二诱骗态相位匹配量子密钥分发方案

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】相位匹配协议是最近被提出的一种能突破密钥容量的量子密钥分发协议，其安全性得到了理论和实践的证明。针对实际应用中光源的非理想性，基于弱相干态光源，提出了一种二诱骗态相位匹配量子密钥分发方案。该方案在简化参量计算式的同时，仅采用 2 个诱骗态 (真空+弱诱骗态) 对求解最终密钥生成率的必要参数进行了估计；随后以光纤信道为背景，对该方案在理想及统计波动情况下的性能进行了仿真分析。仿真结果表明：在同等诱骗态数目条件下，二诱骗态相位匹配方案能突破密钥容量的限制，密钥生成效率及最大传输距离均优于 BB84 协议、测量设备无关协议等；在密钥生成效率及最大传输距离两个性能指标上，理想情况下二诱骗态方案接近已有的三诱骗态方案，但在考虑实际统计波动且数据量小于 10^{14} 时二诱骗态方案反而更优。

关 键 词 诱骗态； 相位匹配协议； 量子密钥分发； 量子光学； 弱相干态光源

中图分类号 O431.2 **文献标志码** A doi:10.12178/1001-0548.2021171

Two-Decoy-State Phase Matching Quantum Key Distribution Method

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

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

Abstract The phase matching protocol is a recent proposed quantum key distribution protocol that breaks the secret key capacity. Its security has been certified by theory and practice. For there is no ideal single photon source in practice, a two-decoy-states phase matching quantum key distribution method is proposed with a weak coherent state source. In this method, the parameters are estimated more easily for only two decoy states (vacuum+weak decoy state) should be taken into consideration that are necessary to solve the final key rate. Then we analyze the performance of the proposed method with fiber channel both in ideal and statistical fluctuation respectively. The simulation results show that the proposed method can break the secure key capacity and has higher key rate and longer max transmission distance than the BB84 (the protocol proposed by Bennett and Brassard in 1984) and measurement device independent protocols under the condition of the same number of decoy state. The proposed method approaches the existing three-decoy-states method in key rate and max transmission distance and breaks the secret key capacity. Taking the statistical fluctuation into consideration, the proposed method will have higher key rate and longer max transmission distance when the data size is less than 10^{14}.

Key words decoy state; phase matching protocol; quantum key distribution; quantum optics; weak coherent state source

量子密钥分发 (quantum key distribution, QKD)[1] 基于量子力学基本原理，具有无条件安全性，是彻底解决通信保密问题最具潜力的手段。经过近 40 年的研究，目前 QKD 已逐渐从实验室走向实际应用[2-5]。1984 年，文献 [6] 提出第一个 QKD 协议——BB84 协议，开启了 QKD 研究的序幕[7-8]。为提升 QKD 的最大传输距离和密钥生成效率，SARG04 协议[9]、测量设备无关 (measurement device independent, MDI) 协议[10] 等被相继提出。但 QKD 的密钥生成效率 R 始终难以突破密钥容量 (secret key capacity, SKC)[11] 的限制，即 $R \leqslant O(\eta)$[12]，其中 η 为量子信道的传输效率。2018 年，文献 [13] 对 MDI 协议进行改进，提出双场 (twin field, TF) 协议，其密钥生成效率 R 和 η 关系改善为 $R \leqslant O(\sqrt{\eta})$，突破了 SKC 的限制，但安全性未得到严格的证明。2019 年，文献 [14] 指出 TF 协议的安全性缺陷，通过研究相位编码

收稿日期：2021－06－17；修回日期：2021－08－03

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：zyy_hjgc@aliyun.com

MDI 协议的单光子检测，对 TF 协议进行改进从而提出相位匹配 (phase matching, PM) 协议，并对其安全性进行了严格的证明，是目前最优的 QKD 协议之一[15]。

