

一种K分布强湍流下的测量设备无关量子密钥分发方案

谷文苑 赵尚弘 东晨 朱卓丹 屈亚运

Measurement-device-independent quantum key distribution under K-distributed strong atmospheric turbulence

Gu Wen-Yuan Zhao Shang-Hong Dong Chen Zhu Zhuo-Dan Qu Ya-Yun

引用信息 Citation: *Acta Physica Sinica*, 68, 090302 (2019) DOI: 10.7498/aps.68.20182130

在线阅读 View online: <https://doi.org/10.7498/aps.68.20182130>

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

弱相干光源测量设备无关量子密钥分发系统的性能优化分析

Analysis on performance optimization in measurement-device-independent quantum key distribution using weak coherent states

物理学报. 2016, 65(10): 100302 <https://doi.org/10.7498/aps.65.100302>

基于弱相干光源测量设备无关量子密钥分发系统的误码率分析

Analysis on quantum bit error rate in measurement-device-independent quantum key distribution using weak coherent states

物理学报. 2015, 64(11): 110301 <https://doi.org/10.7498/aps.64.110301>

基于量子存储的长距离测量设备无关量子密钥分配研究

Long distance measurement device independent quantum key distribution with quantum memories

物理学报. 2015, 64(14): 140304 <https://doi.org/10.7498/aps.64.140304>

基于相干叠加态的非正交编码诱骗态量子密钥分发

Nonorthogonal decoy-state quantum key distribution based on coherent-state superpositions

物理学报. 2016, 65(8): 080301 <https://doi.org/10.7498/aps.65.080301>

PM2.5大气污染对自由空间量子通信性能的影响

Influences of PM2.5 atmospheric pollution on the performance of free space quantum communication

物理学报. 2015, 64(15): 150301 <https://doi.org/10.7498/aps.64.150301>

基于散粒噪声方差实时监测的连续变量量子密钥分发系统的设计与实现

The design and realization of continuous-variable quantum key distribution system based on real-time shot noise variance monitoring

物理学报. 2017, 66(2): 020301 <https://doi.org/10.7498/aps.66.020301>

一种 K 分布强湍流下的测量设备无关量子密钥分发方案*

谷文苑¹⁾ 赵尚弘¹⁾ 东晨^{2)†} 朱卓丹¹⁾ 屈亚运²⁾

1) (空军工程大学信息与导航学院, 西安 710077)

2) (国防科技大学信息与通信学院, 西安 710006)

(2018 年 12 月 3 日收到; 2019 年 3 月 1 日收到修改稿)

研究了 K 分布强湍流下自由空间测量设备无关量子密钥分发协议模型, 采用阈值后选择方法来减少大气湍流对密钥生成率的影响, 对比分析了使用阈值后选择方法前后协议的密钥率和湍流强度之间的关系. 仿真结果表明, 使用阈值后选择方法可以有效地提高协议的密钥生成率, 尤其是在高损耗和强湍流区域, 而且其最佳阈值与湍流强度、信道平均损耗有关, 对实际搭建性能较好的自由空间测量设备无关量子密钥分发协议系统具有一定的参考价值.

关键词: 强湍流, K 分布, 测量设备无关量子分发协议, 自由空间

PACS: 03.67.Dd

DOI: 10.7498/aps.68.20182130

1 引言

量子密钥分发 (quantum key distribution, QKD)^[1-6] 以量子力学基本原理和性质为基础, 在理论上能够保证通信双方密钥分配的绝对安全性, 是量子保密通信领域^[7-10] 的一个重要研究内容, 具有巨大的发展前景. 但实际 QKD 系统的设备往往与理想情况存在一些差距, 使得系统安全通信距离受到限制, 特别是光纤损耗已经成为限制 QKD 安全通信距离的主要原因, 使其很难实现广域量子通信组网. 2016 年, 中国科学技术大学 Pan 课题组^[11] 采用诱骗态测量设备无关量子密钥分发协议 (measurement device independent quantum key distribution, MDI-QKD) 优化方案并使用低损耗光纤实现了 404 km 的通信距离, 这也是目前通过光纤信道进行 QKD 实验能达到的最远安全通信距离. 为实现超远距离量子通信技术的突破,

已有研究试图利用高空平台建立高稳定低损耗的自由空间信道^[12-16]. 2015 年, 意大利小组利用激光测距卫星 Jason-2 实现了平均量子误码率为 6.5% 的偏振编码 QKD 实验^[17]. 2017 年, 日本小组利用微小卫星 SOCRATES 实现了平均量子误码率小于 5% 的偏振编码 QKD 实验^[18]. 中国成功发射的“墨子号”量子卫星完成了星地量子通信等多项实验^[19-22]. 可见, 基于卫星中继的自由空间 QKD 已经成为量子通信研究的一个热点问题.

