第 42 卷 第 3 期/2022 年 2 月/光学学报 研究论文

光学学报

50 km 无特征源的测量设备无关量子密钥分发实验

卢奉宇[1,2,3]，银振强[1,2,3*]，王双[1,2,3**]，王泽浩[1,2,3]，陈巍[1,2,3]，郭光灿[1,2,3]，韩正甫[1,2,3]

[1]中国科学技术大学中科院量子信息重点实验室，安徽 合肥 230026；

[2]中国科学技术大学量子信息与量子科技前沿协同创新中心，安徽 合肥 230026；

[3]密码科学技术国家重点实验室，北京 100878

摘要 测量设备无关量子密钥分发协议可以免疫所有测量端的漏洞，极大地推进量子保密通信的实用化进程。美中不足的是，该协议依然对源端有极强的安全性假设。源端设备的非完美性同样会留下多种侧信道，从而威胁系统的实际安全性。针对此问题，提出无特征源测量设备无关量子密钥分发协议。该协议在量子态制备不完美的情况下依然可以提取出安全的密钥，是理论无条件安全性与实际安全性的完美结合。通过三强度诱骗态方法以及自行研制的 Sagnac-Asymmetric-Mach-Zehnder 编码结构，成功搭建无特征源的测量设备无关量子密钥分发系统，并在长为 50.4 km 的光纤信道和 25 MHz 的系统重复频率下达到 1.91×10^{-6} 的安全密钥分发速率。

关键词 量子信息；量子通信；量子加密；量子密钥分发

中图分类号 O431.2 **文献标志码** A **doi**：10.3788/AOS202242.0327017

Uncharacterized-Source Measurement-Device-Independent Quantum Key Distribution Experiment with over 50 km fiber

Lu Fengyu[1,2,3], Yin Zhenqiang[1,2,3*], Wang Shang[1,2,3**], Wang Zehao[1,2,3], Chen Wei[1,2,3], Guo Guangcan[1,2,3], Han Zhenfu[1,2,3]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui* 230026, *China*;

[2] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui* 230026, *China*;

[3] *State Key Laboratory of Cryptology, P. O. Box* 5159, *Beijing* 100878, *China*

Abstract The measurement-device-independent quantum key distribution (MDI-QKD) can remove all detector side-channel attacks, which greatly boosts the practical application of the quantum key distribution. However, this protocol still has a strict assumption that the states in source side must be perfectly prepared. The imperfections of the modulators in source side would bring side-channels and threaten the practical security of the system. To protect against state-preparation imperfections, the uncharacterized-source MDI-QKD, which can still generate secret keys when the prepared states are uncharacterized, have been put forward. This protocol is a great combination of the theoretical information security and the practical security. Through the three-intensity decoy state method and the self-developed Sagnac-Asymmetric-Mach-Zehnder coding structure, the measurement device-independent quantum key distribution system without characteristic source is successfully built, and the secure key distribution rate of 1.91×10^{-6} is achieved under the fiber channel of 50.4 km and the repetition rate of 25 MHz.

Key words quantum information; quantum communication; quantum cryptography; quantum key distribution

收稿日期：2021-07-06；**修回日期**：2021-08-22；**录用日期**：2021-08-31

基金项目：国家重点研发计划(2016YFA0302600)、国家自然科学基金(61822115，61775207)、中国博士后科学基金(2021M693098)

通信作者：*yinzq@ustc.edu.cn；**wshuang@ustc.edu.cn

1 引 言

量子密钥分发(QKD)是量子信息领域最为成熟和成功的应用之一,它可以使用户 Alice 与 Bob 在存在窃听者 Eve 的情况下安全地进行密钥分发[1-2]。这些密钥可以用于已经被证明为信息论安全的一次一密方法[3]对通信的内容进行加密,进而实现信息论安全层面上的安全通信。

原始的 QKD 协议需要假设通信双方的源端和探测端无法被窃听者控制,并且源端需要准确调制出所需的量子态以确保准确刻画出信息泄漏的情况。然而,由于实际器件具有各种非完美性,源端与探测端的理想特性往往无法得到保证[4-6],这使得窃听者 Eve 可以通过实际器件的侧信道来窃取信息而不被发现[7-10]。

为了应对侧信道攻击,科研人员提出了设备无关的量子密钥分发(DI-QKD)协议[11],该协议可以免疫所有针对实际设备非完美性的攻击。然而,DI-QKD 协议对探测效率与信道损耗的要求过于苛刻,以至于它无法被用在实际通信中。幸运的是,科研人员创造性地提出了测量设备无关的量子密钥分发(MDI-QKD)协议[12],该协议要求通信的双方 Alice 与 Bob 制备所需要的量子态并发送给不受信任的第三方 Charlie 进行测量。MDI-QKD 协议可以免疫所有针对 QKD 系统中最为脆弱的探测端的攻击,并且具有较高的密钥率和通信距离[13-14],是安全性与实用性的完美结合。

然而,MDI-QKD 协议依然保有源端绝对安全的假设。在实际系统中,由于调制误差[7,15-16]和环境干扰的存在[17-18],Alice 与 Bob 所制备的量子态往往存在偏差。这种偏差会在源端留下侧信道,进而导致用户无法准确估计信息泄漏的情况。为了解决态制备不完美的问题,科研人员提出了无特征源的 MDI-QKD 协议[19],并在后续一系列工作中对该协议进行了改进[20-22]。通过分析非匹配基的响应率,该协议在源端量子态特征缺失的情况下依然可以正确估计出信息泄漏的上界,从而安全地进行密钥分发。

