预报相干光子对的测量设备无关量子密钥分发协议

朱卓丹[1]，张茜[2]，赵尚弘[1]，苏力华[3]，王星宇[1]

[1]空军工程大学信息与导航学院，陕西 西安 710077；

[2]中国人民解放军 31007 部队，北京 100079；

[3]西安通信学院信息安全系，陕西 西安 710006

摘要 提出了一种基于预报相干光子对(HPCS)的测量设备无关量子密钥分发(MDI-QKD)协议的改进方案，降低了长距离量子密钥分发中由暗计数引起的误码率。仿真结果表明，与弱相干光源相比，HPCS 能降低空脉冲数量比例从而增加安全传输距离；与预报单光子源相比，HPCS 能提高单光子脉冲数量比例从而提高安全密钥生成率。分析了有限密钥长度对基于 HPCS 的三诱骗态 MDI-QKD 的影响。

关键词 量子光学；测量设备无关量子密钥分发；弱相干光源；预报相干光子对；统计波动分析

中图分类号 TN918 **文献标识码** A

doi：10.3788/LOP54.122703

Measurement-Device-Independent Quantum Key Distribution Protocols for Heralded Pair Coherent State

Zhu Zhuodan[1], Zhang Xi[2], Zhao Shanghong[1], Su Lihua[3], Wang Xingyu[1]

[1] *School of Information and Navigation, Air Force Engineering University, Xi'an, Shaanxi* 710077, *China*;

[2] *No.* 31007 *Unit of PLA, Beijing* 100079, *China*;

[3] *Department of Information Security, Xi'an Communication College, Xi'an, Shaanxi* 710006, *China*

Abstract A modified scheme of measurement-device-independent quantum key distribution (MDI-QKD) protocols based on the heralded pair coherent state (HPCS) is proposed, which decreases the error rate caused by the dark count in the long distance quantum key distribution. The simulation results show that, compared with a weak coherent source, the HPCS can reduce the quantitative proportion of vacuum and thus increase the transmission distance. Compared with a heralded single photon source, the HPCS can enhance the quantitative proportion of single-photon pulse and thus increase the secure key generation rate. The impact of the finite key length on the MDI-QKD of the three decoy state based on the HPCS is analyzed.

Key words quantum optics; measurement-device-independent quantum key distribution; weak coherent source; heralded pair coherent state; statistical fluctuation analysis

OCIS codes 270.5565; 270.5568

1 引 言

量子通信是一种近年来发展迅速的新型通信方式，包括量子隐形传态[1]、量子密钥分发(QKD)[2]、量子密集编码[3]等。其中，QKD[4-6]是量子信息科学最实用化的应用之一。通信双方(Alice 和 Bob)能够在窃听

收稿日期：2017-07-01；**收到修改稿日期**：2017-07-18

基金项目：国家自然科学基金重点项目(61231012)

作者简介：朱卓丹(1993—)，女，硕士研究生，主要从事量子通信方面的研究。E-mail：zzdkgd@163.com

导师简介：赵尚弘(1966—)，男，教授，博士生导师，主要从事激光空间信息技术方面的研究。E-mail：zsh@aliyun.com

者存在的情况下共享一串密钥,具有基于量子力学的无条件安全性[7-9]。然而,实际设备不能满足理论的安全假设要求,这使得量子密钥系统存在潜在的安全漏洞[10],量子黑客可以针对这些漏洞采取光子数分束攻击(PNS)[11]、部分相位随机化攻击[12]、伪态攻击[13]、时移攻击[14]和致盲攻击[15]。在这些攻击中,探测器受到的攻击最频繁。为了消除这些漏洞,学者们对协议进行了改进优化[16]。其中一种方案是采用设备无关量子密钥分发(DI-QKD)[17],但由于目前的设备条件达不到该方案要求,其实用性较差;另一种方案是采用 Lo 等[18]提出的测量设备无关量子密钥分发(MDI-QKD)协议[10],将 Bell 态测量放在非可信第三方进行,消除系统探测端一侧的漏洞。

