

专题: 量子信息处理

光子集成的量子密钥分发和量子随机数
生成器研究进展*于景春¹⁾²⁾ 芦文斌³⁾⁴⁾ 陈宾¹⁾²⁾ 杜永强¹⁾谢锋¹⁾ 李蔚^{3)4)†} 韦克金^{1)‡}

1) (广西大学物理科学与工程技术学院, 广西相对论天体物理重点实验室, 南宁 530004)

2) (广西大学计算机与电子信息学院, 南宁 530004)

3) (上海理工大学智能科技学院, 上海 200093)

4) (上海理工大学光子芯片研究院, 上海 200093)

(2025 年 6 月 18 日收到; 2025 年 7 月 17 日收到修改稿)

量子密钥分发凭借其信息理论层面上的无条件安全性及窃听可探测性等独特优势, 在金融、政务、国防等安全敏感领域展现出广阔的应用前景. 集成光子学技术通过将传统量子密钥分发系统的核心器件高密度集成于单一芯片, 显著提升了系统的小型化程度、成本效益与长期稳定性, 是实现量子密钥分发规模化工程应用的核心技术路径. 本文系统综述了近期基于不同材料平台与架构的光子集成量子密钥分发实验进展, 以及用于生成真随机数的集成量子随机数生成器的最新研究动态. 该综述旨在为未来芯片化量子保密通信技术的发展提供技术路线指引.

关键词: 量子密钥分发, 量子随机数, 集成光子学

PACS: 03.67.Hk, 03.67.-a, 42.82.-m

DOI: 10.7498/aps.74.20250791

CSTR: 32037.14.aps.74.20250791

1 引言

近年来, 量子计算领域呈现突破性发展^[1-4]. 量子计算是基于量子力学原理构建的新型计算架构, 不仅具有超越经典计算的并行处理能力, 其算力更随量子比特数目的增加呈指数级提升. 这一技术演进对基于大数分解、离散对数等数学难题构建的传统密码体系 (如对称加密与非对称加密^[5,6]) 构成严峻挑战.

量子密钥分发 (quantum key distribution, QKD)

是一种基于量子力学基本原理的密钥分发技术, 其安全性由量子态不可克隆原理与海森伯不确定性原理共同保障. 该技术通过物理层特征确保任何窃听行为必然扰动量子态并引入可检测误差, 结合安全认证协议可实现攻击的无条件探测, 从而在理论上提供可严格证明的通信机密性^[7]. 自 1984 年首个 QKD 协议的提出^[8] 及 1992 年首次 QKD 实验的实现^[9] 以来, 该领域历经 40 余年发展, 在协议设计、传输距离、成码速率及实用化集成等方面持续突破. 近期, Li 等^[10] 利用多像素超导纳米线单光子探测器 (SNSPD) 与硅基光子集成调制器, 在 10 km

* 国家自然科学基金 (批准号: 62171144, 62031024)、广西自然科学基金 (批准号: 2025GXNSFAA069137, GXR-1BGQ2424005) 和广西研究生教育创新计划项目 (批准号: YCBZ2024002) 资助的课题.

† 通信作者. E-mail: weil@usst.edu.cn

‡ 通信作者. E-mail: kjwei@gxu.edu.cn

光纤信道中实现了 115.8 Mbit/s 的安全成码率,刷新世界纪录;与此同时,我国基于“济南一号”微纳卫星平台,在国际上首次完成了单轨实时量子密钥分发,并与相距 12900 km 的南非的地面站间实现了密钥生成以及“一次一密”加密传输^[11]. 这些里程碑进展标志着 QKD 技术正从原理验证阶段向高鲁棒性系统构建阶段加速迈进.

尽管 QKD 技术在传输距离与密钥速率等核心指标上取得了显著突破^[12-14],但其大规模工程化应用仍面临显著挑战. 当前,开发兼具小型化、低成本、高稳定性且可大规模部署的高性能 QKD 终端,是该领域亟需攻克的关键技术瓶颈^[15,16]. 值得注意的是,集成光子学为实现这一目标提供了颠覆性的技术路径. 该技术通过将核心光学器件(如光源、调制器、探测器)与驱动控制电路高密度地集成于单一芯片上,能够从根本上减小设备体积、降低大规模制造成本,同时显著增强系统的长期运行稳定性与鲁棒性. 近年来,光子集成的 QKD 技术已发展成为量子保密通信领域最具活力的前沿研究方向,其技术突破对于加速 QKD 系统的实用化进程具有变革性意义.

量子随机数生成器 (quantum random number generator, QRNG) 是量子保密通信系统中不可或缺的安全熵源. QRNG 通过利用量子物理固有的不可预测性生成真随机数,其安全性与随机性远超依赖确定性算法的传统伪随机数生成器. QRNG 的安全性根植于量子力学基本原理,其输出序列具备不可预测性、无偏性及不可复制性等核心特性. 依据物理熵源的差异,主流的 QRNG 技术路线主要包括:基于真空量子涨落的方案^[17,18]、基于单光子路径随机性的方案^[19,20]、基于光子到达时间测量不确定性的方案^[21,22]以及基于自发辐射光子的方案^[23,24]. 其核心性能指标涵盖实时生成速率(如 > 100 Gbit/s)、最小熵以及抗环境干扰的鲁棒性. 随着 QKD 系统向芯片化、集成化方向快速演进,开发与之深度兼容的微型化集成 QRNG 芯片,已成为突破 QKD 系统在功耗、成本与兼容性等方面瓶颈的关键路径. 近年来,基于硅基^[25]和磷化铟^[26]等材料平台的单片集成 QRNG 模块研究进展显著,已实现从理论验证到原型系统的跨越.

本文将重点回顾近期(2022 年—2025 年)光子集成 QKD 在不同材料平台与架构上的实验进展和集成 QRNG 的最新研究动态,旨在为该快速发

展领域提供一份及时更新的系统性综述. 更早的文献综述可参考文献^[16,27,28]. 首先,本文系统对比分析了主流集成光子学平台的关键特性;在此基础上,全面梳理并评述了光子集成 QKD 技术的最新研究进展,重点聚焦离散变量 (discrete variable, DV) 与连续变量 (continuous variable, CV) 两大技术路线的系统级实验验证案例及其性能对比. 随后,探讨了片上集成 QRNG 的技术路线,重点分析基于不同物理熵源的实现方案. 最后,总结了集成光子学平台的优势及其在 QKD 系统中的应用,并对实现芯片化、高鲁棒性集成 QKD 系统和高性能、高集成度 QRNG 的核心技术路线进行了前瞻性展望.

2 集成光量子平台

现阶段光子集成 QKD 的研究主要集中在利用成熟的微纳加工技术,将光源、编码器、解调器和探测器等核心器件集成于单一芯片上. 主流的集成光子学平台包括硅基 (SOI)、磷化铟 (InP)、薄膜铌酸锂 (TFLN) 和氮化硅 (Si_3N_4).

SOI 平台^[29,30]凭借硅材料固有的高折射率差 ($\Delta n \approx 2.0$),可实现亚微米尺度的光波导与高度微型化的功能器件,具备显著的高集成密度优势. 该平台与成熟的互补金属氧化物半导体 (CMOS) 工艺高度兼容,支持大规模、低成本、高良率的芯片制造,是发展面向大规模网络部署的集成化 QKD 系统的关键技术平台. SOI 集成光子学平台卓越的 CMOS 工艺兼容性允许将光学编码单元与电子驱动电路进行单片集成,利用载流子注入 (或耗尽) 型调制器实现超过 GHz 速率的高速量子态制备^[31],为构建集成化、可规模化部署的 QKD 系统提供了切实可行的技术路径. 然而,硅作为间接带隙半导体材料,无法实现高效片上光源集成. 因此,发展集成光源、调制器及驱动电子学的单片集成 QKD 发射芯片,是当前该平台研究的核心挑战与热点.

区别于硅基材料,InP 等 III-V 族化合物半导体具有直接带隙特性,更适于发展高性能集成激光光源. 同时,得益于其非中心对称的晶体结构,在外加电场作用下可通过线性电光效应 (普克尔斯效应) 实现折射率的精确调控,从而完成对光信号相位、幅度的高速调制. InP 的电光系数分量 $r_{41} \approx 1.34$ pm/V (@1550 nm),可以实现调制速率超过

40 GHz 的高速电光调制器. 此外, 其折射率调制主要受控于外电场, 几乎不引入载流子相关的扰动, 可实现近零啁啾调制. 这些性能优势使其在高速率 QKD 系统的精密相位/强度编码方案中具有重要价值. 目前已经有研究人员通过 InP 平台^[32-34]将激光器、高速电光调制器进行单片集成, 为实现高度小型化、高性能的 QKD 发射端芯片提供了极具前景的技术解决方案.

尽管 SOI 和 InP 平台在构建高性能集成化 QKD 系统方面展现出显著优势, 但两者均存在一定局限性: SOI 平台受限于光源集成难题; 同时 SOI 平台和 InP 波导均有相对较高的传输损耗及其调制器通常所需的较高半波电压 ($V_\pi > 4$ V), 在一定程度上制约了集成化 QKD 系统性能的进一步提升. 在此背景下, TFLN 平台^[35,36]因其卓越的线性电光特性 (Pockels 系数 $r_{33} \approx 30$ pm/V) 被认为是高性能电光调制器的重要材料平台. 基于 TFLN 平台, 目前已成功实现了兼具高速 (调制带宽 > 100 GHz)、低半波电压 ($V_\pi < 3$ V) 和低传播损耗 (典型值低于 0.5 dB/cm) 特性的电光调制器. 结合其优异的集成潜力, TFLN 为构建高速、稳定、紧凑且实用的 QKD 编码模块提供了关键硬件基础. 此外, TFLN 平台在实现片上集成纠缠源 (如基于自发参量下转换过程) 以及集成 SNSPD^[37]方面也展现出显著潜力. 当前, TFLN 在晶圆级薄膜制备、键合与微纳加工技术方面进展迅速, 如何开发高良率、低成本的大规模生产工艺是该平台走向广泛应用的核心挑战与研究焦点.

