基于参量下转换光源的被动测量设备无关量子密钥分配

孙 颖[1] 赵尚弘[1] 东 晨[1,2]

[1]空军工程大学信息与导航学院, 陕西 西安 710077

[2]西安通信学院信息安全系, 陕西 西安 710006

摘要 量子密钥分配过程中制备诱骗态信号易引入一些边信息(频率、脉冲宽度等),窃听者可利用这些信息来分辨信号态和诱骗态。因此,提出了基于参量下转换光源和被动诱骗态方案的测量设备无关量子密钥分配协议,分析了其密钥生成率、单光子计数率以及单光子误码率与安全传输距离的关系。仿真结果表明,基于参量下转换光源的被动测量设备无关量子密钥分配协议的密钥安全传输距离达到285 km,远高于基于改造后可输出两路相关信号的弱相干光源的被动测量设备无关量子密钥分配协议,十分接近基于主动诱骗态的测量设备无关量子密钥分配协议,且克服了主动诱骗态方案可能引入边信息的缺点。

关键词 量子光学; 量子密钥分配; 测量设备无关; 被动诱骗态; 参量下转换光源

中图分类号 O431; TN918 **文献标识号** A

doi: 10.3788/AOS201535.1227001

Passive Measurement Device Independent Quantum Key Distribution Based on Parametric down Conversion Source

Sun Ying[1] Zhao Shanghong[1] Dong Chen[1,2]

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

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

Abstract The preparation of decoy state in the quantum key distribution process is easy to introduce some extra information (frequency, pulse width, etc.), and the eavesdropper can use these information to distinguish signal state from decoy state. Therefore, this article proposes passive measurement device independent quantum key distribution (MDI-QKD) based on parametric down conversion source (PDCS) and decoy state plan, and analyzes the key generation rate, single photon counting rate, bit error rate and the secure key transmission distance. The simulation results show that the maximum secure distance of passive MDI-QKD based on PDCS is about 285 km, which is much longer than MDI-QKD based on modified weak coherent source and is close to active MDI-QKD, and overcomes the imperfection of active decoy state plan that may introduce the extra information.

Key words quantum optics; quantum key distribution; measurement device independent; passive decoy-state; parametric down conversion source

OCIS codes 270.5568; 270.5570; 230.6080; 270.5290

1 引 言

量子密钥分配[1-3](QKD)作为量子力学和密码学相结合的产物,与传统的密钥分配不同,其绝对安全性是建立在物理基本规律的基础上。但实际QKD系统中往往会出现一些漏洞,使得窃听者能有针对性地攻击系统。非理想光源使系统容易受到光子数分束(PNS)攻击[4-5],非完美测量设备会导致系统易受到时移攻击[6]、相位重映射攻击[7]等。为克服PNS攻击,Hwang[8]提出了基于诱骗态的QKD协议,允许系统用弱相干光源代

收稿日期: 2015-07-01; **收到修改稿日期**: 2015-08-04

基金项目: 国家自然科学基金(61106068)

作者简介: 孙 颖(1991—),男,硕士研究生,主要从事量子信息科学和量子密钥分配方面的研究。

E-mail: sunyingkgd@163.com

导师简介: 赵尚弘(1964—),男,教授,博士生导师,主要从事空间信息技术和量子信息方面的研究。

E-mail: zhaoshanghong@aliyun.com

替单光子源。为解决测量设备易受攻击的问题，Lo等[9]在2012年提出测量设备无关量子密钥分配协议(MDI-QKD)，可移除所有的探测器侧信道漏洞，并提高系统的密钥安全传输距离[10-11]。