虽然基于卫星中继的自由空间 QKD 存在很多优势, 但其在实际应用中仍会受到大气信道的限制^[23]. 大气温度和压力改变导致的大气折射率的随机变化会引起光束漂移和光强闪烁等大气湍流效应, 具体表现为光信号的光强起伏和相位噪声, 从而导致信道传输率随时间变化, 严重影响安全密钥产生速率. 在强湍流条件下, 光信号受到的影响和干扰将会更大. 针对不同的大气湍流强度, 已经提出了多种信道传输率分布模型, 如对数正态模

* 国家自然科学基金青年科学基金 (批准号: 11704412) 和国防科技大学校内重点项目 (批准号: zk-17-02-09) 资助的课题.

† 通信作者. E-mail: dongchengfk@163.com

型、K 分布模型等^[24–26]. 其中, 在弱湍流情况下应用最为广泛的对数正态模型不能直接用来描述强湍流条件下大气信道传输率的分布. 而 K 分布模型主要用来描述强湍流情况下大气信道传输率的分布^[27–29]. 因此, 本文采用 K 分布信道传输率分布模型分析强湍流条件下的自由空间 MDI-QKD 协议的基本性能, 并使用阈值后选择方法来减少大气湍流对密钥生成率的影响^[30].

2 理论与模型

2.1 强湍流条件下的 MDI-QKD 模型

为克服探测设备的非完美性问题, Lo 等^[31]基于时间反演的 Einstein-Podolsky-Rosen 思想和纠缠分发协议, 于 2012 年首次提出 MDI-QKD 协议. 该协议在关闭探测端所有安全漏洞的同时提高了安全传输距离. 自由空间 MDI-QKD 系统模型如图 1 所示.

Alice 和 Bob 随机选择直角基 (z 基) 或对角基 (x 基) 对产生的相干光脉冲进行编码后将其发送至非可信的第三方进行 Bell 态测量. 第三方公布测量结果, Alice 和 Bob 通过基对比过程对原始密钥进行筛选, 最终生成密钥. 基于三强度的诱骗态的 MDI-QKD 密钥率的公式为^[32]

$$R \geq \mu_2 \nu_2 e^{-\mu_2 - \nu_2} Y_{11}^Z [1 - H(e_{11}^X)] - Q_{\mu_2 \nu_2}^Z f(E_{\mu_2 \nu_2}^Z) H(E_{\mu_2 \nu_2}^Z), \quad (1)$$

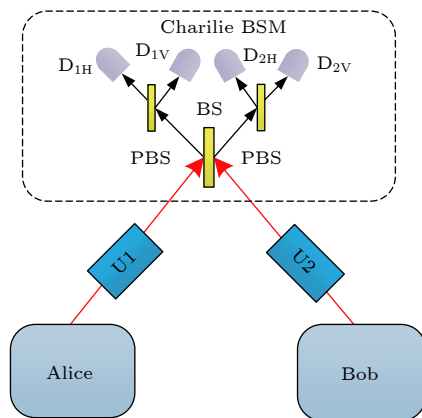


图 1 自由空间测量设备无关量子密钥分发模型示意图 (BS, 50 : 50 光分束器; PBS, 偏振光分束器; D_{1H}, D_{2H}, D_{1V}, D_{2V}, 单光子探测器; U1 (U2), Alice 和 Bob 的大气信道)

Fig. 1. Free space MDI-QKD diagram. BS, 50 : 50 beam splitter; PBS, polarized beam splitter; D_{1H}, D_{2H}, D_{1V}, D_{2V}, single-photon detector; U1 (U2), Alice and Bob's atmospheric channel.