相较而言, Si_3N_4 集成光子学平台^[38-40]在 1550 nm 通信波段展现出低于 0.1 dB/cm 的超低传播损耗, 可显著降低光信号在波导中的传输衰减. 其宽光谱透明性 (覆盖可见光至近红外波段) 使其能够同时兼容 780 nm (自由空间 QKD) 和 1550 nm (光纤 QKD) 双工作波长. 这些优异的光学特性使得 Si_3N_4 平台特别适合发展低损耗的 QKD 接收端芯片, 以提高系统的量子态探测效率^[41,42]. 然而, 该平台的主要挑战在于如何通过异质集成技术, 将高性能的单光子探测器 (如 SNSPD 或 InGaAs 探测器) 与基于 Si_3N_4 的解码单元高效集成, 从而构建功能完备的全集成 QKD 接收端. 克服这一异质集成难题, 实现高探测效率、低暗计数、低时间抖动探测器与低损耗光子回路的协同优化, 是当前该平台研究的重点与热点方向.

表 1 对比了目前主流的集成光子学平台, 分别从折射率、透明窗口、传输损耗、工艺成熟度、光源集成能力、探测器集成能力、调制器性能维度, 系统对比了上述平台的特性. 表中使用符号 (★) 对不同平台在各指标上的表现进行定性评价, 符号数量越多表示该平台在该特性上的性能越优.

表 1 集成光子学平台的比较

Table 1. Comparison of integrated optical quantum platforms.

对比维度	SOI	InP	TFLN	Si_3N_4
折射率 (1550 nm)	~3.48	~3.2	~2.2	~2.0
透明窗口 / μm	1.1—8.0	0.9—1.7	0.4—5.0	0.25—6.00
传输损耗	★★★	★★	★★★★★	★★★★★
工艺成熟度	★★★★★	★★★	★★	★★★
光源	★★★	★★★★★	★★★	★
探测器	★★★	★★★★★	★★★	★★★
调制器	★★★	★★★★★	★★★★★	★★

3 QKD 系统验证

基于上述集成光子学平台在 QKD 领域展现出的技术优势, 近年来, 不同研究团队致力于推动 QKD 系统中的核心器件 (包括光学与电子器件) 向集成化、芯片化方向发展. 本节将围绕不同材料平台的 QKD 演示实验展开综述, 表 2 和表 3 分别按时间顺序汇总了近 4 年 DV-QKD 和 CV-QKD 的代表性研究成果. 其中, 上标“a”表示该数值为基于文献及数据图提取的估计值, 符号“√”表示该器件实现芯片集成, “×”则表示没有实现芯片集成.

3.1 离散变量量子密钥分发 (DV-QKD)

在 DV-QKD 系统中, 密钥信息被编码于单光子的离散自由度 (如偏振、相位或路径) 上, 并通过单光子探测技术进行解码. 目前, 基于传统分立光纤光学器件的 DV-QKD 系统已成功实现千公里级光纤传输^[13], 及天地一体化卫星量子通信网络.

基于前期偏振编码 QKD 系统被广泛的部署在现有网络中, 同时兼容卫星 QKD 平台, 研究人员率先实现了基于硅基光子学平台的偏振编码 QKD 的片上编码器, 并通过实验验证了其在构建高速、稳定且可扩展 QKD 系统方面的潜力^[58-60]. 受限于当时芯片与器件技术水平, 这些集成 QKD 系统通

表 2 基于不同平台集成 DV-QKD 系统
Table 2. Integrate DV-QKD system based on different platforms.

文献	工艺	器件				编码方式	协议	重复频率 /MHz	传输损耗 /dB	平均速率 /kbps
		光源	编码	解调	探测					
[43]	SI	×	✓	×	×	偏振编码	BB84	312.5	20 ^a	42.7
[44]	Si ₃ N ₄	✓	✓	✓	✓	时间戳-相位编码	BB84	3350	10	12170
[45]	Si ₃ N ₄ /InP	×	✓	✓	×	时间戳-相位编码	BB84	1000	9.3	2370
[10]	SI	✓	✓	×	×	偏振编码	BB84	2500	2.2	115800
[46]	SI	×	✓	✓	×	偏振编码	BB84	50	18.857	0.24
[47]	SI	×	✓	✓	×	偏振编码	BB84	50	28.992	0.866
[48]	SI	✓	✓	✓	×	时间戳-相位编码	BB84	2500	39.5	9.4
[49]	TFLN	×	✓	✓	×	时间戳-相位编码	BB84	2500	4.1	1.1×10 ⁴
[50]	TFLN	×	✓	✓	×	时间戳-相位编码/相位编码	BB84	10	6.43	0.77

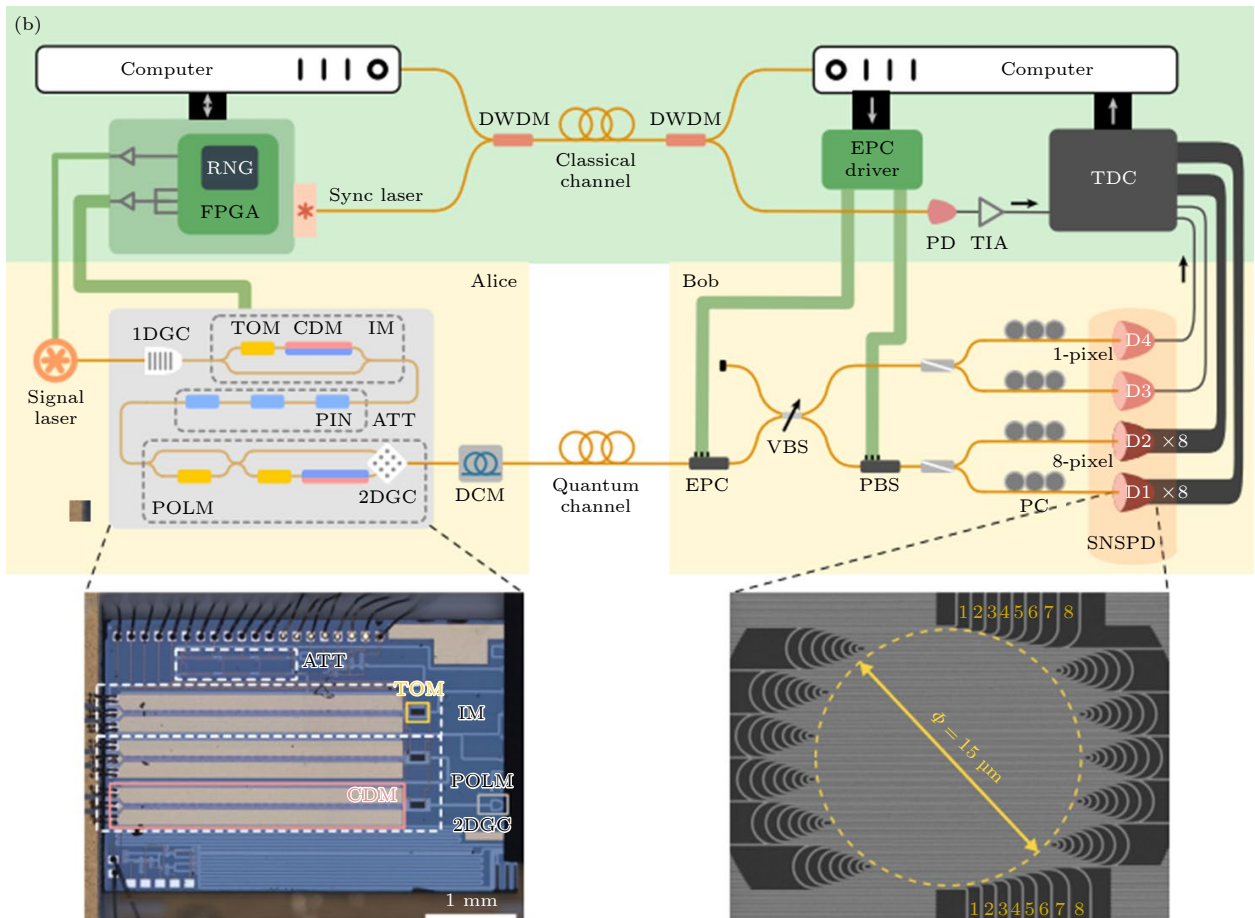
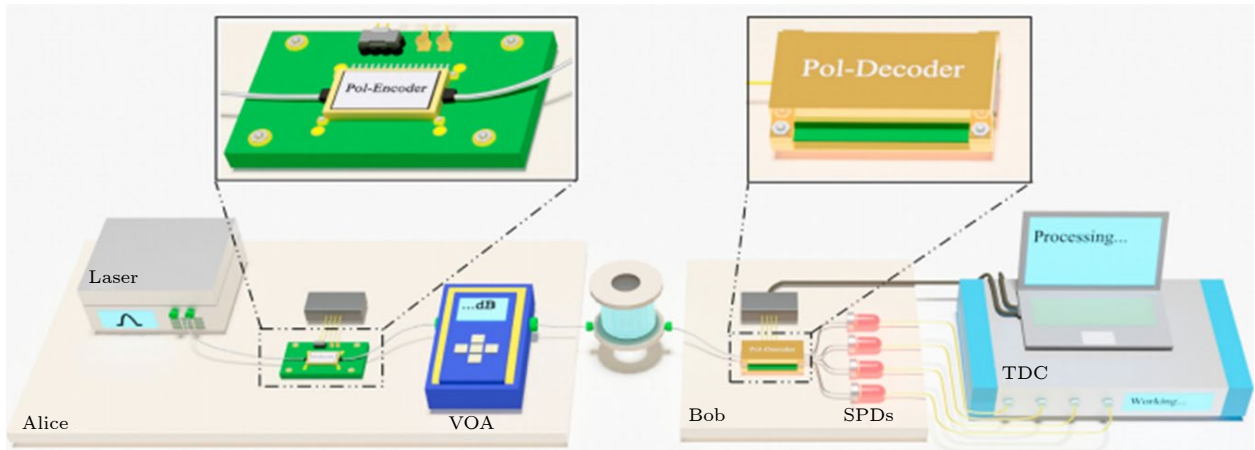
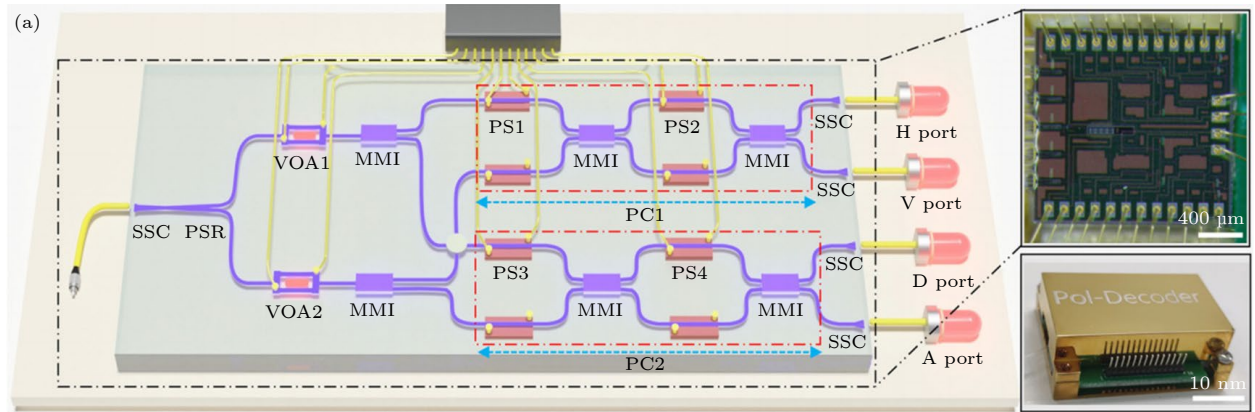
表 3 基于不同平台集成的 CV-QKD 系统
Table 3. Integrate CV-QKD system based on different platforms.

