量子通信技术及应用

DOI: 10.16818/j.issn1001－5868.20260104001

半设备无关量子密钥分发协议参数化研究

林培存,黄安琪*
(国防科技大学 计算机学院,长沙 410073)

摘 要: 半设备无关量子密钥分发协议一定程度解决了因设备不完美性所带来的安全漏洞问题,且实验实现所需的条件相对宽松。然而,目前对其理论和实验的研究仍相对较少。文章采用对现有半设备无关量子密钥分发协议进行参数化的方法,理论推导协议的安全参数范围。基于所求解的安全参数范围,系统探究了实验器件精度对协议安全性的影响。结果表明,在安全参数范围内,实验器件的精度对协议的安全性判断指标并不敏感,体现了对设备非完美性的容忍程度。该研究对半设备无关量子密钥分发协议的实验实现具有指导意义。

关键词: 半设备无关;量子密钥分发;参数化;非完美性容忍

中图分类号: TN918 **文章编号:** 1001－5868(2026)02－0242－06

Parameterization of Semi-Device-Independent Quantum Key Distribution Protocol

LIN Peicun, HUANG Anqi
(College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, CHN)

Abstract: The semi-device-independent quantum key distribution protocol addresses the security vulnerabilities arising from device imperfections to some extent, with relatively relaxed conditions required for experimental implementation. However, studies on both its theoretical and experimental aspects remain scarce. In this study, a parameterization approach is adopted to theoretically derive the range of security parameters for a semi-device-independent quantum key distribution protocol. Based on the derived range of security parameters, the impact of experimental device precision on protocol security is systematically investigated. Theoretical derivation results indicate that within the range of security parameters, the precision of experimental devices is not sensitive to the security evaluation indicators of the protocol, reflecting a tolerance for device imperfections. This study provides guidance for the experimental implementation of semi-device-independent quantum key distribution protocols to aid experimentalists in determining the value ranges and principles for parameter selection.

Key words: semi-device-independent; quantum key distribution; parameterization; imperfection tolerance

0 引言

量子密钥分发(Quantum Key Distribution, QKD)基于量子力学的基本原理,可实现信息论可证安全的密钥分发[1-4]。与依赖于数学假设的经典密钥分发不同,QKD的安全性依赖量子物理定律,如量子态不可克隆、不确定性原理。然而,大多数QKD除要求量子力学正确性外,还需要密钥分发双方对态制备和测量具有理想的控制能力等,这类与设备相关的假设在实际系统中往往难以完全满足。

收稿日期:2026－01－04.

*通信作者:黄安琪

由于实际使用的设备不可避免存在不完美性，理论和实际不一致可能造成系统安全漏洞，从而使窃听者有机会在不被察觉的情况下窃取密钥[5-24]。

设备无关（Device Independent）量子密钥分发的提出，有效解决了上述问题。该方法无需关注设备内部的物理过程，仅依据设备间经典输入输出（如测量基的选择和测量结果）的关联，并借助贝尔不等式类检验来保证密钥分发过程的安全性[25-32]。但检验这些不等式需要克服贝尔实验中的各种漏洞，导致实现长距离的设备无关量子密钥分发相当困难。若可以在更一般化且相对简单的“制备-测量（Prepare-and-Measure，PAM）”场景[33-34]（非贝尔场景）下设计量子密钥分发协议，则有望降低实验难度。

在“制备-测量”场景中，通常需要假设编码密钥信息的量子系统维度，才能设计出安全的协议。具备该额外维度假设的协议被称为半设备无关（Semi-Device-Independent，SDI）量子密钥分发协议。文献[35]首次给出半设备无关 QKD 在个体攻击下的安全性充分条件，但未设计具体可实现的协议；文献[36]给出了半设备无关 QKD 最小熵的下界，但没有给出完整的安全性证明；文献[37]提出一个具体协议，但普适性有限。总体而言，半设备无关 QKD 的理论和实验研究尚处于起步阶段，亟待深入探索。

