大数定理的测量设备无关量子密钥分配统计波动分析

崔树民， 马丽华， 石 磊， 李云霞， 姬一鸣， 李铁飞
（空军工程大学信息与导航学院，西安，710077）

摘要 测量设备无关量子密钥分配方案可以移除所有的探测器侧信道漏洞，结合诱骗态方案实现绝对安全的量子密钥分配。本文采用大数定理对有限密钥长度测量设备无关量子密钥分配方案中单光子计数率和误码率的统计波动进行分析，并对密钥长度为 $N=10^6 \sim 10^{12}$ 的单光子计数率和密钥生成率进行仿真。仿真结果表明：在光纤中传输时，随着密钥长度的减小，安全传输距离由无限密钥长度下的300 km分别下降到260 km（$N=10^{10}$）和75 km（$N=10^6$）。在 $N=10^{12}$ 时，安全传输距离达到295 km，接近理论极限值。

关键词 量子密钥分配；测量设备无关；光子数分流攻击；统计波动
DOI 10.3969/j.issn.1009-3516.2015.06.013
中图分类号 TN913.7 **文献标志码** A **文章编号** 1009-3516(2015)06-0060-04

Statistical Fluctuation Analysis for Measurement Device Independent Quantum Key Distribution Based on the Law of Large Number

CUI Shumin, MA Lihua, SHI Lei, LI Yunxia, JI Yiming, LI Tiefei
(Information and Navigation College, Air Force Engineering University, Xi′an 710077, China)

Abstract: Measurement device independent quantum key distribution is immune from all the detection attacks, so the final key is unconditional secure combined with the decoy state method. This paper analyzes statistical fluctuation analysis of finite key for the yield of single photon and quantum bit error rate of measurement-device-independent quantum key distribution by adopting the law of large number, and simulates the yield of single photon and the key rate by changing the key ($N=10^6 \sim 10^{12}$). The result indicates that the secure transmission distance in optical fibre transmission will decrease to 260 km and 75 km respectively with the reduction of the key length, and the secure transmission distance comes to 295 km, which is close to the limitation when the key reaches to $N=10^{12}$.

Key words: quantum key distribution; measurement device independent; photon number splitting attack; statistical fluctuation

量子密钥分配[1-2]可以使通信双方共享一组绝对安全的密钥，QKD的绝对安全性取决于量子力学基本定理，在理论上已经被严格证明[3]。但是，在实际应用中，由于系统的非完美性造成的安全漏洞可

收稿日期：2015-03-18
基金项目：国家自然科学基金资助项目(61172148)
作者简介：崔树民(1990－)，男，山东聊城人，硕士生，主要从事光纤量子通信研究.E-mail:cuishumin1990@163.com

引用格式：*崔树民，马丽华，石磊，等. 大数定理的测量设备无关量子密钥分配统计波动分析[J]. 空军工程大学学报：自然科学版，2015，16(6)：60-63. CUI Shumin, MA Lihua, SHI Lei, et al.Statistical Fluctuation Analysis for Measurement Device Independent Quantum Key Distribution Based on the Law of Large Number[J]. Journal of Air Force Engineering University: Natural Science Edition, 2015, 16(6): 60-63.*

以被窃听者利用，威胁密钥的安全性。2012 年 Lo 等人首次提出了测量设备无关量子密钥分配（Measurement Device Independent QKD，MDI-QKD）方案[4]，可以移除所有探测器漏洞，结合诱骗态方案[5-6]，在理论上实现绝对安全的量子密钥分配。后来人们分析了不同因素[7-9]对密钥传输距离的影响，在对 MDI-QKD 的安全性进行分析时，假设进行编码的光脉冲数量是无限的。但是由于实际系统的限制，只能实现有限个脉冲的编码，这种情况下就会引入统计涨落，从而降低密钥生成效率和安全传输距离。Ma[10]、Song[11]等人通过引入统计误差分析了统计波动对密钥生成率的影响，Curty[12]从信息论的角度也对统计波动对密钥生成效率造成的影响进行了分析，分析了实际系统与理想情况的误差。本文从另一个角度，采用大数定理在理论上对 MDI-QKD 系统的统计涨落做了系统分析，结合三强度诱骗态方案，对有限密钥长度单光子计数率和误码率分别进行统计涨落分析，在编码脉冲长度达到 $N=10^{12}$ 时，统计波动 δ 接近于 0，而 $N\leqslant 10^{12}$ 时统计波动变得不可忽略。本文对编码脉冲的长度为 $N=10^{6}\sim 10^{12}$ 的单光子计数率和密钥生成率进行仿真。仿真结果表明：随着密钥长度的增加，单光子计数率出现急剧衰减的距离和密钥安全传输距离也随之增加。

