参考系波动下的参考系无关测量设备无关量子密钥分发协议*

谷文苑[1)] 赵尚弘[1)] 东晨[2)3)†] 王星宇[1)] 杨鼎[3)]

1) (空军工程大学信息与导航学院, 西安 710077)

2) (密码科学技术国家重点实验室, 北京 100878)

3) (国防科技大学信息与通信学院, 西安 710006)

(2019 年 9 月 9 日收到; 2019 年 9 月 25 日收到修改稿)

参考系无关测量设备无关量子密钥分发协议是解决实际系统中参考系对准问题的有效途径, 但其安全性的前提是参考系偏移速度缓慢. 考虑到现实参考系波动和信号长度有限的情况, 重点讨论了参考系偏移和波动下的有偏基参考系无关测量设备无关量子密钥分发协议性能的有效性. 仿真结果表明协议密钥率是关于偏移角的周期函数, 同时也是波动角的递减函数, 为下一步参考系无关测量设备无关量子密钥分发协议实用化打下了理论基础.

关键词: 量子密码学, 量子密钥分发, 参考系无关, 测量设备无关

PACS: 03.67.Dd, 03.67.Hk, 91.10.Ws **DOI:** 10.7498/aps.68.20191364

1 引 言

量子密钥分发 (quantum key distribution, QKD) 是基于量子力学及基本定理的一种新型密钥体系[1,2], 以其绝对的安全性得到了广泛的研究, 在理论研究和实验验证方面进展迅速[3–9]. 但现实设备和实验条件总是会与理想模型及假设存在一定差距, 这导致实际的 QKD 系统仍然存在许多安全性问题[10–16]. 2012 年 Lo 等[17] 提出了测量设备无关量子密钥分发 (measurement device independent quantum key distribution, MDI-QKD) 协议, 在克服探测端全部安全漏洞的同时实现了协议性能的提升. 近几年, 基于相位、偏振等编码方式的 MDI-QKD 演示实验已经相继完成[18–20]. 然而, 无论采用何种编码方式, 通信双方都需确立共享参考系以保证 MDI-QKD 系统有效的 Bell 测量, 但同时多参考系之间的校准会增加 MDI-QKD 系统的复杂性, 甚至可能产生信息泄露, 对系统安全产生威胁.

2014 年, Yin 等[21] 提出了参考系无关测量设备无关量子密钥分发 (reference frame independent measurement device independent quantum key distribution, RFI-MDI-QKD) 协议, 有效地解决了参考系校准的问题, 并实现了系统性能在参考系缓慢偏移情况下的稳定性. 然而, 已有研究表明统计波动下的 RFI-MDI-QKD 协议不再具有对参考系偏差的鲁棒性, 会随偏差角的增大产生性能衰减, 但这些分析都只是选取固定的参考系偏差角度进行分析, 并未涉及一般化情况, 且没有考虑参考系波动的情况[22–26]. 在实际环境中, 参考系偏差角会在一定范围内产生波动, 虽然文献 [27, 28] 已经

* 国家自然科学基金 (批准号: 11704412)、密码科学技术国家重点实验室开放课题基金 (批准号: MMKFKT201823)、陕西省重点研发计划 (批准号: 2019ZDLGY09-01) 和国防科技大学校内科研重点项目 (批准号: zk17-02-09) 资助的课题.

† 通信作者. E-mail: dongchengfkd@163.com

© 2019 中国物理学会 Chinese Physical Society

讨论分析了参考系波动对参考系无关 QKD 协议 (reference frame independent quantum key distribution, RFI-QKD) 的影响, 但仍然缺乏对参考系波动下 RFI-MDI-QKD 协议的性能分析.

本文主要研究了参考系波动下 RFI-MDI-QKD 协议的性能. 考虑到实际参考系波动的问题和有限长效应, 通过公式推导和仿真分析, 得到了参考系偏移角和波动角与有偏基 RFI-MDI-QKD 协议相关参数间的关系. 仿真结果表明, 协议的性能与参考系偏差的角度密切相关, 并且其密钥率随参考系偏移角产生周期性波动, 随参考系波动角的增大而减小.

