arXiv:2303.01449v1 [quant-ph] 2 Mar 2023

快速门控单光子探测器辅助的100公里水下光纤量子密钥分发

Domenico Ribezzo，[1,2]Mujtaba Zahidy，[3]Gianmarco Lemmi，[1,2]Antoine Petitjean，[1]Claudia De Lazzari，[4] Ilaria Vagniluca，[4] Enrico Conca，[5] Alberto Tosi，[5] Tommaso Occhipinti，[4]Leif K. Oxenløwe，[6]André Xuereb，[7,8]Davide Bacco，[9, 4, *]和 Alessandro Zavatta[1,4,†][1]意大利国家研究委员会国家光学研究所（*CNR-INO*），*50125*，佛罗伦萨，意大利[2]那不勒斯费德里科二世大学，那不勒斯，意大利[3]硅光子光通信卓越中心（*SPOC*），丹麦技术大学电气与光子工程系，孔斯灵比，丹麦[4]*QTI S.r.l.*，*50125*，佛罗伦萨，意大利[5]米兰理工大学电子、信息与生物工程系，*20133*，米兰，意大利[6]硅光子光通信中心（*SPOC*），丹麦技术大学光子工程系，孔斯灵比，丹麦[7]马耳他大学物理系，姆西达 *MSD 2080*，马耳他[8]*Merqury Cybersecurity Limited*，马耳他[9]佛罗伦萨大学物理与天文系，*50019*，塞斯托菲奥伦蒂诺，意大利

如今，量子密钥分发是最成熟的量子技术，多个国家和私人机构都在建设自己的量子网络。然而，量子密钥分发设备距离成为人人都能使用的产品仍有很大差距。事实上，在与现有电信基础设施的兼容性方面存在限制，而且采用非低温探测系统时，秘密密钥率性能有限，这些问题仍然十分关键。在这项工作中，我们使用两种不同的单光子雪崩二极管（SPAD）探测器，实现了西西里岛（意大利）与马耳他之间的量子密钥分发链路。我们比较了标准商用 SPAD 的性能与新型快速门控系统级封装（SiP）SPAD 原型的表现；结果表明，在损耗为 20 分贝的信道上，SiP 探测器实现的密钥率是商用设备的十四倍。

I. 引言

量子密钥分发（QKD）是一种利用物理定律交换对称密码密钥的方法，也是第二次量子革命中涌现的技术里最成熟的一项 [1–4]。物理实验室中的多项实验以及现场试验链路均已展示了量子密钥分发的潜力和成熟度。如今，连接不同大陆城市的量子密钥分发链路已成为现实 [5, 6]，并应用于商业领域和政府部门。不过，要使量子密钥分发成为日常消费级技术，仍有许多挑战需要克服。一个重要且非常实际的例子是，必须构建便携、可扩展，并能确保长距离链路具有高密钥生成率的量子密钥分发设备。事实上，目前长距离链路密钥生成率的纪录是使用超导纳米线单光子探测器（SNSPDs）实现的 [5–8],；这类探测器具有极低的暗计数率和很高的量子效率。这项技术的主要缺点是其工作温度极低（低于 4 K），因此难以集成到可部署系统中。

相反，在室温或通过紧凑型冷却系统可达到的温度下工作的单光子雪崩二极管（SPAD），能够很好地集成到现有电信网络中。

在这项工作中，我们在地中海中部建立了一条量子密钥分发链路，通过一条长达 100 km 的光纤水下光信道连接意大利和马耳他。发射器位于意大利西西里岛波扎洛市的一家电信中心，接收器则设在马耳他马德利耶纳的 Melita Limited 数据中心。这条链路可视为欧洲量子网络建设中的新进展 [9], ，并被用于测试一款系统级封装（SiP）铟镓砷（InGaAs）单光子雪崩二极管（SPAD） [10]。该探测器配备专用的快速门控主动猝灭电路，可使其与锁定在量子态生成时钟上的门控信号同步 [11]。因此，它受暗计数和后脉冲的影响显著较小。此外，我们还将这款 SiP 探测器与一款商用标准铟镓砷单光子雪崩二极管（IDQuantique 的 ID221 [12]）进行了比较。在 20 分贝衰减链路上，新型 SPAD 的密钥率是商用器件的 14 倍。我们还通过模拟较短的链路预算，研究了该探测器的性能；结果表明，在信道损耗为 3 分贝时，SiP SPAD 仍可保证高达 25 kbit/s 的秘密密钥率。