目前，诱骗态方案可分为两类：1) 主动诱骗态方案[12-13]，用户主动制备诱骗态，在制备过程中易引入一些边信息(频率、脉冲宽度等)，窃听者可利用这些信息来分辨信号态和诱骗态，使得诱骗态方案的安全性难以保证。2) 被动诱骗态方案[14-15]，用户不主动制备诱骗态，信号态和诱骗态是根据用户端探测器的检测结果，靠被动选择的方式来产生，消除了主动诱骗态方案的漏洞。光源能产生两路光子数分布概率相关的信号是实现被动诱骗态方案的基本前提，参量下转换光源(PDCS)的双模式特性完全满足这一要求，因而基于PDCS的被动诱骗态方案相继被提出[16-17]。在MDI-QKD协议中，Alice和Bob将光脉冲发送至非可信任的第三方进行Bell态测量[18]并公布测量结果，Alice和Bob根据基比对过程提取出安全密钥，整个测量过程都在第三方进行，从而可以移除所有的探测器侧信道漏洞。由于MDI-QKD大大提高了QKD系统的现实安全性，针对该协议的改进方案相继被提出[19-20]。

最近，文献[21]提出了基于弱相干光源(WCS)的被动MDI-QKD协议，其安全密钥传输距离达到了225 km。考虑到PDCS能有效减少长距离量子密钥分配过程中暗计数的影响，可增大量子密钥分配的安全传输距离[22-23]。本文结合PDCS和被动诱骗态方案提出了基于PDCS的被动MDI-QKD协议，且在文献[21]的基础上研究了改造的弱相干光源(MWCS)，并通过实验仿真对比分析了基于PDCS的被动MDI-QKD协议和基于MWCS的被动MDI-QKD协议的密钥提取率、单光子计数率以及单光子误码率与安全传输距离之间的关系。

2　被动诱骗态MDI-QKD协议

2.1　MWCS

为满足被动诱骗态方案的要求，需要对WCS的硬件进行改造，使WCS输出两路光子数分布概率具有相关性的信号，MWCS结构模型如图1所示。

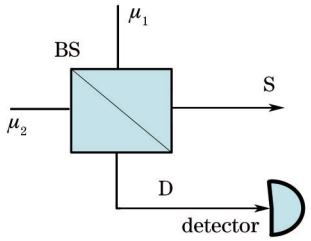

图1　改造的弱相干光源结构模型

Fig.1　Structure of modified weak coherent source

采用两个WCS光源，它们产生相位随机、强度分别为μ_1和μ_2的相干态$|\psi\rangle_1$和$|\psi\rangle_2$，将其输入到分束器并发生干涉，则输出的两路信号S和D的光子数分布概率将具有相关性。在文献[21]的基础上，本文给出了基于MWCS的被动诱骗态MDI-QKD的结构模型，如图2所示。

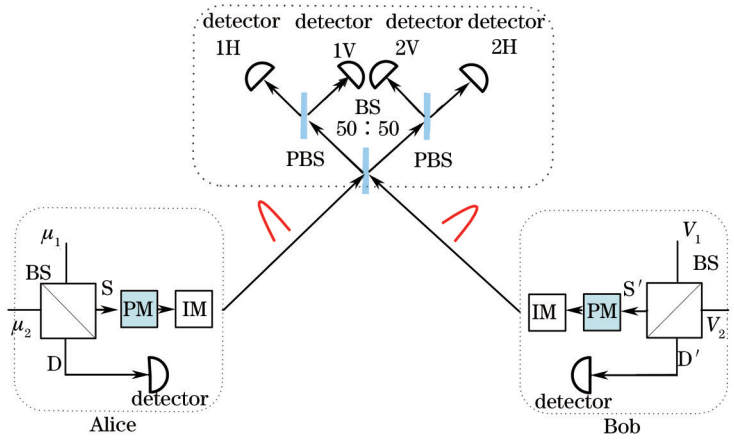

图2　基于MWCS的被动诱骗态MDI-QKD系统模型

Fig.2　Structure of passive MDI-QKD system based on MWCS

MWCS输出的两路信号的光子数概率分布具有一定的相关性，只需要对D(D′)端信号进行检测，就能确定S(S′)端信号的光子数概率分布。设相干态 $|\psi\rangle_1$ 和 $|\psi\rangle_2$ 为：

$$\begin{cases}|\psi\rangle_1=\exp(-\mu_1)\sum\limits_{n=0}^{\infty}\dfrac{\mu_1^n}{n!}|n\rangle\langle n|\\ |\psi\rangle_2=\exp(-\mu_2)\sum\limits_{n=0}^{\infty}\dfrac{\mu_2^n}{n!}|n\rangle\langle n|\end{cases},\tag{1}$$