为系统研究半设备无关 QKD 的安全特性，本文对文献[37]所提出的协议进行一般化，得到更普适性的安全协议形式。该工作为实验实现提供了理论依据，有助于确定协议参数的安全取值范围。与完全设备无关协议类似，半设备无关协议的安全性也易受到探测器漏洞的影响，并进一步讨论了关闭该漏洞的可能性。本研究为推动半设备无关量子密钥分发协议实验实现奠定了理论基础。

1　制备-测量场景与随机访问码

本节将介绍两个在半设备无关量子密钥分发协议安全性证明中的重要理论工具。一个是制备-测量场景下用于界定系统维度的维度见证者（Dimension Witness）[33-34]，另一个是随机访问码（Random Access Code，RAC）[38]。二者之间存在一定的等价关系，已有文献证明可以通过计算制备-测量场景下的维度见证者，或者随机访问码中的平均猜测成功概率来确定量子密钥分发协议在半设备无关场景下的安全性[35,37]。

如图 1 所示，制备-测量场景由制备设备和测量设备组成。本文不对制备设备和测量设备的内部细节和量子物理过程进行描述，即统一描述为黑盒，只关注设备的经典输入输出，并通过这些输入输出来界定物理系统的维度[33-34]。但在一些量子密钥分发协议或实验里，通常会有一些与设备相关（较弱但关键）的假设，如制备设备发送给测量设备的系统维度，具有该额外假设的场景被称为半设备无关场景。

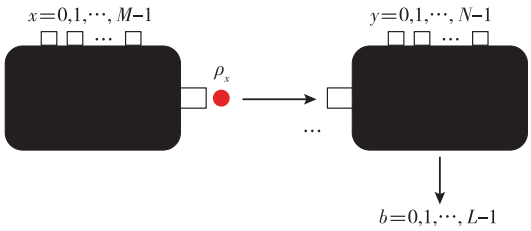


图 1　制备-测量场景的黑盒表示

假设制备设备和测量设备的经典输入输出分别由 M 和 N 个按钮描述。制备方接收一个经典信息 $x\in\{0,1,\cdots,M-1\}$ 后按下制备设备相应的按钮，制备设备发送一个相应的 d 维物理系统 ρ_x 给测量方。在接收到物理系统 ρ_x 后，测量方同样接收一个经典信息 $y\in\{0,1,\cdots,N-1\}$ 并按下相应按钮，基于这两个输入，测量设备输出结果 $b\in\{0,1,\cdots,L-1\}$。该场景下的实验结果由条件概率 $P(b|x,y)$ 完全描述。考虑到制备设备和测量设备之间存在着经典关联（与输入输出之间无关联），在该情况下的维度见证者是线性的，即：

$$S=\sum_{b,x,y}\omega_{b,x,y}P(b|x,y)\leqslant C_d \tag{1}$$

式中，$\omega_{b,x,y}$ 是相应条件概率的系数，C_d 是制备设备所发送的物理系统维度为 d 时 S 所能达到的最大值。

下面介绍另一个理论工具——随机访问码。在随机访问码中同样有两方，分别称之为 Alice 和 Bob。Alice 接收一个经典信息 $x=x_0x_1\cdots x_{k-1}$，其中 $x_i(i\in\{0,1,\cdots,k-1\})$ 为单个经典比特，并将其编码到 t 个经典（量子）比特后发送给 Bob。Bob 接收到 Alice 发给其的信息后同样接收一个经典信息 $y\in\{0,1,\cdots,k-1\}$，其任务为输出一个结果 b 作为其猜测 Alice 第 y 个比特的结果，其成功概率记为

$P(b=x_y|x=x_0x_1\cdots x_{k-1},y)$。将这种通信复杂度问题称为$k\to t$(量子)随机访问码[35,37],并且只考虑$k>t$这种非平凡情况。记其平均成功概率为$P_B$,有:

$$P_B=\frac{\sum_{x_0x_1\cdots x_{k-1},y}P(b=x_y|x=x_0x_1\cdots x_{k-1},y)}{k\times 2^k} \quad (2)$$

