DOI: 10.3969/j.issn.1007-5461.2023.04.013

四强度诱骗态相位匹配量子密钥分发协议

王 晟[1]， 方晓明[1]， 林 昱[1]， 张天兵[2,3]，
冯 宝[2,3]， 余 杨[4]， 王 乐[4*]

（1 国网福建省电力有限公司信息通信分公司， 福建 福州 350003；
2 南京南瑞信息通信科技有限公司， 江苏 南京 211000；
3 南京南瑞国盾量子技术有限公司， 江苏 南京 211000；
4 南京邮电大学， 江苏 南京 210003）

摘 要： 量子密钥分发 (QKD) 具有信息论上的无条件安全性，而相位匹配量子密钥分发 (PM-QKD) 是双场量子密钥分发协议 (TF-QKD) 的一个变体，其最近被提出用来克服没有量子中继器的点对点协议中存在的速率-距离限制。鉴于实践中不存在无限强度的诱骗态，提出了一种具有实用价值的四强度诱骗态相位匹配量子密钥分发协议，即四强度诱骗态相位匹配量子密钥分发协议。给出了该协议的安全密钥速率公式，并通过数值仿真分析了该协议的性能，证明了该协议的有效性。

关 键 词： 量子光学; 量子密钥分发; 相位匹配量子密钥分发; 诱骗态; 密钥率

中 图 分 类 号： O431.2 **文 献 标 识 码：** A **文章编号：** 1007-5461(2023)04-00541-05

Four-intensity decoy-state phase-matching quantum key distribution

WANG Sheng[1], *FANG Xiaoming*[1], *LIN Yu*[1], *ZHANG Tianbing*[2,3],
FENG Bao[2,3], *YU Yang*[4], *WANG Le*[4*]

(1 Information and Communication Branch of State Grid Fujian Electric Power Co., Ltd., Fuzhou 350003, China;
2 NARI Information Communication Technology Co., Ltd, Nanjing 211000, China;
3 NRGD Quantum Technology Co., Ltd., Nanjing 211000, China;
4 Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Quantum key distribution (QKD) has unconditional security in the information theory. The phase-matching quantum key distribution (PM-QKD) is one of the variants of twin-field quantum key distribution (TF-QKD), which has been proposed recently to overcome the rate-distance limits of point-to-point protocol without quantum repeaters. In view of the fact that the infinite decoy states are not available in practice, four-intensity decoy-state PM-QKD protocol is more practical. Therefore, a novel PM-QKD protocol with four-intensity decoy states, namely four-intensity decoy-state PM-QKD protocol,

基金项目： 国网福建省电力有限公司科技项目(52130M19000Y)
作者简介： 王 晟 (1990 -)，硕士，工程师，主要从事量子保密通信技术等方面的研究。E-mail: 496079373@qq.com
收稿日期： 2021-04-27; **修改日期：** 2021-06-02
*通信作者。 E-mail: lewang@njupt.edu.cn

is propsed in this work. The secure key rate formula of the proposed protocol is presented and its performances are analyzed through numerical simulations to prove its validity.

Key words: quantum optics; quantum key distribution; phase-matching quantum key distribution; decoy state; secret key rate

0 引 言

随着能源互联网的高速发展, 我国特高压远距离交直流输电线路不断建设, 风、光、气、地热等新能源接入并网, 大电网广域协调控制日趋复杂, 控制类业务面临的安全形势也日益严峻。近年来, 诸如乌克兰电网攻击等安全事件频发, 导致大停电等事故, 在一定程度上影响了社会稳定和国家安全。因此, 如何提升大电网广域协调控制的安全性已迫在眉睫。

