激光与光电子学进展

基于W态的多方测量设备无关量子密钥分配性能分析

何业锋[1,2]，李丽娜[1*]，白倩[1]，陈思昊[1]，强雨薇[1]

[1]西安邮电大学网络空间安全学院，陕西 西安 710121；

[2]桂林电子科技大学广西密码学与信息安全重点实验室，广西 桂林 541004

摘要 测量设备无关量子密钥分配系统能够抵御任何针对单光子探测器侧信道的攻击。为了进一步优化多方测量设备无关量子密钥分配协议，对基于W态的多方测量设备无关量子密钥分配协议进行了研究，并引入探测器品质因子（暗记数 Y_0 与探测器探测效率 η_d 的比值）作为模拟参量，模拟分析了误码率和密钥生成率的影响因素。仿真结果表明：在信道传输损耗、光纤信道之间的距离和探测器品质因子三个变量中，任意一个变量的增大都会使得误码率增大，密钥生成率减小。

关键词 量子光学；W态；量子密钥分配；测量设备无关；品质因子；密钥生成率

中图分类号 TN918 **文献标志码** A **doi**：10.3788/LOP202158.1127002

Performance Analysis of Multi-Party Measurement-Device-Independent Quantum Key Distribution Based on W States

He Yefeng[1,2], Li Lina[1*], Bai Qian[1], Chen Sihao[1], Qiang Yuwei[1]

[1]*School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*;

[2]*Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*

Abstract The measurement-device-independent quantum key distribution (MDI-QKD) system can resist any attacks on the side channel of the single-photon detector. In order to further optimize the multi-party MDI-QKD protocol, this paper investigates the multi-party MDI-QKD protocol based on W states, and introduces the detector quality factor (ratio of dark count Y_0 to detection efficiency η_d) as an analog parameter to simulate and analyze the factors influencing bit error rate and key generation rate. The simulation results show that the increase of any one among the three variables of channel-transmission loss, fiber-channel distance and detector quality factor enhances the bit error rate and reduces the key generation rate.

Key words quantum optics; W state; quantum key distribution; measurement-device-independent; quality factor; key generation rate

OCIS codes 270.5568; 270.5565; 270.5568; 270.5570

收稿日期：2020-10-27；**修回日期**：2020-11-20；**录用日期**：2020-12-03

基金项目：国家自然科学基金（61802302）、陕西省自然科学基础研究计划项目（2021JM-462）、广西密码学与信息安全重点实验室研究课题（GCIS201923）

***E-mail**：1826971490@qq.com

1 引 言

量子保密通信是量子信息科学的重要组成部分，它的核心是量子密钥分配(Quantum Key Distribution，QKD)[1]。QKD以其在量子力学和信息论框架下的无条件安全性[2-4]，已成为通信安全领域内的研究热点。自1984年BB84协议被提出以来，量子密钥分配得到了广泛的研究[5-7]。然而，在建立实际的量子密钥分配系统时，由于所采用的电学和光学设备的非完美性，系统存在安全漏洞，如探测器的非完美性可能导致系统受到致盲攻击[8]、时移攻击[9]和伪态攻击[10]等，光源的非完美性可能导致系统受到光子束分流攻击[11]，其中针对探测器侧信道的攻击是所有攻击中最为常见的。2012年，Lo等[12]提出了测量设备无关量子密钥分配(Measurement-device-independent quantum key distribution，MDI-QKD)方案，在该方案中，Alice和Bob将单光子脉冲发送到第三方进行贝尔态测量，这种模式既能抵御针对探测器侧信道的攻击，也能提高密钥安全性和传输距离，该方案的提出具有里程碑意义。研究者从实验和理论两方面对MDI-QKD进行了大量的研究，取得了一定的进展[13-17]。然而，实际通信场景中的参与者不仅仅只有两个，为了使MDI-QKD协议的适用性更广，需要进一步地研究多个参与者的通信情况。