当制备-测量场景和随机访问码的x,y和b取值范围相同,以及维度见证者S和平均成功概率P_B中条件概率的系数符合一定的关系时,可以将S和P_B联系起来。具体来说,若公式(1)中S的项的系数满足$\omega_{0,x,y}=(-1)^{x_y}$且$\omega_{1,x,y}=0$,则公式(1)可以改写为:

$$S=\sum_{x_0x_1\cdots x_{k-1},y}P(b=x_y|x=x_0x_1\cdots x_{k-1},y)-k\times 2^{k-1} \quad (3)$$

联立公式(2)和公式(3),得到:

$$P_B=\frac{S+k\times 2^{k-1}}{k\times 2^k} \quad (4)$$

2 半设备无关量子密钥分发协议

半设备无关量子密钥分发协议通常将密钥分发双方的设备以黑盒的方式描述为制备-测量场景,并且假设制备设备发送给测量设备的物理系统为某个固定的维度,即半设备无关。对文献[37]所提出的协议进行一般化,得到更普适的安全半设备无关量子密钥分发协议。该一般化协议的具体步骤如下所描述。

如图2所示,Alice具有两个制备设备P^0和P^1,并且每个设备可以描述为黑盒,并假设这两个设备所发送的量子态是二维的。这两个制备设备分别具有4个按钮,并分别由两位比特描述,即$x^0=x_0^0x_1^0$和$x^1=x_0^1x_1^1$,这些按钮所代表的态分别为:

$$\rho_{00}^0=|0\rangle\langle 0|,\rho_{11}^0=|1\rangle\langle 1|,$$
$$\rho_{10}^0=|+\rangle\langle +|,\rho_{01}^0=|-\rangle\langle -|,$$
$$\rho_{00}^1=|\varphi\rangle\langle\varphi|,\rho_{11}^1=|\varphi^\perp\rangle\langle\varphi^\perp|,$$
$$\rho_{10}^1=|\psi\rangle\langle\psi|,\rho_{01}^1=|\psi^\perp\rangle\langle\psi^\perp|,$$

其中,$\rho_{x_0^ix_1^i}^i(i\in\{0,1\})$代表设备$P^i$按下按钮$x_0^ix_1^i$所发送的态,且$|\varphi\rangle=\cos\alpha|0\rangle+\sin\alpha|1\rangle$,$|\varphi^\perp\rangle=-\sin\alpha|0\rangle+\cos\alpha|1\rangle$,$|\psi\rangle=\cos\beta|0\rangle+\sin\beta|1\rangle$,$|\psi^\perp\rangle=-\sin\beta|0\rangle+\cos\beta|1\rangle$。Alice在设备$P^0$和$P^1$中各随机选一个按钮并同时按下。

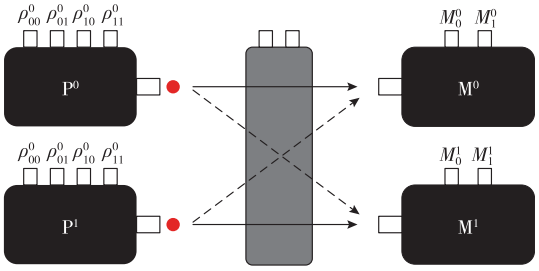


图2 半设备无关QKD协议装置

设备P^0和P^1发送相应的量子态,这两个量子态首先会经过一个黑盒,其作用是充当一个开关。该黑盒具有两个按钮,不同的按钮对应不同的组合方式,将Alice的两个制备设备和Bob的两个测量设备配对。如图2中黑色实线所示,第一种配对方式为$P^0\to M^0$和$P^1\to M^1$;如图2中黑色虚线所示,第二种配对方式为$P^0\to M^1$和$P^1\to M^0$。其中,$P^i\to M^j$表示将Alice的第i个制备设备P^i所制备的量子态发送给Bob的第j个测量设备M^j。需要注意的是,Alice和Bob量子通信阶段结束后,才能知道开关所选择的配对组合。