MDI-QKD 较好地平衡了 QKD 协议的安全性和实用性,近年来得到了研究人员的极大关注[19-20]。在理论方面,Ma 等[21-22]研究了基于弱相干光源(WCS)的三诱骗态 MDI-QKD 方案,在考虑统计波动的情况下,得到了接近理想单光子源(SPS)的密钥率。Yu 等[23]优化了诱骗态 MDI-QKD 协议。在 MDI-QKD 实验方面,Tang 等[24]实现了 10 km 的 MDI-QKD,Tang 等[25]实现了超过 200 km 的长距离相位编码 MDI-QKD,并实现了三节点的 MDI-QKD 组网。

目前,在实际的 MDI-QKD 实验中,通常采用 WCS 代替 SPS。WCS 的光子数遵循泊松分布,这至少会带来两个缺点:一是脉冲中含有大量真空态,降低了 QKD 的效率;二是含有多光子脉冲,影响了 QKD 系统的安全性。为了降低真空态的比例,可以采用参量下转换光源(PDCS)代替 WCS[26-28]。Zhou 等[29]研究了基于 PDCS 的 MDI-QKD,并给出了其中单光子计数率的估计公式。Wang 等[30]采用热分布的 PDCS 代替 WCS,增加了 MDI-QKD 中的单光子计数率。Zhou[31]采用热分布的预报相干光子对(HPCS),增加了 QKD 中的单光子计数率。Zhu 等[32]采用 HPCS 增加了 MDI-QKD 中的单光子计数率。

本文提出了一种基于 HPCS 的改进 MDI-QKD 方案。HPCS 的光子数服从亚泊松分布,含有较低比例的空脉冲,能有效降低长距离 QKD 中由暗计数引起的误码率。与基于 WCS 的方案相比,基于 HPCS 的 MDI-QKD 能有效提高最大安全传输距离。进一步分析了由有限密钥长度引起的统计波动问题[32]。仿真结果表明,最大安全传输距离的增量近 75 km。与基于预报单光子源(HSPS)的 MDI-QKD 相比,本方案能提高安全密钥率。在实际 QKD 系统中,由于对光源的控制不够精确,强度的真实值与理想值存在不断变化的偏差。这种统计波动会引起光源光子数分布的不稳定性,对于密钥生成率特别是接近最大安全传输距离时的密钥生成率有着不可忽略的影响。

2 模型及推论

HPCS 是光子预报技术在相干光子对上的运用[33]。一定强度的抽运光入射到非线性晶体上,进入晶体的一个光子以一定的概率被劈裂为两个光子,分别称为信号态和闲频态。将闲频态发送至探测器用来“预报”信号态,可减小暗计数对探测的影响。信号态经过调制后,被发送至非可信第三方进行 Bell 态测量。其中 HPCS 源的光子数服从亚泊松分布,光子的概率为

$$P(l)=\frac{1}{\mathrm{I}_0(2\mu)}\frac{\mu^{2l}}{(l!)^2}\left[1-(1-\eta_{\mathrm{d}}^{K})^{l}+P_{\mathrm{d}}^{K}\right], \tag{1}$$

式中 η_{d}^{K} 和 P_{d}^{K} 分别为探测效率和触发探测器的暗计数率;$K=\mathrm{A},\mathrm{B}$ 分别表示该探测器位于 Alice、Bob 一侧;$\mathrm{I}_0(\cdot)$为修正的第一类 Bessel 函数;μ 为平均光子数;l 为单个脉冲的光子数。

表 1 在平均光子数为 0.5 的不同光源下的多光子脉冲、单光子脉冲、空脉冲的数量比例

Table 1 Quantitative proportions of multi-photon pulse, single-photon pulse and vacuum pulse for different sources with a mean photon number of 0.5

Optical source	Vacuum pulse	Single-photon pulse	Multi-photon pulse
WCS	0.60653	0.30326	0.09024
HSPS	1.94×10^{-6}	0.72735	0.27265
HPCS	4.93×10^{-6}	0.92550	0.07445

以平均光子数 $\mu=0.5$ 为例,不同光源下多光子脉冲、单光子脉冲、空脉冲的数量比例见表 1,可以看出,相比于 WCS,HPCS 产生的空脉冲数量比例更低,有利于实现长距离的 MDI-QKD;而相比于 HSPS,HPCS