式中 Q_{11}^Z 为 Alice 和 Bob 都发送单光子态且选择 Z 基编码时的增益, e_{11}^X 为 Alice 和 Bob 都发送单光子态且选择 X 基编码时的量子误码率, $Q_{\mu_2 \nu_2}^Z$ 和 $E_{\mu_2 \nu_2}^Z$ 代表着 Alice 脉冲强度为 μ_2 和 Bob 脉冲强度为 ν_2 且两者均选择 Z 基编码时的增益和量子误码率, $\mu_2 (\mu_1, \mu_0)$ 和 $\nu_2 (\nu_1, \nu_0)$ 分别为 Alice 和 Bob 发送的相干光脉冲信号态 (诱骗态、真空态) 的强度. U1 (U2) 是 Alice (Bob) 到第三方的大气信道, 本文假设两者信道是对称的, 即 $\eta_A = \eta_B = \eta$. 在实际的自由空间 QKD 系统中量子态的传输会受到大气湍流的影响, 即 U1 (U2) 信道传输率 η 不再是一个常数, 而是随时间发生改变, 可以得到 MDI-QKD 密钥率的公式为

$$R(\eta) = \iint P_{\alpha, \eta_0}(\eta_A) P_{\alpha, \eta_0}(\eta_B) R(\eta_A, \eta_B) d\eta_A d\eta_B = \iint (P_{\alpha, \eta_0}(\eta))^2 R(\eta) d\eta d\eta, \quad (2)$$

式中 $P_{\alpha, \eta_0}(\eta)$ 为大气湍流信道传输率概率分布. 本文使用 K 分布模型来描述强湍流信道传输率概率分布, 其表达式为^[29]

$$P_{\alpha, \eta_0}(\eta) = \frac{2(\alpha)^{(\alpha+1)/2} \eta^{(\alpha-1)/2}}{\Gamma(\alpha) \eta_0^{(\alpha+1)/2}} K_{\alpha-1} \left(2\sqrt{\alpha \frac{\eta}{\eta_0}} \right), \quad (3)$$

式中 $\Gamma(\cdot)$ 为 gamma 函数; $K_{\alpha-1}(x)$ 是阶数为 $\alpha-1$ 的第二类修正贝塞尔函数; η_0 是大气信道平均传输率, 对于一个 100 km 的大气信道来说, η_0 的取值在 10^{-3} — 10^{-4} 之间; α 是与闪烁系数 σ_I^2 相关的一个信道参数 (图 2), 两者的关系为^[33]

$$\alpha = 2/(\sigma_I^2 - 1). \quad (4)$$

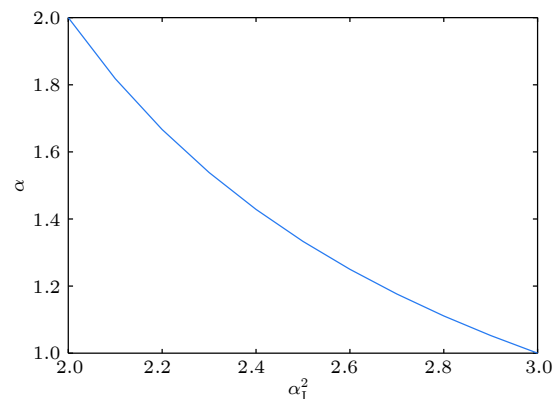


图 2 α 与闪烁系数 σ_I^2 的关系

Fig. 2. Relationship between α and scintillation coefficient σ_I^2 .

研究表明, 只有当闪烁系数 σ_I^2 取值在 (2, 3) 之间时, K 分布模型才适用于强湍流模型 [27]. 由 (4) 式可知, 信道参数 α 取值在 (1, 2) 之间, 且 α 越大, 湍流强度越小. 本文在后续仿真中将 α 随机选取 3 个值: 1.1, 1.5, 1.9.

2.2 阈值后选择下的强湍流 MDI-QKD 模型

为缓解大气湍流效应对 MDI-QKD 协议性能的影响, 本文利用文献 [14] 中的预固定阈值实时选择方法对密钥进行后处理, 即设阈值为 η_T , 当信道传输率 $\eta \geq \eta_T$ 时, 开始对信道信息进行采集, 同时丢弃 $\eta < \eta_T$ 的部分. 改进 MDI-QKD 密钥率的公式变为

$$R_{\text{postselect}}(\eta_T) = \int_{\eta_T}^1 \int_{\eta_T}^1 P_{\alpha, \eta_0}(\eta)^2 R(\langle \eta \rangle) d\eta d\eta, \quad (5)$$