经过黑盒开关后,两个量子态分别以其中一种配对方式发送Bob。Bob拥有两个测量设备M^0和M^1,并且同样也可以描述为黑盒。每个设备拥有两个按钮,每个按钮对应一种测量,具体来说:

$$M_0^0=\left\{|0\rangle\langle 0|,|1\rangle\langle 1|\right\},$$
$$M_1^0=\left\{|+\rangle\langle +|,|-\rangle-|\right\},$$
$$M_0^1=\left\{|\varphi\rangle\langle\varphi|,|\varphi^\perp\rangle\langle\varphi^\perp|\right\},$$
$$M_1^1=\left\{|\psi\rangle\langle\psi|,|\psi^\perp\rangle\langle\psi^\perp|\right\},$$

其中,M_j^i表示第i个测量设备的第j个按钮所执行的测量。

量子通信阶段结束后,Alice和Bob在经典信道上公布他们的测量基,并且双方获知每轮黑盒开关所选择的配对方式。当黑盒开关选择第一种配对方式且P^0和M^0或P^1和M^1的制备和测量都选择同一种基时,那么Alice和Bob可以根据这种事件生成原始密钥。当黑盒开关选择第二种配对方式时,可根据P^1和M^0的经典输入输出来判断密钥分发过程是否安全。具体来说,在个体攻击下,公式(5)为Alice和Bob能获得密钥的充分条件[35]:

$$I(A:B)>I(A:E) \quad (5)$$

式中，A，B 和 E 分别表示 Alice，Bob 和窃听者 Eve。且公式(6)表示 Alice 和 X 方之间的相互信息：

$$I(A:X)=\sum_j 1-h\left[P_X\left(a_{y_j}\right)\right] \tag{6}$$

式中，h 是二进制熵，$P_X\left(a_{y_j}\right)$ 是 X 方在第 j 轮对 Alice 第 $y_j\in\{0,1\}$ 个比特的猜测成功概率。将 P^1 和 M^0 之间的制备测量过程描述为随机访问码，公式(5)成立的一个充分条件为：

$$P_B>P_E \tag{7}$$

而根据文献[35]，有：

$$P_B+P_E\leqslant\frac{5+\sqrt{3}}{4} \tag{8}$$

因此，判断 Bob 的平均猜测成功概率是否满足：

$$P_B>\frac{5+\sqrt{3}}{8} \tag{9}$$

若满足，则公式(7)成立，换句话说，Alice 和 Bob 的密钥分发过程是安全的[35]。需要注意的是，在第二种配对方式下，P^1 和 M^0 之间的经典信息只能用来判断协议是否安全，而不能用来生成密钥。

文献[37]给出了当 $\alpha=\pi/8$ 和 $\beta=3\pi/8$ 时协议是安全的。对其进行一般化扩展，对于不具备实现该特定参数的态制备和测量，若实验条件可以实现参数 α 和 β 在推导范围内的量子态制备和测量，那么该参数范围内均可以实现安全的半设备无关量子密钥分发协议。

3　结果与讨论

3.1　参数 α 与 β 的取值范围

Alice 的制备设备 P^1 和 Bob 的测量设备 M^0 组成的制备-测量场景的维度见证者为[35]：

$$\begin{aligned}S=&+E_{00,0}+E_{00,1}+E_{01,0}-E_{01,1}-\\&E_{10,0}+E_{10,1}-E_{11,0}-E_{11,1}\leqslant 2\end{aligned} \tag{10}$$