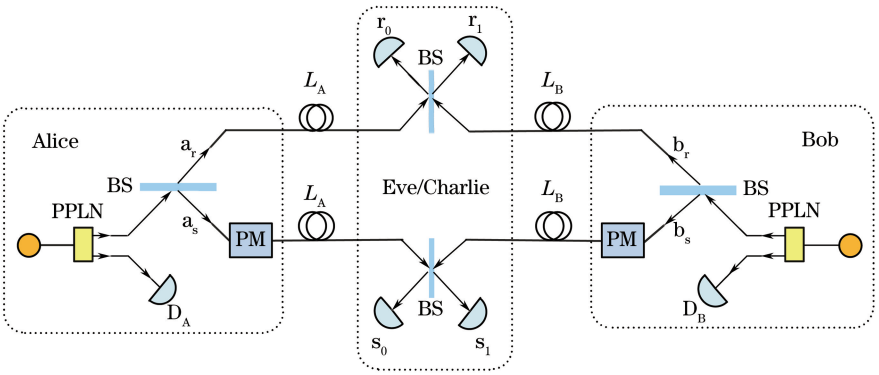

图 1 基于 HPCS 的 MDI-QKD 原理图

Fig. 1 Schematic of MDI-QKD based on HPCS

产生的单光子脉冲数量比例更高,有利于提高密钥生成率。

基于 HPCS 的 MDI-QKD 原理如图 1 所示,其中 D_A、D_B 分别为 Alice、Bob 的探测器;$a_s(a_r)$、$b_s(b_r)$分别为 Alice、Bob 发送的信号光(参考光);L_A、L_B 分别为 Alice、Bob 与非可信第三方 Charlie 的距离;$r_0(r_1)$、$s_0(s_1)$分别为第三方用于探测参考光、信号光的单光子探测器。通信双方 Alice 和 Bob 采用周期极化铌酸锂(PPLN)晶体产生 HPCS 光脉冲,随机选择 z 基或 x 基。若选择 z 基,则调制为 0°或 90°偏振态;若选择 x 基,则调制为±45°偏振态。调制后的脉冲通过分束器(BS)后,分为信号光(a_s,b_s)和参考光(a_r,b_r)两个模式,再由相位调制器(PM)增加相对相位后发送至非可信第三方 Charlie(Eve)。第三方使用分束器(BS)、PBS 和四个探测器(r_0,r_1,s_0,s_1)对收到的光脉冲进行局部 Bell 态测量并公布测量结果。一个成功的 Bell 态测量对应于四个探测器中的两个探测器的响应,在探测器响应的所有可能情况中,只有两个 Bell 态可以被有效区分。在该结果基础上,Alice 和 Bob 通过基比对过程得到安全密钥生成率 R 的公式[34]为

$$\begin{cases} R = P_{\mu_2}(1)P_{\nu_2}(1)Y_{11}^{z}[1-H_2(e_{11}^{x})] - I_{ec} \\ I_{ec} = Q_{\mu_2\nu_2}^{z} f(E_{\mu_2\nu_2}^{z}) H_2(E_{\mu_2\nu_2}^{z}) \end{cases}, \tag{2}$$

式中 I_{ec} 为参数,μ_i,ν_j 分别为 Alice,Bob 的脉冲强度,$i(j)=1,2$ 分别表示诱骗态脉冲、信号态脉冲;上标 $w=x,z$ 表示两种基,其中 x 基用于测试信道参数,z 基用于提取最终密钥;Y_{11}^{z} 为 z 基下的单光子计数率;e_{11}^{z} 为 z 基下的单光子误码率;$H_2(\cdot)$为二元熵函数;f 为纠错效率;$P_{\mu_2}(1)$、$P_{\nu_2}(1)$分别为两端信号态中单光子脉冲的概率;$Q_{\mu_i\nu_j}^{w}$、$E_{\mu_i\nu_j}^{w}$ 分别为接收率和误码率,其表达式为

$$Q_{\mu_i\nu_j}^{w} = \sum_{n,m=0}^{\infty} P_{\mu_i}(n)P_{\nu_j}(m)Y_{nm}^{w}, \tag{3}$$

$$E_{\mu_i\nu_j}^{w}Q_{\mu_i\nu_j}^{w} = \sum_{n,m=0}^{\infty} P_{\mu_i}(n)P_{\nu_j}(m)e_{nm}^{w}Y_{nm}^{w}, \tag{4}$$