2 理论与模型

2.1 有偏基 RFI-MDI-QKD 模型

以偏振编码为例, 在诱骗态 RFI-MDI-QKD 协议中, Alice 和 Bob 使用三组共轭基{Z, X, Y}对量子态进行编码. 协议假设 Alice 和 Bob 的 Z 基完全对准, 而两者的 X 基和 Y 基可以存在 β 角的偏差, Alice 和 Bob 的三组基具体的关系如下[22–26]:

$$\begin{aligned} X_{\rm B} &= \cos\beta X_{\rm A} + \sin\beta Y_{\rm A}, \\ Y_{\rm B} &= \cos\beta Y_{\rm A} - \sin\beta X_{\rm A}, \\ \beta &= |\beta_{\rm A} - \beta_{\rm B}|/2, \\ Z_{\rm A} &= Z_{\rm B} = Z, \end{aligned} \tag{1}$$

式中 $\beta_{\rm A(B)}$ 代表着 Alice 和 Bob 的 X 基和 Y 基偏离标准参考系的角度. 此时, $|0\rangle$和$|1\rangle$构成 Z 基, $|\pm\rangle = (|0\rangle \pm {\rm e}^{{\rm i}\beta_{\rm A(B)}}|1\rangle)/\sqrt{2}$ 和 $|\pm {\rm i}\rangle = (|0\rangle \pm {\rm i}{\rm e}^{{\rm i}\beta_{\rm A(B)}}|1\rangle)/\sqrt{2}$ 分别构成 X 基和 Y 基. 其中 Z 基主要用于密钥的产生, X 基和 Y 基的测量结果主要用于估计限制 Eve 获取的信息量的参数 C. 在渐近极限情况下, RFI-MDI-QKD 协议具备对参考系偏差的鲁棒性, 而现实情况下信号脉冲长度总是有限的.

为缓解有限长效应对 RFI-MDI-QKD 协议的影响, 文献 [29] 提出了有偏基 RFI-MDI-QKD 协议以产生更高的密钥率. 该协议与原始诱骗态 RFI-MDI-QKD 协议不同点在于: 原始诱骗态 RFI-MDI-QKD 协议 Z, X, Y 基编码的信号态和诱骗态的平均光子数是相同的, 而有偏基 RFI-MDI-QKD 协议的量子态有三种强度, 即信号态 μ、诱骗态 ν、真空态 ω, 其中 Z 基下 Alice 和 Bob 只准备信号态 μ, X 和 Y 基下随机准备信号态 μ 和诱骗态 ν. 因此, 有偏基 RFI-MDI-QKD 协议密钥率的计算公式为[29]

$$\begin{aligned} R_{\rm s} =& P_{ZZ}P_{ZZ}^{\mu\mu}[\mu^2{\rm e}^{-2\mu}Y_{ZZ}^{11}(1-I_E) - Q_{ZZ}^{\mu\mu}fH(E_{ZZ}^{\mu\mu})] \\ & - \frac{1}{N}\left[\log_2\frac{2}{\varepsilon_{\rm EC}} + 2\log_2\frac{1}{\varepsilon_{\rm PA}}\right. \\ & \left. + 7n_{ZZ}^{\mu\mu}\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n_{ZZ}^{\mu\mu}}} + 30\log_2(N+1)\right], \end{aligned} \tag{2}$$

式中 $n_{ZZ}^{\mu\mu}$ 为 Alice 和 Bob 同时选择 Z 基对信号态 μ_Z 编码时 Bell 态测量的成功事件数量; $\varepsilon_{\rm EC}(\varepsilon_{\rm PA})$为纠错 (隐私放大) 错误的概率; $\bar{\varepsilon}$是估计平滑最小熵的精度; N是实际的脉冲总数; $Q_{w_{\rm A}w_{\rm B}}$和 $E_{w_{\rm A}w_{\rm B}}$表示当 Alice 和 Bob 分别选择基 $w_{\rm A}$ 和 $w_{\rm B}$时的总增益率和误码率, 右下标

$$w_{\rm A}w_{\rm B} = \{Z_{\rm A}Z_{\rm B}, X_{\rm A}X_{\rm B}, Y_{\rm A}Y_{\rm B}, X_{\rm A}Y_{\rm B}, Y_{\rm A}X_{\rm B}\}$$