式中，$E_{x_0x_1,y}=P(0|x_0x_1,y)$ 表示 Alice 选择按钮 x_0x_1 以及 Bob 选择按钮 y 时获得结果为 0 的概率。公式(10)中项 $E_{x_0x_1,y}$ 的系数满足公式(4)成立的条件。所以要求使协议安全的参数 α 和 β 的范围，只需要使公式(11)成立，即：

$$P_B=\frac{S+4}{8}>\frac{5+\sqrt{3}}{8} \tag{11}$$

将 $E_{00,0}=\cos^2\alpha$，$E_{00,1}=(1+\sin 2\alpha)/2$，$E_{01,0}=\sin^2\beta$，$E_{01,1}=(1-\sin 2\beta)/2$，$E_{10,0}=\cos^2\beta$，$E_{10,1}=(1+\sin 2\beta)/2$，$E_{11,0}=\sin^2\alpha$，$E_{11,1}=(1-\sin 2\alpha)/2$ 代入公式(11)可得：

$$\sin\left(2\alpha+\frac{\pi}{4}\right)+\sin\left(2\beta-\frac{\pi}{4}\right)>\frac{\sqrt{3}+1}{\sqrt{2}} \tag{12}$$

求解不等式(12)可得使协议安全的参数 α 和 β 的范围为：

$$\begin{aligned}&\frac{1}{2}\arcsin\left[C\left(\frac{\pi}{8}\right)\right]+\left(k_1-\frac{1}{8}\right)\pi<\alpha<\\&-\frac{1}{2}\arcsin\left[C\left(\frac{\pi}{8}\right)\right]+\left(k_1+\frac{3}{8}\right)\pi,k_1\in Z\end{aligned} \tag{13}$$

$$\begin{aligned}&\frac{1}{2}\arcsin\left[C(\alpha)\right]+\left(k_2+\frac{1}{8}\right)\pi<\beta<\\&-\frac{1}{2}\arcsin\left[C(\alpha)\right]+\left(k_2+\frac{5}{8}\right)\pi,k_2\in Z\end{aligned} \tag{14}$$

式中，函数 C 定义为 $C(x)=(1+\sqrt{3})/\sqrt{2}-\sin(2x+\pi/4)$。

因此，若实验条件可以实现参数在公式(13)和公式(14)范围内的态制备和测量，则可以实现安全半设备无关量子密钥分发协议，并且通过检验公式(11)来判断是否有窃听者的存在。此外，如图 3 所示，取公式(13)和公式(14)在一个周期内的解($k_1=0$ 和 $k_2=0$)，可视化了 Bob 猜测成功的平均概率 P_B。不难发现，在安全范围内 P_B 的最大值和最小值相差约为 0.01，所以即使实验器件的精度不高，但只要满足公式(13)和公式(14)，P_B 的实际值和理论最大值接近。

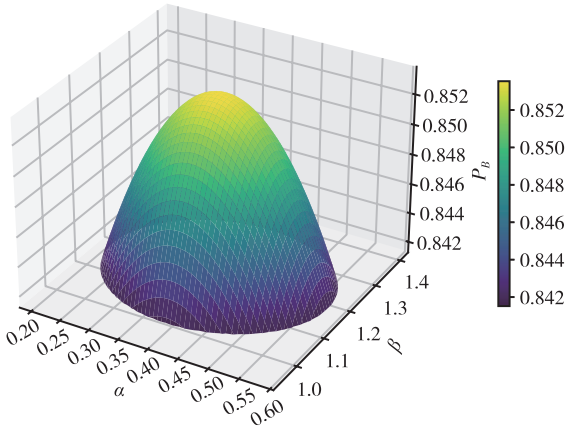


图 3　当 $k_1=0$ 且 $k_2=0$ 时，P_B 关于 α 和 β 的函数图像

3.2　探测器漏洞关闭的讨论

虽然半设备无关和完全设备无关量子密钥分发协议可以以尽量少的假设，保证密钥分发的安全性，但是在实际实现中需要关闭各种可能被窃听者

利用的漏洞,其中最难关闭的是探测器漏洞。不同于贝尔不等式的验证,设备无关的量子密钥分发协议需要更高的探测器效率。

在本文扩展的协议里涉及的设备有Alice的两个制备设备P^0和P^1和Bob的两个测量设备M^0和M^1以及黑盒开关,实际上这些设备组成了一个并行随机访问码(Parallel RAC)[39]。已有文献[39]证明并行随机访问码对任何效率非零的探测器都可以展现出非经典特性。但在本文扩展的协议[37]里只使用了Alice的制备设备P^1和Bob的测量设备M^0组成的非并行随机访问码,所以可能存在探测器漏洞。未来可能的研究方向是将公式(9)中的P_B替换成并行随机访问码下Bob对Alice选择的两个比特串x^0和x^1中某个比特的平均猜测成功概率(公式(11)中的S可能可以替换成16个制备、4个测量以及4种输出的制备-测量场景的维度见证者),并重新推导安全阈值。