文献	工艺	器件				编码方式	协议	重复频率/ MHz	传输损耗/dB	平均速率/kbps
		光源	编码	解调	探测					
[51]	InP/Si ₃ N ₄	✓	×	×	✓	相位编码	GG02	250	10 ^a	750
[52]	SI	×	×	✓	×	相位编码	GG02	1000	5.72 ^a	1380
[53]	SI	×	×	✓	✓	相位编码	GG02	100	4.6	220
[54]	InP	✓	✓	×	×	相位编码	GG02	16	2.04	78
[55]	SI	×	✓	✓	✓	相位编码	DM CV-QKD	10000	2 ^a	3.51×10 ⁵
[56]	SI	×	✓	✓	✓	相位编码	DM CV-QKD	16000	4 ^a	2.46×10 ⁵
[57]	SI	×	✓	✓	✓	偏振编码/相位编码	DM CV-QKD	20000	1.98	1.213×10 ⁶

常依赖外部传统光学组件进行解码,或需采用片外设备进行量子信道偏振补偿.为攻克这一技术瓶颈,Du 等^[46]创新性地提出了一种“偏振-路径转换”的芯片架构,在硅基平台上实现了具备实时偏振追踪能力的硅基偏振解码器,如图 1(a)所示.该团队通过实验验证了该芯片的稳定性及其对光纤偏振漂移的有效补偿能力,最终在 100 km 光纤链路上实现了 240 bit/s 的安全密钥率.基于此突破,Wei 等^[47]进一步融合硅基偏振编解码器芯片,发展了基于量子比特的异地时钟同步与偏振补偿技术,提出了一种资源节约型的芯片级 QKD 方案.该方案无需额外设备,直接利用芯片制备和测量 BB84 协议所需的 4 种偏振态即可完成异地时钟同步与偏振补偿,在 150 km 商用光纤链路上实现了 866 bit/s 密钥率,为低成本、晶圆级制造 QKD 系统奠定了重要基础.

同时集成 QKD 系统在高速方面也有重要突破.其中,Li 等^[10]取得了显著进展:他们开发了片上高速(系统重频达 2.5 GHz)、高保真度偏振态调制技术(量子比特误码率<0.35%);结合尤立星团队^[10]

研制的八像素 SNSPD,实现了高计数率(在 5.5×10^9 光子/秒入射时)下仍保持 62% 探测效率的单光子探测,如图 1(b)所示.基于上述核心技术突破,该团队在 10 km 标准光纤信道下实现了创纪录的 115.8 Mbit/s 安全密钥率,较此前最高水平提升约一个数量级.同年,Sax 等^[48]提出了一种支持相位编码、时钟频率达 2.5 GHz 的高速集成 QKD 系统,如图 1(c)所示.该系统发射端采用硅光子芯片与外部二极管激光器融合方案;接收端则利用飞秒激光微加工技术制备了低损耗二氧化硅光子集成电路,并外接两个单光子探测器.最终在 202 km 光纤链路上实现了 9.4 kbit/s 的安全密钥率.近期,Lin 等^[49]基于 TFLN 光子集成平台,设计并实现了双偏振时间相位编解码全集成 QKD 系统.在 2.5 GHz 重频、25 km 传输距离下,安全成码率高达 11 Mbit/s.Heo 等^[50]进一步验证了 TFLN 平台相位编码 QKD 芯片的实用性,将其部署于 32.16 km 城域实地光纤链路,实现了 770 bit/s 安全密钥率,证明了集成 QKD 器件在实际复杂环境中的鲁棒性.



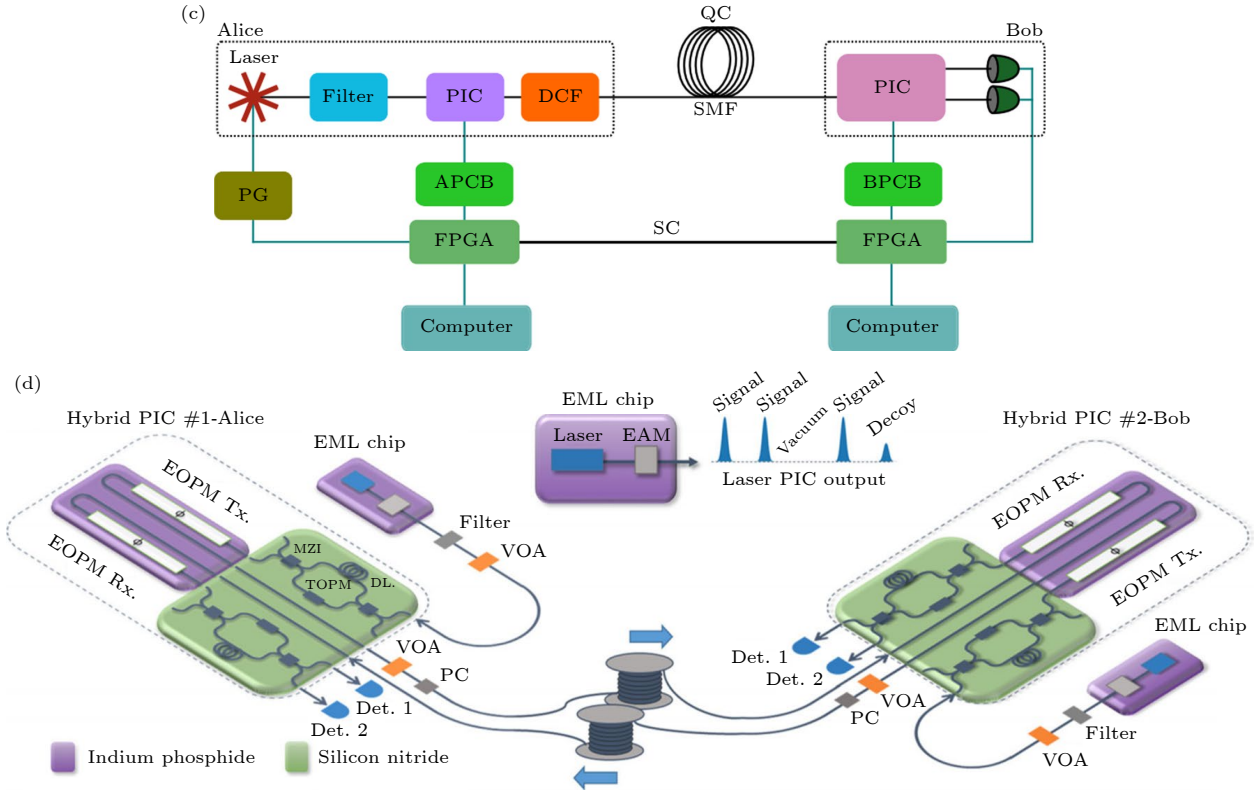


图 1 集成 DV-QKD 系统示意图 (a) 基于硅光子平台的“偏振-路径转换”芯片结构示意图^[46]; (b) 基于多像素 SPSPD 的高速 QKD 系统架构图^[10]; (c) 2.5 GHz 集成 QKD 系统架构图^[48]; (d) 混合集成收发芯片的实验装置图^[45]

Fig. 1. Schematic diagram of integrated DV-QKD systems: (a) “Polarization-path conversion” based on silicon photonics platform^[46]; (b) architecture diagram of high-speed QKD system based on multi-pixel SPSPD^[10]; (c) 2.5 GHz integrated QKD system architecture diagram^[48]; (d) experimental setup diagram of hybrid integrated transceiver chip^[45].