在 PM 协议的实际应用中，首先要考虑如何抵御针对非理想单光子源的光子数分离攻击 (photon number splitting, PNS)[16-18]。诱骗态协议[19]与 QKD 协议的结合[20]能很好地解决这一问题，因而成为当前实际应用中最常用的组合方案。在诱骗态方案的设计中，诱骗态数量的选择、参数估计的方法等都对系统的实际性能及实现难度有较大的影响。针对这一问题，文献 [21-22] 均结合弱相干态 (weak coherent state, WCS) 光源研究了三诱骗态 PM 方案，取得了较好的结果。本文提出一种更加实用的二诱骗态 (真空+弱诱骗态)PM 方案，仅用 2 个诱骗态，得到理论上与之接近的密钥生成效率和最大传输距离；考虑统计波动，在数据量较少时反而具有更高的密钥生成效率和最大传输距离。通过改变光强的形式产生诱骗态，诱骗态数目越多，对光源的要求越高，实现难度越大。单次密钥分发的持续时间越长，数据量越大，对系统的存储、计算、信道稳定性等要求更高。相比之下，本文所提出的方案减少了诱骗态的数量，提升了数据量较少时系统的密钥生成效率和最大传输距离，不仅大幅降低了 PM 协议应用中的实现难度，更拓宽了其应用范围，具有更高的实际应用价值。

本文首先构建基于光纤信道和 WCS 光源的二诱骗态 PM 方案模型，随后对相关参数的估计进行数学推导，并最终得出密钥生成效率的计算公式，最后对密钥生成效率和最大传输距离进行数值仿真分析。

1　基于 WCS 光源的二诱骗态 PM 方案

1.1　基于光纤信道的 WCS+PM 数学模型

WCS 光源可由普通激光器经强衰减得到，具有简单、稳定等特点。其发送的单个光脉冲中光子数是随机的，且服从泊松分布，当光源强度为 μ 时，其光子态密度为：

$$\rho=\sum_{i=0}^{\infty}P_i^{\mu}|i\rangle\langle i|=\sum_{i=0}^{\infty}\frac{\mu^i}{i!}\exp(-\mu)|i\rangle\langle i| \tag{1}$$

式中，$|i\rangle\langle i|$ 表示 i 光子态，$i=1,2,\cdots$；P_i^{μ} 表示光强为 μ 时发送 i 光子态的概率。

光纤信道中，损失系数是其固有特性，为一常数，用 α 表示，那么长度为 l 的光纤信道中，传输效率 t 可以表示为：

$$t=10^{-\alpha l/10} \tag{2}$$

设检测器的检测效率为 η_d，那么从发送端到接收端，包括检测器在内信道的传输效率 η 可表示为：

$$\eta=t\eta_d \tag{3}$$

信源发送 i 个光子，经信道传输后，能在接收端产生有效响应的概率为计数率，记为 Y_i，可表示为：

$$Y_i=Y_0+(1-Y_0)(1-(1-\eta)^i) \tag{4}$$

根据文献 [14]，PM 协议的密钥生成效率可由下式计算：

$$R_{\mathrm{PM}}\geqslant\frac{2}{M}Q_{\mu}[1-fH(E_{\mu}^{Z})-H(E_{\mu}^{X})] \tag{5}$$

式中，M 为相位分片数，$2/M$ 为筛选因子，f 为实际纠错算法效率，均为常数；$H(x)$ 为香农信息熵函数，$H(x)=-x\log_2 x-(1-x)\log_2(1-x)$；$Q_{\mu}$、$E_{\mu}^{Z}$ 表示发送信号强度为 μ 时，总光子数计数率和总量子比特误码率，均通过实验得到，可写为：

$$Q_{\mu}=\sum_{i=0}^{\infty}Y_i\frac{\mu^i}{i!}\exp(-\mu) \tag{6}$$

$$E_{\mu}^{Z}Q_{\mu}=\sum_{i=0}^{\infty}e_i^{Z}Y_i\frac{\mu^i}{i!}\exp(-\mu) \tag{7}$$

式中，e_i^{Z} 为 i 光子态计数错误率；E_{μ}^{X} 表示相位错误率，需进行估计，根据文献 [14] 有：

$$E_{\mu}^{X}\leqslant q_0e_0^{z}+\sum_{k=0}^{\infty}e_{2k+1}^{Z}q_{2k+1}+\left(1-q_0-\sum_{k=0}^{\infty}q_{2k+1}\right) \tag{8}$$

式中，q_k 表示检测到的信号中 k 光子态信号所占比率，可以写为：

$$q_k=P^{\mu}(k)\frac{Y_k}{Q_{\mu}} \tag{9}$$

1.2　二诱骗态 PM 方案

诱骗态数量越多，对相关参数的估计就越准确，系统性能越好，但同时系统实现越复杂。为降低系统实现难度，本文对式 (8) 进行简化。因为 $e_k^{Z}<1$，式 (8) 可以进一步写成如下形式：

$$E_{\mu}^{X}<q_0e_0^{z}+q_1e_1^{z}+(1-q_0-q_1) \tag{10}$$

将式 (9) 代入式 (10) 得：

$$E_\mu^X < 1 + P^\mu(0)\frac{Y_0}{Q_\mu}(e_0^z - 1) + P^\mu(1)\frac{Y_1}{Q_\mu}(e_1^z - 1) \tag{11}$$