4 结论

针对半设备无关量子密钥分发协议的安全特性,本文对已有半设备无关量子密钥分发协议进行一般化扩展,得出在个体攻击下更普适的安全半设备无关量子密钥分发协议。并对其量子密钥分发流程以及安全性检验进行了具体描述,确定了协议关键参数的取值范围,通过仿真验证了该类协议满足安全阈值条件。该推导结果对实验实现具有指导意义,便于实验者确定参数的取值范围和原则,体现出该类半设备无关量子密钥分发协议对设备非完美性的容忍程度。此外,讨论了探测器漏洞对协议影响以及关闭该漏洞的可能性。值得注意的是,该类协议的安全性检验要求Bob的平均猜测成功概率大于特定阈值,而该阈值仅偏小于其平均猜测成功概率的理论最大值,降低协议的安全阈值也是未来减小实验实现难度的可能方式。

参考文献:

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [J]. Theoretical Computer Science, 2014, 560: 7-11

[2] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography [J]. Reviews of Modern Physics, 2002, 74(1): 145-195.

[3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution [J]. Reviews of Modern Physics, 2009, 81(3): 1301-1350.

[4] Xu F, Ma X, Zhang Q, et al. Secure quantum key distribution with realistic devices [J]. Reviews of Modern Physics, 2020, 92(2): 025002.

[5] Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination [J]. Nature Photonics, 2010, 4(10): 686-689.

[6] Xu F, Qi B, Lo H K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system [J]. New Journal of Physics, 2010, 12(11): 113026.

[7] Wiechers C, Lydersen L, Wittmann C, et al. After-gate attack on a quantum cryptosystem [J]. New Journal of Physics, 2011, 13(1): 013043.

[8] Gerhardt I, Liu Q, Lamas-Linares A, et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system [J]. Nature Communications, 2011, 2: 349.

[9] Jain N, Wittmann C, Lydersen L, et al. Device calibration impacts security of quantum key distribution [J]. Physical Review Letters, 2011, 107(11): 110501.

[10] Bugge A N, Sauge S, Ghazali A M M, et al. Laser damage helps the eavesdropper in quantum cryptography [J]. Physical Review Letters, 2014, 112(7): 070503.

[11] Huang A, Sajeed S, Chaiwongkhot P, et al. Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption [J]. IEEE Journal of Quantum Electronics, 2016, 52(11): 8000211.

[12] Huang A, Sun S H, Liu Z, et al. Quantum key distribution with distinguishable decoy states [J]. Physical Review A, 2018, 98: 012330.

[13] Qian Y J, He D Y, Wang S, et al. Hacking the quantum key distribution system by exploiting the avalanche-transition region of single-photon detectors [J]. Physical Review Applied, 2018, 10(6): 064062.

[14] Huang A, Navarrete Á, Sun S H, et al. Laser-seeding attack in quantum key distribution [J]. Physical Review Applied, 2019, 12(6): 064043.

[15] Huang A, Li R, Egorov V, et al. Laser-damage attack against optical attenuators in quantum key distribution [J]. Physical Review Applied, 2020, 13(3): 034017.

[16] Sun S, Huang A. A review of security evaluation of practical quantum key distribution system [J]. Entropy, 2022, 24(2): 260.

[17] Chaiwongkhot P, Zhong J, Huang A, et al. Faking photon number on a transition-edge sensor [J]. EPJ Quantum Technology, 2022, 9(1): 23.