与此同时, 全集成 QKD 系统的研究正通过硅基光电子集成与异质集成技术持续推进. Zhu 等^[43] 基于硅基光电子集成技术开发了小型化硅基发射器芯片, 在 100 km 标准光纤中实现了 42.7 kbit/s 的安全密钥率, 验证了基于集成光电器件 QKD 系统的可行性, 为 CMOS 兼容的 QKD 设备开发奠定了基础. 为克服单一材料平台实现全集成 QKD 的局限性, Dolphin 等^[45] 采用混合集成策略, 将超低损耗 Si_3N_4 波导与 InP 高速电光调制器集成, 研制出 GHz 调制速率的低损耗相位编码 QKD 收发器芯片, 如图 1(d) 所示. 结合外部 InP 激光器芯片, 在 10 dB 信道衰减下实现了 1.82 Mbit/s 安全密钥率. Beutel 等^[44] 则聚焦接收端集成, 基于 Si_3N_4 平台实现了全集成的四通道波分复用型 QKD 接收芯片, 并成功集成 SNSPD. 该系统在 10 dB 信道衰减下实现了高达 12.17 Mbit/s 的密钥率, 标志着全集成接收芯片技术的重大突破.

3.2 连续变量量子密钥分发 (CV-QKD)

CV-QKD 将密钥信息编码于光场量子态的正

交分量上, 并通过相干检测进行解码. 其核心优势在于与现有光通信基础设施的高度兼容性. 近年来, CV-QKD 在协议设计、安全性分析及系统实现方面取得了显著进展, 已成功实现高速安全密钥产生 (如 190 Mbit/s^[61]) 和城域网应用探索^[62].

与 DV-QKD 类似, 面向大规模部署的实用化 CV-QKD 系统同样依赖于光学芯片集成技术以实现小型化、低成本和高稳定性. 该领域的里程碑工作由 Zhang 等^[63] 于 2019 年首次完成. 该团队基于硅基光子平台, 研制了全集成的 CV-QKD 发射器与接收器芯片, 集成了相位调制器、强度调制器、可变光衰减器及零差探测器等关键功能单元, 如图 2 所示. 利用该集成系统, 研究者在 100 km 光纤传输距离下实现了 140 bit/s 的安全密钥率. 这项成果为集成 CV-QKD 系统奠定了坚实基础.

基于本地本振 (LLO) 方案的 CV-QKD 系统展现出解决长距离传输挑战的潜力: 该方案能够保证量子信号在长距离传输后实现量子噪声极限探测, 并通过物理隔离的本振光有效抑制信号串扰, 从而

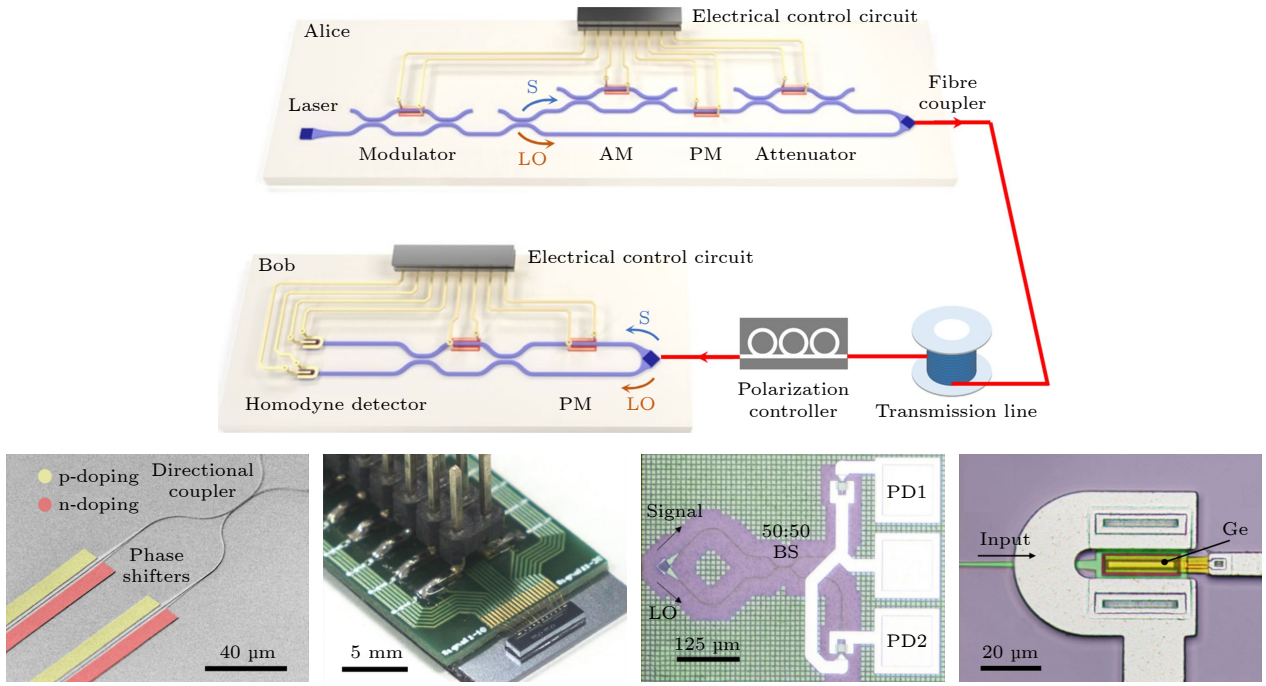


图 2 基于硅光子平台的集成 CV-QKD 系统示意图及该集成芯片的电子显微镜和光学显微镜图像^[63]