为 Alice和 Bob 选择的编码基; Y_{ZZ}^{11} 为 Z 基下单光子增益率; P_{ZZ}为 Alice 和 Bob 同时选择 Z 编码基的概率; $P_{ZZ}^{\mu\mu}$为 Alice 和 Bob 均选择 Z 编码基情况下两者量子态平均强度均为 μ 的概率; 窃听者获取的信息 $I_{\rm E}$ 为[16–18]

$$I_{\rm E} = (1-e_{ZZ}^{11})H[(1+u)/2] + e_{ZZ}^{11}H[(1+v)/2], \tag{3}$$

其中 e_{ZZ}^{11}为 Z 基下单光子误码率,

$$\begin{aligned} v &= \sqrt{C/2 - (1-e_{ZZ}^{11})^2u^2}/e_{ZZ}^{11}, \\ u &= \min[\sqrt{C/2}/(1-e_{ZZ}^{11}), 1], \\ C &= \langle X_{\rm A}X_{\rm B}\rangle^2 + \langle Y_{\rm A}Y_{\rm B}\rangle^2 + \langle X_{\rm A}Y_{\rm B}\rangle^2 + \langle Y_{\rm A}X_{\rm B}\rangle^2, \end{aligned}$$

且 C 值在 0—2 内取值, C 值越小, $I_{\rm E}$ 越大. 参数 C 与不同编码基下的增益和误码率有关, 这些测量结果满足[24]

$$\begin{aligned} Q_{Z_{\rm A}Z_{\rm B}} &= Q_C + Q_E, \\ E_{Z_{\rm A}Z_{\rm B}} &= e_{\rm d}Q_C + (1-e_{\rm d})Q_E, \\ Q_{X_{\rm A}X_{\rm B}} &= Q_{Y_{\rm A}Y_{\rm B}} = 2y^2[2y^2 - 4yI_0(x) + I_0(B) + I_0(E)], \\ E_{X_{\rm A}X_{\rm B}} &= E_{Y_{\rm A}Y_{\rm B}} = 2y^2[y^2 - 2yI_0(x) + e_{\rm d}I_0(B) \\ &\quad + (1-e_{\rm d})I_0(E)]/Q_{X_{\rm A}X_{\rm B}(Y_{\rm A}Y_{\rm B})}, \\ Q_{X_{\rm A}Y_{\rm B}} &= Q_{Y_{\rm A}X_{\rm B}} = 2y^2[2y^2 - 4yI_0(x) + I_0(\Theta) + I_0(\Xi)], \\ E_{X_{\rm A}Y_{\rm B}} &= 2y^2[y^2 - 2yI_0(x) + e_{\rm d}I_0(\Xi) \\ &\quad + (1-e_{\rm d})I_0(\Theta)]/Q_{X_{\rm A}Y_{\rm B}}, \\ E_{Y_{\rm A}X_{\rm B}} &= 2y^2[y^2 - 2yI_0(x) + e_{\rm d}I_0(\Theta) \\ &\quad + (1-e_{\rm d})I_0(\Xi)]/Q_{Y_{\rm A}X_{\rm B}}, \end{aligned} \tag{4}$$

式中 $B = 2x\cos\beta$, $E = 2x\sin\beta$, $\Theta = \sqrt{2}x(\cos\beta + \sin\beta)$,

$\Xi=\sqrt{2}x(\cos\beta-\sin\beta)$, 其余的参数以及不同编码基下单光子误码率和增益率的估计方法在文献 [24] 中给出.

2.2 参考系偏移和波动下的有偏基 RFI-MDI-QKD 模型

如图 1 所示, 在实际不稳定的环境中, 由于相对运动和平台抖动, 通信双方共享的参考系总是会发生偏移且产生波动, 即 Alice 和 Bob 间的参考系方向夹角 β 不再是一个固定的值, 而是在一定的范围内变化、波动[27,28], 即 $[\theta-\delta,\ \theta+\delta]$.