最后，我们报告了在受控实验室条件下对探测器性能的比较。我们在比较中加入了第二个 SiP 探测器，它与第一个探测器相似，但传感器面积更大，适用于自由空间应用。

II. QKD 协议

所采用的协议是采用时间-bin编码和单诱骗态方法的三态高效BB84 [13–16]。在该协议中，一个基用于共享密钥，而

* davide.bacco@unifi.it
† alessandro.zavatta@ino.cnr.it

第二个基则用于安全检查。这种选择有助于简化装置，并且只需制备第二个互为无偏基中的两个本征态之一。密钥生成基是计算**Z**基；根据时间-bin编码，其本征态由脉冲在时隙帧中的发射时间表征。安全检查基**X**基的本征态由**Z**基的叠加态构成，相对相位为（0 或 π）。值得指出的是，即使光子波函数分布在两个脉冲中，每个态也应只包含至多一个光子；含有更多光子的态（即多光子态）会带来安全问题，应当避免。遗憾的是，多光子事件无法被彻底抑制，因此引入了诱骗态方法，以克服因缺少真正的单光子源而产生的漏洞 [17, 18]。该方法通过随机切换强度级别，有助于检测这样的窃听者：他们只截获并重发多光子态，同时阻断其余态，因此无法保持光子数统计稳定。研究已证明，两个不同的强度级别就足够了 [14], ，这一技术称为单诱骗态方法。

对于单诱骗态三态 BB84 协议，在有限密钥情形下，密钥长度l 受限于 [13]:

$$l \le s^{l}_{Z,0} + s^{l}_{Z,1}(1 - H_2(\phi^{u}_{Z})) - \lambda_{EC} - 6\log_2\left(\frac{19}{\varepsilon_{sec}}\right) - \log_2\left(\frac{2}{\varepsilon_{corr}}\right), \tag{1}$$

其中，$s^{l}_{Z,0}$ 和 $s^{l}_{Z,1}$ 分别是对真空事件和单光子事件的下界，ϕ^{u}_{Z} 是相位错误率的上界，λ_{EC} 是纠错阶段公开的比特数，$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ 表示二元熵，$\varepsilon_{sec} = 10^{-12}$和 $\varepsilon_{corr} = 10^{-12}$分别是保密性参数和正确性参数。$\varepsilon$ 参数定义如下 [19]:

$$P[S_A \neq S_B] < \varepsilon_{corr},$$
$$\mathbb{1}(S_A, S_B; Z, C) < \varepsilon_{sec},$$

其中，S_A 和 S_B 分别是 Alice 和 Bob 的筛选密钥，$P[x]$表示x的概率，$\mathbb{1}(\cdot)$表示一般的信息度量，Z 是潜在窃听者拥有的被窃听序列，C 是表示所交换信息的随机变量。第二项表示 ε_{sec} Alice 与 Eve 的字符串之间具有比 Alice 与 Bob 的字符串之间更强相关性的概率。在标准 BB84 中，**Z**基中的相位错误率 ϕ_Z 对应于**X**基中的比特错误率 δ_X；然而，由于在该协议中 Alice 仅在**X**基中发送一个态，ϕ_Z 无法直接测量，因此需要根据**X**基量子比特错误率 QBER_X [20]进行估计；它与接收端干涉仪的可见度 vis_X 通过 $\mathrm{QBER}_X = (1 - \mathrm{vis}_X)/2$相关联。

III. 实验装置

A. 网络架构与量子密钥分发设备

该链路由两条长达 96 km 的光纤构成，铺设于地中海海底，连接马耳他与西西里岛；该信道此前已用于演示 2018 [21] 中的纠缠分发。这两条光纤的衰减分别约为 20 分贝和 21 分贝，因此，我们将前者用于分发量子态，后者则用作服务信道（传输同步信号、估算参数等）。

实验装置如图1所示；编码状态的脉冲由现场可编程门阵列（FPGA）控制强度调制器，对连续波C波段激光器进行切割而生成；切割后，脉冲经可变光衰减器（VOA）衰减至单光子水平。有关发射器件的更多细节见 [22]。硅光子单光子雪崩二极管可接收门控触发信号，用户可以设置随后探测器的门控时间（开启和关闭时间）。

为获取可比数据，两个探测器的量子比特生成率均设定为 119 MHz。不过，该探测器可接受最高150 MHz的门控信号。

Alice和Bob选择相同的概率，在计算基（**Z**基）中生成和测量（$P_{ZA} = P_{ZB} = 0。5$）；对P_{ZA} 和P_{ZB} 的此类选择符合仿真模型，该模型考虑了信道特性和探测阶段的性能。