量子密钥分发 (QKD)[1−3]具有信息论上的无条件安全性, 其安全性由量子物理原理保证, 可提高大电网广域协调控制业务数据的传输安全, 同时可以减少电网环境对QKD系统的影响[4]。然而, 在当前量子中继器技术还不能实际应用的背景下, 由于速率-距离的限制, 传输距离仍然是现有协议在实际实现过程中的主要障碍。2018年, Lucamarini等[1]提出了双场量子密钥分发 (TF-QKD) 协议, 它可以在没有量子中继器的情况下打破限制。受此工作启发, TF-QKD协议出现了几种变体, 如Ma等[5]提出的相位匹配量子密钥分发 (PM-QKD) 协议, Wang等[6]提出的发送或不发送量子密钥分发 (SNS-QKD) 协议, 以及郭光灿团队[7, 8]和Lo团队[9]分别提出的无需相位后选择的QKD协议, 其中SNS-QKD协议已被实验验证[10, 11]。

在PM-QKD协议中, Alice (Bob) 随机准备弱相干态, 并给每个弱相干态增加一个随机相位$\phi_{\mathrm{a}}(\phi_{\mathrm{b}})$。之后, 他们都把这两个态发送给位于信道中央的Charlie (可以是不被信任的)。根据Charlie执行测量后得到的结果, Alice和Bob筛选出满足$\phi_{\mathrm{a}}\approx\phi_{\mathrm{b}}$条件的数据从而得到原始密钥。筛选后需要进行参数估计和密钥提纯, 以生成最终的隐秘的安全密钥。原始的PM-QKD协议采用了无限诱骗态方法来估计该协议的表现, 但这种方法在实践中无法实现。虽然已有研究人员提出使用有限诱骗态方法的QKD协议[12−16], 但是对使用有限诱骗态方法的PM-QKD协议的分析和报道很少[17]。

本文提出了一种具有实用价值的四强度诱骗态PM-QKD协议, 给出了该协议的安全密钥速率公式, 并通过数值仿真分析了其性能, 证明了该协议的有效性。

1 四强度诱骗态PM-QKD协议

1.1 协议流程

本协议采用四强度诱骗态方法, 用来获得与使用无限强度诱骗态方法的原始PM-QKD协议相近的性能, 具体协议流程如下:

步骤 1: Alice (Bob) 首先随机生成一个二进制密钥$k_{\mathrm{a}}(k_{\mathrm{b}})$, 并选择一个随机相位$\phi_{\mathrm{a}}\left(\phi_{\mathrm{b}}\right)\in[0,2\pi)$, 以及一个随机的脉冲强度$\mu_{\mathrm{a}}\left(\mu_{\mathrm{b}}\right)\in\{\mu/2,\nu_1/2,\nu_2/2,\nu_3/2\}$。其中$\mu/2$为信号态强度, $\nu_1/2$、$\nu_2/2$、$\nu_3/2$分别为三种不同诱骗态的强度, 且满足$\mu\geq\nu_1\geq\nu_2\geq\nu_3$以及$\mu>\nu_1+\nu_2+\nu_3$的条件。

然后, Alice (Bob) 准备一个相干态$|\sqrt{\mu_{\mathrm{a}}}\,\mathrm{e}^{\mathrm{i}\left(\phi_a+\pi k_a\right)}\rangle$ ($|\sqrt{\mu_{\mathrm{b}}}\,\mathrm{e}^{\mathrm{i}\left(\phi_b+\pi k_b\right)}\rangle$), 并将其发送给第三方Charlie (可以是不被信任的)。

步骤2: 第三方Charlie使用分束器对接收到的脉冲进行干涉测量, 并记录每轮哪个探测器发出响应。

步骤3: Alice 和Bob以及第三方Charlie重复 步骤1和 步骤2, 进行N次。

步骤4: Charlie宣布所有测量结果, Alice (Bob) 宣布自己选择的所有信号强度和随机相位。当第 i 次测量的结果只有一个探测器响应, 并且满足条件

$$\left|\phi_{\mathrm{a}}-\phi_{\mathrm{b}}-k\pi\right| \leq \frac{2\pi}{M}(k=0,1), \tag{1}$$

