DOI: 10.3969/j.issn.1007-5461.2023.05.010

基于光源检测的相位匹配量子密钥分发协议

胡倩倩[1,2]， 冯 宝[1,2]， 闫龙川[3]， 赵晓红[4]，
陈智雨[3]， 李文婷[5]， 李 威[5*]

(1 南瑞集团有限公司/国网电力科学研究院有限公司， 江苏 南京 210000;
2 南京南瑞国盾量子技术有限公司， 江苏 南京 210000;
3 国家电网有限公司信息通信分公司， 北京 100000;
4 国网山东省电力公司电力科学研究院， 山东 济南 250000;
5 南京邮电大学， 江苏 南京 210003)

摘 要: 量子密钥分发 (QKD) 在信道中容易丢失信息载体, 因此有限的通信距离和密钥生成速率是其应用的主要瓶颈。一般而言, 密钥速率受信道传输速率的限制, 而相位匹配量子密钥分发 (PM-QKD) 协议的提出克服了线性密钥速率的约束, 即安全密钥速率与传输速率的平方根成正比。虽然PM-QKD协议可以保证探测器的安全性, 但光源方面仍存在一些缺陷。在PM-QKD协议中, 一般假设光源为理想相干态, 而这与实际的QKD系统不完全相符, 从而造成一些安全问题。本研究讨论了光子数分布未知条件下的PM-QKD协议, 证明了光子数分布未知条件下的安全性分析仍然是合理的, 也表明基于光源检测的PM-QKD协议产生的密钥率与理想光源下的密钥率基本一致。

关 键 词: 量子信息; 量子密钥分发; 相位匹配; 光源监测; 光源涨落; 光子数分布
中图分类号: O431.2 **文献标识码:** A **文章编号:** 1007-5461(2023)05-00712-07

Phase-matching quantum key distribution with light source monitoring

HU Qianqian[1,2], *FENG Bao*[1,2], *YAN Longchuan*[3], *ZHAO Xiaohong*[4],
CHEN Zhiyu[3], *LI Wenting*[5], *LI Wei*[5*]

(1 NARI Group Co., Ltd. (State Grid Electric Power Research Institute Co., Ltd.) , Nanjing 210000, China;
2 NRGD Quantum Technology Co., Ltd., Nanjing 210000, China;
3 State Grid Information Communication Technology Co., Ltd, Beijing 100000, China;
4 Electric Power Research Institute of State Grid Fujian Electric Power Co., Ltd., Jinan 250000, China;
5 Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Quantum key distribution (QKD) is easy to lose information carriers in channels, so the limited communication distance and key generation rate are the main bottlenecks of its application. Generally, the

基金项目: 国家电网公司科技项目 (SGSDDK00WJJS1900368)
作者简介: 胡倩倩 (1986 -) , 女, 安徽怀宁人, 硕士, 工程师, 主要从事量子通信技术、电力通信技术等方面的研究。
E-mail: huqianqian@sgepri.sgcc.com.cn
收稿日期: 2021-05-07; **修改日期:** 2021-07-01
*通信作者。 E-mail: alfred_wl@njupt.edu.cn

key rate is limited by the channel transmission rate. The proposed phase-matching quantum key distribution (PM-QKD) protocol overcomes the linear key rate constraint that the secure key rate is proportional to the square root of the transmission rate. Although the PM-QKD protocol can guarantee the security of the detector, there are still some defects in the light source. In the PM-QKD protocol, it is generally assumed that the light source is an ideal coherent state, which is not consistent with the actual QKD system, resulting in some security problems. In this paper, the PM-QKD protocol is discussed under the condition of unknown photon number distribution (UPD), and it's confirmed that the security analysis is still reasonable under the condition of unknown photon number distribution, and it's also shown that the key rate generated by PM-QKD protocol based on light source detection is basically consistent with the key rate under ideal light source.