在服务信道上，两个部分之间共享两路经典信号：一路是频率为 145 kHz 的同步信号，另一路是频率为 119 MHz 的信号，用作探测器的门控信号。仿真模型中选择的每脉冲平均光子数使密钥率达到最大，相关数值见表II。

光子经过水下光纤信道后到达接收端装置；在此处，光子入射到一个 50:50 分束器上，该分束器用于被动基选择。**Z**基输出将光子直接送至一个单光子探测器（SPD），而**X**基输出则使光子先通过延迟线干涉仪（DLI），再到达探测部分。DLI 是一种马赫-曾德尔干涉仪，其中一臂比另一臂长 800 ps，因此，表征**X**基波函数态的两个脉冲会发生重叠，从而可以测量其相对相位。干涉仪由锁相环（PLL）稳定，锁相环通过调节移相器来补偿相位波动。该环路的反馈通过发送一束与量子信号反向传播的弱经典激光器，并监测其相位波动来实现。最后，对服务信道中传输的同步信号和门控信号进行解复用，并发送至相应模块。

B. 探测阶段

所使用的科研产品级SiP探测器是米兰理工大学（PoliMi）开发的先进 InGaAs/InP单光子雪崩二极管，设计用于实现低暗计数率、具有竞争力的光子探测效率以及较低的定时抖动。该探测器的主要特点是具备时间门控能力。传统门控电路通常采用简单的被动淬灭电路，无法在高

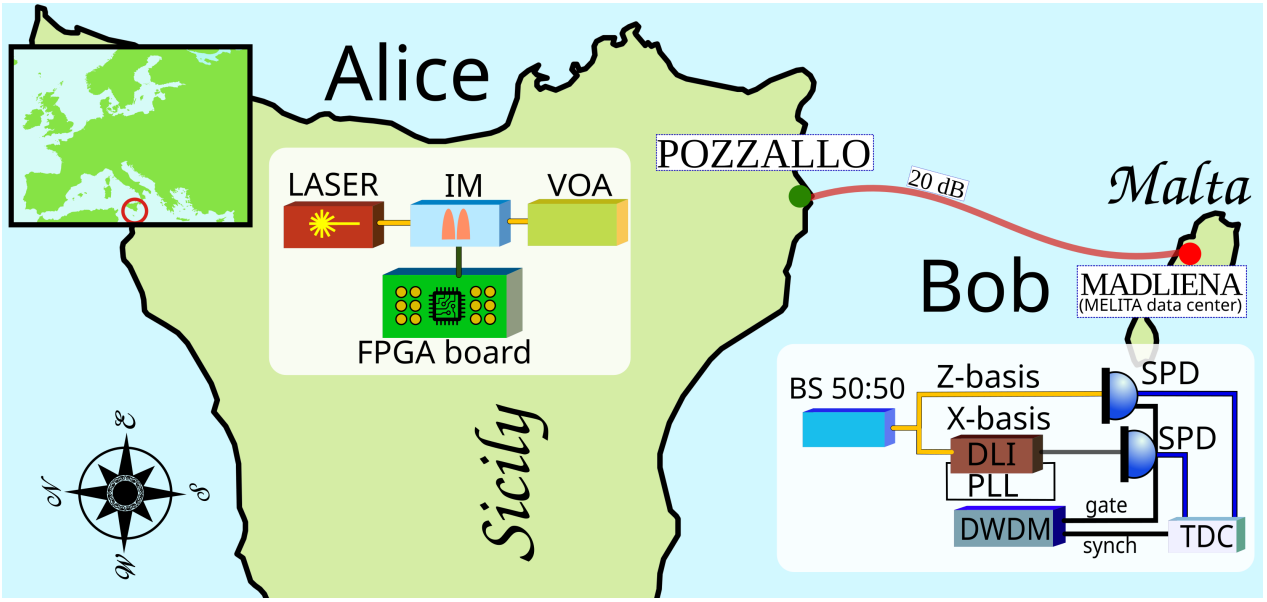


图 1. **装置示意图**。 Alice 通过对连续波激光器进行刻脉冲（强度调制器级——IM）和衰减（可变光衰减级——VOA）来产生量子态。Bob 使用分束器（BS 50:50）进行基选择，随后直接读取光子的到达时间（Z基），或使用延迟线干涉仪（DLI）进行干涉测量（X基）。第二根光纤用于传输同步信号和门控信号；这两种信号经密集波分复用器（DWDM）复用后再分离。单光子探测器连接到时间数字转换器（TDC），由其生成时间戳，供 Bob 的计算机处理。