则Alice 和Bob将该轮结果作为原始比特保留下来。其中M表示Alice和Bob选择划分区间$[0,2\pi)$的片数。而第 i 次测量结果也被称为成功测量事件。请注意, 如果Alice 和Bob都选择脉冲强度等于信号态强度 $\mu/2$, 则称此时获得的原始比特是在Z基下获得; 如果Alice 和Bob都选择脉冲强度等于诱骗态强度 $v_1/2$、$v_2/2$、$v_3/2$, 则称此时获得的原始比特是在X基下获得。

步骤5: X基中的原始比特用于参数估计。在Z基中随机地选取一定数量的比特进行误码估计, 其余的用于密钥提纯。

1.2　安全密钥率

协议执行后可以得到一些测量值, 包括总体增益 $Q_x(x=\mu,v_1,v_2,v_3)$ 和比特误码率 E_μ^Z。根据原 PM-QKD协议[2], 密钥率可表示为

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

式中: f为误差修正效率, E_μ^Z为比特误码率, E_μ^X为相位误码率, $H(x)=-x\log_2 x-(1-x)\log_2(1-x)$为二元香农信息函数。相位误码率可以表示为

$$E_\mu^{\mathrm{X}}=\sum_{k=0}^{\infty}q_{2k+1}e_{2k+1}^{\mathrm{Z}}+\sum_{k=0}^{\infty}q_{2k}(1-e_{2k}^{Z})\leq q_0e_0^Z+\left(q_1e_1^Z+q_3e_3^Z+q_5e_5^Z\right)+\left(1-q_0-q_1-q_3-q_5\right), \tag{3}$$

式中: $q_k=Q_{k,\mu}/Q_\mu$表示光子数为 k 的脉冲的增益在总增益中的比例, e_k^Z 表示光子数为 k 的脉冲的误码率, $Q_{k,\mu}$表示光子数为 k 的脉冲增益, 并且 $e_0^Z=0.5$。根据 (3) 式可计算 q_k 和 e_k^Z 在$0\leq k\leq 5$ 时的值。

对于本研究所提出的四强度诱骗态PM-QKD协议, 其密钥率可修正为

$$R=\frac{2}{M}\left\{\sum_{k=0}^{2}Q_{k,\mu}\left[1-H\left(E_\mu^{\mathrm{X}}\right)\right]-fQ_\mu H\left(E_\mu^{\mathrm{Z}}\right)\right\}, \tag{4}$$

式中: $Q_{k,\mu}=p_\mu(k)Y_k$为信号态中光子数为 k 的脉冲的增益, $p_\mu(k)$表示强度为μ的脉冲中光子数为k的概率。Y_k为光子数为 k 的脉冲的增益, 不能直接测量得到, 但它和光子数为 k 的脉冲的误码率 e_k^Z 可以通过诱骗态法估算出来。

相位误码率可以被改写为

$$\begin{aligned}E_\mu^X=&\sum_{k=0}^{\infty}q_{2k+1}e_{2k+1}^Z+q_0e_0^Z+q_2\left(1-e_2^Z\right)+\sum_{k=2}^{\infty}q_{2k}-\sum_{k=2}^{\infty}q_{2k}e_{2k}^Z\leq\\&\sum_{k=0}^{\infty}q_{2k+1}e_{2k+1}^Z+q_0e_0^Z+q_2\left(1-e_2^Z\right)+\left(1-q_0-q_2-q_{odd}\right)=\\&\sum_{k=0}^{\infty}q_{2k+1}e_{2k+1}^Z+q_0e_0^Z-q_2e_2^Z+\left(1-q_0-q_{\mathrm{odd}}\right).\end{aligned} \tag{5}$$

在存在1个信号态和3个诱骗态的情况下, 只能估计$0\le k\le 2$时的q_k和e_k^Z, 则相位误码率为

$$E_\mu^X = q_0 e_0^Z + q_1 e_1^Z - q_2 e_2^Z + \left(1 - q_0 - q_1\right). \tag{6}$$