Key words: quantum information; quantum key distribution; phase-matching; light source monitoring; source fluctuation; photon number distribution

0　引　言

量子密钥分发 (QKD)[1, 2]是量子信息科学中最成功的应用之一, 其安全性在20世纪末已经得到证明[3−5]。目前, 量子技术在生活中的应用开发引起了广泛关注, 包括20世纪90年代初32 cm通信距离的首次演示[6]到最近距离地球1200多公里的墨子号卫星上进行的QKD[7]。QKD技术在理论和实践上都取得了很大进步, QKD协议的发展从最开始的BB84协议[1], 到为解决各种潜在的安全性问题衍生出的多种协议, 例如诱骗态协议、测量设备无关协议 (MDI)[8]以及循环差分相移协议 (RRDPS)[9]。光子因高传输速度和对环境退相干具有较强的抵抗力, 在QKD的实验论证和实际应用中被用作信息载体[10]。此外, 光量子通信还可以很容易并入到当前的电信网络基础设施。光量子通信实际应用的主要障碍是光子的传输损耗, 这导致QKD协议生成的密钥率受到了一定的限制。传输的码率由信道的传输效率η表征, 它被定义为单个光子成功通过信道并被探测到的概率。目前实施的主流QKD方案 (例如BB84协议[1]) 都将单光子源用于密钥信息的编码, 其中η成为密钥生成速率的基本上限。更严格的推导表明, 密钥速率界限正比于η[11]。2018 年, Lucamarini等[12]提出一种基于一阶干涉的双场量子密钥分发协议 (TF-QKD) , 其可以突破现有的传输距离对密钥率的限制, 超越QKD协议中的PLOB界[11], 成为量子信息领域的研究热点[13−15]。TF-QKD协议的主要缺点是由相位随机化引起的安全问题, 因此, 研究人员不断提出了改进的TF-QKD协议[16−18], 从而通过不同方法来弥补原工作中不完整的安全性分析, 例如使用预先选择的全局相位或其他方法来对信号进行分类。

受TF-QKD协议[12]的启发, Cui等[19]提出了相位匹配量子密钥分发协议 (PM-QKD), 该协议通过增加额外的测试模式, 解决了原TF-QKD协议的安全漏洞。在PM-QKD协议中, 通信双方Alice和Bob独立地准备两个相干态, 并通过选择后相位匹配将密钥信息编码到公共相位中, 通过第三方的检测结果获得密钥。仿真结果表明, PM-QKD协议可以超越基于单光子的QKD协议中传输效率对密钥率的限制; 在安全性方面, 由于测量设备的独立性, PM-QKD协议可以抵抗所有的探测攻击。PM-QKD协议存在的问题是在光源端制备的量子态假设为理想相干态, 而实际上, 由于激光器的非理想性, 制备态将偏离理想相干态, 因此假设可能被打

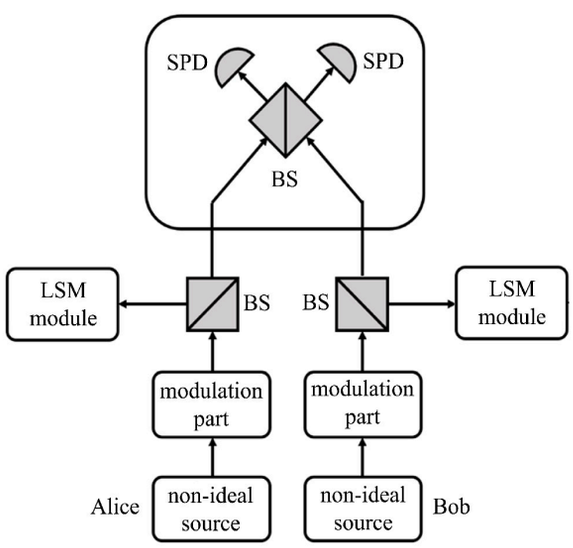
破[20]。除此之外, PM-QKD 协议中的光源结构类似于 BB84 协议, 因此光源部分还会出现不可信问题, 这导致光源的光子数分布 (PND) 未知, 所制备的量子态可能不再是相干态。