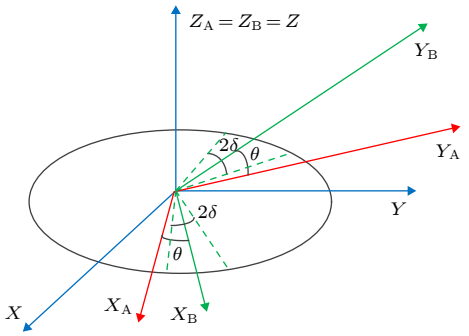

图 1 Alice 和 Bob 的三组共轭基的实际位置关系图

Fig. 1. Relationship among reference frames of Alice and Bob.

文献 [27, 28] 通过在波动范围进行积分详细讨论了参考系偏移角和波动角与 RFI-QKD 协议性能间的关系. 本文将此扩展到二维, 采用相同的方法来分析参考系波动下的有偏基 RFI-QKD 协议的性能. 将参考系偏差 $\beta=[\theta-\delta,\ \theta+\delta]$ 代入求积分可得

$$\begin{aligned}
B' &= \frac{1}{2\delta}\int_{\theta-\delta}^{\theta+\delta} 2x\cos\beta\mathrm{d}\beta = 2x\cos\theta\frac{\sin\delta}{\delta},\\
E' &= \frac{1}{2\delta}\int_{\theta-\delta}^{\theta+\delta} 2x\sin\beta\mathrm{d}\beta = 2x\sin\theta\frac{\sin\delta}{\delta},\\
\Theta' &= \frac{1}{2\delta}\int_{\theta-\delta}^{\theta+\delta} \sqrt{2}x(\cos\beta+\sin\beta)\mathrm{d}\beta\\
&= \sqrt{2}x(\cos\theta+\sin\theta)\frac{\sin\delta}{\delta},\\
\Xi' &= \frac{1}{2\delta}\int_{\theta-\delta}^{\theta+\delta} \sqrt{2}x(\cos\beta-\sin\beta)\mathrm{d}\beta\\
&= \sqrt{2}x(\cos\theta-\sin\theta)\frac{\sin\delta}{\delta},
\end{aligned}\tag{5}$$

其中 θ 为参考系偏移的角度, δ 为参考系波动的角度, 假设它们的取值范围均为 $[0°,90°]$. 将 (5) 式代入 (1)—(4) 式, 可以求得参考系波动下有偏基 RFI-MDI-QKD 协议 C 值和密钥率 R 的关系式.

3 仿真与分析

考虑到实际信号脉冲的数量有限的实际情况, 根据上述推导的公式可以得到参考系偏移角 θ 和波动角 δ 与有偏基 RFI-MDI-QKD 协议的参数 C 和密钥率 R 的关系. 为方便比较, 固定协议的传输距离为 20 km, 并假设切尔诺夫界失败的概率为 $\varepsilon=10^{-10}$, 脉冲总数为 $N=3\times10^{12}$, 纠错 (隐私放大) 失败的概率为 $\varepsilon_{\mathrm{EC}}(\varepsilon_{\mathrm{PA}})=\bar{\varepsilon}=10^{-5}$. 表 1 列出了该协议其他的仿真参数[24–26].

表 1 有偏基 RFI-MDI-QKD 协议的主要仿真参数

Table 1. List of parameters of RFI-MDI-QKD with biased bases in the simulation.

Y_0	e_{d}	e_0	f	η_{d}
1.2×10^{-6}	0.005	0.5	1.16	0.125

图 2 显示了参考系偏移和波动下有偏基 RFI-MDI-QKD 协议的 C 值变化. 由图 2(a) 可知: 当固定波动角 δ 时, C 值为偏移角 θ 的最小周期为 $\pi/2$ 的函数, 而且在 $[0°,90°]$ 范围内存在 $C(\pi/4+\theta)=C(\pi/4-\theta)$; 当改变波动角 δ 时, C 值随波动角 δ 增大而减小. 图 2(b) 则显示了有偏基诱骗态 RFI-MDI-QKD 协议 C 值与波动角 δ 的关系. 当固定偏移角 θ 时, C 值与图 2(a) 曲线趋势相同, 这说明波动角 δ 越大, 窃听者可能窃取的信息 I_{E} 就越多; 当改变偏移角 θ 时, 可以注意到曲线 $\theta=40°$ 与曲线 $\theta=70°$ 完全重合, 这是因为 C 值是关于偏移角 θ 的对称轴为 $\pi/4$ 的周期函数.