式中 n、m 分别表示 Alice、Bob 侧脉冲所含光子数,e_{nm}^{w} 为误码率,Y_{nm}^{w} 为计数率。

(2)式包括纠错和隐私放大两个部分。纠错部分 I_{ec} 只依赖于参数 $E_{\mu_2\nu_2}^{z}$,该参数与 $Q_{\mu_2\nu_2}^{z}$ 可以在实验中直接测得,故(2)式中纠错部分 I_{ec} 是固定的。对于隐私放大部分,需要估计诱骗态下 Y_{11}^{z} 和 e_{11}^{w} 两个参数。

目标是获得最小值 $\min Y_{11}^{z}[1-H_2(e_{11}^{x})]$。注意到(4)式与 w 无关,故在下文中忽略上标 w。同时,假设 Alice 和 Bob 两方探测器的探测效率和暗计数率相同,即 $\eta_d^A=\eta_d^B=\eta_d$,$P_d^A=P_d^B=P_d$。则信号态 (μ_2,ν_2) 和诱骗态 (μ_1,ν_1) 的接收率和量子误码率分别为

$$\begin{aligned} Q_{\mu_i\nu_j} &= \sum_{n,m=0}^{\infty} P_{\mu_i}(n)P_{\nu_j}(m)Y_{nm} = \\ &\sum_{n,m=0}^{\infty} \frac{1}{I_0(2\mu_i)} \times \frac{\mu_i^{2n}}{(n!)^2}[1-(1-\eta_d)^n + P_d] \frac{1}{I_0(2\nu_j)} \times \\ &\frac{\nu_j^{2m}}{(m!)^2}[1-(1-\eta_d)^m + P_d]Y_{nm}, \end{aligned} \tag{5}$$

$$E_{\mu_i\nu_j}Q_{\mu_i\nu_j}=\sum_{n,m=0}^{\infty}P_{\mu_i}(n)P_{\nu_j}(m)e_{nm}Y_{nm}=\sum_{n,m=0}^{\infty}\frac{1}{\mathrm{I}_0(2\mu_i)}\times\frac{\mu_i^{2n}}{(n!)^2}\times$$
$$[1-(1-\eta_\mathrm{d})^n+P_\mathrm{d}]\times\frac{1}{\mathrm{I}_0(2\nu_j)}\times\frac{\nu_j^{2m}}{(m!)^2}\times[1-(1-\eta_\mathrm{d})m+P_\mathrm{d}]e_{nm}Y_{nm}=$$
$$\frac{P_\mathrm{d}}{\mathrm{I}_0(2\mu_i)}\times\frac{P_\mathrm{d}}{\mathrm{I}_0(2\nu_j)}e_{00}Y_{00}+\frac{(\eta_\mathrm{d}+P_\mathrm{d})\mu_i^2}{\mathrm{I}_0(2\mu_i)}\times\frac{P_\mathrm{d}}{\mathrm{I}_0(2\nu_j)}e_{10}Y_{10}+$$
$$\frac{P_\mathrm{d}}{\mathrm{I}_0(2\mu_i)}\times\frac{(\eta_\mathrm{d}+P_\mathrm{d})\nu_j^2}{\mathrm{I}_0(2\nu_j)}e_{01}Y_{01}+\sum_{n,m=1}^{\infty}P_{\mu_i}(n)P_{\nu_j}(m)e_{nm}Y_{nm}。\tag{6}$$

因此，求最小值问题 $\min Y_{11}^z[1-H_2(e_{11}^x)]$可以转化为分别求 Y_{11} 的下限和 e_{11} 的上限问题，并可进一步通过线性规划得到这两个极限。这里利用文献[21]的方法估计 Y_{11} 的下限和 e_{11} 的上限。当 Y_{11} 和 e_{11} 分别取其下限和上限时，即取得最小值 $\min Y_{11}^z[1-H_2(e_{11}^x)]$。

在实际情况中，有限长度密钥会在参数估计中引起统计波动，给 QKD 系统带来一定的安全隐患。利用文献[26]中的标准分析方法，分析基于 HPCS 的 MDI-QKD 方案有限长度密钥的问题。