式中 μ_1 和 μ_2 表示两路输入信号的强度，此时S(S′)端输出的是 n 光子态，D(D′)端输出的是 m 光子态，两者的联合概率为：

$$\begin{cases}p_{n,m}=\dfrac{\nu^{n+m}\exp(-\nu)}{n!m!}\dfrac{1}{2\pi}\int_0^{2\pi}r^n(1-r)^m\mathrm{d}\theta\\ \nu=\mu_1+\mu_2\\ r=\dfrac{1}{2}-\dfrac{\sqrt{\mu_1\mu_2}\sin\theta}{\mu_1+\mu_2}\end{cases},\tag{2}$$

式中 θ 表示两路输入信号的相位差，可以看出 $p_{n,m}$ 是两个泊松分布的乘积，只要Alice(Bob)检测得到D(D′)端输出的 m 光子态的概率分布，则S(S′)输出的 n 光子态的概率分布可确定为：

$$q_{n,s}=\sum_{m=0}^{\infty}p_{n,m}=\frac{\nu^n}{n!}\frac{1}{2\pi}\int_0^{2\pi}r^n\exp(-\nu r)\mathrm{d}\theta\,.\tag{3}$$

D(D′)端输出的 m 光子态未被Alice(Bob)端探测器检测到时，对应S(S′)端输出的 n 光子态为信号态，其概率分布为：

$$\begin{aligned}q_{n,s}^{t_0}&=(1-\varepsilon)\sum_{m=0}^{\infty}(1-\eta_{\mathrm{d}})^m p_{n,m}\\ &=(1-\varepsilon)\frac{\nu^n\exp(-\eta_{\mathrm{d}}\nu)}{n!}\frac{1}{2\pi}\int_0^{2\pi}r^n\exp\left[-(1-\eta_{\mathrm{d}})\nu r\right]\mathrm{d}\theta\end{aligned},\tag{4}$$

反之，D(D′)端输出的 m 光子态被Alice(Bob)端探测器检测到时，则对应S(S′)输出的 n 光子态为诱骗态，其概率分布为：

$$q_{n,s}^{t_1}=q_{n,s}-q_{n,s}^{t_0},\tag{5}$$

式中 t_0 表示未被检测到，t_1 表示被检测到。

2.2 PDCS

在光的自发参量下转换过程中，一个高频光子在非线性晶体内会以某一概率自发地分裂为两个低频光子，分别称为信号光子和闲频光子，合称为PDC光子对，在特定条件下的自发参量下转换可以获得双模态[24]：

$$|\phi\rangle_{\mathrm{SD}}=\sum_{n=0}^{\infty}\sqrt{p_n}|n\rangle_{\mathrm{S}}|n\rangle_{\mathrm{D}},\tag{6}$$

参量下转换产生的信号光子态(闲频光子态)的光子数分布为：

$$p_n(\mu)=\frac{\mu^n}{(1+\mu)^{n+1}},\tag{7}$$

式中 n 表示光子数，μ 表示平均光强度。如图3所示，S(S′)端输出的是PDC光子对中的信号光子，D(D′)端输出的是闲频光子。PDCS输出的信号光子数和闲频光子数是相等的，只要Alice(Bob)端检测得到D(D′)端输出的 n 光子态分布概率，就可以确定S(S′)端输出的 n 光子态的分布概率。

当Alice(Bob)端探测器响应时(即闲频光子被本端探测器探测到)，表示Alice(Bob)发送给Charlie的是信号态；若不响应，则表示Alice(Bob)发送给Charlie的是诱骗态。因此，Alice(Bob)所发出的信号态和诱骗态的 n 光子态概率分布 $q_{n,s}^{t_0}$ 和 $q_{n,s}^{t_1}$ 分别为：

$$\begin{cases}q_{n,s}^{t_0}=\left[1-\varepsilon\right]p_n(\mu)(1-\eta_{\mathrm{d}})^n\\ q_{n,s}^{t_1}=p_n(\mu)-q_{n,s}^{t_0}\end{cases},\tag{8}$$