在这项工作中,本文通过自行研制的 Sagnac-Asymmetric-Mach-Zehnder 编码结构搭建无特征源的 MDI-QKD 通信系统,并通过诱骗态方法与 GLLP 公式[23-25]来估算出安全密钥率。结合 Hwang 等[20]提出的改进协议,在长为 10.0,20.0,50.4 km 的光纤信道中每脉冲实现 1.54×10^{-5},8.54×10^{-6},1.91×10^{-6} bit 的安全密钥分发。

2 无特征源的 MDI-QKD 系统

2.1 基于三强度诱骗态的无特征源 MDI-QKD 协议

原始的无特征源的 MDI-QKD 协议的安全性基于单光子源,然而目前尚无可以稳定产生单光子信号的理想单光子源,通常使用相干态光源结合诱骗态的方法来估算出成功事件中单光子成分所占的比例。在这里给出基于三强度诱骗态的无特征源 MDI-QKD 协议的协议流程以及安全密钥率的计算方法,步骤如下。

1)态制备:发送端 Alice 和 Bob 分别从各自预定的光强集合$\{\mu,\nu,o\}$与$\{\mu',\nu',o\}$中随机选择一个光强 $l\in\{\mu,\nu,o\}$与 $r\in\{\mu',\nu',o\}$,并将相位随机化的弱相干态衰减到该强度,其中 o 为真空态,$\mu(\mu')$和 $\nu(\nu')$分别为 Alice(Bob)所制备的信号态和诱骗态光强。接着,发送端 Alice 和 Bob 分别产生随机数 $n\in\{0,1,2\}$与 $m\in\{0,1,2\}$,并根据各自的随机数编码二维量子态$|\varphi_n\rangle$与$|\varphi'_m\rangle$,并且满足关系式

$$\begin{cases}|\varphi_2\rangle=c_0\,|\varphi_0\rangle+c_1\exp(\mathrm{i}\theta)\,|\varphi_1\rangle\\ |\varphi'_2\rangle=c'_0\,|\varphi'_0\rangle+c'_1\exp(\mathrm{i}\theta')\,|\varphi'_1\rangle\end{cases},\tag{1}$$

式中:θ 与 θ'表示相对相位;c_0、c_1、c'_0和 c'_1表示非负实数,且满足 $c_0^2+c_1^2=1$,$c_0'^2+c_0'^2=1$。为了方便表述,定义当 $n(m)=0,1$ 时,Alice(Bob)发送了 Z 基;当 $n(m)=2$ 时,Alice(Bob)发送了 X 基。对于通信的双方而言,c_0、c_1、θ、c'_0、c'_1和 θ'都是未知的参数。之后,发送端 Alice 和 Bob 将各自制备好的态发送给第三方 Charlie 进行测量。

2)态测量与原始密钥生成:Charlie 对接收到的量子态进行贝尔态测量,并宣布是否有预先定义的成功事件发生。如果 Charlie 宣布有成功事件,且 Alice 发送的态是$|\varphi_0\rangle$或$|\varphi_1\rangle$,那么 Alice 记录下对应的原始密钥 0 或 1;而 Bob 则需要进行一次比特翻转,即当 Bob 发送的态是$|\varphi'_0\rangle$或$|\varphi'_1\rangle$时,Bob 记录下对应的原始密钥 1 或 0。

3)筛选:Alice 与 Bob 重复以上步骤多次,并在之后公布自己所发的是 Z 基还是 X 基。当两人没有同时选择 Z 时,原始密钥将被丢弃。同时,两人需要随机选择一部分通信结果并公开当次通信所发送的态与光强,统计发送各种态和光强组合的响应率,公布发送具体态的原始密钥也需要被丢弃,此时剩下的密钥被称为筛后密钥。定义 Alice 选择光强 l 与态$|\varphi_n\rangle$、Bob 选择光强 r 与态$|\varphi'_m\rangle$的成功事件

的响应率为 $Q_{nm}^{(lr)}$，其中下标 nm 指 Alice 与 Bob 编码的态分别为 $|\varphi_n\rangle$ 与 $|\varphi'_m\rangle$。

4）参数估计：Alice 与 Bob 利用步骤 3）统计到的各项相干态响应率 $Q_{nm}^{(lr)}$ 对单光子对的成功事件概率 Y_{nm} 进行估计。进一步利用单光子响应率，Alice 与 Bob 可以估算出信息泄漏量 I_{AE}。

5）提取安全密钥：Alice 与 Bob 对筛后密钥进行纠错，并根据步骤 4）估算的信息泄漏量 I_{AE} 进行密性放大[1-4]，最终剩下的密钥被称为安全密钥。