1　理论与模型

大数定理是一种描述当试验次数很大时所呈现一种概率性质的定律，假设用 M 个测量样本对事件进行估计，在试验精度范围内如下式：

$$|\kappa^{M}-\kappa^{\infty}|\leqslant\frac{1}{2}\xi(M,\varepsilon)=\frac{1}{2}\sqrt{\frac{2\left[\ln(\frac{1}{\varepsilon})+d\ln(M+1)\right]}{M}} \tag{1}$$

式中：κ^{M} 为对 M 个样本测量后得到的测量值；κ^{∞} 为对无穷个样本测量后得到的真实值；ε 为试验精度，即系统的最大失误概率，可以取任意小的值。这里 $d=2$，是因为测量设备无关量子密钥分配系统中存在 2 种可能（Alice=Bob 和 Alice≠Bob）。

在进行实际量子密钥分配时，采用的若相干光源中光子数服从泊松分布，采用文献[6]中所采用的信号强度 $\mu=0.36$，光子数 n 分别为 0、$1\leqslant n\leqslant 7$、$n\geqslant 8$ 时，所占比例为 ≈ 0.7、≈ 0.3、$\approx 2.0\times 10^{-6}$。可见，光子数大于 7 的概率非常低，可以忽略不计。

由于光子数大于 7 的概率非常低（$0.7>0.3\gg 2.0\times 10^{-6}$），对最终的密钥生成率的影响可以忽略不计。因此，本文只考虑光子数处于 1 到 7 光子数统计涨落的影响，对有限密钥长度信号态和诱骗态单光子计数率 Y_{11} 和误码率 e_{11} 存在的统计涨落进行分析。在三强度诱骗态方案中，A、B 双方分别准备强度为 $\{\mu_0,\mu_1,\mu_2\}$ 和 $\{\nu_0,\nu_1,\nu_2\}$ 的光脉冲，其中 μ_2（ν_2）为 $A(B)$ 的信号态强度，μ_0，μ_1（ν_0，ν_1）为 $A(B)$ 的诱骗态强度。根据大数定理，可得计数率和误码率相对统计涨落表达式：

$$\delta_{Y_{nm\mu\nu}}=|\ Y^{c}_{nm\mu\nu}-Y^{\infty}_{nm\mu\nu}\ |\leqslant\frac{1}{2}\xi(Np_{nm\mu\nu},t) \tag{2}$$

$$\delta_{e_{nm\mu\nu}}=|\ e^{c}_{nm\mu\nu}-e^{\infty}_{nm\mu\nu}\ |\leqslant\frac{1}{2}\xi(Np_{nm\mu\nu}Y^{c}_{nm\mu\nu},t) \tag{3}$$

式中：n（m）表示 $A(B)$ 发送光子态中的光子数，N 表示某一光子态脉冲数量，$\mu\in\{\mu_0,\mu_1,\mu_2\}$，$\nu\in\{\nu_0,\nu_1,\nu_2\}$。由于 A、B 双方发送的脉冲光子数服从泊松分布，所以有：