图 3 为有偏基 RFI-MDI-QKD 协议密钥率 R 与偏移角 θ、波动角 δ 的三维关系图. 由图 3 可知, 该协议的密钥率 R 会随偏移角 θ、波动角 δ 变化而发生变化. 其中, 密钥率 R 随偏移角 θ 呈周期性变化, 并且变化范围较小, 而波动角 δ 对密钥率 R 的影响较大. 图 4(a) 和图 4(b) 分别是有偏基 RFI-MDI-QKD 协议密钥率 R 与偏移角 θ、波动角 δ 的关系图. 由图 4 可知, 由于密钥率 R 与描述窃听者获取的信息 I_{E} 的参数 C 有关, R 随偏移角 θ、波动角 δ 变化的趋势与参数 C 相同, 即密钥率 R 是关于偏移角 θ 的周期为 $\pi/2$ 且对称轴为 $\pi/4$ 的

函数, 同时也是波动角 δ 的递减函数. 可以注意到当偏移角 θ 接近 22.5° (67.5°)时, R 会随波动角 δ 的增大而产生骤减, 这是因为 22.5° (67.5°)对应于密钥率 R 关于偏移角 θ 的函数谷值, 所以当 δ 较大时, 协议性能会迅速下降.

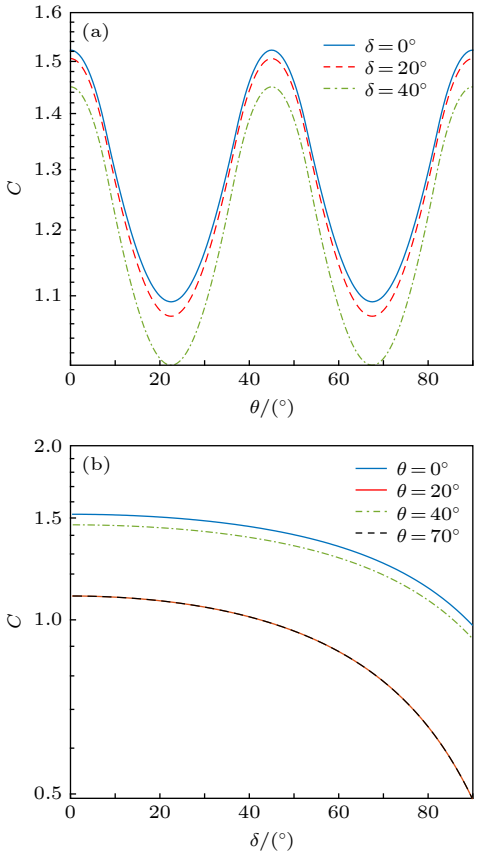

图 2 参考系偏移和波动下有偏基 RFI-MDI-QKD 协议的 C 值 (a) 参数 C 与偏移角 θ 的关系图; (b) 参数 C 与波动角 δ 的关系图

Fig. 2. Parameter C of RFI-MDI-QKD with biased bases under reference frame deviation and fluctuation: (a) The parameter C vs. the reference frame deviation θ; (b) the parameter C vs. the reference frame fluctuation δ.

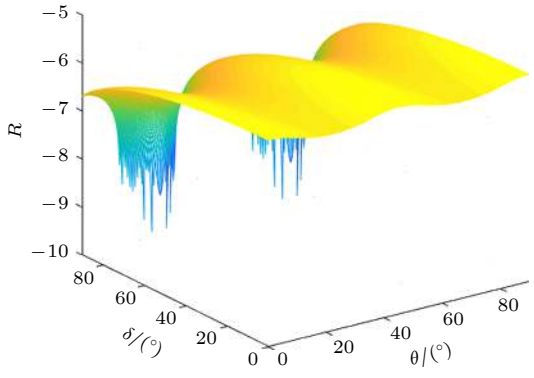

图 3 有偏基 RFI-MDI-QKD 协议密钥率 R 与偏移角 θ、波动角 δ 的关系图

Fig. 3. Secure key rates R of RFI-MDI-QKD with biased bases in regard to the reference frame deviation θ and fluctuation δ.