从式 (5) 和式 (11) 可以看出，为保证系统的安全性，需估计E_μ^X的最大值。可考虑用真空态估计Y_0的下限和e_0^Z的上限，用弱诱骗态估计Y_1的下限和e_1^Z的上限。因此本文综合考虑提出二诱骗态 PM 方案，信号态、弱诱骗态、真空态光源强度分别为μ、v、0。

二诱骗态 PM 方案原理如图 1 所示。

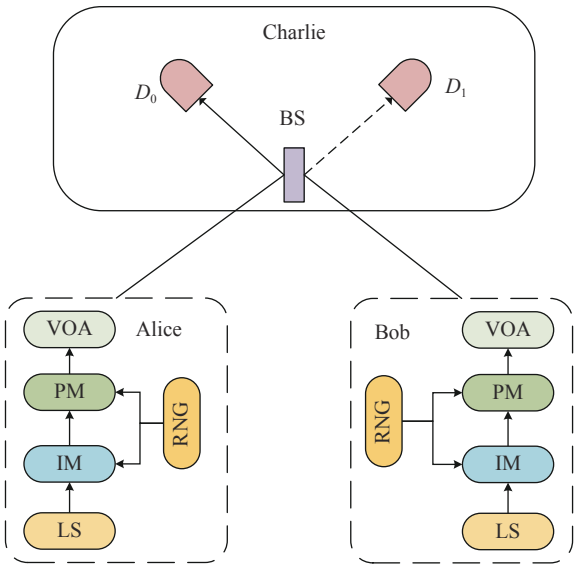


图 1 二诱骗态 PM 方案原理图

具体流程如下：

1) 相干态制备：Alice 和 Bob 分别随机产生信息比特$\kappa_a(\kappa_b) \in \{0,1\}$、附加相位$\phi_a(\phi_b) \in [0,2\pi)$，分别发送强度$x_a(x_b) \in \{\mu, v, 0\}$的光脉冲。制备的相干态为$\left|\sqrt{x_a/2}e^{i(\pi\kappa_a+\phi_a)}\right\rangle_A$和$\left|\sqrt{x_b/2}e^{i(\pi\kappa_b+\phi_b)}\right\rangle_B$，不失一般性，假设 Alice 与 Bob 光源强度相同，即$x_a = x_b$；

2) 不可信测量：Alice 和 Bob 分别将已调制的光脉冲经独立信道发送给第三方 Charlie，Charlie 进行相干检测，记录探测器D_0和D_1的响应情况；

3) 信息公开：Charlie 公开其测量结果，将$[0,2\pi)$分成 M 个区间 $\{\Delta_j\}$，$0 \leqslant j \leqslant M-1$，$\Delta_j = [2\pi j/M, 2\pi(j+1)/M)$，Alice 和 Bob 声明$\phi_a$、$\phi_b$所处区间索引$j_a$、$j_b$，并随机选取一定数量的密钥比特进行公布；

4) 密钥筛选：重复执行步骤 1)～3)，直至次数满足要求。对每一个脉冲对，当 Charlie 宣布“成功检测”时，Alice 与 Bob 保留相应比特，若D_1响应，Bob 反转其发送的比特。在保留的比特中，Alice 与 Bob 先进行相位补偿，再根据筛选条件进行密钥筛选。Bob 根据 Alice 公布的密钥比特值，查找$j_d \in \{0,1,\cdots,M/2-1\}$，使得量子比特错误率$E_\mu^Z$最小，$j_d$即为系统相位补偿参数。筛选密钥条件：$|j_b + j_d - j_a| \bmod M$为 0 或者 $M/2$，若结果为 $M/2$，Bob 还需再次进行比特翻转操作；

5) 参数估计：Alice 与 Bob 分析不同信号强度总的增益Q_0、Q_v、Q_μ和量子比特错误率e_0^Z、E_v^Z、E_μ^Z，估计相位错误率E_μ^X等参数；

