, Molecular, and Optical Physics, 2012, 86: 052305.

编 辑 蒋 晓