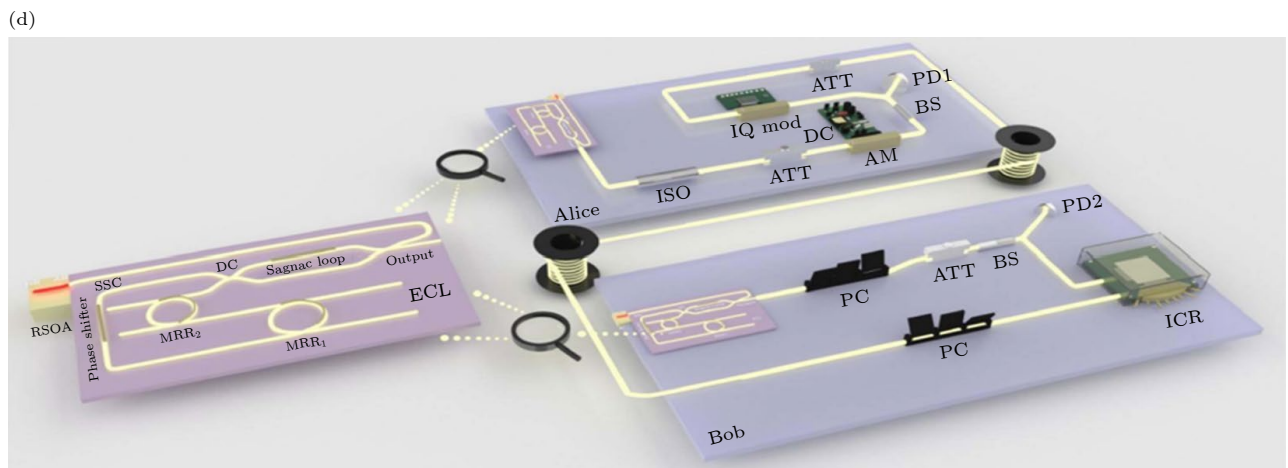
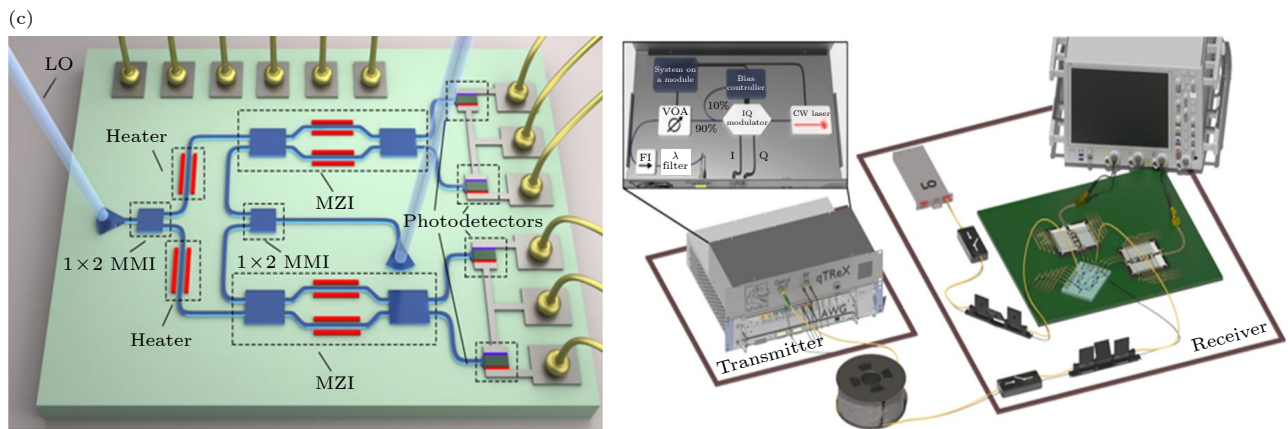
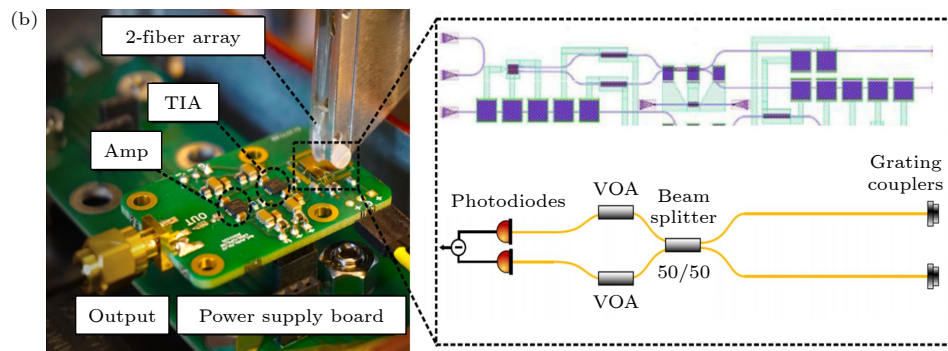
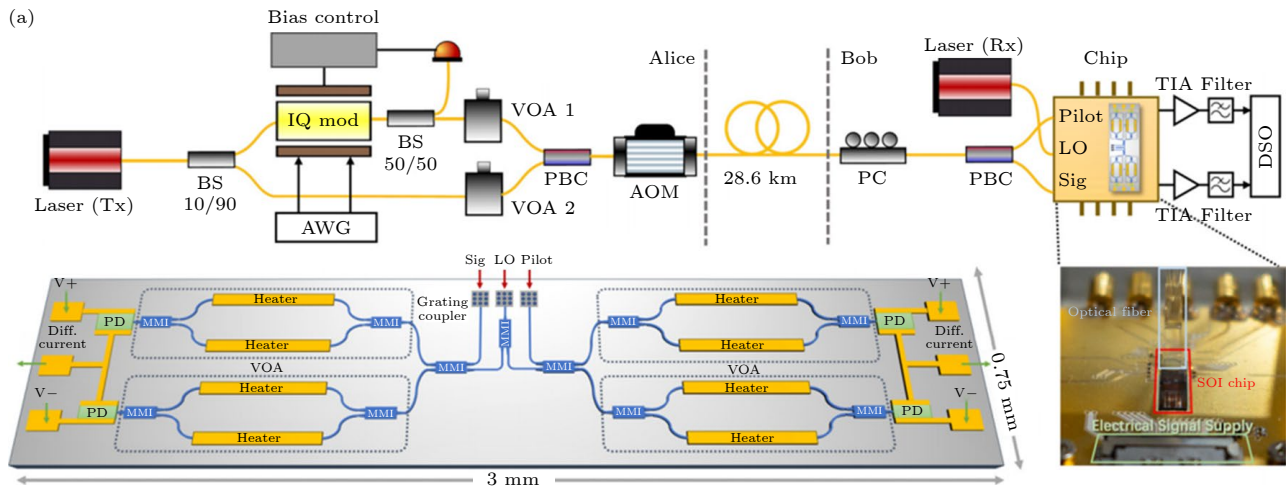
Fig. 2. Schematic diagram of the integrated CV-QKD system based on the silicon photonics platform and electron microscope and optical microscope images of the integrated chip^[63].

实现高性能、长距离的安全密钥分发. 因此, LLO 方案已成为当前集成 CV-QKD 系统研究的重点方向之一. Bian 等^[52] 基于标准绝缘体上硅光子集成平台, 开发了一款 LLO 方案的 CV-QKD 接收器芯片 (尺寸: $3\text{ mm} \times 0.75\text{ mm}$), 如图 3(a) 所示. 在 28.6 km 光纤链路上, 该芯片实现了 1.38 Mbit/s 的渐进密钥率, 显著推动了集成 CV-QKD 系统在较长通信距离下实现高密钥速率的研究进程. 随后, Piétri 等^[53] 也报道了一种硅基集成 CV-QKD 接收器芯片. 该接收器由光子芯片 (包含采用硅锗工艺制造的平衡零差探测器) 与信号放大电路构成, 如图 3(b) 所示. 在 10 km 和 23 km 距离的仿真实验中, 渐进密钥率分别达到 2.4 Mbit/s 和 0.22 Mbit/s, 这证明了该方案在实现高速、安全通信的全集成设备方面具有潜力.

为突破集成 CV-QKD 接收器带宽限制、实现更高安全密钥率, Hajomer 等^[55] 提出并实现了一种高性能硅光子集成 CV-QKD 接收器芯片, 如图 3(c) 所示. 该系统采用高带宽集成器件和低噪声设计, 成功在 20 GHz 检测速率下观测到散粒噪声极限特性. 基于此接收器, 在 10 GBaud 符号速率、5 km 光纤距离下实现了 737 Mbit/s 的渐进密钥率, 在 10 km 距离下密钥率可达 315 Mbit/s. 一年

后, Hajomer 等^[56] 进一步优化系统, 在 16 GBaud 符号速率、20 km 光纤链路条件下, 将渐进密钥率与有限长密钥率分别提升至 289 Mbit/s 与 246 Mbit/s. Ng 等^[57] 提出了一种基于硅基集成的 CV-QKD 收发系统, 除激光源外, 所有核心光学组件均实现芯片级集成. 其中发射端采用双偏振复用架构, 通过偏振正交信道并行传输, 将符号率有效提升至 40 GBaud/s (等效 20 GBaud/s per polarization). 接收端结合宽带平衡零差探测器与实时数字信号处理技术 (集成色散补偿、导频辅助载波相位恢复等算法), 支持 40 GBaud/s 超高速量子态测量. 实验基于离散调制 CV-QKD 协议, 在 10 km 光纤链路上实现了高达 1.213 Gbit/s 的密钥速率. 这一系列成果标志着基于光子集成的 CV-QKD 系统向可扩展、经济高效及大规模部署的量子安全通信网络迈出了关键一步.

尽管上述工作在高速率、远距离集成 CV-QKD 方面取得了显著进展, 片上高性能量子光源的实现仍面临重大挑战. 特别是基于 LLO 的 CV-QKD 方案, 对片上光源提出了更高要求, 亟需同时满足高频率调谐性、高输出功率及窄线宽等关键特性. 近期, Li 等^[51] 在此方向取得突破: 通过片上集成 III-V 族激光器与低损耗 Si_3N_4 微腔耦合, 如图 3(d)



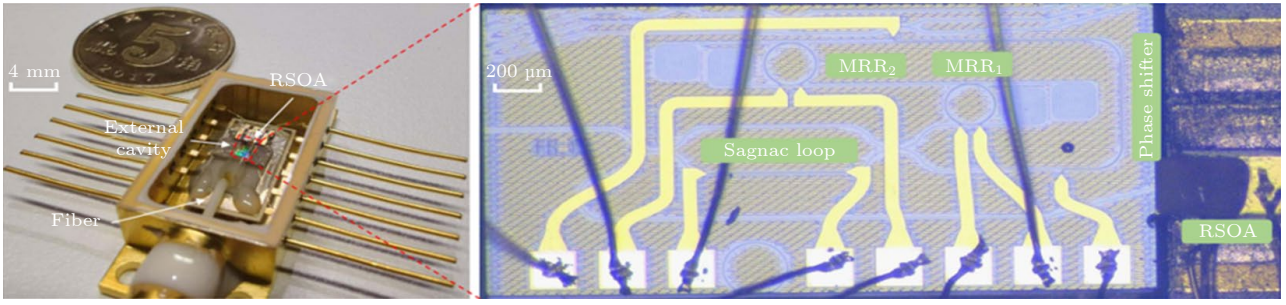
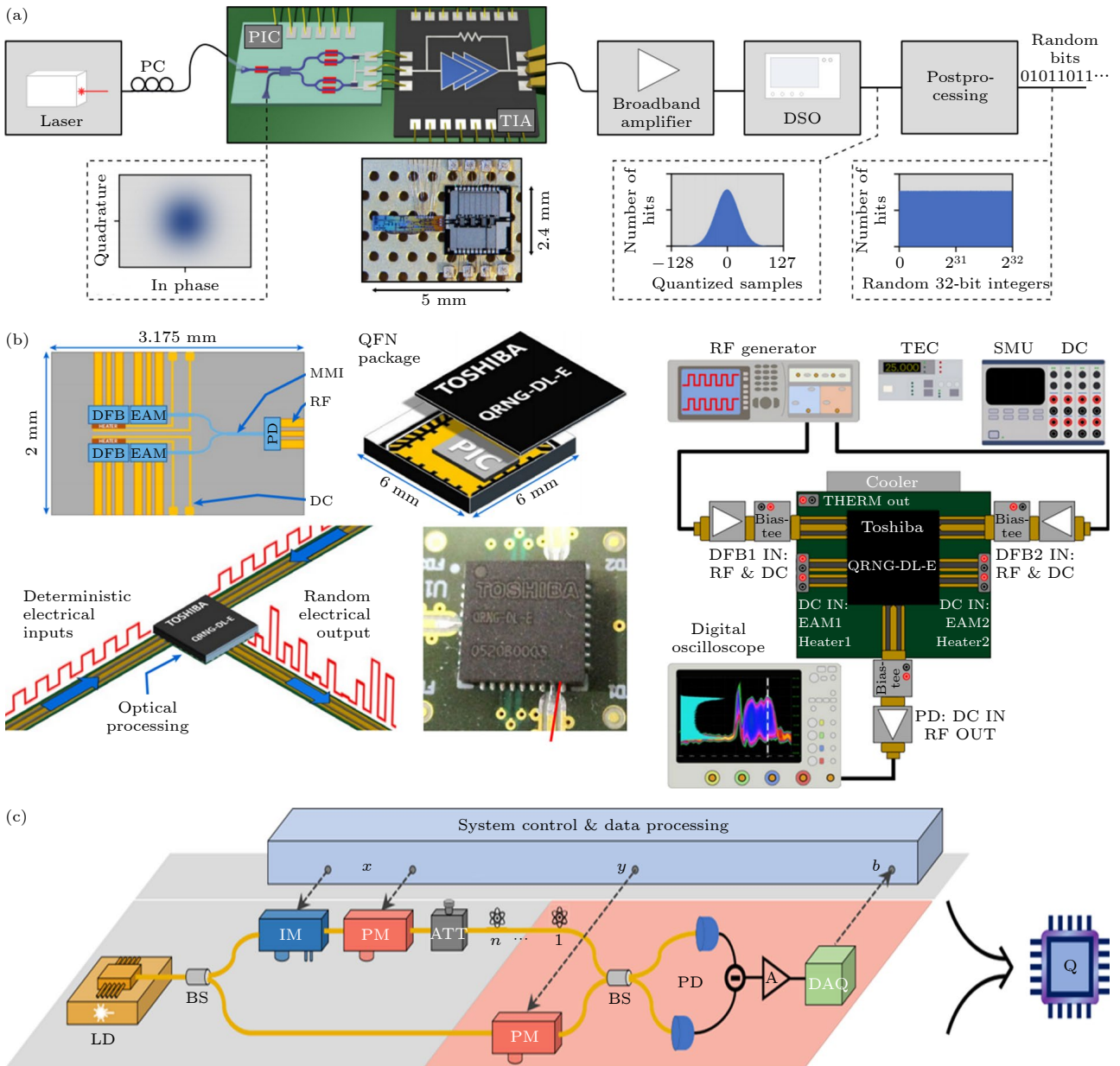