可以通过诱骗态法得到Y_0、Y_1、Y_2的下界和e_1、e_2的上界[15]。使用相同的方法可以估算出Y_1、Y_2的上界和e_1、e_2的下界, 分别表示为

$$Y_1^{\mathrm{U}} = \frac{Q_{v_1}\mathrm{e}^{v_1} - Q_{v_2}\mathrm{e}^{v_2}}{v_1 - v_2}, \tag{7}$$

$$Y_2^{\mathrm{U}} = \frac{2\left[\left(v_2 - v_3\right)Q_{v_1}\mathrm{e}^{v_1} - \left(v_1 - v_3\right)Q_{v_2}\mathrm{e}^{v_2} + \left(v_1 - v_2\right)Q_{v_3}\mathrm{e}^{v_3}\right]}{(v_1 - v_2)(v_1 - v_3)(v_2 - v_3)}, \tag{8}$$

$$e_1^{\mathrm{L}} = \frac{\mu\left(E_{v_1}Q_{v_1}\mathrm{e}^{v_1} - E_{v_2}Q_{v_2}\mathrm{e}^{v_2}\right)}{(v_1 - v_2)(\mu - v_1 - v_2)Y_1^{\mathrm{U}}} - \frac{v_1 + v_2}{\mu(\mu - v_1 - v_2)Y_1^{\mathrm{U}}}\left(E_\mu Q_\mu \mathrm{e}^{\mu} - e_0^Z Y_0^{\mathrm{L}}\right), \tag{9}$$

$$e_2^{\mathrm{L}} = \frac{2\mu\left[(v_2 - v_3)\left(E_{v_1}Q_{v_1}\mathrm{e}^{v_1} - E_{v_2}Q_{v_2}\mathrm{e}^{v_2}\right) - (v_1 - v_2)\left(E_{v_2}Q_{v_2}\mathrm{e}^{v_2} - E_{v_3}Q_{v_3}\mathrm{e}^{v_3}\right)\right]}{(v_1 - v_2)(v_1 - v_3)(v_2 - v_3)(\mu - v_1 - v_2 - v_3)Y_2^{\mathrm{U}}} - \frac{2\left(v_1 + v_2 + v_3\right)}{\mu^2(\mu - v_1 - v_2 - v_3)Y_2^{\mathrm{U}}}\left(E_\mu Q_\mu \mathrm{e}^{\mu} - e_0^Z Y_0^{\mathrm{L}} - e_1^L Y_1^{\mathrm{L}}\mu\right). \tag{10}$$

2 仿真结果与性能分析

对四强度诱骗态PM-QKD协议的性能进行了仿真, 仿真参数[17]为探测器的暗计数率$p_{\mathrm{d}} = 1\times10^{-8}$, 空脉冲的错误率$e_0 = 0.5$, 探测器的响应效率$\eta_{\mathrm{d}} = 0.2$, 光纤的传输损耗$\alpha = 0.2$ dB/km, 数据协商的效率f=1.1。此外, 不对准错误率为0.38%[5]。

图1为本研究所提出的使用四诱骗态方法的PM-QKD协议和原始PM-QKD协议 (使用三个诱骗态和无限诱骗态的PM-QKD协议) 的性能仿真曲线。结果表明, 这两种协议的密钥速率都随着传输距离的增加而减小, 并且本研究所提出协议的性能始终接近于原始协议的性能。原始协议中使用的无限诱骗态方法实际上无法实现, 所以四强度诱骗态PM-QKD协议可以在实际实现中替代原始协议。此外, 还给出了使用三强度诱骗态的PM-QKD协议的性能曲线, 其性能与四强度诱骗态的PM-QKD协议基本相同。