	SiP PoliMi	ID221
τ_{off} (μ秒)	1	20
$\mathbf{r}_{\mathrm{DC}}$ (千赫)	10.8	2.5
n_Z	10^9	
$p_{Z,A}$	50%	
$p_{Z,B}$	50%	
ν_{rep} (兆赫)	119	
ε_{sec}	10^{-12}	
ε_{corr}	10^{-12}	
τ_Z (分贝)	1	
τ_X (分贝)	3	

表 I。**装置参数**。 τ_{off} 为探测器的保持关闭时间，$\mathbf{r}_{DC}$ 为暗计数率，n_Z 为块大小，$p_{Z,A}$ 以及 $p_{Z,B}$ 分别为 Alice 和 Bob 选择 Z 基的概率，ν_{rep} 为重复频率，ε_{sec} 和 ε_{corr} 为安全性和正确性参数，τ_Z 和 τ_X 为 Bob 在 Z 基和 X 基下的损耗。SiP PoliMi 探测器是感光面积直径为 10 μ米的 SiP PoliMi 探测器。

频率下进行门控，且需要较长的死区时间来抑制后脉冲效应（APE）。当雪崩过程中产生的载流子被俘获，并在一段时间后（对于工作在 220–240 K 的 InGaAs/InP SPAD，最长可达几微秒）随机释放时，就会发生 APE，从而引发二次雪崩，尽管并无真实光子入射到 SPAD 上。通过采用快速主动淬灭电路替代简单的被动淬灭电路，可大幅减少后脉冲。经测试的探测器采用了一种新开发的电路，可在最高 150 MHz 的频率下对探测器进行快速门控，导通时间短至数百皮秒。检测到光子后，该电路会为 SPAD 施加保持关闭时间，跳过可编程数量的门控周期，从而抑制后脉冲的影响 [11]。SPAD 的光敏区域直径约为 10 μ米，使其成为基于光纤的应用的理想选择。采用相同的光学装置，对另一款特性相同但感光面积更大的探测器（25 μ米）进行了测试。论文 [23] 详细介绍了该探测器，并准确表征了其在实验室条件下的具体规格。

IV. 结果

A. 现场试验

所述装置已用于建立从西西里岛到马耳他的 QKD 协议。我们使用 IDQuantique 的 ID221 探测器和所述 SiP 米兰理工大学 SPAD，进行了实验和数据采集。对于 ID221，为了将后脉冲控制在可管理的范围内，我们将保持关闭时间设为 $\tau_{\mathrm{off}} = 20\mu$ 秒。保持关闭功能会在每次探测事件后使 SPAD 关闭 τ_{off}，以清除有效面积中可能被俘获的载流子。对于快速门控探测器，由于后脉冲概率较低，我们能够将其设为 $\tau_{\mathrm{off}} = 1\mu$ 秒。

当保持关闭时间设置为 1 μs 时，SiP PoliMi 探测器的暗计数率高于商用 SPAD（10.8 kHz 对比 2.5 KHz）。然而，最大计数率 $CR_{\max} = 1/\tau_{\mathrm{off}}$ 使其能够探测到比商用 SPAD 更高的事件速率。需要注意的是，较高的 τ_{off}也会降低 SPAD 的饱和能力，从而限制其性能

	3 分贝	5 分贝	10 分贝	15 分贝	20 分贝
PoliMi 的单光子雪崩二极管					
μ_1	0.36	0.41	0.46	0.46	0.41
μ_2	0.16	0.16	0.16	0.16	0.16
μ_3			0		
$\varepsilon_Z(\%)$	0.7	0.8	1.1	1.8	4.6
$\varepsilon_X(\%)$	2.8	3.0	3.1	3.4	6.4
安全密钥率（千比特每秒）	24.65	21.75	13.10	5.80	1.50
ID221 单光子雪崩二极管					
μ_1	0.21	0.31	0.31	0.36	0.41
μ_2	0.06	0.11	0.11	0.16	0.16
μ_3			0		
5ttt$\varepsilon_Z(\%)$	4.4	4.4	5.0	6.0	9.3
$\varepsilon_X(\%)$	4	2.9	3.2	4.0	7.2
安全密钥率（千比特每秒）	3.25	3.05	2.10	1.05	0.11