图 3 集成 CV-QKD 系统示意图 (a) 基于硅基集成的 CV-QKD 接收平台^[52]; (b) 基于硅基集成的 CV-QKD 接收器芯片^[53]; (c) 基于硅基集成的 CV-QKD 接收器结构图及该 CV-QKD 系统^[55]; (d) 基于 III-V/Si₃N₄ 的片上激光器^[51]

Fig. 3. Schematic diagrams of integrated CV-QKD systems: (a) CV-QKD receiving platform based on silicon-based integration^[52]; (b) CV-QKD receiver chip based on silicon-based integration^[53]; (c) schematic diagram of the CV-QKD receiver based on silicon-based integration and the CV-QKD system^[55]; (d) III-V/Si₃N₄-based on-chip lasers^[51].



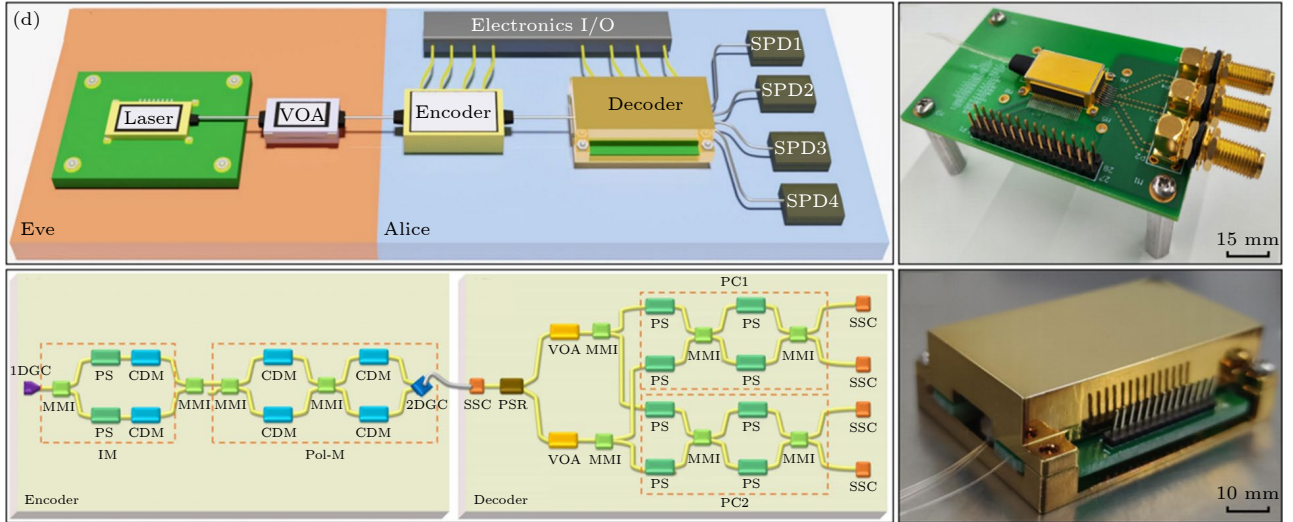


图 4 集成 QRNG 系统示例 (a) 基于硅基集成芯片的完全可信 QRNG 系统^[66]; (b) 基于 InP 光学平台的集成 QRNG 系统^[26]; (c) 基于自制零差检测器的实验系统^[64]; (d) 基于硅基集成芯片的 SI-QRNG 系统^[68]

Fig. 4. Examples of integrated quantum random number generator systems: (a) a fully trusted QRNG system based on silicon-based integrated chips^[66]; (b) an integrated QRNG system based on an InP optical platform^[26]; (c) experimental systems based on self-made aberration detectors^[64]; (d) SI-QRNG system based on silicon-based integrated chips^[68].

所示, 实现了 1.6 kHz 的超窄线宽激光输出; 进一步利用双微环腔的游标卡尺效应, 获得了超过 70 nm 的宽调谐范围, 且边模抑制比达到 75 dB. 基于该高性能集成光源, 该团队成功演示了超过 100 km 的长距离 QKD 实验.

除硅基平台外, 其他材料体系 (如 InP) 的集成研究也在推进. Aldama 等^[54] 提出并实现了一种基于 InP 集成平台的 CV-QKD 发射器芯片, 集成了电吸收调制器、相位调制器和可变光衰减器等组件. 在实验中采用片外激光源, 在 11 km 超低损耗光纤链路上实现了 0.078 Mbit/s 的渐近密钥率.

4 量子随机数生成器 (QRNG)

QRNG 基于量子力学的不确定性原理, 能够生成具备内在随机性的真随机数, 为 QKD 系统提供高安全性密钥. 典型的 QRNG 由产生量子态的熵源和探测该量子态并输出随机比特的测量装置构成. 当前, 根据对设备的信任程度, QRNG 分为完全可信、设备无关 (DI) 和半设备无关 (Semi-DI) 三类. 得益于高质量光学元件的成熟与光子集成技术的潜力, QRNG 在量子熵源与探测器的小型化方面均取得了显著进展. 表 4 按时间顺序梳理了近期集成 QRNG 的技术进展.

在完全可信的 QRNG 中, 包括光源、探测器在内的所有设备均被视为完全可信且经过精确校

准. 随机性源于量子过程, 如单光子探测、真空涨落或激光相位噪声等. 随机数生成速率是 QRNG 的核心性能指标之一, 其瓶颈主要受限于探测器的死区时间、探测效率、量子熵源特性、信号处理链路带宽以及环境噪声等因素. 为突破速率瓶颈, Bruynsteen 等^[66] 提出了一种基于硅光子集成芯片的集成化 QRNG 方案, 该方案以真空噪声为熵源, 通过定制化光电集成电路协同设计, 集成了高速平衡零差探测器, 如图 4(a) 所示. 另外还提出了一个设备依赖性安全框架, 该框架能同时抵御经典侧信道信息 (如电子学噪声) 和量子侧信道信息 (如环境纠缠) 的影响, 充分考虑了模数转换器数字化过程中的非线性效应; 实验最终实现了创纪录的 100 Gbit/s 真随机数生成速率. 区别于传统的单通道真空噪声熵源设计, Tanizawa 等^[69] 提出了一种基于空间复用的 QRNG 方案. 该方案利用二氧化硅平面光波导电路分束器构建了多通道并行探测架构, 由单个激光二极管驱动多通道平衡零差探测器, 实现了对 4 个通道真空涨落的并行探测, 并采用 FPGA 进行数据的并行处理. 实验验证表明, 该系统的随机数生成速率达到 50 Gbit/s, 且在连续 1 h 运行中, 其输出数据的相对标准偏差小于 1%. 这两项研究显著提升了 QRNG 在高速应用场景下的性能.

随着集成 QRNG 的生成速率不断提升, 其集成度、稳定性及功耗已成为当前的研究热点. 现

表 4 基于不同平台的集成 QRNG
Table 4. Integrated QRNG based on different platforms.