式中 ε 为探测器的暗计数率，η_{d} 为探测器探测效率。这里假设系统中所有探测器的暗计数率和探测效率相等。

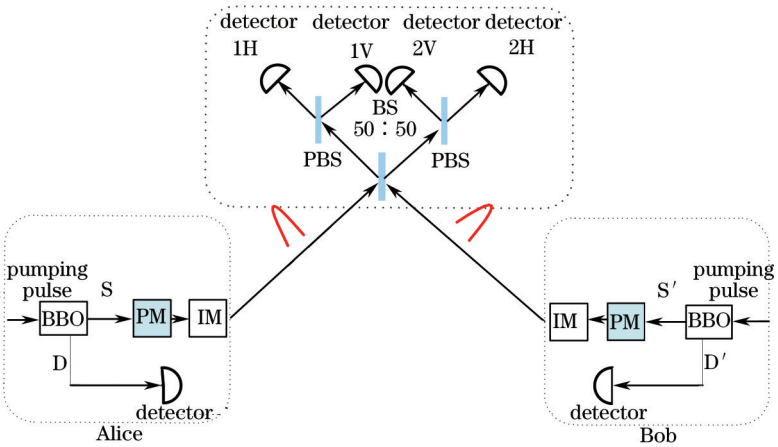

图 3 基于 PDCS 的被动诱骗态 MDI-QKD 系统模型

Fig.3 Structure of passive MDI-QKD system based on PDCS

2.3 基于两种光源的安全密钥率估计

基于 PDCS 的被动诱骗态 MDI-QKD 协议和基于 MWCS 的被动诱骗态 MDI-QKD 协议都可按照 GLLP 公式来提取安全密钥[25]：

$$R \geqslant q_{1,s}^{t_0} q_{1,s'}^{t_0} Y_{11}^{z}\left[1-H\left(e_{11}^{X}\right)\right]-Q_{t_0 t_0}^{Z} f\left(E_{t_0 t_0}^{Z}\right) H\left(E_{t_0 t_0}^{Z}\right), \tag{9}$$

式中 $H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ 是二进制香农熵函数，$f(x)$ 是低效率纠错函数，Y_{11}^{Z} 是 Z 基下单光子态的计数率，e_{11}^{X} 是 X 基下单光子态的误码率，$Q_{t_0 t_0}^{Z}$ 和 $E_{t_0 t_0}^{Z}$ 分别指 Z 基下全局计数率和全局误码率。

不考虑基选择的情况下，在 Charlie 端得到的成功贝尔态测量概率满足：

$$\begin{aligned} Q_{t_i t_j} = & \sum_{n,m=0}^{\infty} q_{n,s}^{t_i} q_{m,s'}^{t_j} Y_{n,m}^{w} = \\ & q_{0,s}^{t_i} q_{0,s'}^{t_j} Y_{00} + q_{0,s}^{t_i} \sum_{m=1}^{\infty} q_{m,s'}^{t_j} Y_{0m} + q_{0,s'}^{t_j} \sum_{n=1}^{\infty} q_{n,s}^{t_i} Y_{n0} + q_{1,s}^{t_i} q_{0,s'}^{t_j} Y_{11} + , \\ & q_{1,s}^{t_i} \sum_{m=2}^{\infty} q_{m,s'}^{t_j} Y_{1m} + q_{1,s'}^{t_j} \sum_{n=2}^{\infty} q_{n,s}^{t_i} Y_{n1} + \sum_{n,m=2}^{\infty} q_{n,s}^{t_i} q_{m,s'}^{t_j} Y_{nm} \end{aligned} \tag{10}$$