表 II. **所选参数和测量值：** μ_1、μ_2 和 μ_3分别是根据诱骗态方法设定的每脉冲光子数，ε_Z 和 ε_X 分别是两个基中的量子比特错误率，最后，安全密钥率即为 SKR。各 μ 的选择概率经过优化，以使密钥率最大化。

阈值，导致探测效率降低。较低的 τ_{off}设置使 SiP PoliMi 探测器能够避免这种情况。

相比之下，ID221 在 $\tau_{\text{off}} = 1\mu$ 秒内的暗计数率约为 200 kHz。专门设计的淬灭电路能够管理快速门控信号，使 SiP PoliMi SPAD 在低 τ_{off}下的性能显著提升。

随后，为了评估探测器在不同信道损耗下的性能，我们在信道较短的区段上重复实验。为模拟这一情况，我们逐步提高输入功率，以补偿光子在不同信道长度上传输时遇到的损耗。这相当于将 Alice 的发射器放置在链路上相应的损耗补偿位置。

获得的安全密钥率列于表II，并显示于图2中。

B. 实验室测试

该探测器先后在受控实验室条件下进行了测试。另将感光面积直径为 25 μm 的第二个 SiP 探测器加入比较。由于更大的感光面积会带来更高的暗计数率，因此该探测器采用了 10 μs 的保持关闭时间。我们通过在 Alice 和 Bob 的装置之间加入可调衰减器，引入不同的信道损耗来进行测试。结果列于表III 和图3中。第二个 SiP PoliMi 探测器相比商用 SPAD 并未表现出显著改善。我们观察到，在信道损耗达到 15 分贝之前，安全密钥率有所小幅提升；然而，由于过量噪声和较低的信噪比（SNR），在更高的信道损耗下，安全密钥率降为零。最后，对具有较小有效面积的 SiP 探测器（直径为10 μm）在不同过偏压下进行了测试。提高过偏压可以提升探测器的效率，但也会增加后脉冲效应和暗计数率。测试结果显示

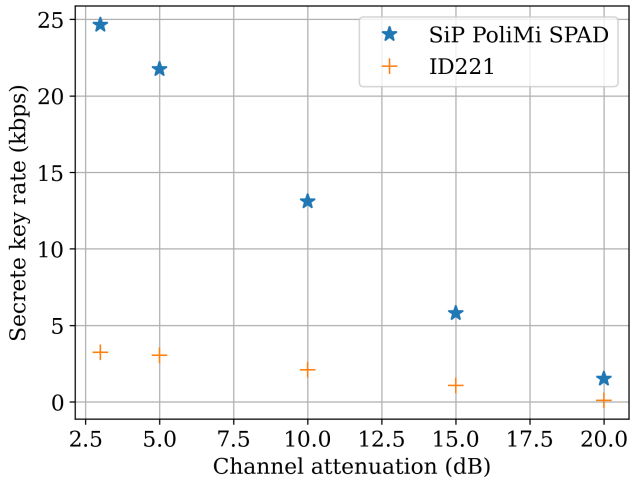


图 2. **密钥率结果（现场试验）**。该图展示了商用探测器（ID221）和由米兰理工大学研究团队制造并进行测试的 SiP 探测器（SiP Polimi SPAD）所实现的安全密钥率。得益于应用门控信号的快速淬灭电路，在衰减较小的链路中，SiP PoliMi SPAD 的密钥率是商用器件的七倍；考虑整个信道（20 分贝）时，密钥率最高可达商用器件的十四倍。

低信道损耗下性能有所提升，但随着过偏压增加，信噪比降低，性能也随之下降。

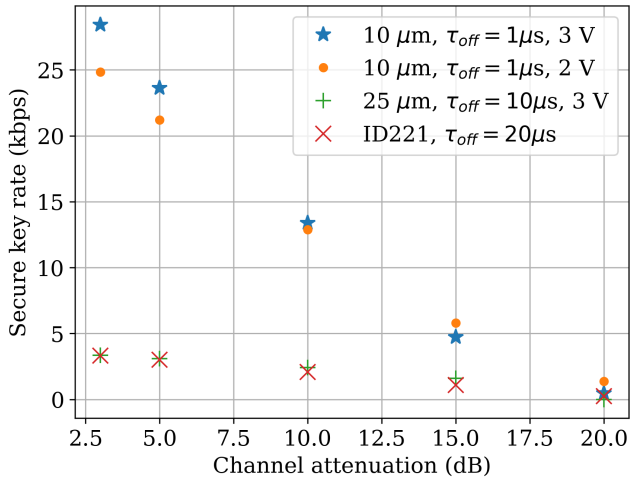


图 3. 在实验室条件下，使用不同探测器测得的密钥率随不同信道衰减值的变化。 10 μm 和 25 μm 是两款 SiP PoliMi SPAD，其数值对应于各自的光敏有效面积直径。所选探测器设置列于图例中（保持关闭时间、过偏压电压）。