式中 $\langle \eta \rangle$ 为 Alice 和 Bob 与第三方间信道的平均传输率, 其计算公式为

$$\langle \eta \rangle = \frac{\int_{\eta_T}^1 \eta P_{\alpha, \eta_0}(\eta) d\eta}{\int_{\eta_T}^1 P_{\alpha, \eta_0}(\eta) d\eta}. \quad (6)$$

由 (4) 和 (5) 式可知, 当其他实验参数固定不变时, MDI-QKD 密钥率只与阈值 η_T 有关, 即当 η_T 为最佳阈值时, $R_{\text{postselect}}(\eta_T)$ 取最大值且满足 $dR_{\text{postselect}}(\eta_T)/d\eta_T = 0$. 根据该式对 (5) 式进行求导, 并代入 (1) 和 (6) 式可以得到最佳阈值 η_T^{opt} :

$$R(\langle \eta \rangle) + R(\eta_T^{\text{opt}}) = 0. \quad (7)$$

而由 (6) 式可知, $\langle \eta \rangle$ 与信道参数 α 、平均传输率 η_0 有关. 利用 (7) 式, 通过仿真得到最佳阈值 η_T^{opt} 与信道参数 α 、平均传输率 η_0 的三维图, 如图 3 所示.

由图 3 可知, 最佳阈值 η_T^{opt} 会随信道参数 α 、平均传输率 η_0 的改变而改变. 当确定平均传输率 η_0 时, 随着信道参数 α 逐渐增大, 即湍流强度逐渐减少时, 最佳阈值 η_T^{opt} 缓慢增大, 而当信道参数 α 固定时, 随着平均传输率 η_0 逐渐增大, 最佳阈值 η_T^{opt} 逐渐增大. 然而自由空间星地上行链路损耗一般为 43 dB [34], 取此时 η_T^{opt} 的最小值 0.0018 作为最佳阈值.

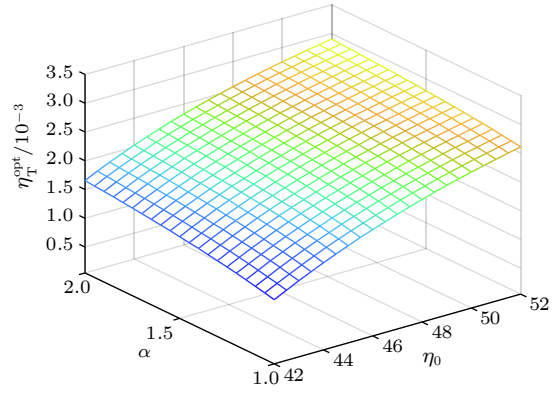


图 3 最佳阈值 η_T^{opt} 与信道参数 α 、平均传输率 η_0 的关系
Fig. 3. Relationship of optimal threshold value η_T^{opt} to channel parameter α and average transmission rate η_0 .

3 分析与讨论

根据上述推导的公式, 可以得到阈值与强湍流下 MDI-QKD 密钥率、湍流强度与强湍流下 MDI-QKD 密钥率之间的关系. 在仿真过程中, 主要采用以下参数数据 [35]: $p_d = 3 \times 10^6$ 为每个探测器的背景计数率, $f = 1.16$ 是纠错效率, $\eta_d = 14.5\%$ 是探测效率, $e_d = 1.5\%$ 是 Alice 和 Bob 总的未对准误差, 信号态和诱骗态光强分别取 0.2, 0.01.

图 4 给出了强湍流下 MDI-QKD 密钥率与阈值、信道参数的关系, 此时信道的平均损耗为 43 dB. 由图 4 可知, 当信道参数 $\alpha = 1.1$ 时, 使用阈值选择方法的 MDI-QKD 的密钥率随阈值的变化而变化, 在 η_T 趋近于 0.0018 时取最大值, 且此时的密钥率明显要高于原始的 MDI-QKD 模型. 当改变 α 的值时, 本文的方案性能发生改变, 即当 α 值增大 (湍流

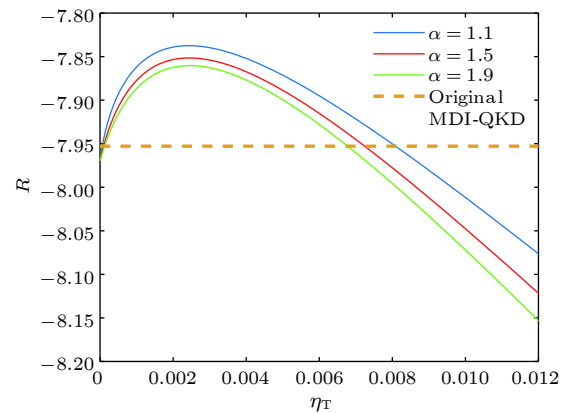


图 4 强湍流下 MDI-QKD 密钥率与阈值、信道参数的关系
Fig. 4. Relationship of key rate of MDI-QKD under strong turbulence to threshold and channel parameters.