研究人员提出了各种多方的QKD协议。一般来说，有三种类型的多方QKD方案。第一种是基于可信中心(TC)[18]的方案，在这种类型的方案中，每个用户与TC共享秘密密钥并构建公共会话密钥。第二种是基于纠缠的多方QKD协议，Cabello[19]提出了一种使用Greenberger-Horne-Zeilinger(GHZ)状态的多方QKD协议，该协议是基于两方纠缠的QKD协议的扩展。第三种是Matsumoto[20]提出的多方QKD协议，其中Alice分别向Bob和Charlie发送相同的量子比特序列，并在后续处理中使用具有相同基的量子比特来构建密钥。但以上三种方案都存在一些不足，如：在第一种方案中，由于预共享秘密密钥的重复使用，信息可能被泄露；在第二种方案中，要求GHZ态是绝对完美的；在第三种方案中，所有的多方量子密码协议的安全性都是基于测量设备是可信的，但实际中测量设备并非都是可信的。为了消除QKD对可信测量设备的依赖，人们研究分析了多方的MDI-QKD协议[21-23]，通过选择合适的纠缠态以及分析器，进行了多方的MDI-QKD协议的研究。

文献[23]提出了一种基于GHZ态的多方的MDI-QKD协议，该协议中三方的MDI-QKD协议在实践中具有很高的可行性。然而，文献[23]主要局限于三个参与者，并且在有更多参与者的情况下，密钥生成率会大打折扣。多方MDI-QKD协议的另一种方案是基于簇态的，但由于簇态分析仪性能的局限性，目前该方案仅仅适用于单光子，不能应用于弱相干态光源。因此，为了设计一个多方MDI-QKD协议并实现高密钥率，需要一个更好的分析仪和不同类型的纠缠态，而W态就是比较好的选择。W态是一类多粒子纠缠态，可用于多种量子信息处理协议[24]。与Bell态相比较，W态、簇态和GHZ态的结构截然不同。其中，Bell态是两光子的最大纠缠态，GHZ态是三光子的最大纠缠态，但它们有个共同的弱点，即一旦它们之中某个比特被检测到，则其余的比特会失去纠缠特性；簇态是四光子的最大纠缠态，不会因为某个光子的单量子比特被检测到而变为直积压态，所以稳健性较强，但是簇态分析仪自身存在一定的局限性[25]。虽然W态不是四光子的最大纠缠态，但损失掉一个比特后不会干扰其他光子的纠缠性，且可以用弱相干态(WCS)光源来代替单光子源(single photon source，SPS)。

本文研究了基于四粒子W态的MDI-QKD协议[22]，在偏振编码和相位编码系统中，依据量子力学原理，对各个器件进行了量子化处理，同时为了探究单光子探测器的性能对误码率的影响，引入了单光子探测器的品质因子作为模拟参量[15,26]，分别模拟了不同单光子探测器品质因子、光纤信道之间距离和信道传输损耗下误码率和密钥生成率的变化趋势。

2 基本原理

2.1 基于W态的四方测量设备无关量子密钥分配

四方的MDI-QKD协议可以利用时间翻转w_4状态协议来实现，在该协议中，每个用户都可以准备一个纠缠的EPR光子对，每个光子对中保留一个光子，并将另一个光子发送到中心中继，然后通过中继对光子的状态进行投影测量。如果该状态被中继投射到w_4状态，则用户中剩余的四个光子的状态被投影到相同的w_4状态。通过使用虚拟量子比

特[27]的思想，可以构造一个四方的MDI-QKD方案。

四方的MDI-QKD协议的系统模型如图1所示。有四位参与者：Alice、Bob、Charlie和David。来自单光子源的光子用时间单元编码[27]，一般情况下，可用弱相干态光源结合诱骗态技术[28-30]来代替SPS。

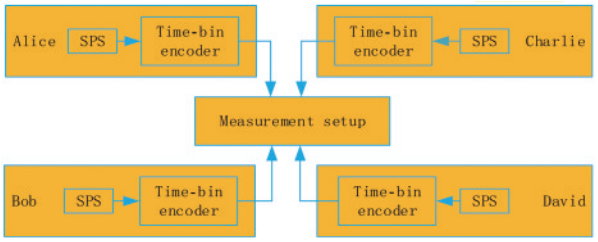

图1　基于w_4的四方MDI-QKD协议系统模型

Fig. 1　System model of four-party MDI-QKD protocol based on w_4

Alice、Bob、Charlie和David在不同的时间单元编码状态下准备单光子脉冲，每个单光子的选取都是独立且随机的。时间单元编码器可以按照参考文献[31]中的方案进行设计。测量装置会接收Alice、Bob、Charlie和David发送的信号，随后一起发送给W-state分析仪。具体步骤如下。