3 分贝	5 分贝	10 分贝	15 分贝	20 分贝
10 μm 单光子雪崩二极管, 1 μs, 2V (千比特每秒)				
24.83	21.19	12.89	5.80	1.38
10 μm 单光子雪崩二极管, 1 μs, 3V (千比特每秒)				
28.42	23.62	13.39	4.72	0.47
25 μm 单光子雪崩二极管, 10 μs, 3V (千比特每秒)				
3.34	3.10	2.42	1.61	0
IDQ, 20 μs, 20% 探测效率 (千比特每秒)				
3.32	3.00	2.07	1.10	0.15

表III. 在实验室条件下，使用两台 SiP PoliMi 探测器测得的安全密钥率。感光面积为 10 μm 的探测器设置了 1 μs 的保持关闭时间，并在 2V 和 3V 过偏压下进行了测试。对于传感器面积为 25 μm 的探测器，设置参数为 10 μs 的保持关闭时间和 3V 过偏压。ID221 的保持关闭时间设为 20 μs，探测效率设为 20%。

V. 讨论

提升长距离链路上的密钥率，是广泛部署量子密钥分发技术的首要任务。许多新协议正在试验中，并展现出应用潜力：双场量子密钥分发 [24] 和高维协议 [25–29] 便是其中的几个例子。与此同时，随着超导纳米线单光子探测器 [30, 31] 和光子数分辨探测器 [32, 33] 的出现，探测阶段受到了广泛关注。尽管凭借便携性和成本效益，InGaAs/InP SPAD已成为C波段单光子探测最常用的技术，但与较新的技术相比，其在量子效率、死时间和定时抖动方面的性能有限。此外，它们还更容易受到暗计数和后脉冲现象的影响。

本文实现了两个欧洲国家之间的量子通信。尽管已有多项研究展示了规模有限的欧洲量子网络，但要实现全面部署，仍面临范围、成本等方面的诸多挑战 [22]。本研究提出了一种更具成本效益的方法，是迈向欧洲量子基础设施的又一步。

我们证明，在真实的量子密钥分发场景中，无需进行重大的技术替换，仅改进探测阶段，借助先进的传感器设计和主动淬灭电路实现，密钥率最高可提升 14 倍。

先进的新型内置淬灭电路结合自适应门控技术，通过将探测器的开启时间缩短至预期的光脉冲宽度，在提高探测率的同时，还能减小后脉冲的影响。得益于快速淬灭，门控频率最高可达 150 MHz，从而对最终密钥率作出显著贡献。相比之下，在旧技术中，必须采用较长的保持关闭时间来克服后脉冲的影响，而这反过来会降低探测率。此外，两个 SiP SPAD 均经过专门设计与制造，在本征暗计数、定时抖动和探测效率方面展现出业界领先的性能。

本文还根据感光面积的尺寸对性能进行了比较。第二个 SiP PoliMi 探测器配备直径为 25 μm 的有效面积，并采用类似的电路，其对暗计数和后脉冲表现出更高的敏感性。相比之下，新探测器产生的结果略优于商用探测器。需要注意的是，该 25 μm 探测器专为自由空间应用而设计，因为此类应用需要更大的感光面积。

我们的演示证明了新引入的探测器技术在降低每个安全比特的成本和提高最终密钥生成率方面的有效性，并将有助于让量子密钥分发成为用户更容易使用的技术。

VI. 致谢

本研究部分得到了卓越中心 SPOC（编号 DNRF123）、Innovationsfonden 项目 Fire-Q（编号 9090-00031B）、北约“科学促和平与安全”计划（资助编号 G5485，项目 SEQUEL）、Rita Levi Montalcini QOMUNE 计划（PGR19GKW5T）、欧盟“地平线 2020”研究与创新计划资助协议 No.731473 下的 EraNET联合资助倡议 QuantERA（项目 SQUARE）、由欧盟委员会通过数字欧洲计划资助、资助协议编号为 101091561 的 EQUO（欧洲量子生态系统）项目、由欧盟 NextGenerationEU 资助的意大利大学与研究部国家复苏与韧性计划下的 SER-ICS 项目（PE00000014），以及由意大利国家研究委员会（CNR）资助的“Progetti di Ricerca@CNR”计划下的 QuONTENT 项目支持。