3 仿　　真

首先，对三种不同实用光源各自的光子数分布进行仿真，结果如图 2 所示。分别计算出空脉冲、单光子脉冲、多光子脉冲的比例并作对比。

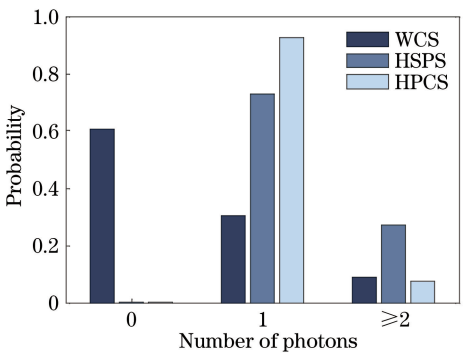

图 2　在平均光子数为 0.5 的不同光源下的光子数分布

Fig. 2　Photon number distribution for different sources with a mean photon number of 0.5

从图 2 可以看出，与 WCS 相比，HPCS 和 HSPS 中的空脉冲数量比例小，这是由于后者光子数分布中的空脉冲项与暗计数相乘而变成了一个高阶小量，从而大大降低了长距离 QKD 中由探测器的暗计数引起的误码率。与 HSPS 相比，HPCS 可以通过抽运光源的参量下转换来增加单光子脉冲的比例，从而在一定程度上提高密钥生成率。

为方便比较，采用与文献[18]相同的实验参数。另外，文献[32]指出，在 MDI-QKD 实验中，Alice(Bob)常使用非退化转换过程来产生两组光子以进一步减小暗计数的影响：其中一组光子作为预报信号，另一组进入远程通信窗口经光纤传输后作为信号态，仅当预报信号一侧探测到单光子时，信号态一侧的单光子探测器才开启。采用典型的硅雪崩光电二极管($P_\mathrm{d}=10^{-6}$，$\eta_\mathrm{d}=0.75$)[33]作为 HSPS、HPCS 的探测器，进一步研究密钥率与探测系数 η_d 的相关性。而非可信第三方的主要实验参数[18]见表 2，其中 $\eta_\mathrm{d}^\mathrm{c}$、$P_\mathrm{d}^\mathrm{c}$ 分别为 Charlie 端的探测效率和暗计数，N_data 为脉冲数。

表 2　Charlie/Eve 的实验参数[18]

Table 2　Experimental parameters for Charlie/Eve[18]

$\eta_\mathrm{d}^\mathrm{c}$	P_d^c	f	N_data
14.5%	3×10^{-6}	1.16	10^{12}

在参数估计过程中，由于 Y_{11}^w 和 e_{11}^w 前的系数(亚泊松分布密度函数)随着 n 的增大呈指数型减小趋势，进一步简化(3)式，舍去次数大于 6 的高阶项。

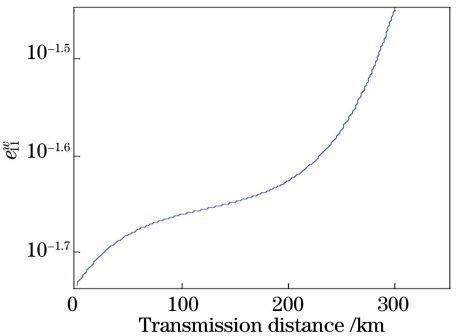

图 3 单光子误码率 e_{11}^{w} 随传输距离的变化（HPCS 光源）

Fig. 3 Single-photon error rate e_{11}^{w} versus transmission distance (HPCS source)

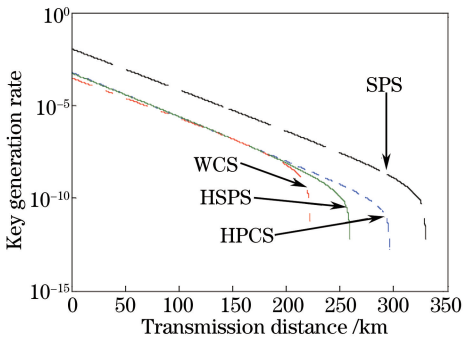

图 4 不同光源下密钥生成率随传输距离的变化

Fig. 4 Key generation rate versus transmission distance under different sources

在信号态强度最佳的条件下，比较了三强度诱骗态 MDI-QKD 的单光子误码率及最终密钥生成率，结果如图 3、4 所示。从图 4 可以看出，使用 WCS 的 MDI-QKD 的最大传输距离仅为 220 km，而基于 HPCS 的方案能达到的最大安全传输距离约为 295 km，增加了近 75 km。这主要是由于 HPCS 产生了更少的真空态，进而真空态的计数率及暗计数的影响减小。