本文进一步讨论了光子数分布未知条件下的 PM-QKD 协议。通过使用之前提出的光源检测 (LSM) 方法[21, 22], 可以为所有相关参数提供更加紧致的估值, 从而获得在光源未知 (UPC) 条件下 PM-QKD 协议的密钥率, 数值仿真表明, 该协议在 UPC 下的性能几乎同理想光源条件保持一致。此外, 本文分析了 PM-QKD 协议的诱骗态方法, 并给出了 PM-QKD 协议的密钥率计算方法; 利用 LSM 方法得到了计算密钥率所需参数的严格界限; 给出了在光子数分布未知下将 LSM 方法应用于 PM-QKD 协议的仿真结果。

1 光源检测下的 PM-QKD 协议

1.1 LSM 结构模型

PM-QKD 协议中的光源结构类似于测量设备无关的量子密钥分发协议 (MDI-QKD) 和发送或不发送的量子密钥分发协议 (SNS-QKD) , 因此可以将 MDI-QKD 协议和 SNS-QKD 协议中提出的 LSM 方案应用于 PM-QKD 协议来估计光子数概率 $P_n(\mu_k)$。Qiao 等[23]在 SNS-QKD 协议中提出一个新的 LSM 方案, 其中给出了 Alice 和 Bob 各自的严格的 $P_n(\mu_k)$、$P_n(k)$ 界限, 相同的 LSM 模块可以应用于图 1 所示的 PM-QKD 协议。



SPD: single-photon detector; BS: beam splitter; LSM: light source monitoring

图 1 具有 LSM 模块的 PM-QKD 协议结构

Fig. 1 PM-QKD protocol structure with LSM model

图 1 所示 PM-QKD 协议的具体过程如下: 1) 相干态的制备: Alice 和 Bob 两个通信方独立地产生相干态脉冲 $\sqrt{\mu_{\mathrm{A}}}\exp\left[\mathrm{i}\left(\pi k_{\mathrm{a}}+\phi_{\mathrm{a}}\right)\right]$ 和 $\sqrt{\mu_{\mathrm{B}}}\exp\left[\mathrm{i}\left(\pi k_{\mathrm{b}}+\phi_{\mathrm{b}}\right)\right]$, 并将他们的密钥信息 $k_{\mathrm{a}}, k_{\mathrm{b}}\in\{0,1\}$ 编码在相干态的相位上, 其中, ϕ_{a}, $\phi_{\mathrm{b}}\in\left\{j_{\mathrm{a}}\frac{2\pi}{M}, j_{\mathrm{b}}\frac{2\pi}{M}\right\}$, $j_{\mathrm{a}}, j_{\mathrm{b}}\in\{0,1,\cdots,M-1\}$, M 是相位划分片数; 2) 测量: 光束经过 BS 被分为两路, 一路被 LSM 模块用于估计光源的光子数分布概率, 然后通过改变光源检测模块中衰减器 (VOA) 的衰减率 η_i, 获得对应衰减率下光源模块中探测器不响应的概率 $P^{\mu_k}(\eta_i)$; 另一路被发送到不可信第三方 Charlie 进行干涉测量 (成功的测量事件是两个探测器有且只有一个响应), 这种相干测量将 Alice 和 Bob 的信号相位进行匹

配; 3) 公布参数: Charlie 宣布每轮的测量结果, 在所公布的成功测量事件下, Alice 和 Bob 的密钥是相关的; Alice 和 Bob 宣布各自信号的强度设置(μ_A,μ_B)及其随机相位数(j_a,j_b); 随后使用相位后补偿的方式计算相位差(ϕ_δ)并宣布对应的相位片数j_δ; 4) 筛选: Charlie 宣布测量成功的事件后, 如果右边探测器响应且$|j_a-j_b-j_s|\bmod M\in\frac{M}{2}$、相位差$\phi_{ab}=\phi_a-\phi_b-\phi_\delta\in\left(-\frac{\pi}{M}+\pi,\ \frac{\pi}{M}+\pi\right)$, Bob 将翻转其密钥信息$k_b$; Alice 和 Bob 将以$j_s=(j_a-j_b)\bmod M$来分组信号, 这些$j_s$组成集合$J$; 5) 参数估计: 根据 LSM 模块中获得的$P^{\mu_k}(\eta_i)$估计出光源中零光子、单光子、双光子的概率, 由此使用诱骗态方法估计出单光子率的下界(q_{1L})及相位错误$(E^{ph}=q_{evenU})$; 6) 密钥率生成: 重复上述步骤 1) ～5), 直到筛选出足够的密钥信息; 最后在密钥信息上执行错误纠正及保密增强获得最终完整的密钥。