Charlie 端得到的单光子错误贝尔态测量概率满足：

$$\begin{aligned} E_{t_1 t_1} Q_{t_1 t_1} = & \sum_{n,m=0}^{\infty} q_{n,s}^{t_i} q_{m,s'}^{t_j} e_{n,m}^{w} Y_{n,m}^{w} = \\ & -q_{0,s}^{t_1} q_{0,s'}^{t_1} e_{00} Y_{00} + q_{1,s}^{t_1} q_{1,s'}^{t_1} e_{11} Y_{11} + q_{0,s}^{t_1} \sum_{m=0}^{\infty} q_{m,s'}^{t_1} e_{0m} Y_{0m} + q_{0,s'}^{t_1} \sum_{n=0}^{\infty} q_{n,s}^{t_1} e_{n0} Y_{n0} + , \\ & q_{1,s}^{t_1} \sum_{m=2}^{\infty} q_{m,s'}^{t_1} e_{1m} Y_{1m} + q_{1,s'}^{t_1} \sum_{n=2}^{\infty} q_{n,s}^{t_1} e_{n1} Y_{n1} + \sum_{n,m=2}^{\infty} q_{n,s}^{t_1} q_{m,s'}^{t_1} e_{nm} Y_{nm} \end{aligned} \tag{11}$$

式中 $Y_{n,m}^{w}$ 为 w 基 $(w=X、Z)$ 下在 Charlie 端 Alice 和 Bob 发送的 (n,m) 光子数信号态获得的成功贝尔态测量的概率，$e_{n,m}^{w} Y_{n,m}^{w}$ 为 w 基下对应产生的错误贝尔态测量的概率。

3 仿真结果与比较分析

结合文献[21]可得到 Z 基下单光子计数率的下限 $\underline{Y_{11}^{Z}}$ 和 X 基下单光子误码率的上限 $\overline{e_{11}^{X}}$。求解密钥生成率所需要的 X 基下的全局计数率和 Z 基下的全局误码率可在实验中测得的，联合(1)~(11)式可得到两种光源下最终密钥生成率、Y_{11}^{Z} 和 e_{11}^{X} 与安全传输距离之间的关系，主要仿真参数如表 1 所示。