步骤 5）要求用户能够准确估计出单光子响应的成分以及信息泄漏量，在这里详细介绍协议中的参数估计方法。在步骤 3）中，Alice 与 Bob 通过随机公开一部分通信所发送的态与光强，可以统计出 Alice 选择光强 l 与态 $|\varphi_n\rangle$、Bob 选择光强 r 与态 $|\varphi'_m\rangle$ 的成功事件的响应率 $Q_{nm}^{(lr)}$。由于多光子响应产生的密钥不安全，故需要估算出单光子成分的响应率。对于 Alice 与 Bob 分别发送单光子且编码分别为 $|\varphi_n\rangle$ 与 $|\varphi'_m\rangle$，单光子对的成功事件概率为 Y_{nm}。使用 MDI 协议的三强度诱骗态方法[26-28]可以估算出 Y_{nm} 的上下界，表达式为

$$Y_{nm}\leqslant\bar{Y}_{nm}=\frac{(Q_{nm}^{(\nu\nu')}+p_0^{(\nu)}p_0^{(\nu')}Q_{nm}^{(oo)})-(p_0^{(\nu)}Q_{nm}^{(o\nu')}+p_0^{(\nu')}Q_{nm}^{(\nu o)})}{p_1^{(\nu)}p_1^{(\nu')}},\tag{2}$$

$$Y_{nm}\geqslant\underline{Y}_{nm}=\frac{M_{nm}^{+}-M_{nm}^{-}}{p_1^{(\mu)}p_2^{(\mu)}(p_1^{(\nu')}p_2^{(\mu')}-p_2^{(\nu')}p_1^{(\mu')})},\tag{3}$$

式中：$\bar{Y}_{nm}$ 和 $\underline{Y}_{nm}$ 分别表示各项单光子响应率的上界和下界；$M_{nm}^{+}=p_1^{(\mu)}p_1^{(\mu')}Q_{nm}^{(\nu\nu')}+p_1^{(\nu)}p_2^{(\nu')}p_0^{(\mu)}Q_{nm}^{(o\mu')}+p_1^{(\nu)}p_2^{(\nu')}p_0^{(\mu')}Q_{nm}^{(\mu o)}+p_1^{(\mu)}p_2^{(\mu')}p_0^{(\nu)}p_0^{(\nu')}Q_{nm}^{(oo)}$；$M_{nm}^{-}=p_1^{(\nu)}p_1^{(\nu')}Q_{nm}^{(\mu\mu')}+p_1^{(\mu)}p_2^{(\mu')}p_0^{(\nu)}Q_{nm}^{(o\nu')}+p_1^{(\mu)}p_2^{(\mu')}p_0^{(\nu')}Q_{nm}^{(\nu o)}+p_0^{(\mu)}p_0^{(\mu')}p_1^{(\nu)}p_2^{(\nu')}Q_{nm}^{(oo)}$；$p_k^{(\omega)}=\mathrm{e}^{-\omega}\omega^k/k!$ 表示光强为 ω 的相干态中含有 k 光子的概率。

根据 Hwang 等[20]提出的简化协议，在已经估算出 $\bar{Y}_{nm}$ 与 $\underline{Y}_{nm}$ 之后可以将相位误码率 e_{p} 的上界 $\bar{e}_{\mathrm{p}}$ 表示为

$$e_{\mathrm{p}}\leqslant\bar{e}_{\mathrm{p}}=\max\left[\frac{Y_{00}+Y_{11}}{Y_{00}+Y_{01}+Y_{10}+Y_{11}}+\frac{f(c_0,c'_0,c_1,c'_1)}{2(Y_{00}+Y_{01}+Y_{10}+Y_{11})}\right],\tag{4}$$

其中

$$f(c_0,c'_0,c_1,c'_1)=\min\left[\frac{\sqrt{Y_{22}}+c_0c'_1\sqrt{Y_{00}}+c_1c'_0\sqrt{Y_{11}}+|c_0c'_0-c_1c'_1|^2\sqrt{Y_{10}}}{(c_0c'_0)^2},\frac{\sqrt{Y_{22}}+c_0c'_1\sqrt{Y_{00}}+c_1c'_0\sqrt{Y_{11}}+|c_0c'_0-c_1c'_1|^2\sqrt{Y_{10}}}{(c_1c'_1)^2}\right]。$$

使用非线性优化算法并按照

$$\begin{cases}\underline{Y}_{nm}\leqslant Y_{nm}\leqslant\bar{Y}_{nm},\text{for }n,m\in\{0,1,2\}\\(c_0-c_1)^2\leqslant1\leqslant(c_0+c_1)^2\\(c'_0-c'_1)^2\leqslant1\leqslant(c'_0+c'_1)^2\\(\sqrt{Y_{00}c_0}-\sqrt{Y_{10}c_1})^2\leqslant Y_{20}\leqslant(\sqrt{Y_{00}c_0}+\sqrt{Y_{10}c_1})^2\\(\sqrt{Y_{01}c_0}-\sqrt{Y_{11}c_1})^2\leqslant Y_{21}\leqslant(\sqrt{Y_{01}c_0}+\sqrt{Y_{11}c_1})^2\\(\sqrt{Y_{00}c'_0}-\sqrt{Y_{01}c'_1})^2\leqslant Y_{02}\leqslant(\sqrt{Y_{00}c'_0}+\sqrt{Y_{01}c'_1})^2\\(\sqrt{Y_{10}c'_0}-\sqrt{Y_{11}c'_1})^2\leqslant Y_{12}\leqslant(\sqrt{Y_{10}c'_0}+\sqrt{Y_{11}c'_1})^2\end{cases}\tag{5}$$