文献	工艺	熵源	设备信任	探测	采样方式	生成速率/Mbps
[64]	SI	真空噪声	测量设备无关	零差探测	FPGA(实时)	—
[65]	InP	自发辐射相位噪声	完全可信	光电探测	示波器(离线)	6110
[66]	SI	真空噪声	完全可信	零差探测	示波器(离线)	1×10^5
[67]	SI	真空态涨落	源设备无关	零差探测	示波器(离线)	146.2
[68]	SI	光子偏振态	源设备无关	单光子探测	单光子探测器+ 时间数字转换器(离线)	4.04
[69]	SiO ₂	真空噪声	完全可信	零差探测	FPGA(实时)	5×10^4
[70]	SI/InP	真空噪声	完全可信	零差探测	FPGA(实时)	1.02
[26]	InP	真空态涨落	完全可信	光电探测	FPGA(实时)	2×10^3
[71]	SI	真空噪声	源设备无关	零差探测	FPGA(实时)	2×10^4
[25]	SI	光子偏振态	源设备无关	单光子探测	单光子探测器+ 时间数字转换器(离线)	9.49
[72]	SI	真空态涨落	源设备无关	外差探测	示波器(离线)	20212

注: 表中所有基于不同平台集成的QRNG工作均采用了“Toeplitz Hashing”后处理技术.

有的基于硅光子平台的 QRNG 通常需要外接激光器, 难以实现真正的单片集成系统. 针对此问题, Wang 等^[70]研制出一种混合集成芯片的紧凑型 QRNG. 该芯片集成了 InP 激光二极管与硅光子芯片, 并采用对称的 1×2 多模干涉仪结构, 实现了大于 40 dB 的共模抑制比. 系统采用锗硅光电二极管构建平衡零差探测器, 在 $1 \mu\text{A}$ 光电流条件下获得了约 9 dB 的量子噪声与经典噪声功率比. 最终该系统在 80 mW 的低功耗下实现了 1.02 Mbit/s 的随机数生成速率, 显著提升了集成 QRNG 的实用化性能. Chrysostomidis 等^[65]则展示了一种基于 InP 光子集成平台的集成 QRNG 芯片. 该芯片集成了两个分布式布拉格反射镜 (DBR) 激光器、一个平衡马赫-曾德尔干涉仪 (MZI) 用于功率分配、一个非平衡 MZI 及一个高速光电探测器. 其中一个 DBR 激光器产生的相位扩散作为量子熵源, 通过非平衡 MZI 将相位随机波动转化为强度波动, 实现高速随机数生成. 在 300 min 测试中, 去除经典噪声后, 芯片输出的最小熵均值保持稳定 (标准差 $\sigma = 0.053$), 随机数生成速率达 6.11 Gbit/s. 近期, Marangon 等^[26]开发出一种基于 InP 光子集成芯片的 QRNG. 其核心是一个紧凑封装 ($6 \text{ mm} \times 6 \text{ mm}$) 的光学熵源模块, 如图 4(b) 所示, 该模块集成了完整的片上光学组件 (包含激光器、电吸收调制器、多模干涉仪和探测器). 该方案利用双激光增益开关产生的相位随机化光脉冲在多模干涉仪处干涉作为量子熵源. 在非受控环境中连续运行 38 天后, 该集成 QRNG 输出的物理随机性特征变化

极小 (基于超过 2.9×10^6 个采集直方图的分析, 总变差距离均值为 0.007, 标准差为 0.003), 展现出优异的长期稳定性. 通过实时监测和参数调整, 该系统能稳定地以 2 Gbit/s 的速率生成随机数.

在 SDI-QRNG 框架下, 根据测量设备和源的可信与否, 可进一步细分为源无关 QRNG (SI-QRNG) 和测量设备无关 QRNG (MDI-QRNG). 传统的完全可信 QRNG 通常需要精确校准测量设备以完成安全性分析, 而设备表征的困难不仅带来实验挑战, 还可能引入潜在的侧信道漏洞, 危及安全性. 为解决测量设备表征难题, Wang 等^[64]提出并实验演示了一种新型半设备无关量子随机性扩展协议. 该协议完全移除了对测量设备 (零差探测器) 的校准要求, 并严格考虑了有限尺寸效应, 同时移除了测量过程的独立同分布假设, 具备自测试特性和可证明的安全性. 重要的是, 该协议仅使用标准光学元件, 在硅光子集成平台上易于实现. 为验证协议可行性, 研究人员搭建了基于自制高效率零差检测器 (1550 nm 处有效效率达 91.7%) 的光纤实验系统, 如图 4(c) 所示. 系统工作在 2.5 MHz 重复频率下, 在完成 10^{10} 轮协议执行后, 成功实现了 4.98 kbit/s 的净随机性扩展率. 这一成果为发展具有自测试特性和可证明安全性的集成化 QRNG 铺平了道路.

SI-QRNG 的核心假设是随机源不可信, 而测量设备可信. 其核心思想是利用测量结果实时监控源的状态. 这通常需要在不同的 (常为互补的) 测量基之间随机切换, 使得源 (假定受对手控制) 无

法预知后续测量. 传统芯片级 QRNG 依赖量子源 (如真空涨落) 产生随机数, 但量子源本身存在被攻击者操控的风险 (例如通过注入恶意光信号), 可能导致随机数可预测, 构成严重安全威胁. 针对此挑战, Du 等^[25] 提出一个基于硅基集成芯片的离散变量 SI-QRNG 方案, 利用 FPGA 控制不可信激光源与硅基偏振解码器芯片, 通过共轭基 (如 X 基和 Z 基) 实时监测光源状态, 实现光子偏振态的片上解码测量. 随后在实验中, 该系统的安全随机数生成速率最高可达 9.49 Mbit/s, 成功展示了基于硅集成芯片的 QRNG 在集成度、速度和安全性的良好平衡. 集成 SI-QRNG 虽发展迅速, 但其安全性仍依赖测量设备的可信性及精确表征, 实际器件的缺陷会直接影响随机数质量. 为了解决这个问题, Zhao 等^[68] 提出了一个基于硅基集成芯片的高安全性的 SI-QRNG, 可从不可信光源和未表征测量设备中提取安全随机数. 不可信源采用基于商用激光器, 实验装置如图 4(d) 所示. 经参数优化 (平均光子数 $\mu = 19.33$), 随机数生成速率达 4.04 Mbit/s, 为开发高安全性、低成本和小型化随机数生成系统提供了有效途径.

在确保安全性的前提下, 为实现高速率的集成 SI-QRNG, 近期研究也在基于连续变量方案的集成 QRNG 方面取得了显著突破. Li 等^[67] 提出并实现了一种集成化硅光子芯片 QRNG 方案. 该方案的核心在于利用片上相位调制器随机切换测量基, 并结合为实际芯片环境 (不可拆卸、存在非理想因素) 设计的量子条件最小熵评估框架来保障安全性. 通过实现高带宽 (裸片 27.7 GHz)、低失真的片上锗探测器以及低半波电压 (3.7 V) 的高精度片上相位调制器, 该芯片系统成功实现了 146.2 Mbit/s 的安全随机数生成速率, 其裸片理论极限速率高达 248.47 Gbit/s. 此项工作为 QRNG 在通信、加密等场景的大规模应用奠定了重要基础. Bertapelle 等^[72] 也提出了一种基于硅光子学平台的集成 QRNG 方案, 其安全随机数生成速率超过 20 Gbit/s. 该方案将系统分为量子源和外差接收器两个子系统, 其中量子源被视为不可信 (由潜在攻击者控制), 而外差接收器则完全可信并经过严格表征. 研究人员采用 220 nm 绝缘体上硅技术制造了单片光子集成电路, 集成了的 4×4 多模干涉仪作为 90° 光学混频器, 无需主动相位反馈控制. 实验中以外部 1550 nm 分布反馈激光器作为本振. 在最大本振功

率 (~ 21 mW) 下, 测得量子条件最小熵 $H_{\min}(X|E)$ 下限为 (10.106 ± 0.005) B, 据此提取的安全生成速率达 20.212 Gbit/s. 此外, Bian 等^[71] 基于硅光子平台构建的集成 QRNG 实现了 20 Gbit/s 实时生成速率. 该系统将除光源外的核心组件集成于单片硅光子芯片之上, 充分展示了硅光子集成电路技术在实现高速生成随机数方面的潜力.

5 总结与展望

本文系统综述了光子集成 QKD 与集成 QRNG 领域近年来的突破性进展. 通过实现微型化设计、提升稳定性、降低成本、优化性能并增强安全性, 集成光子学平台成为推动 QKD 和 QRNG 从实验室走向大规模应用的关键使能技术. 在 QKD 的系统验证与 QRNG 的研究中, DV-QKD, CV-QKD 以及 QRNG 在光子集成层面的关键突破, 有效推动了相关系统在密钥生成速率、传输距离及运行稳定性等核心性能指标上的显著提升. 尽管该领域已积累丰硕的研究成果, 未来仍面临若干关键挑战.

1) QKD 系统实际安全性分析: QKD 系统在理论上具备无条件安全性, 但实际工程实现中器件的非理想特性 (如光源频率与强度抖动、探测器后脉冲、器件参数与理论模型的偏差) 为窃听者引入了潜在的攻击面. 虽然已有针对上述问题的安全性研究^[73-75], 然而, 随着 QKD 系统向集成化、芯片化架构演进以及新型光电器件材料 (如硅光子集成芯片、SNSPD) 的应用, 新型安全威胁持续涌现^[76-79] (例如量子态制备误差和高速调制引入制备不准确、硅光子强度调制器中的双光子吸收效应会引入漏洞等). 因此, 对集成 QKD 系统进行全面且深入的实际安全性分析, 并据此设计出鲁棒性更强的工程化系统, 是推进其大规模实用化的关键环节.