表 1 主要仿真参数

Table 1 Main simulation parameters

Ref [26]	e_0	e_d	ε	α	η_d
	0.5	1.5%	10^{-6}	0.17	0.2

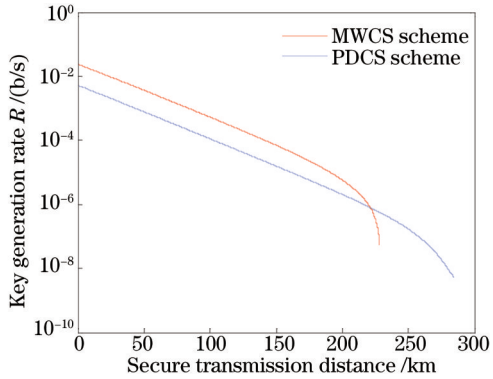

图 4 密钥生成率与安全传输距离

Fig.4 Key generation rate and the secure transmission distance

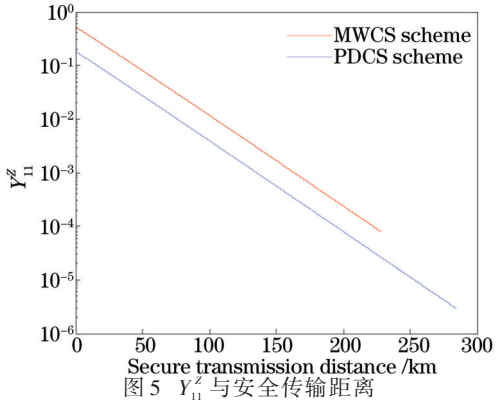

图 5 Y_{11}^{Z} 与安全传输距离

Fig.5 Y_{11}^{Z} and the secure transmission distance

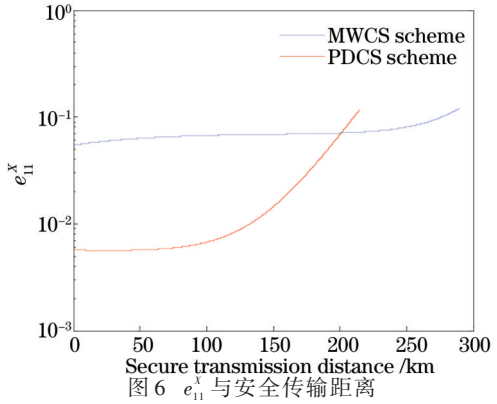

图 6 e_{11}^{X} 与安全传输距离

Fig.6 e_{11}^{X} and the secure transmission distance

系统误码率较大时，可能存在窃听，要确保能检测到窃听行为，就必须将误码率限制在一定范围内[7]，也就限制了密钥的安全传输距离[27]，使该方案也不可避免存在极限值。考虑到目前最好的纠错码的纠错能力可达到 12.9%[28]，将误码率的阈值设为 11%。如图 4 所示，PDCS 方案的最大安全传输距离约为 285 km，明显高于 MWCS 方案的 225 km，且十分趋近于主动诱骗态 MDI-QKD 协议，原因是 PDCS 能有效减少长距离量子密钥分配过程中暗计数的影响，从而增大量子密钥分配的安全传输距离。在安全传输距离小于 220 km 的情况下，PDCS 方案的密钥生成率比 MWCS 方案低，原因是 PDCS 产生的信号中多光子脉冲所占的比例要大于 MWCS，从而导致一定传输距离内密钥生成率的降低。

如图 5 所示，两种方案的 Y_{11}^{Z} 曲线保持平行，但是 MWCS 方案中的 Y_{11}^{Z} 要明显高于 PDCS 方案，这是因为 MWCS 产生的信号中单光子脉冲比重大，Z 基下的单光子计数率相对较高。如图 6 所示，在安全传输距离小于 200 km 的情况下，MWCS 方案的 e_{11}^{X} 比 PDCS 方案小，但是随着安全传输距离的增加而急剧增大，说明 MWCS 方案的单光子误码率对传输损耗更加敏感。

4 结 论

提出了基于 PDCS 的被动 MDI-QKD 协议，它具备被动诱骗态协议和 MDI-QKD 协议的双重优势，消除了探测端信道漏洞，克服了主动诱骗态方案可能引入边信息的缺点，且 PDCS 可以有效减少密钥分配过程中暗计数的影响，增大安全传输距离。还比较了 PDCS 方案和 MWCS 方案的密钥生成率、单光子计数率、单光子误码率与安全传输距离的关系，仿真结果表明基于 PDCS 的被动 MDI-QKD 的安全传输距离达到了 285 km，远高于基于 MWCS 的被动 MDI-QKD 协议，非常接近于主动诱骗态 MDI-QKD 协议。因此，基于 PDCS 的被动 MDI-QKD 协议具有很好的发展前景。另外，没有考虑不对称信道传输率对密钥分配系统的影响(只是理想化假定信道传输率 $\eta_a=\eta_b$)，以及 MWCS 的两路输出相干光的强度差异对密钥生成率的影响。将在下一步深入研究这两个影响因子，提出改进方案，以增大密钥的安全传输距离。

参 考 文 献

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

2 Dong Chen, Zhao Shanghong, Dong Yi, *et al*.. Measurement of device-independent quantum key distribution for the rotation invariant photonic state[J]. Acta Physica Sinica, 2014 , 63(17): 170303.

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.

3 Zhu Feng, Wang Qin. Quantum key distribution protocol based on heralded single photon source[J]. Acta Optica Sinica, 2014, 34(6): 0627002.

朱 峰, 王 琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014, 34(6): 0627002.

4 R D Somma, R J Hughes. Security of decoy-state protocols for general photon-number-splitting attacks[J]. Phys Rev A, 2013, 87(6): 062330.

5 W Liu, S Sun, L Liang, *et al*.. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution [J]. Phys Rev A, 2011, 83(4): 042326.

6 Y Zhao, C H F Fung, B Qi, *et al*.. Quantum hacking: experimental demonstration of time shift attack against practical quantum key distribution systems[J]. Phys Rev A, 2008, 78(4): 042333.

7 C H F Fung, B Qi, K Tamaki, *et al*.. Phase-remapping attack in practical quantum key distribution systems[J]. Phys Rev A, 2007, 75(3): 032314.

8 W Y Hwang. Quantum key distribution with high loss: toward global secure communication[J]. Phys Rev Lett, 2003, 91(5): 057901.

9 H K Lo, M Curty, B Qi. Measurement-device-independent quantum key distribution[J]. Phys Rev Lett, 2012, 108(13): 130503.

10 P Chan, J A Slater, I Lucio Martinez, *et al*.. Modeling a measurement device independent quantum key distribution system[J]. Optics Express, 2014, 22(11): 12716-12736.