各项约束条件来优化(4)式中的变量（c_0、c'_0、c_1、c'_1 和 Y_{nm}），即可解出(4)式中相位误码的上界使用 $\bar{e}_{\mathrm{p}}$ 可以估算出信息泄漏量的上界为 $\bar{I}_{\mathrm{AE}}=H(\bar{e}_{\mathrm{p}})$，其中 $H(x)=-x\mathrm{lb}\,x-(1-x)\mathrm{lb}(1-x)$ 为二元香农熵函数。经过纠错和密性放大之后最终的安全密钥率 R 可由 GLLP 公式[23-25]表示为

$$R=p_1^{(\mu)}p_1^{(\mu')}\underline{Y}_{\mathrm{ZZ}}(1-I_{\mathrm{AE}})-Q_{\mathrm{ZZ}}^{(\mu\mu')}fH(E_{\mathrm{ZZ}}^{(\mu\mu')}),\tag{6}$$

式中：$\underline{Y}_{\mathrm{ZZ}}=(\underline{Y}_{00}+\underline{Y}_{01}+\underline{Y}_{10}+\underline{Y}_{11})/4$ 表示 Alice 与 Bob 均发送单光子且编码在 Z 基下的成功事件响应率；$Q_{\mathrm{ZZ}}^{(\mu\mu')}=\frac{(Q_{00}^{(\mu\mu')}+Q_{01}^{(\mu\mu')}+Q_{10}^{(\mu\mu')}+Q_{11}^{(\mu\mu')})}{4}$ 表示 Z 基信号态下的响应率；$E_{\mathrm{ZZ}}^{(\mu\mu')}=\frac{(Q_{00}^{(\mu\mu')}+Q_{11}^{(\mu\mu')})}{(Q_{00}^{(\mu\mu')}+Q_{01}^{(\mu\mu')}+Q_{10}^{(\mu\mu')}+Q_{11}^{(\mu\mu')})}$ 表示 Z 基信号态下的误码率；f 表示纠错效率，实验中取值为 1.16。

2.2 无特征源 MDI-QKD 实验

结合三强度诱骗态方法与时间戳-相位编码系统，成功搭建了无特征源的 MDI-QKD 系统，并在 10.0，20.0，50.4 km 的距离下成功实现了密钥分发。实验装置如图 1 所示，图中 LD 表示激光器，

PM 表示相位调制器，IM 表示强度调制器[29]，PC 表示偏振控制器，CIRC 表示环形器，VOA 表示可调衰减器，BS 表示分束器，PBS 表示偏振分束器，SPD 表示单光子探测器。发送端使用一个中心波长为 1542.38 nm、精度为 0.0001 nm 的 Clarity NLL-1542-HP 型连续光激光器，产生连续光相干态。之后相位调制器 PM 1 将每个相干态脉冲进行相位随机化[30-31]，使用户制备的相干态变为光子数态的混态。铌酸锂强度调制器 IM 1 由一个自制的窄脉冲生成电路控制，并将连续光斩波[30-31]为脉宽 500 ps、间隔为 40 ns 的脉冲光序列。IM 2 由一个自制的 2 bit-数字模拟转换器(DAC)驱动，并根据三强度诱骗态方法将脉冲调制为信号态 μ、诱骗态 ν 与真空态 o 三种不同的强度。偏振控制器 PC 1 与 PC 2 用于调节光的偏振态，使其与调制器所需的偏振方向保持一致。之后通过虚线框中的 Sagnac-Asymmetric-Mach-Zehnder 型编码模块调制出需要发送的量子态，脉冲经过环形器 CIRC 和 50∶50 的分束器 BS 1 进入 Sagnac 环，并分为顺时针和逆时针两个方向的脉冲。其中顺时针脉冲与逆时针脉冲会先后通过相位调制器 PM 2，到达的时间相差 10 ns。调节 PM 2 的电压使顺逆时针脉冲的相位差为 0 或 π，可以使其在 BS 1 处干涉后分别进入不等臂 Mach-Zehnder 干涉仪的长臂(path-L)和短臂(path-S)中，并定义这两种情况分别为编码 Z 基的 $|\varphi_0\rangle$ 与 $|\varphi_1\rangle$；当相位差为 $\pi/2$ 时，长短臂通过的光强相等，并定义这两种情况分别为编码 X 基的 $|\varphi_2\rangle$。短臂上的相位调制器 PM 3 用于附加一个额外的相位，以补偿 Alice 与 Bob 之间的参考系漂移[13-14]。最后脉冲经过一个固定衰减器衰减至单光子量级，并通过长为 25 km 的量子信道发送给 Charlie 进行测量。