$$p_{nm\mu\nu}=\frac{\mu^{n}\nu^{m}}{n!\ m!}e^{-\mu-\nu} \tag{4}$$

根据文献[6]中的公式可以得到：

$$\begin{aligned}e^{\mu_1+\nu_1}Q_{\mu_1\nu_1}&=\sum_{n,m=0}^{\infty}p_{nm\mu_1\nu_1}Y^{c}_{nm\mu_1\nu_1}\leqslant Y_{00\mu_1\nu_1}+\\&\sum_{m=1}^{7}\frac{\nu_1^{m}}{m!}(Y^{c}_{0m\mu_1\nu_1}+\delta_{Y_{0m\mu_1\nu_1}})+\sum_{m=8}^{\infty}\frac{\nu_1^{m}}{m!}Y_{0m\mu_1\nu_1}+\\&\mu_1[(Y^{c}_{10\mu_1\nu_1}+\delta_{Y_{10\mu_1\nu_1}})+\\&\nu_1(Y^{c}_{11\mu_1\nu_1}+\delta_{Y_{11\mu_1\nu_1}})+\sum_{m=2}^{7}\frac{\nu_1^{m}}{m!}(Y^{c}_{1m\mu_1\nu_1}+\delta_{Y_{1m\mu_1\nu_1}})+\\&\sum_{m=8}^{\infty}\frac{\nu_1^{m}}{m!}Y_{1m\mu_1\nu_1}]+\sum_{n=2}^{7}\frac{\mu_1^{n}}{n!}[\sum_{m=0}^{7}\frac{\nu_1^{m}}{m!}(Y^{cnm\mu_1\nu_1}_{nm\mu_1\nu_1}+\delta_{Y_{nm\mu_1\nu_1}})+\\&\sum_{m=8}^{\infty}\frac{\nu_1^{m}}{m!}Y_{nm\mu_1\nu_1}]+\sum_{n=8}^{\infty}\frac{\mu_1^{n}}{n!}(\sum_{m=0}^{\infty}\frac{\nu_1^{m}}{m!}Y_{nm\mu_1\nu_1})=\\&e^{\nu_1}Q_{0\nu_1}+e^{\mu_1}Q_{\mu_1 0}-Q_{00}+\mu\nu Y^{c}_{11\mu\nu}+h(\mu_1,\nu_1)+A_1\end{aligned} \tag{5}$$

同理可以推导出：

$$\begin{aligned}e^{\mu_2+\nu_2}Q_{\mu_2\nu_2}&=\sum_{n,m=0}^{\infty}p_{nm\mu_2\nu_2}Y^{c}_{nm\mu_2\nu_2}\geqslant e^{\nu_2}Q_{0\nu_2}+\\&e^{\mu_2}Q_{\mu_2 0}-Q_{00}+\mu\nu Y^{c}_{11\mu\nu}+h(\mu_2,\nu_2)-A_2\end{aligned} \tag{6}$$

式中：

$$A_1=\sum_{n,m=1}^{7}\frac{\mu_1^{n}\nu_1^{m}}{n!\ m!}\delta_{Y_{nm\mu_1\nu_1}}+\nu_1\delta_{Y_{01\mu_1\nu_1}}+\mu_1\delta_{Y_{10\mu_1\nu_1}} \tag{7a}$$

$$A_2=\sum_{n,m=1}^{7}\frac{\mu_2^{n}\nu_2^{m}}{n!\ m!}\delta_{Y_{nm\mu_2\nu_2}}+\nu_2\delta_{Y_{01\mu_2\nu_2}}+\mu_2\delta_{Y_{10\mu_2\nu_2}} \tag{7b}$$

结合式(5)和(6)可以进一步推导单光子计数率下限 $Y^{L}_{11\mu\nu}$：

$$\begin{aligned}Y_{11\mu\nu}\geqslant Y^{L}_{11\mu\nu}&=\frac{1}{\mu_1\nu_1-\mu_2\nu_2+\beta\mu_2\nu_1+\beta\mu_1\nu_2}[g_1+g_2+g_3-\\&e^{\mu_2+\nu_2}Q_{\mu_2\nu_2}+e^{\mu_1+\nu_1}Q_{\mu_1\nu_1}-(e^{\mu_1+\nu_1}-\sum_{n,m=0}^{7}\frac{\mu_1^{n}\nu_1^{m}}{n!\ m!})-A]\end{aligned} \tag{8}$$

$$A=\sum_{n,m=1}^{7}(\frac{\mu_1^{n}\nu_1^{m}}{n!\ m!}\delta_{Y_{nm\mu_1\nu_1}}+\frac{\mu_2^{n}\nu_2^{m}}{n!\ m!}\delta_{Y_{nm\mu_2\nu_2}})+$$

$$(\nu_2\delta_{Y_{01\mu_2\nu_2}}+\nu_1\delta_{Y_{01\mu_1\nu_1}})+(\mu_1\delta_{Y_{10\mu_1\nu_1}}+\mu_2\delta_{Y_{10\mu_2\nu_2}}) \tag{9}$$