1）准备：每一个参与者（Alice、Bob、Charlie和David）从四个可能的时间单元编码状态中选取所需要的单个光子，然后将它们发送给不可信的继电器Emma。

2）测量：Emma使用分析仪[22]执行w_4状态的测量。

3）筛选：Emma宣布成功的测量事件，当所有参与者使用直线(z)基时，其中两个参与者宣布他们的比特，另外两个参与者根据表1所示的场景执行操作。

Emma宣布成功输出状态$\left|w_{4,0}\right\rangle$或$\left|w_{4,1}\right\rangle$（$\left|w_{4,c}\right\rangle$或$\left|w_{4,d}\right\rangle$）后，四名参与者进行后选择。任意两个参与者都会宣布他们所发送的经典比特，如果比特是“00”或“11”，则其余两个参与者可以获得原始密钥。比如当Alice和Bob宣布自己发送的经典比特为“00”或“11”时，Charlie和David中的一个会翻转自己的比特。这样，任何两个参与者都可以执行QKD。

4）后处理：在获得筛选出的密钥后，两个参与者进行信息协调和隐私放大[22]。

表1　Emma成功测量后，四位参与者的后选择状态[22]

Table 1　Post-selection states of four participants after successful measurement by Emma [22]

Announced bit				Participants who obtain key bits and their operation
Alice	Bob	Charlie	David	
0(1)	0(1)	-	-	Charlie & David, one of their bit flips
0(1)	-	0(1)	-	Bob & David, one of their bit flips
0(1)	-	-	0(1)	Bob & Charlie, one of their bit flips
-	0(1)	0(1)	-	Alice & David, one of their bit flips
-	0(1)	-	0(1)	Alice & Charlie, one of their bit flips

2.2　密钥生成率分析

任何两个参与者都可以在Emma宣布成功测量事件后生成一个密钥，另外两个参与者的经典位是“00”或“11”。因此，可以参考两方的MDI-QKD协议[12]以及Shor等[2]的工作来获得密钥率。根据表1，四方MDI-QKD协议与三方MDI-QKD协议的不同之处在于，四方中的增益是指Emma宣布成功输出的联合概率，参与者的经典比特中有两位是“00”（或“11”）。由于任意两个参与者都可以建立一个密钥，因此考虑了数据协调中的最大信息损失值和每对参与者的隐私放大过程，密钥生成率可以表示为

$$R_0=qQ_1\left\{1-\mathrm{Max}\left[H_2\left(e_{\mathrm{cd}}^x\right),H_2\left(e_{\mathrm{bd}}^x\right),H_2\left(e_{\mathrm{bc}}^x\right),H_2\left(e_{\mathrm{ad}}^x\right),H_2\left(e_{\mathrm{ac}}^x\right),H_2\left(e_{\mathrm{ab}}^x\right)\right]-\mathrm{Max}\left[H_2\left(e_{\mathrm{cd}}^z\right),H_2\left(e_{\mathrm{bd}}^z\right),H_2\left(e_{\mathrm{bc}}^z\right),H_2\left(e_{\mathrm{ad}}^z\right),H_2\left(e_{\mathrm{ac}}^z\right),H_2\left(e_{\mathrm{ab}}^z\right)\right]\right\},\tag{1}$$

式中：q为基协调因子；Q_1为z基下的增益；$H_2(x)$为二元信息熵，其表达式为$H_2(x)=-x\mathrm{lb}(x)-(1-x)\mathrm{lb}(1-x)$；$e_{jk}^x\left(e_{jk}^z\right)$表示合法用户$j$和$k$发送的脉冲选择$x(z)$基时的误码率，

$j,k\in\{\text{Alice(a)},\text{Bob(b)},\text{Charlie(c)},\text{David(d)}\}$。在本协议中，$z$基和$x$基下的误码率相同，即$e_{jk}^{x}=e_{jk}^{z}$。此外，用户使用$z$基的概率接近1，即$q\approx1$。假设数据是无限长，为了简化，令$e_1=e_{jk}^{z}$，则(1)式可以简化为

$$R_0=Q_1\left[1-2H_2(e_1)\right]。\tag{2}$$

由文献[30]可知：

$$Q_1=\frac{1}{128}(1-Y_0)^{12}\left[1024(1-\eta)^4Y_0^4+1440\eta(1-\eta)^3Y_0^3+496\eta^2(1-\eta)^2Y_0^2+49\eta^3(1-\eta)Y_0+8(D_{\rho0}+D_{\rho1})\eta^4\right],\tag{3}$$