[18] Gao B, Wu Z, Shi W, et al. Ability of strong-pulse illumination to hack self-differencing avalanche photodiode detectors in a high-speed quantum-key-distribution system [J]. Physical Review A, 2022, 106(3): 033713.

[19] Ponosova A, Ruzhitskaya D, Chaiwongkhot P, et al. Protecting fiber-optic quantum key distribution sources against

light-injection attacks [J]. PRX Quantum, 2022, 3(4): 040307.

[20] Huang A, Mizutani A, Lo H K, et al. Characterization of state-preparation uncertainty in quantum key distribution [J]. Physical Review Applied, 2023, 19: 014048.

[21] Peng Q, Gao B, Zaitsev K, et al. Security boundaries of an optical-power limiter for protecting quantum-key-distribution systems[J]. Physical Review Applied, 2024, 21: 014026.

[22] Xing T, Liu J, Zhang L, et al. Characterization of intensity correlation *via* single-photon detection in quantum key distribution [J]. Optics Express, 2024, 32(18): 31767-31782.

[23] Liu J, Xing T, Liu R, et al. Intensity correlations in measurement-device-independent quantum key distribution [J]. Optics Express, 2024, 32(22): 38394.

[24] Peng Q, Chen J P, Xing T, et al. Practical security of twin-field quantum key distribution with optical phase-locked loop under wavelength-switching attack [J]. npj Quantum Information, 2025, 11: 7.

[25] Mayers D, Yao A. Quantum cryptography with imperfect apparatus [C]//Proceedings 39th Annual Symposium on Foundations of Computer Science, 2002: 503-509.

[26] Barrett J, Hardy L, Kent A. No signaling and quantum key distribution[J]. Physical Review Letters, 2005, 95: 010503.

[27] Acín A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks [J]. Physical Review Letters, 2007, 98(23): 230501.

[28] Masanes L, Pironio S, Acín A. Secure device-independent quantum key distribution with causally independent measurement devices [J]. Nature Communications, 2011, 2: 238.

[29] Vazirani U, Vidick T. Fully device-independent quantum key distribution [J]. Physical Review Letters, 2014, 113(14): 140501.

[30] Xu F, Zhang Y Z, Zhang Q, et al. Device-independent quantum key distribution with random postselection [J]. Physical Review Letters, 2022, 128(11): 110506.

[31] Nadlinger D P, Drmota P, Nichol B C, et al. Experimental quantum key distribution certified by Bell's theorem [J]. Nature, 2022, 607(7920): 682-686.

[32] Zhang W, van Leent T, Redeker K, et al. A device-independent quantum key distribution system for distant users [J]. Nature, 2022, 607(7920): 687-691.

[33] Gallego R, Brunner N, Hadley C, et al. Device-independent tests of classical and quantum dimensions [J]. Physical Review Letters, 2010, 105(23): 230501.

[34] Bowles J, Quintino M T, Brunner N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices [J]. Physical Review Letters, 2014, 112(14): 140407.

[35] Pawłowski M, Brunner N. Semi-device-independent security of one-way quantum key distribution[J]. Physical Review A, 2011, 84: 010302.

[36] Woodhead E, Pironio S. Secrecy in prepare-and-measure clauser-horne-shimony-holt tests with a qubit bound [J]. Physical Review Letters, 2015, 115(15): 150501.

[37] Avesani M. Security of Quantum Protocols certified by the dimension of the Hilbert space[D]. Padova: Università degli Studi di Padova, 2015.

[38] Nayak A. Optimal lower bounds for quantum automata and random access codes [C]//40th Annual Symposium on Foundations of Computer Science, 2002: 369-376.

[39] Hameedi A, Marques B, Mironowicz P, et al. Experimental test of nonclassicality with arbitrarily low detection efficiency [J]. Physical Review A, 2020, 102(3): 032621.

作者简介：

林培存(2001—)，男，广东省潮州市人，硕士研究生，主要研究方向为量子信息安全；

黄安琪(1990—)，女，湖南省资兴市人，博士，副研究员，主要研究方向为量子信息安全。