6) Alice 与 Bob 进行纠错和私密放大等操作，得到最终密钥。

1.3 参数估计

利用真空态可估计Y_0、e_0^Z得：

$$\begin{cases} Y_0 = Q_0 \\ e_0^Z Y_0 = E_0 Q_0 \end{cases} \tag{12}$$

估计Y_1。不失一般性，令：$0 < v \ll \mu < 1$，则$\frac{v^i}{\mu^i} \leqslant \frac{v^2}{\mu^2}, i \geqslant 2$。将$v$代入式 (6) 得：

$$Q_v \exp(v) \leqslant Y_0 + Y_1 v + \frac{v^2}{\mu^2}\sum_{i=0}^{\infty}\frac{Y_i}{i!}\mu^i = Y_0 + Y_1 v + \frac{v^2}{\mu^2}\left(Q_\mu \exp(\mu) - Y_0 - Y_1\mu\right) \tag{13}$$

解式 (13) 可得Y_1的下界Y_1^L：

$$Y_1 \geqslant Y_1^L = \frac{\mu}{\mu v - v^2} \times \left(Q_v \exp(v) - Q_\mu \exp(\mu)\frac{v^2}{\mu^2} - \frac{\mu^2 - v^2}{\mu^2}Y_0\right) \tag{14}$$

估计e_1^Z。将v代入式 (7) 得：

$$E_v^Z Q_v \exp(v) = e_1^Z Y_0 + e_1^Z Y_1 v + \sum_{i=2}^{\infty}\frac{e_i^Z Y_i v^i}{i!} \tag{15}$$

由式 (15) 可得e_1^Z的表达式，又因为$\sum_{i=2}^{\infty}\frac{e_i^Z Y_i v^i}{i!} > 0$，可求得$e_1^Z$的上界$e_1^U$：

$$e_1^Z \leqslant e_1^U = \frac{1}{Y_1^L}\frac{E_v^Z Q_v \exp(v) - e_0 Y_0}{v} \tag{16}$$

综上所述，将式 (11)、(12)、(14)、(16) 分别代入式 (5)，即可得到最终的密钥生成效率公式。

2 统计波动分析

在实际应用中，有限长数据会导致对e_i^Z、Y_i的估计存在偏差[23]。为了确保 QKD 协议的无条件安全性，需进行统计波动分析[24]。切诺夫界[25-26]是一种较优的统计波动分析方法。本文基于切诺夫界进

行统计波动分析。

切诺夫界：若随机变量$X_1,X_2,\cdots,X_n$相互独立且服从伯努利分布$\Pr(X_i=1)=p$，其中$i=1,2,\cdots,n$，令$c=\sum_{i=1}^{n}E[X_i]$，那么$\forall\delta>0$，有：

$$\Pr\left\{\sum_{i=1}^{n}X_i\geqslant(1+\delta)c\right\}\leqslant\left[\frac{\exp(\delta)}{(1+\delta)^{1+\delta}}\right]^c<\exp\left(-c\frac{\delta^2}{2}\right)\tag{17}$$

$$\Pr\left\{\sum_{i=1}^{n}X_i\leqslant(1-\delta)c\right\}\leqslant\left[\frac{\exp(-\delta)}{(1-\delta)^{1-\delta}}\right]^c<\exp\left(-c\frac{\delta^2}{2}\right)\tag{18}$$

设置信度为$1-\theta$，数据长度为 n，当发送信号强度为v时，估计量Q_v的偏差为ε，根据切诺夫界有：

$$\begin{cases}\exp\left(-c\dfrac{\varepsilon^2}{2}\right)=\dfrac{\theta}{2}\Rightarrow\varepsilon=\sqrt{\dfrac{2(\ln 2-\ln\theta)}{nQ_v}}\\ c=nQ_v\end{cases}\tag{19}$$

Q_v的估计值上下波动的边界分别为：

$$\begin{cases}Q_v^{\mathrm{U}}=Q_v(1+\varepsilon)\\ Q_v^{\mathrm{L}}=Q_v(1-\varepsilon)\end{cases}\tag{20}$$

3　仿真及分析

利用 matlab 进行仿真。仿真参数主要来源于文献 [14, 21]，是 QKD 典型实验系统的参数，具体如表 1 所示。

表 1　仿真参数表

暗记数 p_d	纠错效率f	检测效率η_d/%	相位分片数M	检测错误率e_d/%	置信度 $1-\theta$	信道损失系数α
8×10^{-8}	1.15	14.5	16	1.5	$1-5.73\times10^{-7}$	0.2