$$\begin{cases} g_1=e^{\nu_2}Q_{0\nu_2}+e^{\mu_2}Q_{\mu_20}-e^{\nu_1}Q_{0\nu_1}-e^{\mu_1}Q_{\mu_10} \\ g_2=\beta(e^{\mu_2+\nu_1}Q_{\mu_2\nu_1}-e^{\nu_1}Q_{0\nu_1}-e^{\mu_2}Q_{\mu_20}+Q_{00}) \\ g_3=\beta(e^{\mu_1+\nu_2}Q_{\mu_1\nu_2}-e^{\nu_2}Q_{0\nu_2}-e^{\mu_1}Q_{\mu_10}+Q_{00}) \end{cases} \tag{10}$$

$$\beta=\min\left(\frac{\mu_2\nu_2^2-\mu_1\nu_1^2}{\mu_2\nu_1^2+\mu_1\nu_2^2},\frac{\mu_2^2\nu_2-\mu_1^2\nu_1}{\mu_2^2\nu_1+\mu_1^2\nu_2},\frac{\mu_2^2\nu_2^2-\mu_1^2\nu_1^2}{\mu_2^2\nu_1^2+\mu_1^2\nu_2^2}\right) \tag{11}$$

同理可推导出单光子误码率上限 $e_{11\mu\nu}^U$：

$$e_{11\mu\nu}\leqslant e_{11\mu\nu}^U=\frac{E_{\mu_2\nu_2}Q_{\mu_2\nu_2}e^{\mu_2+\nu_2}-E_{\mu_1\nu_1}Q_{\mu_1\nu_1}e^{\mu_1+\nu_1}+B}{Y_{11\mu\nu}(\mu_2\nu_2-\mu_1\nu_1)} \tag{12}$$

$$B=\sum_{n,m=1}^{7}\left(\frac{\mu_1^n\nu_1^m}{n!\ m!}\delta_{Y_{nm\mu_1\nu_1}}+\frac{\mu_2^n\nu_2^m}{n!\ m!}\delta_{Y_{nm\mu_2\nu_2}}+\frac{\mu_1^n\nu_1^m}{n!\ m!}\delta_{e_{nm\mu_1\nu_1}}+\frac{\mu_2^n\nu_2^m}{n!\ m!}\delta_{e_{nm\mu_2\nu_2}}\right)+(\nu_2\delta_{Y_{01\mu_2\nu_2}}+\nu_1\delta_{Y_{01\mu_1\nu_1}}+\nu_2\delta_{e_{01\mu_2\nu_2}}+\nu_1\delta_{e_{01\mu_1\nu_1}})+(u_2\delta_{Y_{10\mu_2\nu_2}}+u_1\delta_{Y_{10\mu_1\nu_1}}+u_2\delta_{e_{10\mu_2\nu_2}}+u_1\delta_{e_{10\mu_1\nu_1}}) \tag{13}$$

将单光子计数率和误码率表达式带入密钥生成效率公式中可以得到：

$$R\geqslant\mu_2\nu_2e^{-\mu_2-\nu_2}Y_{11\mu\nu}^L[1-H(e_{11\mu\nu}^U)]-Q_{\mu_2\nu_2}fH(E_{\mu_2\nu_2}) \tag{14}$$

式中：$H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$，为香农熵函数；$Q_{\mu_2\nu_2}$、$E_{\mu_2\nu_2}$ 为全局计数率和误码率，可通过实验直接获得；f 为误差修正系数。

在进行量子密钥分配时，A、B 双方会随机准备属于 X 基或 Z 基的偏振态，但是属于 X 基的偏振态最终会导致较高的误码率，因此，本文只考虑 Z 基的影响。从文献[6]可得：

$$Q_{\mu_2\nu_2}=Q_C+Q_E \tag{15a}$$

$$E_{\mu_2\nu_2}Q_{\mu_2\nu_2}=e_dQ_C+(1-e_d)Q_E \tag{15b}$$

$$Q_E=2P_d(1-P_d)^2e^{\frac{-\mu}{2}}[I_0(2s)-(1-P_d)e^{\frac{-\mu}{2}}] \tag{15c}$$

$$Q_C=2(1-P_d)^2e^{\frac{-\mu}{2}}[1-(1-P_d)e^{\frac{-\eta_a\mu}{2}}]\times[1-(1-P_d)e^{\frac{-\eta_b\mu}{2}}] \tag{15d}$$