以及误码率e_1为

$$e_1=\frac{1}{16Q_1}(1-Y_0)^{12}\left[64(1-\eta)^4Y_0^4+90\eta(1-\eta)^3Y_0^3+31\eta^2(1-\eta)^2Y_0^2+3\eta^3(1-\eta)Y_0\right],\tag{4}$$

式中：Y_0为暗记数；η为信道传输效率。

在引入品质因子P后，令$\eta_d=\frac{Y_0}{P}$，即$\eta=10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}$，则(3)式和(4)式可表示为

$$\begin{aligned}Q_1=\frac{1}{128}(1-Y_0)^{12}\Bigg[&1024\left(1-10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^4Y_0^4+1440\left(10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)\left(1-10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^3Y_0^3+\\&496\left(10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^2\left(1-10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^2Y_0^2+49\left(10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^3\left(1-10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)Y_0+\\&8(D_{\rho0}+D_{\rho1})\left(10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^4\Bigg],\end{aligned}\tag{5}$$

$$\begin{aligned}e_1=\frac{1}{16Q_1}(1-Y_0)^{12}\Bigg[&64\left(1-10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^4Y_0^4+90\eta\left(1-10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^3Y_0^3+\\&31\left(10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^2\left(1-10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^2Y_0^2+3\left(10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)^3\left(1-10^{\frac{-\alpha l}{10}}\cdot\frac{Y_0}{P}\right)Y_0\Bigg],\end{aligned}\tag{6}$$

式中：$\eta=10^{\frac{-\alpha l}{10}}\cdot\eta_d$；$\alpha$和$l$分别为信道传输损耗率和两方光纤信道之间的距离；$\eta_d$为单光子探测器的探测效率；$D_{\rho0}$和$D_{\rho1}$分别为$|w_{4,0}\rangle$和$|w_{4,1}\rangle$的检测概率。一般地，$D_{\rho0}=0.0469$，$D_{\rho1}=0.0156$，$Y_0=6.02\times10^{-6}$。

3　仿真结果与分析

本文根据(1)、(5)、(6)式，分别模拟了不同单光子探测器品质因子、光纤信道之间距离和信道传输损耗下误码率和密钥生成率的变化趋势。

图2所示是不同探测器品质因子下两方光纤信道之间的距离与误码率之间的关系。可以看出，随着两方光纤信道之间距离的增加，误码率整体呈现出递增的趋势，即距离越大，误码率越大。这是因为随着两方光纤信道之间距离的增加，信道传输效率减小，从而误码率增大。当两方通信距离相等时，随着品质因子的增大，误码率逐渐增大。

图3所示是不同Y_0下探测器品质因子与误码率之间的关系。通过进一步的研究，可以得出与

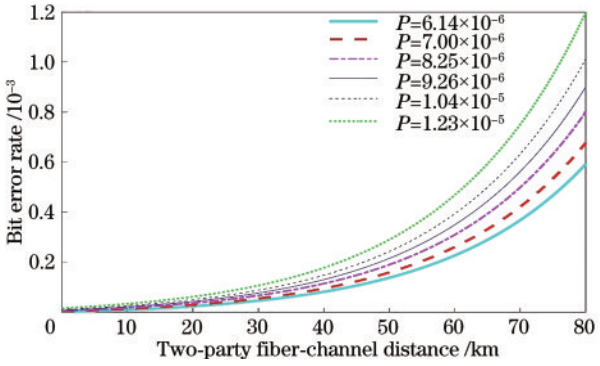

图2　不同品质因子下两方光纤信道之间的距离与误码率之间的关系

Fig. 2　Relationship between two-party fiber-channel distance and bit error rate under different quality factors

图2一致的结论，随着探测器品质因子的增大，误码率逐渐增大，即单光子探测器的性能越差，误码率越高。这是因为实验中单光子探测器探测效率的取值固定，随着暗记数的逐渐增大，品质因子增大，从而误码率增大。