其中暗记数表示由于背景噪声的影响，在发送端没有发送光脉冲时，检测器产生响应的概率。纠错效率指因为纠错编码而产生的额外的比特损耗。检测效率指检测器产生有效响应的概率。检测错误率指检测器产生有效的响应但出错的概率。

图 2 对比了本文二诱骗态 (vacuum+weak-PM)、文献 [21] 中三诱骗态 (真空+二弱诱骗态) 方案 (vacuum+2weak-PM) 及无穷诱骗态方案 (inf-decoy-PM) 的密钥生成效率与传输距离的关系。从图中可看出，3 种方案曲线都非常接近，文献 [21] 中方案密钥生成效率及最大传输距离均略微优于二诱骗态方案，更加接近无穷诱骗态情况。增加诱骗态数量可对更多参量进行更精确的估计，但是对密钥生成效率及最大传输距离的提升极其有限，这是因为 i-光子态信号对密钥生成效率的贡献随 i 的增加越来越小。增加诱骗态数量需要使用更多不同强度的光源，不仅增加系统对硬件的要求，而且对光强的优化更加复杂，从而极大增加了实现难度。因此从实用的角度看，本文提出的二诱骗态方案更加可行。

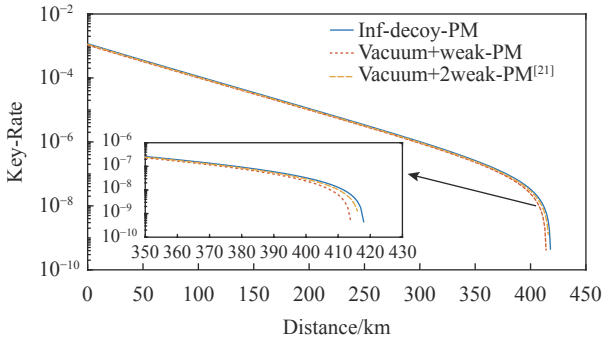


图 2　3 种诱骗态协议密钥生成效率随传输距离变化曲线

由图 3 可知，本文提出的二诱骗态 PM 协议最大传输距离达 414 km，相较 BB84 协议增加了 176 km，相较 MDI 协议增加了 8 km。二诱骗态 PM 方案突破了密钥生成效率边界 (SKC) 而另外两种均未能突破。相较最大传输距离更远的 MDI 协议，二诱骗态 PM 方案在密钥生成效率上提升了 3~4 个数量级。可见，在同等实现难度条件下，本文提出的方案更优。

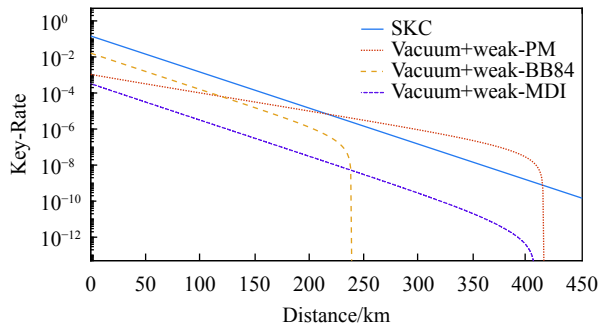
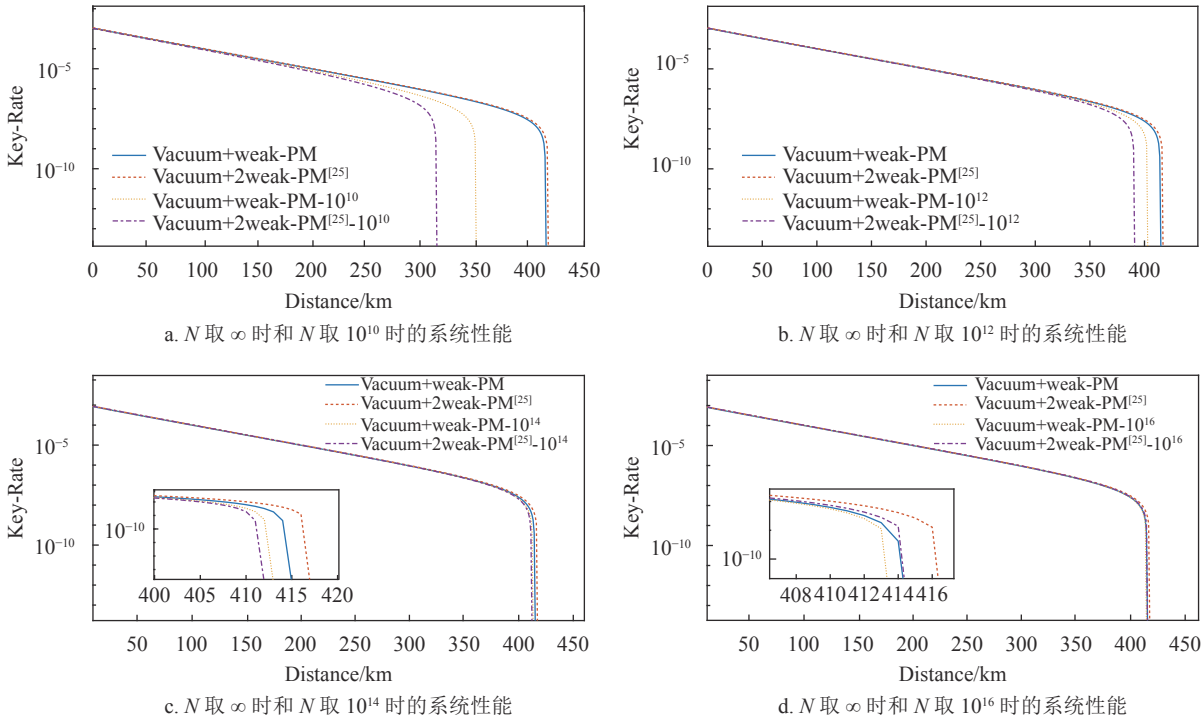