强度变小) 时, MDI-QKD 密钥率整体有所下降, 最大密钥率对应的阈值逐渐增大.

图 5 给出了强湍流下 MDI-QKD 密钥率与信道损耗间的关系, 此时阈值为 $\eta_T = 0.0018$. 由图 5 可知, 当信道损耗较小时, 使用阈值后选择方法的 MDI-QKD 与原始的 MDI-QKD 模型密钥率曲线几乎重合, 当信道损耗较大时, 使用阈值后选择方法的 MDI-QKD 性能更优, 最多能够抵抗 52 dB 的损耗, 比原始 MDI-QKD 大 6 dB. 而且强湍流下 MDI-QKD 密钥率与信道参数有关, 即 α 越小 (湍流强度越大), MDI-QKD 抗干扰能力越强. 说明阈值后选择方法能够有效地抑制湍流对 MDI-QKD 的影响, 且湍流强度越大, 抑制效果越好.

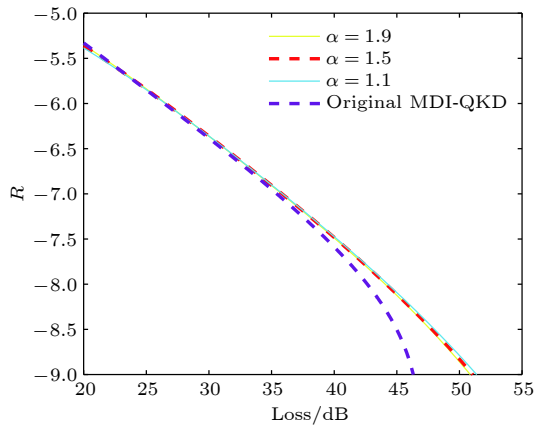


图 5 强湍流下 MDI-QKD 密钥率与信道损耗间的关系
Fig. 5. Relationship between key rate of MDI-QKD under strong turbulence and channel loss.

强湍流条件下的自由空间 MDI-QKD 在理论上是无条件安全的, 因为其采用的仍然是经典的 MDI-QKD 协议, 只是研究的信道由光纤变为了自由空间, 其后选择方案并没有发生改变, 而经典的 MDI-QKD 协议是利用该协议的后选择性关闭了探测器侧信道所有漏洞, 其安全性与信道类型无关, 因此自由空间 MDI-QKD 的安全性等同于经典的 MDI-QKD 协议^[31]. 但该协议在实际条件下的安全性问题还需要进一步深入研究, 本文就是利用阈值后选择技术降低误码率, 解决大气湍流引起的高损耗问题, 提高 QKD 系统的实际安全性.

4 结 论

本文研究了阈值后选择方法对强湍流条件下自由空间 MDI-QKD 的影响, 并分析了在 K 分布

强湍流下自由空间 MDI-QKD 系统中, 采用阈值后选择方法产生的密钥率与信道损耗、信道参数 α 、阈值之间的关系. 仿真结果表明使用阈值后选择方法的 MDI-QKD 比原始 MDI-QKD 性能更优, 尤其是在高损耗和强湍流区域, 而且其最佳阈值与湍流强度、信道平均损耗有关, 对实际搭建性能较好的自由空间 MDI-QKD 协议系统具有一定的参考价值.