1.2　密钥参数估计

在上述 PM-QKD 协议中, 利用参考文献 [24] 中 LSM 模块的估计方法可以获得对光源的光子数分布概率估计。对于 LSM 模块, 分别设置衰减器的衰减率为$\eta_0=0.95$, $\eta_1=0.95$, $\eta_2=0.9$; 通过 LSM 模块中探测器不响应的概率$P^{\mu_k}(\eta_i)$与光子数概率$P_n(\mu_k)$的关系$P^{\mu_k}(\eta_i)=(1-P_d)\sum_{n=0}(1-\eta_i)P_n(\mu_k)$, 可以获得对应不同光源强度下零光子、单光子、双光子概率的严格上下界$P_{nL(U)}(\mu_k)$, 其中$n=0,1,2$分别对应于零光子态、单光子态和双光子态, $L(U)$表示概率的下界 (上界) , μ_k表示光源的强度。

根据 PM-QKD 协议[25]中的密钥率分析, 其相位错误率$E^{ph}=q_{even}$, 其中q_{even}是偶光子数概率, 此时具有 LSM 模块的 PM-QKD 协议的密钥率即可表示为

$$R=\frac{2Q_\mu}{M}\sum_{j_s\in J}\left[1-H\left(q_{even,U}\right)-fH\left(E_{j_s}\right)\right], \tag{1}$$

式中: Q_μ是一个光源强度μ下的产生率, M是 PM 协议中所选择的相位数, $q_{even,U}$是偶光子数概率估计的上界, 此处主要使用三强度诱骗态方法及 LSM 模块去估计$q_{even,U}$, 用v_0、v_1、μ表示三个光源强度, 其中Q_0可以通过真空诱骗态$(v_0=0)$直接获得。在原始的 PM-QKD 协议中, 要假设光源能够制备理想的相干态; 然而在光源检测下的 PM-QKD 协议舍弃了理想信源的假设, 可以这种光源检测的方法严格得到光子数的概率, 即可严格估计出相位错误率

$$E^{ph}=q_{even,U}=1-q_{1L}=1-P_{1L}(\mu)\frac{Y_{1L}}{Q_\mu}\ , \tag{2}$$

其中, 使用诱骗态方法可以估计出单光子响应率的下界

$$Y_{1L}=\frac{P_{2L}(\mu)Q_{v1}-P_{2L}(\mu)P_{0U}(v1)Y_0+P_{2U}(v1)P_{0L}(\mu)Y_0-P_{2U}(v1)Q_\mu}{P_{2U}(\mu)P_{1U}(v1)-P_{1L}(v1)P_{1L}(\mu)}\ . \tag{3}$$

1.3　光源涨落

在实际的 QKD 系统中, 光源信号的光子数分布 (PND) 是非固定的, 即存在光源强度涨落的问题。在这种情况下, 即使不考虑未知 PND 所造成的安全问题, PM-QKD 协议的性能也会大大降低。因此, 通过考虑光源强度涨落来分析 PM-QKD 协议是必要的。假设光源发出的信号可以被认为是强度存在一定涨落的相干

态, 其平均光子数呈高斯分布。

对于LSM模块, 假设光源的光子数满足泊松分布, 则探测器不响应的概率为$P^{\mu_k}(\eta_i)=(1-P_{\rm d})\mathrm{e}^{-\eta\mu_k}$, 并且信号经过衰减后仍会有高斯分布的平均光子数$\mu_k$, 因此概率$P^{\mu_k}(\eta_i)$可以模拟成

$$P^{\mu_k}(\eta_i)=(1-P_{\rm d})\exp\left[-\eta_i\mu_0-\frac{(\eta_i\sigma_{\mu_k})^2}{2}\right], \tag{4}$$