式中：$I_0(s)$ 为第 1 类修正贝塞尔函数；P_d 为单光子探测器暗计数；η_a（η_b）为 $A(B)$ 的传输效率，$\bar{\mu}=\eta_a\mu_2+\eta_b\nu_2$，$s=\sqrt{\eta_a\mu_2\eta_b\nu_2/2}$。将(15)式代入式(14)可得基于大于定理下的实际系统中量子密钥生成率公式。

2 仿真结果与分析

仿真时，采取“真空态＋双弱相干态”的三强度诱骗态方案，即 $\mu_0=\nu_0=0$，$\mu_1=\nu_1$，$\mu_2=\nu_2$。计算过程中，诱骗态强度分别取 0 和 0.01，信号态强度为 0.36，其余取值参考文献[13]，e_0 取 0.5、e_d 取 1.5%、P_d 取 3×10^{-6}、f 取 1.16、η_C 取 14.5%。

单光子计数率的统计波动大小与系统要求的精度有关，如图 1 所示。随着精度的提高，单光子计数率的统计波动随之增加，当 $N\geqslant10^{12}$ 时，统计波动趋向于 0，对密钥生成率的影响可以忽略不计；而当 $N\leqslant10^6$ 时，统计波动的影响过大，最终导致极低的密钥生成效率。因此，本文考虑密钥长度为 $10^6\leqslant N\leqslant10^{12}$ 时统计波动的影响，分别分析了该密钥长度范围内统计波动对单光子计数率和密钥生成率的影响。

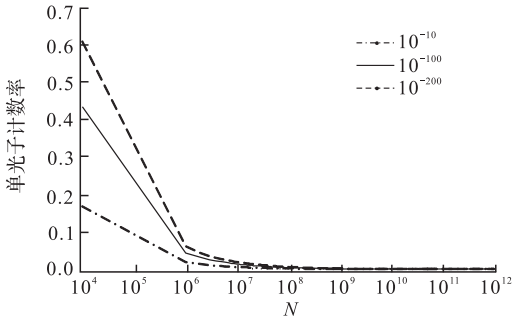

图 1 不同精度下单光子计数率统计波动与编码脉冲长度的关系

Fig.1 The relation between the statistical fluctuation of single photon count rate and key length under different precisions

随着密钥长度的增加，单光子计数率出现急剧衰减的距离随之增加，见图 2。

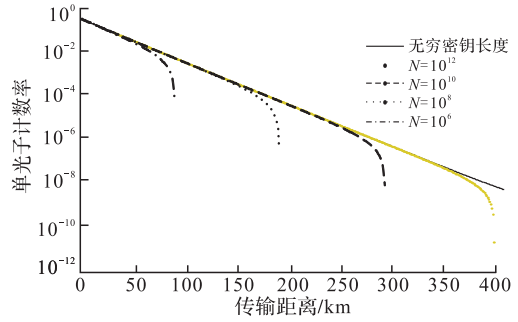

图 2 不同编码脉冲长度下单光子计数率与传输距离的关系

Fig.2 The relation between single photon count rate and transmission distance under different key length

当 $N=10^6$ 时，单光子计数率在 90 km 处出现急剧衰减，当 $N=10^{12}$ 时，单光子计数率在 400 km 处出现急剧衰减。随着密钥长度的增加，统计波动的影响减小，实际系统中的单光子计数率趋向于理论值。

在实际系统中考虑统计波动影响时，安全密钥生成率随着传输距离变化关系见图 3。从图中可以看出，在密钥长度 $N=10^6$ 时，安全传输距离只有 80 km，当 $N=10^{12}$ 时，安全传输距离达到了 295 km，接近理论极限值。这是因为，在密钥长度 $N\leqslant10^6$ 时，统计波动的影响较大，限制了单光子的传输距离和计数率，从而影响最终的密钥生成效率和传输距

离；当密钥长度 $N \geqslant 10^{12}$ 时，统计波动的影响可以忽略不计，接近无限密钥长度的理论极限值。

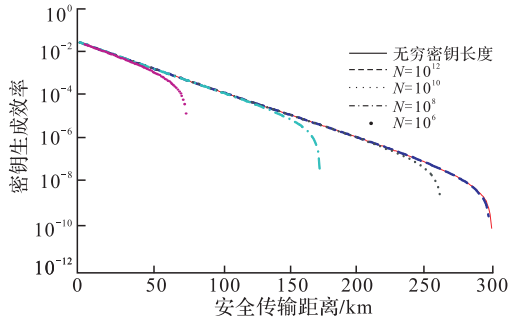

图 3　不同编码脉冲长度下密钥生成率与传输距离的关系

Fig.3　The relation between the key generation rate and transmission distance under different key length