图4所示是不同传输距离(L)下信道传输损耗

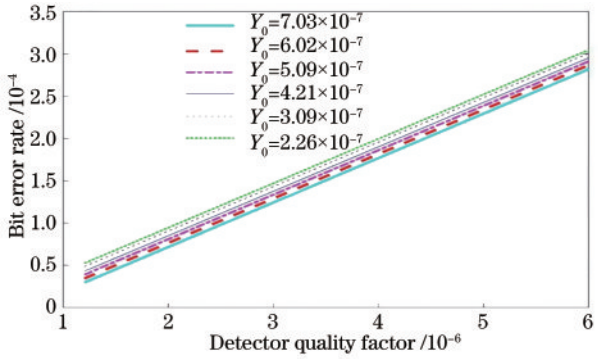

图 3　不同 Y_0 下探测器品质因子与误码率之间的关系

Fig. 3　Relationship between detector quality factor and bit error rate under different Y_0

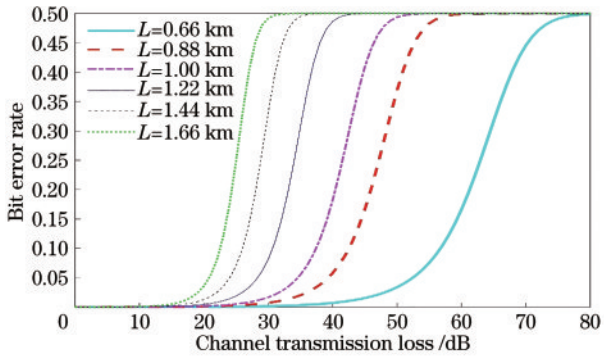

图 4　不同 L 下信道传输损耗与误码率之间的关系

Fig. 4　Relationship between channel transmission loss and bit error rate under different L

和误码率之间的关系。可以看出，随着信道传输损耗的增加，误码率均呈现出递增的趋势，且均逼近 50%，其中在 $L=1.66$ km 的条件下，当信道传输损耗为 32 dB 时，误码率为 50%；在 $L=1.22$ km 的条件下，当信道传输损耗为 42 dB 时，误码率为 50%；在 $L=0.66$ km 的条件下，当信道传输损耗为 78 dB 时，误码率为 50%。

图 5 所示是不同探测器品质因子下两方光纤信道之间的距离与密钥生成率之间的关系。可以看出，随着两方光纤信道之间距离的增加，密钥生成率整体呈现出递减的趋势，即距离越大，密钥生成率越小。这是因为随着距离的增大，信道传输效率减小，误码率逐渐增大，从而密钥生成率减小。当两方通信距离相等时，随着品质因子的增大，密钥生成率逐渐减小，即单光子探测器的性能越差，密钥生成率越低。这是因为在距离相等的条件下，品质因子的增大会使得误码率增大，从而导致密钥生成率减小。

图 6 所示是不同 Y_0 下探测器品质因子与密钥生成率之间的关系。通过进一步的研究，可以得出

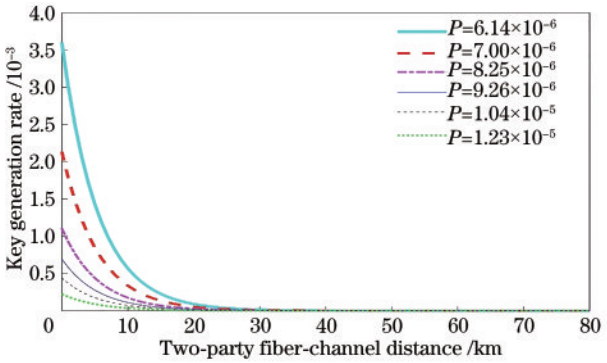

图 5　不同品质因子下两方光纤信道之间的距离与密钥生成率之间的关系

Fig. 5　Relationship between two-party fiber-channel distance and key generation rate under different quality factors