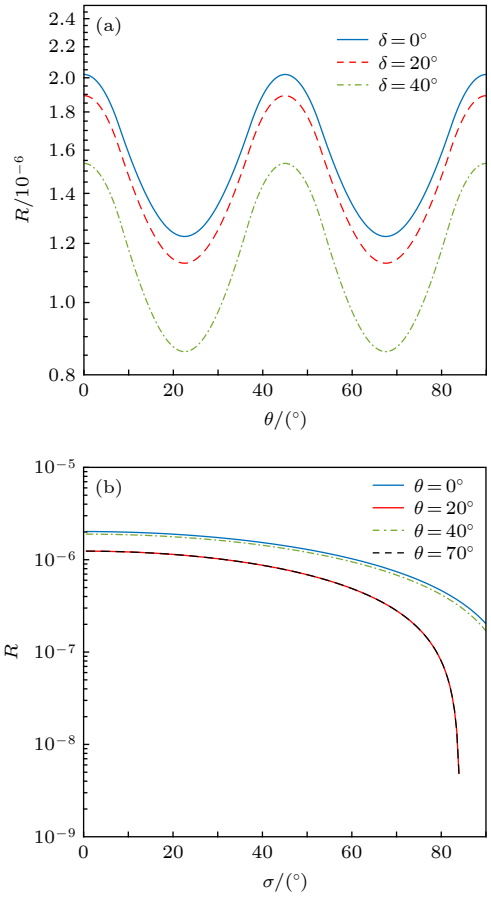

图 4 参考系偏移和波动下有偏基 RFI-MDI-QKD 协议密钥率变化图 (a) 密钥率 R 与偏移角 θ 的关系图; (b) 协议密钥率 R 与波动角 δ 的关系图

Fig. 4. Secure key rates of RFI-MDI-QKD with biased bases under reference frame deviation and fluctuation: (a) The secure key rates R vs. the reference frame deviation θ; (b) the secure key rates R vs. the reference frame fluctuation δ.

4 结 论

为解决 MDI-QKD 系统参考系需校准的问题, 本文重点研究了有偏基 RFI-MDI-QKD 协议. 针对现实环境中参考系波动的问题并考虑到有限长效应的情况, 分析了参考系偏移和抖动下有偏基 RFI-MDI-QKD 协议的有效性, 并分别讨论了参考系偏移角 θ 和波动角 δ 与协议参数 C 及密钥率 R 间的关系. 仿真结果表明参数 C 和密钥率 R 均为关于偏移角 θ 的最小周期为 $\pi/2$ 且对称轴为 $\pi/4$ 的函数, 同时也是波动角 δ 的递减函数, 为下一步 RFI-MDI-QKD 协议实用化打下了理论基础.