3　结语

本文对三强度诱骗态 MDI-KD 方案的统计波动进行了系统分析，分析了统计波动与编码脉冲长度的关系，比较了不同编码脉冲长度下统计波动对计数率和密钥生成率的影响。与文献[10]、[11]相比，论文不是直接引入统计误差公式，而是采用理论性更强的数学工具——大数定理，从密钥生成率公式的推导中引入统计波动参数，对统计波动影响的分析更加精确，为 MDI-QKD 方案在实际系统中的应用提供了理论依据。采用大数定理对统计波动给单光子计数率和最终密钥生成率的影响进行了系统的分析，仿真结果表明在一定的系统精度要求下，随着密钥长度的增加，MDI-QKD 的安全传输距离也随之增加。在实际实验中，当 $N \geqslant 10^{12}$ 统计波动对密钥生成率的影响可以忽略，安全传输距离达到 300 km，接近理论极限值。

参考文献(References)：

[1] Charles H. Bennett, Gilles Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing [C]//Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing Bangalore: IEEE, 1984: 175-179.

[2] Xiong-Feng Ma, Bin Qi, Yi Zhao, et al. Practical Decoy State for Quantum Key Distribution[J]. Physical Review A, 2005, 72 (1): 012326.

[3] Lo H K, Chau H F, Ardehali M, Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security[J]. Journal of Cryptology, 2000, 18 (2): 133-165.

[4] Lo H K, Curty M, Bin Q. Measurement Device Independent Quantum Key Distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[5] Zhi-Yuan Tang, Zhong-Fa Liao, Fei-Hu Xu, et al. Experimental Demonstration of Polarization Encoding Measurement Device Independent Quantum Key Distribution[J]. Physical Review Letters, 2014, 112 (19): 190503.

[6] Shi-Hai Sun, Ming Gao, Chun-Yan Li, et al. Practical Decoy State Measurement Device Independent Quantum Key Distribution[J]. Physical Review A, 2013, 87 (5): 052329.

[7] 东晨，赵尚弘，赵卫虎，等. 非对称信道传输效率的测量设备无关量子密钥分配研究[J]. 物理学报，2014，63 (3): 030302.
DONG Chen, ZHAO Shanghong, ZHAO Weihu, et al. Analysis of Measurement Device Independent Quantum Key Distribution with an Asymmetric Channel Transmittance Efficiency[J]. Acta Physica Sinica, 2014, 63(3): 030302. (in Chinese)

[8] 东晨，赵尚弘，董毅，等. 基于旋转不变态的测量设备无关量子密钥分配协议研究[J]. 物理学报，2014，63 (17): 170303.
DONG Chen, ZHAO Shanghong, DONG Yi, et al. Measurement Device Independent Quantum Key Distribution for The Rotation Invariant Photonic State [J]. Acta Physica Sinica, 2014, 63 (17): 170303. (in Chinese)

[9] Chen Dong, Shang-Hong Zhao, Wei-Hu Zhao, et al. Analysis of Measurement Device Independent Quantum Key Distribution under An Asymmetric Channel Transmittance Efficiency [J]. Quantum Information Processing, 2014: 2525-2534.

[10] X F Ma, C H F Fung, M Razavi. Statistical Fluctuation Analysis for Measurement Device Independent Quantum Key Distribution[J]. Physical Review A, 2012, 86(5): 052305.

[11] Ting-Ting Song, Qiao-Yan Wen, Fen-Zhuo Guo, et al. Finite Key Analysis for Measurement Device Independent Quantum Key Distribution[J]. Physical Review A, 2012, 86(2): 022332.

[12] Marcos Curty, Fei-Hu Xu, Wei Cui, et al. Finite Key Analysis for Measurement Device Independent Quantum Key Distribution [J]. Nature Communications, 2013, 5(4): 643-648.

[13] Qin Wang, Xiang-Bin Wang. Efficient Implementation of the Decoy State Measurement Device Independent Quantum Key Distribution with Heralded Single Photon Sources[J]. Physical Review A, 2013, 88(5): 052332.

(编辑：姚树峰)