式中$\sigma_{\mu_k}=\sigma\mu_0$, σ_{μ_k}是μ_k的标准差。在不同的涨落系数$\sigma=\frac{\sigma_{\mu_k}}{\mu_0}$下, 利用上述光源涨落模型来模拟原始PM-QKD协议和具有LSM模块的PM-QKD协议的性能, 具有LSM模块的PM-QKD协议在原始PM-QKD协议上相对不同的传输距离进行了优化。

2 仿真分析

表1为本研究所用到相关仿真参数, 其中α为信道损耗系数, $P_{\rm d}$为探测器暗计数率, $\eta_{\rm d}$为检测效率, $e_{\rm d}$为QKD系统的失调误差, f为纠错效率, M为PM -QKD协议中的相位片数。用表1中的参数对具有LSM模块的PM-QKD协议与原始PM-QKD协议进行模拟仿真, 仿真结果如图2所示, 其中LSM方案 (红色曲线) 的性能几乎与具有理想光源的PM-QKD协议 (蓝色曲线) 一样好, 它们的传输最大距离分别为504 km和507 km。

表 1 PM−QKD−LSM协议仿真参数

Table 1 Simulation parameters of PM−QKD−LSM protocol

Parameter	Value
Coefficient of transmittance loss α	0.2
Dark count rate $P_{\rm d}$	10^{-8}
Misalignment error $e_{\rm d}$	0.1
Number of phase slices M	16
Error correction efficiency f	1.14
Detector efficiency $\eta_{\rm d}$	0.2

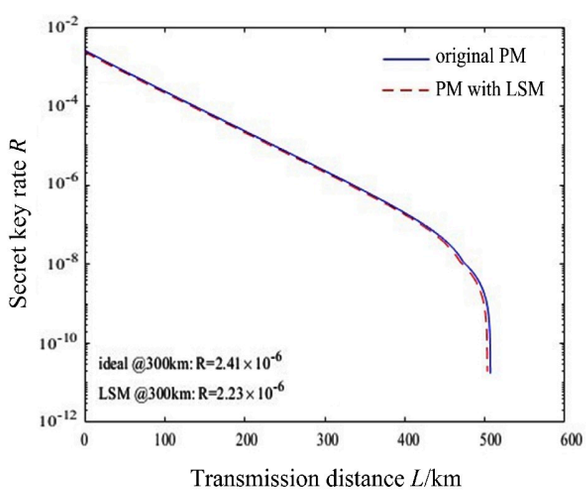


图 2 具有 LSM 模块的PM-QKD 协议与原始 PM-QKD 协议仿真图

Fig. 2 Simulation of PM-QKD with LSM model and the original PM-QKD

使用相同参数分别对考虑光源强度涨落的原始PM-QKD 协议和具有LSM模块的 PM-QKD 协议进行仿真, 结果如图 3所示, 在光源强度涨落下, 强度涨落虽然会对具有LSM模块的PM-QKD协议的密钥率产生微小的影响, 但是其性能明显优于在光源强度涨落条件下的原始PM-QKD协议。

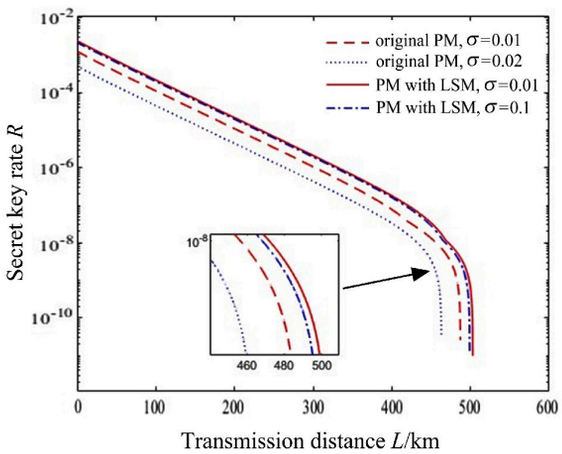


图 3　在 LSM 模块下考虑光源涨落的 PM-QKD 协议仿真图

Fig. 3　Simulation of PM-QKD with LSM model under the condition of light source fluctuation