图 3　采用相同诱骗态时，不同协议密钥生成效率随传输距离变化曲线

仅考虑数据长度对系统的影响，假设信号态、弱诱骗态、真空态随机发送且概率均为 1/3，不同数据长度下系统密钥生成效率随传输距离变化如图 4 所示。



a. N 取 ∞ 时和 N 取 10^{10} 时的系统性能

b. N 取 ∞ 时和 N 取 10^{12} 时的系统性能

c. N 取 ∞ 时和 N 取 10^{14} 时的系统性能

d. N 取 ∞ 时和 N 取 10^{16} 时的系统性能

图 4 不同数据长度对二诱骗态及三诱骗态方案的性能影响

由图 4 可知，当数据长度为 10^{10} 时，本文提出的二诱骗态方案密钥生成效率更高，最大传输距离更远；随着数据长度的增大，二者差距越来越小，当数据长度达到 10^{14} 时，二者性能相差极小；当数据长度达 10^{16} 时，三诱骗态方案性能超过二诱骗态方案，接近数据无限长的极限情况。三诱骗态方案所用的诱骗态数量更多，当总的数据长度一定时，各诱骗态的数据长度相对更小，因而在参数估计过程中统计波动影响更大，而需要估计的参数也相对更多，统计波动的影响叠加起来使其对统计波动更加敏感。当数据量达到一定数量级，统计波动影响可以忽略，两种协议都能趋于无限长数据情况。一般在实际系统中，若想把单次密钥分发时间控制在 10 小时以内，数据长度需控制在 10^{13} 以内，此时本文提出的二诱骗态 PM 方案更有优势。

4 结 束 语

本文基于 WCS 光源，提出了一种二诱骗态 PM 方案。与现有 PM 方案相比，本文以小幅牺牲系统性能为代价，减少一个信源强度的制备，进一步简化了系统的实现。与 BB84、MDI 等方案相比，在采用真空+弱诱骗态的同等条件下，本文所提方案最大传输距离最远，密钥生成效率在远距离时更高，性能更优，成功突破 SKC 限制。考虑统计波动，相较三诱骗态方案，数据长度小于 10^{14} 时，本文提出的方案最大传输距离更远；数据长度大于 10^{14} 时，二者最大传输距离都趋于无穷数据长度时的极限值，性能相近；实际应用中，为减小系统延时，数据长度通常控制在 10^{13} 以内，在此条件下，本文提出的方案较优。综合来看，本文提出的二诱骗态 PM 量子密钥分发方案具有较高的实用价值。

参 考 文 献

[1] ARTUR K, EKERT. Quantum cryptography based on bell's theorem[J]. Phys Rev Lett, 1991, 67: 661-663.