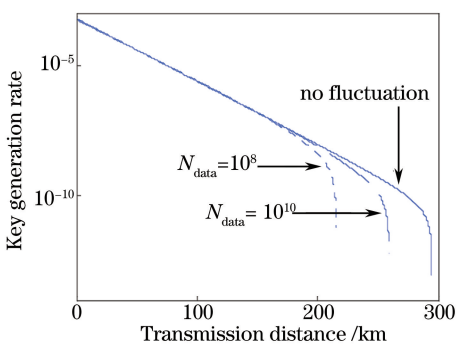

图 5 HPCS 下密钥生成率随传输距离的变化

Fig. 5 Key generation rate versus transmission distance under HPCS

图 5 给出了不同密钥长度条件下的密钥生成率，受统计波动影响，脉冲数目越大，密钥生成率和最大传输距离越大。达到无限密钥长度时，无统计波动的影响，此时最大传输距离为 295 km。由此可以认为基于 HPCS 的 MDI-QKD 协议受统计波动的影响较大。

4 结 论

提出了一种基于 HPCS 的三强度诱骗态 MDI-QKD 的改进方案。HPCS 的脉冲中含有较低比例的真空态，有利于降低长距离 QKD 中由暗计数引起的误码率。与基于弱相干态的诱骗态 QKD 相比，本方案能将最大安全传输距离提高 75 km；与基于 HSPS 的诱骗态 QKD 相比，本方案具有较高的单光子比例，有利于提高密钥生成率。另外，用标准分析方法进行了估计，分析了由有限密钥带来的统计波动问题及其对密钥生成率和最大传输距离的影响。

参 考 文 献

[1] Sheng Y B, Deng F G. Efficient quantum entanglement distribution over an arbitrary collective-noise channel[J]. Physical Review A, 2010, 81(4): 042332.

[2] Bennett C H. Quantum cryptography: public key distribution and coin tossing[C]. IEEE International Conference on Computers Systems and Signal Processing, 1984: 175-179.

[3] Das T, Prabhu R, De A S, *et al*. Distributed quantum dense coding with two receivers in noisy environments[J].

Physical Review A, 2015, 92(5): 052330.

[4] Lo H K, Lütkenhaus N. Quantum cryptography: from theory to practice[J]. Physics in Canada, 2007, 63(4): 191-196.

[5] Jiao Rongzhen, Tang Shaojie, Zhang Chao. Analysis of statistical fluctuation in decoy state quantum key distribution system[J]. Acta Physica Sinica, 2012, 61(5): 050302.
焦荣珍, 唐少杰, 张弨. 诱惑态量子密钥分配系统中统计涨落的研究[J]. 物理学报, 2012, 61(5): 050302.

[6] Liu Youming, Wang Chao, Huang Duan, *et al*. Study of synchronous technology in high-speed continuous variable quantum key distribution system[J]. Acta Optica Sinica, 2015, 35(1): 0106006.
刘友明, 汪超, 黄端, 等. 高速连续变量量子密钥分发系统同步技术研究[J]. 光学学报, 2015, 35(1): 0106006.

[7] Gottesman D, Lo H K, Lütkenhaus N, *et al*. Security of quantum key distribution with imperfect devices[C]. IEEE International Symposium on Information Theory, 2004: 8178599.

[8] Sheng Y B, Zhou L, Cheng W W, *et al*. Complete Bell-state analysis for a single-photon hybrid entangled state[J]. Chinese Physics B, 2013, 22(3): 179-183.

[9] Sun Ying, Zhao Shanghong, Dong Chen. Long distance measurement device independent quantum key distribution with quantum memories[J]. Acta Physica Sinica, 2015, 64(14): 140304.
孙颖, 赵尚弘, 东晨. 基于量子存储的长距离测量设备无关量子密钥分配研究[J]. 物理学报, 2015, 64(14): 140304.

[10] Braunstein S L, Pirandola S. Measurement device independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 4089-4091.

[11] Brassard G, Lutkenhaus N, Mor T, *et al*. Limitations on practical quantum cryptography[J]. Physical Review Letters, 2000, 85(6): 1330-1333.