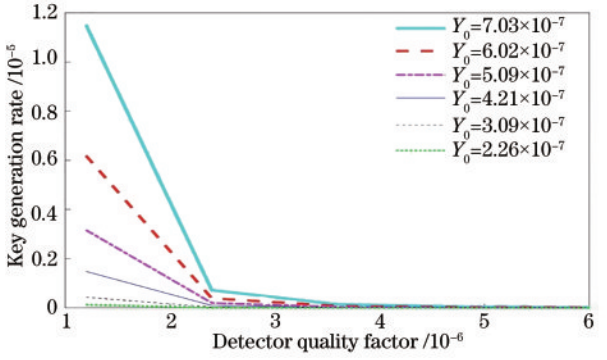

图 6　不同 Y_0 下探测器品质因子与密钥生成率之间的关系

Fig. 6　Relationship between detector quality factor and key generation rate under different Y_0

与图 5 一致的结论，随着探测器品质因子的增大，密钥生成率逐渐减小，这是因为随着品质因子的增大，误码率增大，从而密钥生成率减小。

图 7 所示是不同 L 下信道传输损耗和密钥生成率之间的关系。可以看出，随着信道传输损耗的增

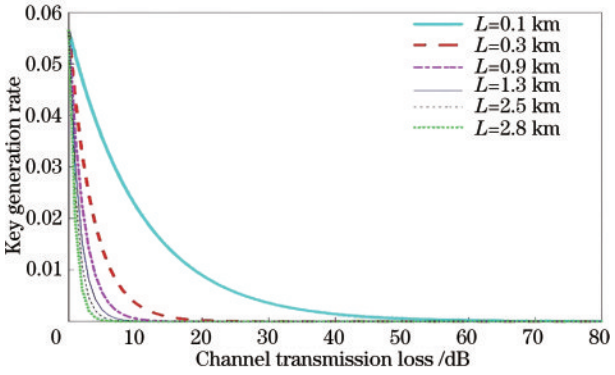

图 7　不同 L 下信道传输损耗与密钥生成率之间的关系

Fig. 7　Relationship between channel transmission loss and key generation rate under different L

加，密钥生成率逐渐减小，这是因为随着α的增大，单边传输效率降低，Emma成功测量的概率减小，进而密钥生成率降低。当信道传输损耗相同时，距离越大，得到的密钥生成率越低。

4 结　论

研究并仿真了基于W态的多方测量设备无关量子密钥分配协议的误码率和密钥生成率的影响因素。研究发现，误码率和密钥生成率的变化与两方光纤信道距离、探测器品质因子和信道传输损耗有关。随着两方光纤信道之间距离的增加，误码率逐渐增大，密钥生成率逐渐减小。随着探测器品质因子的增大，误码率逐渐增大，密钥生成率逐渐减小。随着信道传输损耗的增加，误码率逐渐增大，密钥生成率逐渐减小。研究结论对于获取性能较好的MDI-QKD系统具有一定的参考价值。

参 考 文 献

[1] Bennett C H, Brassard G. An update on quantum cryptography[M]//Blakley G B, Chaum D. Advances in cryptology. Heidelberg: Springer, 1984, 196: 475-480.

[2] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441-444.

[3] Mayers D. Unconditional security in quantum cryptography[J]. Journal of the ACM, 2001, 48(3): 351-406.

[4] Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices[C]//International Symposium On Information Theory, June 27-July 2, 2004, Chicago, IL, USA. New York: IEEE Press, 2004: 136.

[5] Bennett C H, Brassard G, Ekert A K, et al. Quantum cryptography[J]. Scientific American, 1992, 267(4): 50-57.

[6] Wang Q, Wang X B. 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.

[7] Zhu Q L, Shi L, Wei J H, et al. Background light suppression in free space quantum key distribution[J]. Laser & Optoelectronics Progress, 2018, 55(6): 060004.
朱秋立, 石磊, 魏家华, 等. 自由空间量子密钥分配的背景光抑制[J]. 激光与光电子学进展, 2018, 55(6): 060004.

[8] Makarov V. Controlling passively quenched single photon detectors by bright light[J]. New Journal of Physics, 2009, 11(6): 065003.

[9] 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, 2008, 78(4): 042333.

[10] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols[J]. Quantum Information & Computation, 2008, 8(6&7): 622-635.

[11] Lydersen L, Skaar J, Makarov V. Tailored bright illumination attack on distributed-phase-reference protocols[J]. Journal of Modern Optics, 2011, 58(8): 680-685.