[2] CHEN Y A, ZHANG Q, CHEN T Y, et al. An integrated space-to-ground quantum communication network over 4600 kilometers[J]. Nature, 2021, 589(7841): 214.

[3] POPPE A, PEEV M, MAURHART O, et al. Outline of the SECOQC quantum-key-distribution network in Vienna[J]. International Journal of Quantum Information, 2008, 6(2): 209-218.

[4] MA X F, QI B, ZHAO Y, et al. Practical decoy state for quantum key distribution[J]. Phys Rev A, 2005, 72: 012326.

[5] YIN J, CAO Y, LI Y H, et al. Satellite-to-Ground entanglement-based quantum key distribution[J]. Phys Rev Lett, 2017, 119(20): 200501.

[6] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[C]//Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, Indian: IEEE, 1984, 175-179.

[7] 茅晨晨. 新型量子密钥分配协议的实际安全性分析及计算[D]. 南京: 南京邮电大学, 2019.

MAO C C. The realistic safety analysis and calculation of the new quantum key distribution protocol[J]. Nanjing: Nanjing University of Posts and Telecommunications, 2019.

[8] LO H K, CURY M, BING Q. Measurement-device-independent quantum key distribution[J]. Phys Rev Lett, 2012, 108(13): 130503.

[9] SCARANI V, ACIN A, RIBORDY G, et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations[J]. Phys Rev Lett, 2004, 92: 057901.

[10] MA X F, RAZAVI M. Alternative schemes for measurement device independent quantum key distribution[J]. Phys Rev A, 2012, 86(6): 3818-3821.

[11] PIRANDOLA S, LAURENZA R, OTTAVIANI C, et al. Fundamental limits of repeaterless quantum communications[J]. Nat Commun, 2017, 8: 15043.

[12] TAKEOKA M, GUHA S, WILDE M. Fundamental rate-loss trade off for optical quantum key distribution[J]. Nat Commun, 2014, 5: 5235.

[13] 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(7705): 400.

[14] MA X F, ZENG P, ZHOU H Y. Phase-Matching quantum key distribution[J]. Phys Rev X, 2018, 8(3): 031043.

[15] XU F H, MA X F, ZHANG Q, et al. Secure quantum key distribution with realistic devices[J]. Reviews of Modern Physics, 2020, 92: 2.

[16] PFISTER C, COLESP J, WEHNER S, et al. Sifting attacks in finite-size quantum key distribution[J]. New J Phys, 2016, 18(5): 053001.

[17] HUANG J Z, YIN Z Q, WANG S, et al. Effect of intensity modulator extinction on practical quantum key distribution[J]. Eur Phys J D, 2012, 66(6): 159.

[18] SUN S H, GAO M, JIANG M S, et al. Partially random phase attack to the practical two-way quantum-key-distribution system[J]. Phys Rev A, 2012, 85(3): 032304.

[19] HWANG W Y. Quantum key distribution with high loss: Toward global secure communication[J]. Phys Rev Lett, 2003, 91: 057901.

[20] LO H K, MA X F, CHEN K. Decoy state quantum key distribution[J]. Phys Rev A, 2005, 94: 230504.

[21] 虞味, 周媛媛, 周学军. 基于弱相干态光源的相位匹配诱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 decoy-state quantum key distribution scheme with weak coherent source[J]. Chinese Journal of Quantum Electronics, 2021, 38(1): 37-44.

[22] YANG Y, WANG L, ZHAO S M, et al. Decoy-state phase-matching quantum key distribution with source errors[J]. Optics Express, 2021, 29: 2227-2238.

[23] WEN X, LI Q, WANG H J, et al. A Bayesian based finite-size effect analysis of QKD[M]. [S.l.]: Springer, 2017.

[24] ZHU J R, LI J, ZHANG C M, et al. Parameter optimization in biased decoy-state quantum key distribution with both source errors and statistical fluctuations[J]. Quantum Information Processing, 2017, 16(10): 238-243.

[25] SONG T T, QIN S J, WEN Q Y, et al. Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources[J]. Scientific Reports, 2018, 10(5): 015276.

[26] YU W, ZHOU Y Y, ZHOU X J. Study on statistical analysis scheme of decoy-state quantum Key distribution with finite-length data[C]//2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). [S.l.]: IEEE, 2020: 2435-2440.

编　辑　蒋　晓