参考文献

- [1] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656
- [2] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441
- [3] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325
- [4] Xu G, Chen X B, Dou Z, Yang Y X, Li Z P 2015 *Quantum Inf. Process.* **14** 2959
- [5] Dong C, Zhao S H, Zhao W H, Shi L, Zhao G H 2014 *Acta Phys. Sin.* **63** 030302 (in Chinese) [东晨, 赵尚弘, 赵卫虎, 石磊, 赵顾颢 2014 物理学报 **63** 030302]
- [6] Dong C, Zhao S H, Dong Y, Zhao W H, Zhao J 2014 *Acta Phys. Sin.* **63** 170303 (in Chinese) [东晨, 赵尚弘, 董毅, 赵卫虎, 赵静 2014 物理学报 **63** 170303]
- [7] Chen X B, Tang X, Xu G, Dou Z, Chen Y L, Yang Y X 2018 *Quantum Inf. Process.* **17** 225
- [8] Chen X B, Sun Y R, Xu G, Jia H Y, Qu Z G, Yang Y X 2017 *Quantum Inf. Process.* **16** 244
- [9] Xu G, Chen X B, Li J, Wang C, Yang Y X, Li Z P 2015 *Quantum Inf. Process.* **14** 4297
- [10] Chen X B, Wang Y L, Xu G, Yang Y X 2019 *IEEE Access* **7** 13634
- [11] Yin H L, Chen T Y, Yu Z W, Liu H, You L X, Zhou Y H, Chen S J, Mao Y, Huang M Q, Zhang W J, Chen H, Li M J, Nolan D, Zhou F, Jiang X, Wang Z, Zhang Q, Wang X B, Pan J W 2016 *Phys. Rev. Lett.* **117** 190501
- [12] Bedington R, Arrazola J M, Ling A 2017 *EPJ Quantum Inf.* **3** 30
- [13] Buttler W T, Hughes R J, Lamoreaux S K, Morgan G L, Nordholt J E, Peterson C G 2000 *Phys. Rev. Lett.* **84** 5652
- [14] Richard J H, Jane E N, Derek D, Charles G P 2002 *New J. Phys.* **4** 43
- [15] Manderbach S T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J G, Zeilinger A, Weinfurter H 2007 *Phys. Rev. Lett.* **98** 010504
- [16] Liao S K, Yong H L, Liu C, Shentu G L, Li D D, Lin J, Dai H, Zhao S Q, Li B, Guan J Y, Chen W, Gong Y H, Li Y, Lin Z H, Pan G S, Pelc S J, Fejer M M, Zhang W Z, Liu W Y, Yin J, Ren J G, Wang X B, Zhang Q, Peng C Z, Pan J W 2017 *Nat. Photon.* **11** 509
- [17] Vallone G, Bacco D, Dequal D, Gaiarin S, Luceri V, Bianco G, Villoresi P 2015 *Phys. Rev. Lett.* **115** 040502
- [18] Oi D K, Ling A, Vallone G, Villoresi P, Greenland S, Kerr E, Macdonald M, Weinfurter H, Kuiper H, Charbon E, Ursin R 2017 *EPJ Quantum Technol.* **4** 6
- [19] Liao S K, Cai W Q, Liu W Y, Zhang L, Li Y, Ren J G, Yin J, Shen Q, Cao Y, Li Z P, Li F Z, Chen X W, Sun L H, Jia J J, Wu J C, Jiang X J, Wang J F, Huang Y M, Wang Q, Zhou Y L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y A,