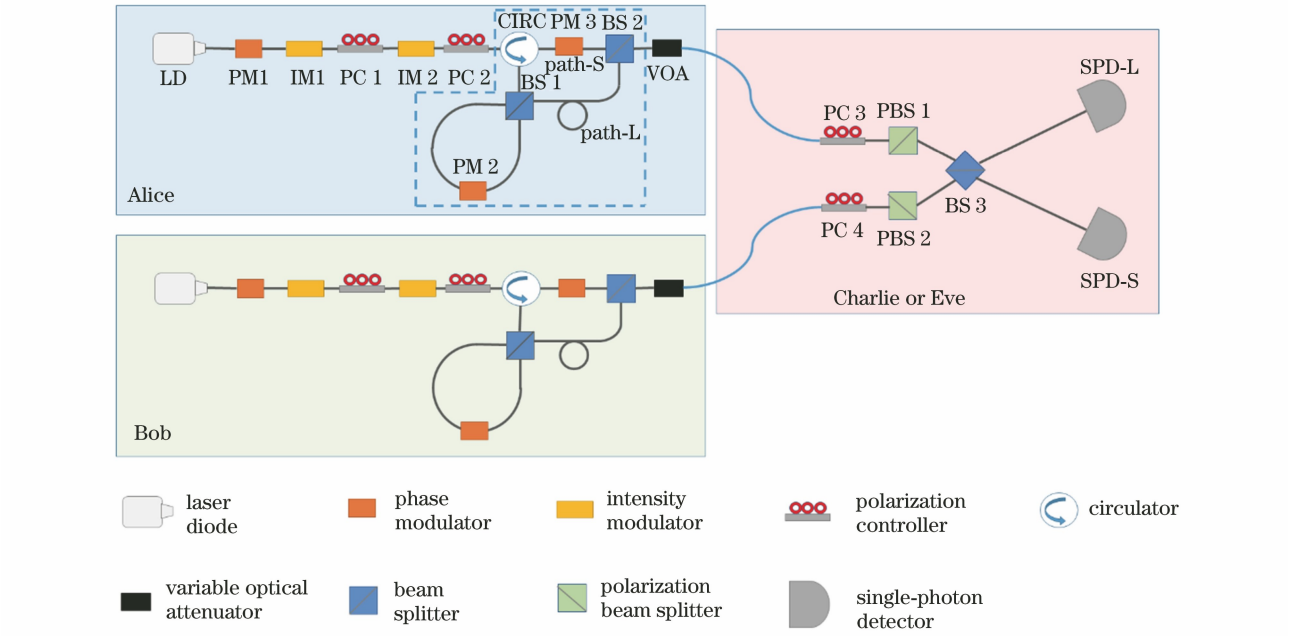

图 1 无特征源 MDI-QKD 实验装置

Fig. 1 Experimental setup for uncharacterized-source MDI-QKD

Charlie 首先通过 PC 3 与 PC 4 来调节偏振[32]，使通过 PBS 后进入探测器的光达到最大，从而使得 Alice 与 Bob 的量子态偏振一致以保持 HOM(Hong-Ou-Mandel)干涉[33]的干涉可见度达到最大。BS 的两端分别接两台探测效率为 20%、暗计数率分别为 3×10^{-6} 和 1×10^{-6} 的单光子探测器(SPD-300-Qasky)，并将它们分别记为 SPD-L 与 SPD-S。两台探测器均以 25 MHz 的频率、1 ns 的门宽开门，Charlie 调节延时使 SPD-L 仅在长臂时间戳开门，SPD-S 仅在短臂时间戳开门。当两探测器同时响应时，Charlie 宣布成功事件发生。根据 Charlie 宣布的成功事件，Alice 与 Bob 记录原始密钥以及统计各种态组合的成功事件响应率，并进行参数估计、密性放大与纠错，从而生成安全密钥。

首先根据文献[34-35]提出的方法仿真计算出三种距离下发送不同平均光子数的成功事件响应率，并根据仿真的响应率与(2)～(6)式计算出安全密钥率。通过仿真可以判断出平均光子数与密钥率的关系，并据此对实验所调制的光强 μ 与 ν 进行优化[36-37]，以使安全密钥率达到最大。根据优化的结果，实验中的三

组诱骗态平均光子数设置如表 1 所示。

表 1 诱骗态强度

Table 1 Intensity of decoy state

Distance /km	μ	ν	o
10.0	0.26	0.025	0
20.0	0.25	0.024	0
50.4	0.24	0.023	0

实验测得的 Alice 与 Bob 编码 $|\varphi_n\rangle$ 与 $|\varphi'_m\rangle$(n，$m\in\{0,1,2\}$)且发送平均光子数为 l 与 r 的相干态的成功事件响应率，如表 2～4 所示，其中行 $|n\rangle|m\rangle$ 代表编码的态为 $|\varphi_n\rangle|\varphi'_m\rangle$，列 lr 代表选择的强度。根据表 1 的测量值，使用(2)式与(3)式可以计算出编码 $|\varphi_n\rangle$ 与 $|\varphi'_m\rangle$ 的单光子事件的成功事件响应率的上下界，如表 5～7 所示，其中行 $|n\rangle|m\rangle$ 代表编码的态为 $|\varphi_n\rangle|\varphi'_m\rangle$，列 UB 与 LB 分别代表上界与下界。

表 2 10.0 km 通信距离下实验测量的成功事件响应率

Table 2 Successful event response rate measured experimentally at 10.0 km communication distance

$Q_{nm}^{(lr)}$	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|2\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|1\rangle\|2\rangle$	$\|2\rangle\|0\rangle$	$\|2\rangle\|1\rangle$	$\|2\rangle\|2\rangle$
$\mu\mu$	5.02×10^{-6}	3.83×10^{-4}	3.03×10^{-4}	3.91×10^{-4}	4.20×10^{-6}	3.07×10^{-4}	3.05×10^{-4}	3.13×10^{-4}	1.91×10^{-4}
$\nu\nu$	6.92×10^{-8}	4.42×10^{-6}	3.28×10^{-6}	4.11×10^{-6}	6.40×10^{-8}	2.94×10^{-6}	3.10×10^{-6}	2.98×10^{-6}	2.14×10^{-6}
μo	5.60×10^{-8}	5.60×10^{-8}	5.60×10^{-8}	6.20×10^{-8}	6.20×10^{-8}	6.20×10^{-8}	1.02×10^{-4}	1.02×10^{-4}	1.02×10^{-4}
$o\mu$	5.94×10^{-8}	6.26×10^{-8}	1.04×10^{-4}	5.94×10^{-8}	6.26×10^{-8}	1.04×10^{-4}	5.94×10^{-8}	6.26×10^{-8}	1.04×10^{-4}
νo	6.12×10^{-9}	6.12×10^{-9}	6.12×10^{-9}	5.46×10^{-9}	5.46×10^{-9}	5.46×10^{-9}	1.09×10^{-6}	1.09×10^{-6}	1.09×10^{-6}
$o\nu$	5.72×10^{-9}	6.48×10^{-9}	1.07×10^{-6}	5.72×10^{-9}	6.48×10^{-9}	1.07×10^{-6}	5.72×10^{-9}	6.48×10^{-9}	1.07×10^{-6}