[12] Sun S H, Liang L M. Experimental demonstration of an active phase randomization and monitor module for quantum key distribution[J]. Applied Physics Letters, 2012, 101(7): 175-179.

[13] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols[J]. Quantum Information & Computation, 2007, 8(6): 622-635.

[14] Zhao Y, Fung C H F, Qi B, *et al*. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems[J]. Physical Review A, 2007, 78(4): 4702-4705

[15] Yuan Z L. Avoiding the blinding attack in QKD[J]. Nature Photonics, 2010, 4(12): 800-801.

[16] Deng F G, Long G L. Bidirectional quantum key distribution protocol with practical faint laser pulses[J]. Physical Review A, 2004, 70(1): 012311.

[17] Vazirani U, Vidick T. Device independent quantum key distribution[J]. Physics Review Letters, 2014, 113(14): 140501.

[18] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[19] Sun Ying, Zhao Shanghong, Dong Chen. Passive measurement device independent quantum key distribution based on parametric downconversion source[J]. Acta Optica Sinica, 2015, 35(12): 1227001.
孙颖, 赵尚弘, 东晨. 基于参量下转换光源的被动测量设备无关量子密钥分配[J]. 光学学报, 2015, 35(12): 1227001.

[20] Sun Ying, Zhao Shanghong, Dong Chen. Measurement device independent quantum key distribution network based on quantum memory and entangled photon sources[J]. Acta Optica Sinica, 2016, 36(3): 0327001.
孙颖, 赵尚弘, 东晨. 基于量子存储和纠缠光源的测量设备无关量子密钥分配网络[J]. 光学学报, 2016, 36(3): 0327001.

[21] Ma X F, Fung C H F, Razavi M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(5): 052305.

[22] Sun S H, Gao M, Li C Y, *et al*. Practical decoy-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2013, 87(5): 052329.

[23] Yu Z W, Zhou Y H, Wang X B. Three-intensity decoy state method for device independent quantum key distribution[J]. Physical Review A, 2013, 88(6): 3869-3876.

[24] Tang Z, Liao Z, Xu F, *et al*. Experimental demonstration of polarization encoding measurement-device-independent

quantum key distribution[J]. Physical Review Letters, 2014, 112(19): 190503.

[25] Tang Y L, Yin H L, Chen S J, *et al*. Measurement-device-independent quantum key distribution over 200 km[J]. Physical Review Letters, 2014, 113(19): 190501.

[26] Yuan C, Hao L, Juan Y, *et al*. Entanglement-based quantum key distribution with biased basis choice via free space [J]. Optics Express, 2013, 21(22): 27260-27268.

[27] Adachi Y, Yamamoto T, Koachi M, *et al*. Simple and efficient quantum key distribution with parametric down-conversion[J]. Physical Review Letters, 99(18): 180503.

[28] Horikiri T, Kobayashi T. Polarization-entangled mode-locked photons from cavity-enhanced spontaneous parametric down-conversion[J]. Physical Review A, 2004, 70(4): 628-628.

[29] Zhou C, Bao W S, Chen W, *et al*. Phase-encoded measurement device independent quantum key distribution with practical spontaneous parametric-down-conversion sources[J]. Physical Review A, 2014, 88(5): 052333.

[30] Wang Q, Wang X B. An 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.

[31] Zhou C. Decoy-state quantum key distribution for the heralded pair coherent state photon source with intensity fluctuations[J]. Science China Information Sciences, 2010, 53(12): 2485-2494.

[32] Zhu F, Zhang C H, Liu A P, *et al*. Enhancing the performance of the measurement-device-independent quantum key distribution with heralded pair-coherent sources[J]. Physics Letters A, 2016, 380(16): 1408-1413.

[33] Zhou Yuanyuan, Zhang Heqing, Zhou Xuejun, *et al*. Performance analysis of decoy-state quantum key distribution with a heralded pair coherent state photon source[J]. Acta Physica Sinica, 2013, 62(20): 200302.
周媛媛, 张合庆, 周学军, 等. 基于标记配对相干态光源的诱骗态量子密钥分配性能分析[J]. 物理学报, 2013, 62(20): 200302.

[34] Ma X, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(6): 3818-3821.