[1] C. H. Bennett 和 G. Brassard，量子密码学：公钥分发与掷硬币，《理论计算机科学》**560**，7（2014），量子密码学的理论方面——纪念 BB84 诞生 30 周年。[2] H.-K. Lo、M. Curty 和 K. Tamaki，安全量子密钥分发，《自然·光子学》**8**，595（2014）。[3] F. Xu、X. Ma、Q. Zhang、H.-K. Lo 和 J.-W. Pan，采用现实器件的安全量子密钥分发，《现代物理评论》**92**，025002（2020）。

[4] V. Scarani、H. Bechmann-Pasquinucci、N. J. Cerf、M. Dušek、N. Lütkenhaus 和 M. Peev，《实用量子密钥分发的安全性》，《现代物理评论》**81**，1301（2009）。[5] S.-K. Liao、W.-Q. Cai、W.-Y. Liu、L. Zhang、Y. Li、J.-G. Ren、J. Yin、Q. Shen、Y. Cao、Z.-P. Li、F.-Z. Li、X.-W. Chen、L.- H. Sun、J.-J. Jia、J.-C. Wu、X.-J. Jiang、J.-F. Wang、Y.-M. Huang、Q. Wang、Y.-L. Zhou、L. Deng、T. Xi、L. Ma、T. Hu、Q. Zhang、Y.-A. Chen、N.-L. Liu、X.-B. Wang、Z.-C. Zhu、C.-Y. Lu、R. Shu、C.-Z. Peng、J.-Y. Wang 和 J.-W. Pan，《卫星到