- Liu N L, Wang X B, Zhu Z C, Lu C Y, Shu R, Peng C Z, Wang J Y, Pan J W 2017 *Nature* **549** 43
- [20] Yin J, Cao Y, Li Y H, Liao S K, Zhang L, Ren J G, Cai W Q, Liu W Y, Li B, Dai H, Li G B, Lu Q M, Gong Y H, Xu Y, Li S L, Li F Z, Yin Y Y, Jiang Z Q, Li M, Jia J J, Ren G, He D, Zhou Y L, Zhang X X, Wang N, Chang X, Zhu Z C, Liu N L, Chen Y A, Lu C Y, Shu R, Peng C Z, Wang J Y, Pan J W 2017 *Science* **356** 1140
- [21] Ren J G, Xu P, Yong H L, Zhang L, Liao S K, Yin J, Liu W Y, Cai W Q, Yang M, Li L, Yang K X, Han X, Yao Y Q, Li J, Wu H Y, Wan S, Liu L, Liu D Q, Kuang Y W, He Z P, Shang P, Guo C, Zheng R H, Tian K, Zhu Z C, Liu N L, Lu C Y, Shu R, Chen Y A, Peng C Z, Wang J Y, Pan J W 2017 *Nature* **549** 70
- [22] Liao S K, Cai W Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J G, Liu W Y, Li Y, Shen Q, Cao Y, Li F Z, Wang J F, Huang Y M, Deng L, Xi T, Ma L, Hu T, Li L, Liu N L, Koidl F, Wang P, Chen Y A, Wang X B, Steindorfer M, Kirchner G, Lu C Y, Shu R, Ursin R, Scheidl T, Peng C Z, Wang J Y, Zeilinger A, Pan J W 2018 *Phys. Rev. Lett.* **120** 030501
- [23] Carrasco-Casado A, Fernández V, Denisenko N 2016 *Free-Space Quantum Key Distribution* (Switzerland: Springer International Publishing) pp589–607
- [24] Hill R J, Frehlich R G 1997 *J. Opt. Soc. Am. A* **14** 1530
- [25] Lyke S D, Voelz D G, Roggemann M C 2009 *Appl. Opt.* **48** 6511
- [26] McLaren J R, Thomas J C, Mackintosh J L, Mudge K A, Grant K J, Clare B A, Cowley W G 2012 *Appl. Opt.* **51** 5996
- [27] Kiasaleh K 2006 *IEEE Trans. Commun.* **54** 604
- [28] Vallone G, Marangon D G, Canale M, Vallone G, Marangon D G, Canale M, Savorgnan I, Bacco D, Barbieri M, Calimani S, Barbieri C, Laurenti N, Villoresi P 2015 *Phys. Rev. A* **91** 042320
- [29] Erven C, Heim B, Meyerscott E, Bourgoin J P, Laflamme R, Weihs G, Jennewein T 2012 *New J. Phys.* **14** 129401
- [30] Wang W, Xu F, Lo H K 2018 *Phys. Rev. A* **97** 32337
- [31] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
- [32] Ma X, Razavi M 2012 *Phys. Rev. A* **86** 062319
- [33] Niu M, Cheng J, Holzman J F 2011 *IEEE Trans. Commun.* **59** 664
- [34] Bourgoin J, Meyerscott E, Higgins B L, Helou B, Erven C, Hübel H, Kumar B, Hudson D, D'Souza I, Girard R, Laflamme R, Jennewein T 2014 *New J. Phys.* **16** 069502
- [35] Xu F, Curty M, Qi B, Lo H K 2013 *New J. Phys.* **15** 113007

Measurement-device-independent quantum key distribution under K-distributed strong atmospheric turbulence^{*}

Gu Wen-Yuan¹⁾ Zhao Shang-Hong¹⁾ Dong Chen^{2)†} Zhu Zhuo-Dan¹⁾
 Qu Ya-Yun²⁾

1) (*Air Force Engineering University, Xi'an 710077, China*)

2) (*National University of Defense and Technology, Xi'an 710006, China*)

(Received 3 December 2018; revised manuscript received 1 March 2019)

Abstract

Free-space quantum key distribution (QKD) allows two distant parties to share secret keys with information-theoretic security, which can pave the way for satellite-ground quantum communication to set up a global network for sharing secret message. However, free-space channels in the presence of atmospheric turbulence are affected by losses and fluctuating transmissivity which further affect the quantum bit error rate and the secure key rate. To implement free-space QKD, it is indispensable to study the effect of atmospheric turbulence. Different models have been used to describe the probability distribution for channel transmission coefficient under atmospheric turbulence, including the log-normal distribution and K distribution. In this paper, we focus on free space measurement-device-independent quantum key distribution (MDI-QKD) under K-distributed strong atmospheric turbulence. The MDI-QKD can close all loopholes on detection and achieve a similar performance to QKD, relying on time-reversed version of entanglement-based QKD protocol. Threshold post-selection method is adopted to restrain detrimental effects of the atmospheric turbulence, which is based on the selection of the intervals with higher channel transmissivity. By combining the general MDI-QKD system model with this method, we present a framework for the optimal choice of threshold. Our simulation result shows that the optimal threshold is dependent on the turbulence intensity and expected channel loss. Furthermore, compared with the original MDI-QKD protocols, the proposed protocol with threshold post-selection method can acquire a considerable better performance in key rate, especially in regions of high turbulence and high loss. What is more, this is instructive to the building of a practical free-space MDI-QKD system with better performance.

Keywords: strong atmospheric turbulence, K-distributed model, measurement-device-independent quantum key distribution, free space

PACS: 03.67.Dd

DOI: 10.7498/aps.68.20182130

^{*} Project supported by the Young Scientists Fund of the National Natural Science Foundation of China (Grant No. 11704412) and the School Key Development Program for National University of Defense Technology, China (Grant No. zk-17-02-09).

[†] Corresponding author. E-mail: dongchengfkd@163.com