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

[13] He Y F, Wang D, Yang H J, et al. Quantum key distribution based on heralded single photon sources and quantum memory[J]. Chinese Journal of Lasers, 2019, 46(4): 0412001.
何业锋, 王登, 杨红娟, 等. 基于指示单光子源和量子存储的量子密钥分配[J]. 中国激光, 2019, 46(4): 0412001.

[14] Li M, Zhang C M, Yin Z Q, et al. Measurement-device-independent quantum key distribution with modified coherent state[J]. Optics Letters, 2014, 39(4): 880-883.

[15] He Y F, Li C Y, Guo J R, et al. Passive measurement-device-independent quantum key distribution based on heralded pair coherent states[J]. Chinese Journal of Lasers, 2020, 47(9): 0912002.
何业锋, 李春雨, 郭佳瑞, 等. 基于标记配对相干态的被动测量设备无关量子密钥分配[J]. 中国激光, 2020, 47(9): 0912002.

[16] He Y F, Li D Q, Song C, et al. Quantum key distribution protocol based on odd coherent sources and orbital angular momentum[J]. Chinese Journal of Lasers, 2018, 45(7): 0712001.
何业锋, 李东琪, 宋畅, 等. 基于奇相干光源和轨道角动量的量子密钥分配协议[J]. 中国激光, 2018, 45(7): 0712001.

[17] He Y F, Guo J R, Li C Y, et al. Fluctuation analysis of key distribution protocol based on heralded single-photon source and orbital angular momentum[J]. Chinese Journal of Lasers, 2020, 47(4): 0412001.
何业锋, 郭佳瑞, 李春雨, 等. 基于指示单光子源和轨道角动量的密钥分配协议的波动分析[J]. 中国激

光, 2020, 47(4): 0412001.

[18] Hwang T, Lee K C, Li C M, et al. Provably secure three-party authenticated quantum key distribution protocols[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(1): 71-80.

[19] Cabello A. Multiparty key distribution and secret sharing based on entanglement swapping [EB/OL]. (2000-09-07) [2020-10-25]. https://arxiv. org/abs/quant-ph/0009025.

[20] Matsumoto R. Multiparty quantum-key-distribution protocol without use of entanglement[J]. Physical Review A, 2007, 76(6): 062316.

[21] Liu C Q, Zhu C H, Ma S Q, et al. Multi-party measurement-device-independent quantum key distribution based on cluster states[J]. International Journal of Theoretical Physics, 2018, 57(3): 726-739.

[22] Zhu C H, Xu F H, Pei C X, et al. W-state analyzer and multi-party measurement-device-independent quantum key distribution[J]. Scientific Reports, 2015, 5: 17449.

[23] Fu Y, Yin H L, Chen T Y, et al. Long-distance measurement-device-independent multiparty quantum communication[J]. Physical Review Letters, 2015, 114(9): 090501.

[24] Gorbachev V N, Trubilko A I. On multiparticle W states, their implementations and application in the quantum informational problems[J]. Laser Physics Letters, 2006, 3(2): 59-70.

[25] Liu C Q. Research on practical measurement-device independent quantum key distribution system[D]. Xi'an: Xidian University, 2017.
刘传起. 实用化测量设备无关量子密钥分发系统研究[D]. 西安: 西安电子科技大学, 2017.

[26] Wu C F, Du Y N, Wang J D, et al. Analysis on performance optimization in measurement-device-independent quantum key distribution using weak coherent states[J]. Acta Physica Sinica, 2016, 65(10): 100302.
吴承峰, 杜亚男, 王金东, 等. 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[J]. 物理学报, 2016, 65(10): 100302.

[27] Xu F H, Curty M, Qi B, et al. Measurement-device-independent quantum cryptography[J]. IEEE Journal of Selected Topics in Quantum Electronics, 2015, 21(3): 148-158.

[28] Hwang W Y. Quantum key distribution with high loss: toward global secure communication[J]. Physical Review Letters, 2003, 91(5): 057901.

[29] Lo H K, Ma X F, Chen K, et al. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 230504.

[30] Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography[J]. Physical Review Letters, 2005, 94(23): 230503.

[31] Rubenok A, Slater J A, Chan P, et al. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks[J]. Physical Review Letters, 2013, 111(13): 130501.