11 X F Ma, M Razavi. Alternative schemes for measurement-device-independent quantum key distribution[J]. Phys Rev A, 2012, 86(6): 062319.

12 H Chi, Z Yu, X Wang. Decoy-state method of quantum key distribution with both source errors and statistics fluctuations[J]. Phys Rev A, 2012, 86(4): 042307.

13 Mi Jinglong, Wang Faqiang, Lin Qingqun, *et al*.. Decoy state quantum key distribution with dual detector sheralded single photon source [J]. Acta Physica Sinica, 2008, 57(2): 678-684.

米景隆, 王发强, 林青群, 等. 诱惑态在"双探测器"准单光子光源量子密钥分发系统中的应用[J]. 物理学报, 2008, 57(2): 678-684.

14 Y Zhang, W Chen, S Wang, *et al*.. Practical non-Poissonian light source for passive decoy state quantum key distribution[J]. Opt Lett, 2010, 35(20): 3393-3395.

15 W Mauerer, C Silberhorn. Quantum key distribution with passive decoy state selection[J]. Phys Rev A, 2007, 75(5): 050305.

16 C Zhou, W Bao, W Chen, *et al*.. Phase-encoded measurement device independent quantum key distribution with practical spontaneous parametric down conversion sources[J]. Phys Rev A, 2013, 88(5): 052333.

17 Y Adachi, T Yamamoto, M Koashi, *et al*.. Simple and efficient quantum key distribution with parametric down-conversion[J]. Phys Rev Lett, 2007, 99(18): 180503.

18 Y Liu, T Chen, L Wang, *et al*.. Experimental measurement device independent quantum key distribution[J]. Phys Rev Lett, 2013, 111 (13): 130502.

19 X Ma, S Sun, M Jiang, *et al*.. Gaussian-modulated coherent-state measurement device independent quantum key distribution[J]. Phys Rev A, 2014, 89(4): 042335.

20 F Xu, B Qi, Z Liao, *et al*.. Long distance measurement device independent quantum key distribution with entangled photon sources[J]. Appl Phys Lett, 2013, 103(6): 061101.

21 Y Shan, S Sun, X Ma, *et al*.. Measurement-device-independent quantum key distribution with a passive decoy-state method [J]. Phys Rev A, 2014, 90(4): 042334.

22 Q Wang, X Wang, G Björk, *et al*.. Improved practical decoy state method in quantum key distribution with parametric down conversion source[J]. Europhys Lett, 2007, 79(4): 40001.

23 Quan Dongxiao, Pei Changxing, Zhu Changhua, *et al*.. New method of decoy state quantum key distribution with a heralded single-photon source[J]. Acta Physica Sinica, 2008, 57(9): 5600-5604.

权东晓, 裴昌幸, 朱畅华, 等. 一种新的预报单光子源诱骗态量子密钥分发方案[J]. 物理学报, 2008, 57(9): 5600-5604.

24 S Mori, J Söderholm, N Namekata, *et al*.. On the distribution of 1550 nm photon pairs efficiently generated using a periodically poled lithium niobate waveguide[J]. Opt Commun, 2006, 264(1): 156-162.

25 D Gottesman , H K Lo, N Lütkenhaus, *et al*.. Security of quantum key distribution with imperfect devices[J]. Quantum Information & Computation, 2004, 4(5): 325-360.

26 S Abruzzo, H Kampermann, D Bruss. Measurement device independent quantum key distribution with quantum memories[J]. Phys Rev A, 2014, 89(1): 012301.

27 Jiao Rongzhen, Feng Chenxu, Tang Shaojie. Communication rate and error rate in the quantum-key-distribution system[J]. Acta Optica Sinica, 2008, 28 (S2): 167-169.

焦荣珍, 冯晨旭, 唐少杰. 量子密钥分配系统中的通信速率和误码率[J]. 光学学报, 2008, 28(S2): 167-169.

28 G Smith, J M Renes, J A Smolin. Structured codes improve the Bennett Brassard 84 quantum key rate[J]. Phys Rev Lett, 2008, 100(17): 170502.

栏目编辑: 刘丰瑞