3　结　论

分析了具有LSM模块的 PM-QKD协议的安全性, 并利用 LSM方案解决了信源的不可信问题, 该问题实际上是PM-QKD协议的一个安全漏洞。将LSM方案应用于PM-QKD协议, 精确地估计光子数的概率分布 $P_n(\mu_k)$, 并得到密钥率的一个紧致的下界。仿真结果表明, 在UPC的情况下, 使用LSM方案可以使该协议的性能几乎可以和具有理想信源的原PM协议相同。此外在考虑光源涨落的情况下, LSM方案提高了 PM-QKD协议的性能, 表明在实际QKD系统中PM-QKD协议在考虑光源强度涨落的情况下仍然具有很长的传输距离。

参考文献:

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [J]. *Theoretical Computer Science*, 2014, 560: 7-11.

[2] Ekert A K. Quantum cryptography based on Bell's theorem [J]. *Physical Review Letters*, 1991, 67(6): 661-663.

[3] Mayers D. Unconditional security in quantum cryptography [J]. *Journal of the ACM*, 2001, 48(3): 351-406.

[4] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances [J]. *Science*, 1999, 283 (5410): 2050-2056.

[5] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. *Physical Review Letters*, 2000, 85(2): 441-444.

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

[7] Liao S K, Cai W Q, Liu W Y, *et al*. Satellite-to-ground quantum key distribution [J]. *Nature*, 2017, 549(7670): 43-47.

[8] 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.

[9] Guan J Y, Cao Z, Liu Y, *et al*. Experimental passive round-robin differential phase-shift quantum key distribution [J]. *Physical Review Letters*, 2015, 114(18): 180502.

[10] Wang S, Yin Z Q, Chen W, *et al*. Experimental demonstration of a quantum key distribution without signal disturbance monitoring [J]. *Nature Photonics*, 2015, 9(12): 832-836.

[11] Pirandola S, Laurenza R, Ottaviani C, *et al*. Fundamental limits of repeaterless quantum communications [J]. *Nature Communications*, 2017, 8: 15043.

[12] 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.

[13] Chen G, Wang L, Li W, *et al*. Multiple-pulse phase-matching quantum key distribution [J]. *Quantum Information Processing*, 2020, 19(11): 416.

[14] Tamaki K, Lo H K, Wang W Y, *et al*. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound [OL]. 2018, arXiv: 1805.05511, https: //arxiv.org/abs/1805.05511.

[15] 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.

[16] Grasselli F, Curty M. Practical decoy-state method for twin-field quantum key distribution [J]. *New Journal of Physics*, 2019, 21 (7): 073001.

[17] 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.

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

[19] Cui C H, Yin Z Q, Wang R, *et al*. Twin-field quantum key distribution without phase post selection [J]. *Physical Review Applied*, 2019, 11(3): 034053.

[20] Wang X B. Decoy-state quantum key distribution with large random errors of light intensity [J]. *Physical Review A*, 2007, 75 (5): 052301.

[21] Wang G, Li Z Y, Qiao Y C, *et al*. Light source monitoring in quantum key distribution with single-photon detector at room temperature [J]. *IEEE Journal of Quantum Electronics*, 2018, 54(3): 1-10.

[22] Qiao Y C, Wang G, Li Z Y, *et al*. Monitoring an untrusted light source with single-photon detectors in measurement-device-independent quantum key distribution [J]. *Physical Review A*, 2019, 99(5): 052302.

[23] Qiao Y C, Chen Z Y, Zhang Y C, *et al*. Sending-or-not-sending twin-field quantum key distribution with light source monitoring [J]. *Entropy*, 2020, 22(1): 36.

[24] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution [J]. *Physical Review Letters*, 2005, 94(23): 230504.

[25] Zeng P, Wu W J, Ma X F. Symmetry-protected privacy: Beating the rate-distance linear bound over a noisy channel [J]. *Physical Review Applied*, 2020, 13(6): 064013.