参考文献

[1] Shannon C E 1949 *Bell Sys. Tech. J.* **28** 656
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Lo H K, Ma X, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[4] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R, Ten S 2009 *New J. Phys.* **11** 075003
[5] Wang S, Chen W, Guo J F, Yin Z Q, Li H W, Zhou Z, Guo G C, Han Z F 2012 *Opt. Lett.* **37** 1008
[6] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C, Han Z F 2015 *Nat. Photon.* **9** 832
[7] Tang G Z, Sun S H, Li C Y 2019 *Chin. Phys. Lett.* **36** 070301
[8] Wang X Y, Zhao S H, Dong C, Zhu Z D, Gu W Y 2019 *Quantum Inf. Process.* **18** 304
[9] Liu H W, Qu W X, Dou T Q, Wang J P, Zhang Y, Ma H Q 2018 *Chin. Phys. B* **27** 100309
[10] Liu K, Li J, Zhu J R, Zhang C M, Wang Q 2017 *Chin. Phys. B* **26** 120302
[11] Gan Y H, Wang Y, Bao W S, He R S, Zhou C, Jiang M S 2019 *Chin. Phys. Lett.* **36** 040301
[12] Du G H, Li H W, Wang Y, Bao W S 2019 *Chin. Phys. B* **28** 090301
[13] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[14] Chen Y H, Wang J D, Du C 2019 *Acta Phys. Sin.* **68** 130301 (in Chinese) [陈艳辉, 王金东, 杜聪 2019 物理学报 **68** 130301]
[15] Shen Y, Zou Y X 2010 *Acta Phys. Sin.* **59** 1473 (in Chinese) [沈咏, 邹宏新 2010 物理学报 **59** 1473]
[16] Huang J Z, Yin Z Q, Wang S, Li H W, Chen W, Han Z F 2012 *Eur. Phys. J. D* **66** 159
[17] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[18] Silva T F D, Vitoreti D, Xavier G B, Temporão G P, von der Weid J P 2013 *Phys. Rev. A* **88** 052303
[19] Tang Z Y, Liao Z F, Xu F H, Qi B, Qian L, Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[20] Yin H L, Chen T Y, Yu Z W, Liu H, You L X, Zhou Y H, Chen S J, Mao Y Q, 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
[21] Yin Z Q, Wang S, Chen W, Li H W, Guo G C, Han Z F 2014 *Quantum Inf. Process.* **13** 1237
[22] Wang C, Yin Z Q, Wang S, Chen W, Han Z F 2017 *Optica* **4** 1016
[23] Zhang C M, Zhu J R, Wang Q 2017 *Phys. Rev. A* **95** 032309
[24] Liu H W, Wang J P, Ma H Q, Sun S H 2018 *Optica* **5** 902
[25] Zhang H, Zhang C H, Zhang C M, Guo G C, Wang Q 2019 *Quantum Inform.. Process.* **18** 313
[26] Xue Q Y, Jiao R Z 2019 *JOSA B* **36** 476
[27] Pramanik T, Park B K, Cho Y, Han S W, Kim Y S, Moon S 2017 *Phys. Lett. A* **381** 2497
[28] Yoon J, Pramanik T, Park B K, Han S W, Kim S, Kim Y S, Moon S 2019 *Opt. Commun.* **441** 64
[29] Zhang C M, Zhang J R, Wang Q 2017 *J. Lightwave Technol.* **35** 4574

Reference-frame-independent measurement-device-independent quantum key distribution under reference frame fluctuation*

Gu Wen-Yuan [1)] Zhao Shang-Hong [1)] Dong Chen [2)3)†]
Wang Xing-Yu [1)] Yang Ding [3)]

1) (*Information and Navigation College, Air Force Engineering University, Xi'an* 710077, *China*)

2) (*State Key Laboratory of Cryptology, Beijing* 100878, *China*)

3) (*College of Information and Communication, National University of Defense and Technology, Xi'an* 710006, *China*)

(Received 9 September 2019; revised manuscript received 25 September 2019)

Abstract

Reference-frame-independent measurement-device-independent quantum key distribution is adopted to avoid aligning the reference frames in realistic setup, which can guarantee the system security against the slow drift of reference frame. However, the relative motion of reference frame including deviation and fluctuation can influence the performance of reference-frame-independent measurement-device-independent quantum key distribution in practical experimental demonstration. In this paper, taking finite effect into consideration, the performance of reference-frame-independent measurement-device-independent quantum key distribution with biased bases under reference frame deviation and fluctuation is presented to evaluate the effect of the relative motion of reference frame on our scheme, which makes the analysis conform to reality. Our simulation results imply that the key rates fluctuate periodically with the reference frame rotating, while declining with the reference frame fluctuation increasing.

Keywords: quantum cryptography, quantum key distribution, reference frame independent, measurement device independent

PACS: 03.67.Dd, 03.67.Hk, 91.10.Ws **DOI:** 10.7498/aps.68.20191364

* Project supported by the National Natural Science Foundation of China (Grant No. 11704412), the Open Foundation of State Key Laboratory of Cryptography Science and Technology, China (Grant No. MMKFKT201823), the Key Research and Development Program of Shaanxi Province, China (Grant No. 2019ZDLGY09-01), and the Key Development Program of the National University of Defense Technology, China (Grant No. zk17-02-09).

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