地面量子密钥分发，《自然》549，43（2017）。[6] C.-Y. Lu、Y. Cao、C.-Z. Peng 和 J.-W. Pan，《墨子号的太空量子实验》，《现代物理评论》94，035001（2022）。[7] B. D. Lio、D. Bacco、D. Cozzolino、F. D. Ros、X. Guo、Y. Ding、Y. Sasaki、K. Aikawa、S. Miki、H. Terai、T. Yamashita、J. S. Neergaard-Nielsen、M. Galili、K. Rottwitt、U. L. Andersen、L. K. Oxenløwe 和 T. Morioka，《通过37芯光纤进行经典与量子联合传输，实现创纪录的秘密密钥率》，载于2018年IEEE光子学会议（IPC）（2018），第1–2页。[8] S. P. Neumann、A. Buchner、L. Bulla、M. Bohmann 和 R. Ursin，《通过跨国248 km光纤链路连续分发纠缠》，《自然·通讯》13，6134（2022）。[9]EuroQCI，《欧洲量子通信基础设施倡议》（2017），https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci。[10] F. Signorelli、F. Telesca、E. Conca、A. D. Frera、A. Ruggeri、A. Giudice 和 A. Tosi，《用于基于光纤和自由空间应用的低噪声InGaAs/InP单光子雪崩二极管》，《IEEE量子电子学精选主题期刊》28，1 2022( )。[11] A. Ruggeri、P. Ciccarella、F. Villa、F. Zappa 和 A. Tosi，《用于InGaAs/InP单光子雪崩二极管亚纳秒门控的集成电路》，《IEEE量子电子学期刊》51，1（2015）。[12] IDQuantique，Id221红外单光子探测器，https://www.idquantique.com/resources/id221/。[13] A. Boaron、G. Boso、D. Rusca、C. Vulliez、C. Autebert、M. Caloz、M. Perrenoud、G. Gras、F. Bussières、M.-J. Li、D. Nolan、A. Martin 和 H. Zbinden，《通过421 121 km光纤实现安全量子密钥分发》，《物理评论快报》190502（2018）。[14] D. Rusca、A. Boaron、F. Grünenfelder、A. Martin 和 H. Zbinden，《单诱骗态量子密钥分发协议的有限密钥分析》，《应用物理快报》112，171104（2018），https://doi.org/10.1063/1.5023340。[15] D. Rusca、A. Boaron、M. Curty、A. Martin 和 H. Zbinden，《简化版Bennett–Brassard 1984量子密钥分发协议的安全性证明》，《物理评论A》98，052336（2018）。[16] M. Hayashi 和 R. Nakayama，《有限密钥长度下采用Bennett–Brassard 1984协议的诱骗态方法安全性分析》，《新物理学杂志》16，063009（2014）。[17] W.-Y. Hwang，《高损耗条件下的量子密钥分发：迈向全球安全通信》，《物理评论快报》91，057901（2003）。[18] H.-K. Lo、X. Ma 和 K. Chen，《诱骗态量子密钥分发》，《物理评论快报》94，230504（2005）。[19] M. Canale，《量子信息安全的经典处理算法》，博士论文，信息工程系，帕多瓦大学（2014）。[20] A. Boaron、B. Korzh、R. Houlmann、G. Boso、C. C. W. Lim、A. Martin 和 H. Zbinden，《探测器设备无关量子密钥分发：安全性分析与快速实现》，《应用物理学杂志》120，063101（2016）。[21] S. Wengerowsky、S. K. Joshi、F. Steinlechner、H. Hübel 和 R. Ursin，《基于纠缠的波分复用量子通信网络》，《自然》564，225（2018）。[22] D. Ribezzo、M. Zahidy、I. Vagniluca、N. Biagi、S. Francesconi、T. Occhipinti、L. K. Oxenløwe、M. Lonˇcari´c、I. Cviti´c、M. Stipˇcevi´c、Z. Pušavec、R. Kaltenbaek、A. Ramšak、F. Cesa、G. Giorgetti、F. Scazza、A. Bassi、P. De Natale、F. S. Cataliotti、M. Inguscio、D. Bacco 和 A. Zavatta，《部署一个泛欧洲量子网络》，《先进量子技术》n/a，2200061（2022）。[23] A. Tosi、F. Acerbi、M. Anti 和 F. Zappa，具有低后脉冲和灵敏定时响应（尾部为 30 ps）的 InGaAs/InP 单光子雪崩二极管，《IEEE量子电子学杂志》48，1227（2012）。[24] M. Lucamarini、Z. L. Yuan、J. F. Dynes 和 A. J. Shields，《无需量子中继器突破量子密钥分发的速率–距离极限》，《自然》557，400（2018）。[25] H. Bechmann-Pasquinucci 和 W. Tittel，《使用更大字母表的量子密码学》，《物理评论A》61，062308（2000）。[26] I. Vagniluca、B. Da Lio、D. Rusca、D. Cozzolino、Y. Ding、H. Zbinden、A. Zavatta、L. K. Oxenløwe 和 D. Bacco，《面向实用高维量子密钥分发的高效时间-bin编码》，《物理评论应用》14，014051（2020）。[27] M. Zahidy、D. Ribezzo、C. D. Lazzari、I. Vagniluca、N. Biagi、T. Occhipinti、L. K. Oxenløwe、M. Galili、T. Hayashi、C. Antonelli、A. Mecozzi、A. Zavatta 和 D. Bacco，《基于已部署多芯光纤的 52 公里四维量子密钥分发协议》，载于《2022年欧洲光通信会议》（Optica出版集团，2022），第 Th3C.6 页。[28] B. Da Lio、D. Cozzolino、N. Biagi、Y. Ding、K. Rottwitt、A. Zavatta、D. Bacco 和 L. K. Oxenløwe，《通过 2 公里多芯光纤实现路径编码高维量子通信》，《npj量子信息》7，63（2021）。[29] D. Bacco、N. Biagi、I. Vagniluca、T. Hayashi、A. Mecozzi、C. Antonelli、L. K. Oxenløwe 和 A. Zavatta，《面向量子应用的已部署多芯光纤表征与稳定性测量》，《光子学研究》9，1992（2021）。[30] C. M. Natarajan、M. G. Tanner 和 R. H. Hadfield，《超导纳米线单光子探测器：物理原理与应用》，《超导体科学与技术》25，063001（2012）。[31] E. A. Dauler、M. E. Grein、A. J. Kerman、F. Marsili、S. Miki、S. W. Nam、M. D. Shaw、H. Terai、V. B. Verma 和 T. Yamashita，《超导纳米线单光子探测器系统设计方案及其已验证性能综述》，《光学工程》53，081907（2014）。[32] A. Divochiy、F. Marsili、D. Bitauld、A. Gaggero、R. Leoni、F. Mattioli、A. Korneev、V. Seleznev、N. Kaurova、O. Minaeva、G. Gol’tsman、K. G. Lagoudakis、M. Benkhaoul、F. Lévy 和 A. Fiore，《电信波长下的超导纳米线光子数分辨探测器》，《自然·光子学》2，302（2008）。[33] J. Provazník、L. Lachman、R. Filip 和 P. Marek，《光子数分辨探测器的基准测试》，《Optics Express》28，14839（2020）。