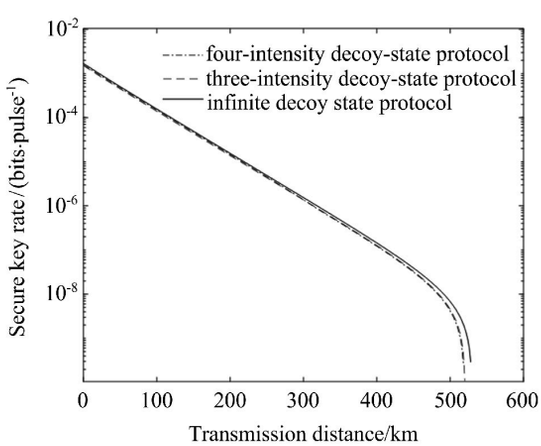

图1 具有四个诱骗态、三个诱骗态和无限诱骗态的PM-QKD协议的密钥生成率

Fig.1 Key generation rate of the PM-QKD protocol with four decoy states, three decoy states and infinite decoy states

3 结　论

提出了使用四强度诱骗态放入PM-QKD协议, 推导了所提出协议的安全密钥率公式并对参数进行了估计。仿真结果表明, 所提出协议的密钥生成速率略小于原PM-QKD协议, 证明了该协议在实际应用中能够替代原协议, 为大电网广域协调控制的安全性提升奠定了基础。

参考文献:

[1] 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): 400-403.

[2] Sha Y T, Feng B, Jia W, *et al*. A method to eliminate influence of fluctuation of light source on performance of quantum key distribution [J]. *Chinese Journal of Quantum Electronics*, 2020, 37(1): 57-62.
沙倚天, 冯 宝, 贾 玮, 等. 减轻光源抖动对量子密钥分发性能影响的方法 [J]. 量子电子学报, 2020, 37(1): 57-62.

[3] Jiang H H, Feng B, Lu M, *et al*. Round-robin differential-phase-shift quantum key distribution without three-photon pulses [J]. *Chinese Journal of Quantum Electronics*, 2020, 37(2): 172-178.
姜红红, 冯 宝, 陆 丞, 等. 不含三光子脉冲的环回差分相位量子密钥分发[J]. 量子电子学报, 2020, 37(2): 172-178.

[4] Li F Y, Wang D, Wang S, *et al*. Effect of electromagnetic disturbance on the practical QKD system in the smart grid [J]. *Chinese Physics B*, 2014, 23(12): 124201.

[5] Ma X F, Zeng P, Zhou H Y. Phase-matching quantum key distribution [J]. *Physical Review X*, 2018, 8(3): 031043.

[6] 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): 062323.

[7] 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): 034053.

[8] Wang S, He D Y, Yin Z Q, *et al*. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system [J]. *Physical Review X*, 2019, 9(2): 021046.

[9] Curty M, Azuma K, Lo H K. Simple security proof of twin-field type quantum key distribution protocol [J]. *NPJ Quantum Information*, 2019, 5: 64.

[10] Chen J P, Zhang C, Liu Y, *et al*. Twin-field quantum key distribution over 511 km optical fiber linking two distant metropolitans [OL]. 2021, arXiv: 2102.00433, https://arxiv.org/abs/2102.00433.

[11] Chen J P, Zhang C, Liu Y, *et al*. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km [J]. *Physical Review Letters*, 2020, 124(7): 070501.

[12] Wang X B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light [J]. *Physical Review A*, 2005, 72(1): 012322.

[13] Yu Z W, Zhou Y H, Wang X B. Three-intensity decoy-state method for measurement-device-independent quantum key distribution [J]. *Physical Review A*, 2013, 88(6): 062339.

[14] Wang L, Zhao S M, Gong L Y, *et al*. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum [J]. *Chinese Physics B*, 2015, 24(12): 120307.

[15] Zhang Y Y, Bao W S, Zhou C, *et al*. Practical round-robin differential phase-shift quantum key distribution [J]. *Optics Express*, 2016, 24(18): 20763-20773.

[16] Zhou Y H, Yu Z W, Wang X B. Making the decoy-state measurement-device-independent quantum key distribution practically useful [J]. *Physical Review A*, 2016, 93(4): 042324.

[17] 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): 2227-2243.