表 3 20.0 km 通信距离下实验测量的成功事件响应率

Table 3 Successful event response rate measured experimentally at 20.0 km communication distance

$Q_{nm}^{(lr)}$	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|2\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|1\rangle\|2\rangle$	$\|2\rangle\|0\rangle$	$\|2\rangle\|1\rangle$	$\|2\rangle\|2\rangle$
$\mu\mu$	3.06×10^{-6}	2.50×10^{-4}	1.74×10^{-4}	2.52×10^{-4}	2.76×10^{-6}	1.94×10^{-4}	1.98×10^{-4}	1.82×10^{-4}	1.18×10^{-4}
$\nu\nu$	3.80×10^{-8}	2.32×10^{-6}	1.84×10^{-6}	2.96×10^{-6}	3.72×10^{-8}	2.21×10^{-6}	1.96×10^{-6}	1.82×10^{-6}	1.34×10^{-6}
μo	4.86×10^{-8}	4.86×10^{-8}	4.86×10^{-8}	4.74×10^{-8}	4.74×10^{-8}	4.74×10^{-8}	5.79×10^{-5}	5.79×10^{-5}	5.79×10^{-5}
$o\mu$	4.88×10^{-8}	4.50×10^{-8}	6.58×10^{-5}	4.88×10^{-8}	4.50×10^{-8}	6.58×10^{-5}	4.88×10^{-8}	4.50×10^{-8}	6.58×10^{-5}
νo	4.46×10^{-9}	4.46×10^{-9}	4.46×10^{-9}	4.16×10^{-9}	4.16×10^{-9}	4.16×10^{-9}	7.38×10^{-7}	7.38×10^{-7}	7.38×10^{-7}
$o\nu$	5.48×10^{-9}	4.76×10^{-9}	5.49×10^{-7}	5.48×10^{-9}	4.76×10^{-9}	5.49×10^{-7}	5.48×10^{-9}	4.76×10^{-9}	5.49×10^{-7}

表 4 50.4 km 通信距离下实验测量的成功事件响应率

Table 4 Successful event response rate measured experimentally at 50.4 km communication distance

$Q_{nm}^{(lr)}$	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|2\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|1\rangle\|2\rangle$	$\|2\rangle\|0\rangle$	$\|2\rangle\|1\rangle$	$\|2\rangle\|2\rangle$
$\mu\mu$	7.56×10^{-7}	5.80×10^{-5}	4.76×10^{-5}	6.21×10^{-5}	7.71×10^{-7}	4.66×10^{-5}	4.32×10^{-5}	4.79×10^{-5}	2.71×10^{-5}
$\nu\nu$	1.08×10^{-8}	4.92×10^{-7}	4.26×10^{-7}	3.72×10^{-7}	1.22×10^{-8}	4.41×10^{-7}	4.33×10^{-7}	4.52×10^{-7}	2.98×10^{-7}
μo	2.40×10^{-8}	2.40×10^{-8}	2.40×10^{-8}	2.48×10^{-8}	2.48×10^{-8}	2.48×10^{-8}	1.44×10^{-5}	1.44×10^{-5}	1.44×10^{-5}
$o\mu$	2.04×10^{-8}	2.16×10^{-8}	1.41×10^{-5}	2.04×10^{-8}	2.16×10^{-8}	1.41×10^{-5}	2.04×10^{-8}	2.16×10^{-8}	1.41×10^{-5}
νo	3.20×10^{-9}	3.20×10^{-9}	3.20×10^{-9}	2.00×10^{-9}	2.00×10^{-9}	2.00×10^{-9}	1.51×10^{-7}	1.51×10^{-7}	1.51×10^{-7}
$o\nu$	3.60×10^{-9}	2.40×10^{-9}	1.51×10^{-7}	3.60×10^{-9}	2.40×10^{-9}	1.51×10^{-7}	3.60×10^{-9}	2.40×10^{-9}	1.51×10^{-7}

表 5 10.0 km 通信距离下单光子对在不同编码态下的响应率上下界

Table 5 Upper and lower bound of responsivity of single photon pair at 10.0 km communication distance under different coding states

Y_{nm}	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|2\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|1\rangle\|2\rangle$	$\|2\rangle\|0\rangle$	$\|2\rangle\|1\rangle$	$\|2\rangle\|2\rangle$
LB	8.98×10^{-5}	6.84×10^{-3}	3.19×10^{-3}	6.27×10^{-3}	8.25×10^{-5}	2.58×10^{-3}	2.13×10^{-3}	1.90×10^{-3}	0
UB	9.30×10^{-5}	7.11×10^{-3}	3.42×10^{-3}	6.61×10^{-3}	8.44×10^{-5}	2.88×10^{-3}	2.47×10^{-3}	2.28×10^{-3}	5.56×10^{-5}

表 6 20.0 km 通信距离下单光子对在不同编码态下的响应率上下界

Table 6 Upper and lower bound of responsivity of single photon pair at 20.0 km communication distance under different coding states

Y_{nm}	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|2\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|1\rangle\|2\rangle$	$\|2\rangle\|0\rangle$	$\|2\rangle\|1\rangle$	$\|2\rangle\|2\rangle$
LB	4.71×10^{-5}	3.83×10^{-3}	2.20×10^{-3}	5.07×10^{-3}	4.83×10^{-5}	2.87×10^{-3}	1.99×10^{-3}	1.76×10^{-3}	1.04×10^{-4}
UB	5.00×10^{-5}	4.08×10^{-3}	2.30×10^{-3}	5.21×10^{-3}	5.03×10^{-5}	2.95×10^{-3}	2.18×10^{-3}	1.93×10^{-3}	1.48×10^{-4}

表 7 50.4 km 通信距离下单光子对在不同编码态下的响应率上下界

Table 7 Upper and lower bound of responsivity of single photon pair at 50.4 km communication distance under different coding states

Y_{nm}	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|2\rangle$	$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|1\rangle\|2\rangle$	$\|2\rangle\|0\rangle$	$\|2\rangle\|1\rangle$	$\|2\rangle\|2\rangle$
LB	6.97×10^{-6}	8.92×10^{-4}	4.97×10^{-4}	6.18×10^{-4}	1.51×10^{-5}	5.32×10^{-4}	5.22×10^{-4}	5.52×10^{-4}	0
UB	8.24×10^{-6}	9.63×10^{-4}	5.45×10^{-4}	7.26×10^{-4}	1.57×10^{-5}	5.77×10^{-4}	5.58×10^{-4}	5.98×10^{-4}	5.69×10^{-6}

如表 8 所示，在 10.0，20.0，50.4 km 三个距离下，实验中测得 Z 基信号态下的响应率 $Q_{ZZ}^{(\mu\mu')}$ 分别为 1.96×10^{-4}、1.27×10^{-5} 和 3.04×10^{-5}，误码率 $E_{ZZ}^{(\mu\mu')}$ 分别为 1.17%、1.14%和 1.26%。由表 5～7 的数据，可以计算出三个距离下双方都发送 Z 基单光子的成功事件响应率的下界 $\underline{Y}_{ZZ}$，分别为 3.32×10^{-3}、2.25×10^{-3} 和 3.83×10^{-4}，并且由(4)式可以计算出相位误码率 e_p，分别为 0.203、0.214 和 0.150。实验最终生成的每脉冲安全密钥率 R 分别为 1.54×10^{-5}、8.54×10^{-6} 和 1.91×10^{-6}。

表 8 重要中间变量

Table 8 Important intermediate variables

Distance /km	$\underline{Y}_{ZZ}/10^{-4}$	e_p	$Q_{ZZ}^{(\mu\mu')}/10^{-5}$	$E_{ZZ}^{(\mu\mu')}$/%	R /10^{-6}
10.0	33.20	0.203	19.6	1.17	15.40
20.0	22.50	0.214	1.27	1.14	8.54
50.4	3.83	0.150	3.04	1.26	1.91

图 2 为通信距离与安全密钥率的关系，横轴表示通信距离，纵轴表示每脉冲安全密钥率。实线表示不同距离下的仿真最优密钥率，圆圈表示实验测得的安全密钥率。从图 2 可以看到，实验测量的结果与理论仿真结果几乎一致。本实验验证了该协议的可行性，证明了该协议在编码不完美情形下的优势，进一步推动了 MDI-QKD 协议的实用化进程。

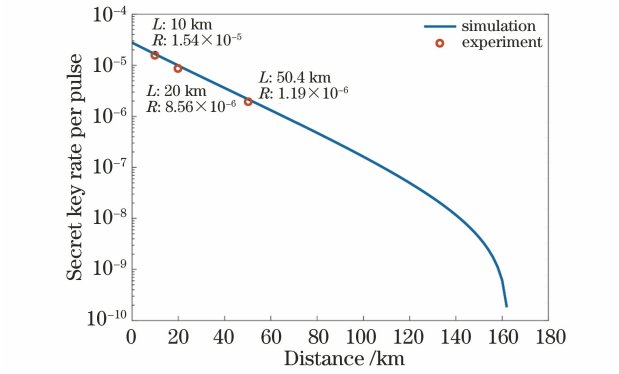

图 2 通信距离与安全密钥率的关系

Fig. 2 Relationship between communication distance and security key rate

3 结 论

本文成功在长为 10.0，20.0，50.4 km 的光纤信道中实现了无特征源的测量设备无关量子密钥分发，并在 25 MHz 的系统重复频率下实现了安全密钥分发。对于原始的测量设备无关量子密钥分发协议中的非匹配基数据，即当 Alice 与 Bob 选基不同时，通信数据将被丢弃，然而，这些被丢弃的非匹配基数据包含了有用的信息。在原始的 MDI-QKD 协议中，通信的双方必须完美地制备出协议所要求的 4 种 BB84 态。而在本实验中，通过分析非匹配基数据，通信的双方可以仅编码三种态且在编码态未知的情况下生成安全密钥。相比于原始的 MDI-QKD 系统，该实验系统不仅免疫所有针对探测端的攻击，同时也避免了源端态制备不完美所带来的安全漏洞。该实验系统提升了 MDI-QKD 协议的鲁棒性与安全性，进一步推动了 MDI-QKD 协议走向实际应用，并为 QKD 网络等复杂场景奠定了基础。

参 考 文 献

[1] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050-2056.

[2] Renner R. Security of quantum key distribution[J]. International Journal of Quantum Information, 2008, 6(1): 1-127.

[3] Shannon C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

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

[5] 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.

[6] 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.

[7] Yoshino K I, Fujiwara M, Nakata K, et al. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses[J]. Npj Quantum Information, 2018, 4: 8.

[8] Liu W T, Sun S H, Liang L M, et al. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution[J]. Physical Review A, 2011, 83(4): 042326.

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

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

[11] 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.

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

[13] 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.

[14] Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber[J]. Physical Review Letters, 2016, 117(19): 190501.

[15] Wang X B, Peng C Z, Pan J W. Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source[J]. Applied Physics Letters, 2007, 90(3): 031110.

[16] Tang Y L, Yin H L, Ma X F, et al. Source attack of decoy-state quantum key distribution using phase information[J]. Physical Review A, 2013, 88(2): 022308.

[17] Ding Y Y, Chen W, Chen H, et al. Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits[J]. Optics Letters, 2017, 42(6): 1023-1026.

[18] Liu J Y, Ding H J, Zhang C M, et al. Practical phase-modulation stabilization in quantum key distribution via machine learning[J]. Physical Review Applied, 2019, 12: 014059.

[19] Yin Z Q, Fung C H F, Ma X F, et al. Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources[J]. Physical Review A, 2014, 90(5): 052319.

[20] Hwang W Y, Su H Y, Bae J. Improved measurement-device-independent quantum key distribution with uncharacterized qubits[J]. Physical Review A, 2017, 95(6): 062313.

[21] Wang C, Wang S, Yin Z Q, et al. Experimental measurement-device-independent quantum key distribution with uncharacterized encoding[J]. Optics Letters, 2016, 41(23): 5596-5599.

[22] Zhou X Y, Ding H J, Zhang C H, et al. Experimental three-state measurement-device-independent quantum key distribution with uncharacterized sources[J]. Optics Letters, 2020, 45(15): 4176-4179.

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

[24] Wang X B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light[J]. Physical Review A, 2005, 72(1): 012322.

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

[26] Wang X B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors[J]. Physical Review A, 2013, 87(1): 012320.

[27] Zhou Y H, Yu Z W, Wang X B. Making the decoy-state measurement-device-independent quantum key distribution practically useful[J]. Physical Review A, 2016, 93(4): 042324.

[28] Yu Z W, Zhou Y H, Wang X B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method[J]. Physical Review A, 2015, 91(3): 032318.

[29] Chen F, Liu R P, Qi Z M. Design, fabrication and characterization of $LiNbO_3$-based integrated optical waveguide Mach-Zehnder interferometer[J]. Acta Optica Sinica, 2011, 31(5): 0513001.
陈方, 刘瑞鹏, 祁志美. 铌酸锂基集成光波导马赫-曾德尔干涉仪的设计、制备及其特性的初步测试[J]. 光学学报, 2011, 31(5): 0513001.

[30] Wang C, Yin Z Q, Wang S, et al. Measurement-device-independent quantum key distribution robust against environmental disturbances[J]. Optica, 2017, 4(9): 1016-1023.

[31] Wang C, Song X T, Yin Z Q, et al. Phase-reference-free experiment of measurement-device-independent quantum key distribution[J]. Physical Review

Letters, 2015, 115(16): 160502.

[32] Huang Y, Zhao J Y, Wang J D, et al. A real-time polarization compensation system based on wavelength-division multiplexing for optical fiber communication systems [J]. Acta Optica Sinica, 2020, 40(14): 1406003.
黄媛, 赵家钰, 王金东, 等. 一种基于波分复用的实时光纤信道偏振补偿系统[J]. 光学学报, 2020, 40(14): 1406003.

[33] Wang C, Wang F X, Chen H, et al. Realistic device imperfections affect the performance of Hong-ou-Mandel interference with weak coherent states [J]. Journal of Lightwave Technology, 2017, 35(23): 4996-5002.

[34] Wang Q, Wang X B. Simulating of the measurement-device independent quantum key distribution with phase randomized general sources [J]. Scientific Reports, 2014, 4: 4612.

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

[36] Xue Y, Ma L H, Shi L, et al. Performance analysis of MDI-QKD global estimation based on modified coherent source [J]. Chinese Journal of Quantum Electronics, 2017, 34(4): 446-450.
薛阳, 马丽华, 石磊, 等. 基于修正相干态光源的MDI-QKD全局估计性能分析[J]. 量子电子学报, 2017, 34(4): 446-450.

[37] Guo D B, Zhang Y H, Wang Y Y. Performance optimization for the reconciliation of Gaussian quantum key distribution [J]. Acta Optica Sinica, 2014, 34(1): 0127001.
郭大波, 张彦煌, 王云艳. 高斯量子密钥分发数据协调的性能优化[J]. 光学学报, 2014, 34(1): 0127001.