2) 前沿 QKD 协议的片上实现: 当前基于集成光子芯片的 QKD 研究主要集中于 BB84、测量设备无关等经典协议. 然而, 集成光子技术在器件小型化、功能模块化及系统低功耗化方面的突破性进展, 为新型 QKD 协议提供了极具潜力的实施平台. 相较于经典协议, 例如: 具备长距离成码能力的双场 QKD(TF-QKD) 协议^[13,80], 具有低系统复杂度的模式匹配 QKD(MP-QKD) 协议^[81,82], 以及具有强抗噪能力的高维 QKD(HD-QKD) 协议^[83,84] 等.

这些新型协议的片上实现不仅能突破传统协议在安全密钥率、传输距离及抗环境噪声能力上的固有局限,还可为未来量子中继、多用户量子网络等先进架构提供技术支撑.因此,亟需将更多研究精力投向新型 QKD 协议的集成化实现与性能验证,以充分释放集成光子平台在协议创新方面的巨大潜力.

3) 实用化全集成 QKD 系统实现:当前集成化 QKD 系统已从分立器件向芯片级集成迈进,然而,实现工程实用化的全单片集成架构仍存在显著挑战.关键瓶颈包括:实现基于 III-V 族材料的高性能激光器、高速量子态调制器及其驱动电路的高效异质/异构集成;实现低损耗量子态测量单元与高性能单光子探测器(如 SNSPD)在单片或先进封装平台上的协同集成.攻克上述挑战,亟需在跨材料体系低温集成技术、晶圆级缺陷检测与工艺控制、低功耗高速调制驱动电路设计以及统一的性能测试等方面取得突破.

4) 集成 QRNG(高性能与高集成度)的协同优化:集成 QRNG 当前面临的核心挑战源于硅基平台与 InP 平台的技术特性差异.硅基平台凭借成熟的 CMOS 兼容性,易于集成电子逻辑处理单元(如 SPAD 阵列及后处理电路),但其光源的非理想性及探测器性能局限(如暗计数、后脉冲效应),制约了随机数生成速率的提升;而 InP 平台虽在量子态制备与操控及相干检测上优势显著(支持>10 Gbit/s 的高带宽),却由于 III-V 族材料与硅基电子元件的工艺失配,在高速跨阻放大器(TIA)、模数转换器(ADC)、及后处理电路的片上集成方面面临严峻挑战.为此,电子-光子异构集成与探测链路优化成为关键突破方向:通过硅光互连技术(如混合键合)实现 InP 光子芯片与硅电子芯片的高效协同集成;采用 SiGe BiCMOS 工艺开发低功耗宽带 TIA 以抑制噪声;同时探索光子辅助 ADC 方案(如光频梳采样)替代传统电子转换以突破采样率瓶颈.

总之,集成光学芯片技术是推动量子保密通信从实验室走向大规模实际应用的核心使能技术.尽管挑战犹存,该领域持续涌现的创新成果正不断夯实其技术基础.随着材料、工艺、设计和系统集成能力的协同进步,集成量子保密通信技术有望在构建未来高度安全的信息基础设施中扮演至关重要的角色.

参考文献

- [1] Proctor T, Young K, Baczewski A D, Blume Kohout R 2025 *Nat. Rev. Phys.* **7** 105
- [2] Fauseweh B 2024 *Nat. Commun.* **15** 2123
- [3] Proctor T, Rudinger K, Young K, Nielsen E, Blume Kohout R 2022 *Nat. Phys.* **18** 75
- [4] Ding X, Guo Y P, Xu M C, Liu R Z, Zou G Y, Zhao J Y, Ge Z X, Zhang Q H, Liu H L, Wang L J, Chen M C, Wang H, He Y M, Huo Y H, Lu C Y, Pan J W 2025 *Nat. Photonics* **19** 387
- [5] Fujisaki E, Okamoto T 1999 *19th Annual International Cryptology Conference* Santa Barbara, California, USA, August 15–19, 1999 p537
- [6] Simmons G J 1979 *ACM Comput. Surv.* **11** 305
- [7] Akter M S, Rodriguez C J, Shahriar H, Cuzzocrea A, Wu F 2023 *IEEE International Conference on Big Data (BigData)* Sorrento, Italy, December 15–18, 2023 p5408
- [8] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, India, December 10–12, 1984 p175
- [9] Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J 1992 *J. Cryptol.* **5** 3
- [10] Li W, Zhang L K, Tan H, Lu Y C, Liao S K, Huang J, Li H, Wang Z, Mao H K, Yan B Z, Li Q, Liu Y, Zhang Q, Peng C Z, You L X, Xu F H, Pan J W 2023 *Nat. Photonics* **17** 416
- [11] Li Y, Cai W Q, Ren J G, Wang C Z, Yang M, Zhang L, Wu H Y, Chang L, Wu J C, Jin B, Xue H J, Li X J, Liu H, Yu G W, Tao X Y, Chen T, Liu C F, Luo W B, Zhou J, Yong H L, Li Y H, Li F Z, Jiang C, Chen H Z, Wu C, Tong X H, Xie S J, Zhou F, Liu W Y, Ismail Y, Petruccione F, Liu N L, Li L, Xu F, Cao Y, Yin J, Shu R, Wang X B, Zhang Q, Wang J Y, Liao S K, Peng C Z, Pan J W 2025 *Nature* **640** 47
- [12] Li W, Zhang L K, Lu Y C, Li Z P, Jiang C, Liu Y, Huang J, Li H, Wang Z, Wang X B, Zhang Q, You L X, Xu F H, Pan J W 2023 *Phys. Rev. Lett.* **130** 250802
- [13] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X, Ma D, Dong H, Xiong J M, Zhang C J, Li H, Wang R C, Wu J, Chen T Y, You L X, Wang X B, Zhang Q, Pan J W 2023 *Phys. Rev. Lett.* **130** 210801
- [14] Zhang L K, Li W, Pan J W, Lu Y C, Li W W, Li Z P, Huang Y Z, Ma X F, Xu F H, Pan J W 2025 *Phys. Rev. X* **15** 021037
- [15] Diamanti E, Lo H K, Qi B, Yuan Z L 2016 *npj Quantum Inf.* **2** 16025
- [16] Liu Q, Huang Y M, Du Y Q, Zhao Z G, Geng M M, Zhang Z R, Wei K J 2022 *Entropy* **24** 1334
- [17] Gabriel C, Wittmann C, Sych D, Dong R F, Maurer W, Andersen U L, Marquardt C, Leuchs G 2010 *Nat. Photonics* **4** 711
- [18] Zheng Z Y, Zhang Y C, Huang W N, Yu S, Guo H 2019 *Rev. Sci. Instrum.* **90** 043105
- [19] Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A 2000 *Rev. Sci. Instrum.* **71** 1675
- [20] Ren M, Wu E, Liang Y, Jian Y, Wu G, Zeng H P 2011 *Phys. Rev. A* **83** 023820
- [21] Wayne M A, Kwiat P G 2010 *Opt. Express* **18** 9351
- [22] Wahl M, Leifgen M, Berlin M, Röhlicke T, Rahn H J, Benson O 2011 *Appl. Phys. Lett.* **98** 171105
- [23] Guo Y, Cai Q, Li P, Jia Z W, Xu B J, Zhang Q W, Zhang Y M, Zhang R N, Gao Z S, Shore K A, Wang Y C 2021 *APL Photonics* **6** 066105
- [24] Wei S H, Yang J, Fan F, Huang W, Li D S, Xu B J 2017

- Rev. Sci. Instrum.* **88** 123115
- [25] Du Y Q, Hua X, Zhao Z G, Sun X R, Zhang Z R, Xiao X, Wei K J **2025** *Commun. Phys.* **8** 9
- [26] Marangon D G, Smith P R, Walk N, Paraíso T K, Dynes J F, Lovic V, Sanzaro M, Roger T, De Marco I, Lucamarini M, Yuan Z L, Shields A J **2024** *Nat. Electron.* **7** 396
- [27] Pirandola S, Andersen U L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J L, Razavi M, Shamsul Shaari J, Tomamichel M, Usenko V C, Vallone G, Villoresi P, Wallden P **2020** *Adv. Opt. Photon.* **12** 1012
- [28] Xu F H, Ma X F, Zhang Q, Lo H K, Pan J W **2020** *Rev. Mod. Phys.* **92** 025002
- [29] Siew S Y, Li B, Gao F, Zheng H Y, Zhang W, Guo P, Xie S W, Song A, Dong B, Luo L W, Li C, Luo X, Lo G Q **2021** *J. Lightwave Technol.* **39** 4374
- [30] Chen X, Milosevic M M, Stanković S, Reynolds S, Bucio T D, Li K, Thomson D J, Gardes F, Reed G T **2018** *Proc. IEEE* **106** 2101
- [31] Reed G T, Mashanovich G, Gardes F Y, Thomson D J **2010** *Nat. Photonics* **4** 518
- [32] Ogiso Y, Ozaki J, Ueda Y, Wakita H, Nagatani M, Yamazaki H, Nakamura M, Kobayashi T, Kanazawa S, Hashizume Y, Tanobe H, Nunoya N, Lda M, Miyamoto Y, Lshikawa M **2019** *J. Lightwave Technol.* **38** 249
- [33] Abellan C, Amaya W, Domenech D, Muñoz P, Capmany J, Longhi S, Mitchell M W, Pruneri V **2016** *Optica* **3** 989
- [34] Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner M G, Natarajan C M, Hadfield R H, O'Brien J L, Thompson M G **2017** *Nat. Commun.* **8** 13984
- [35] Zhang M, Wang C, Kharel P, Zhu D, Lončar M **2021** *Optica* **8** 652
- [36] Berikaa E, Alam M S, Li W J, Bernal S, Krueger B, Pittalà F, Plant D V **2023** *IEEE Photon. Technol. Lett.* **35** 850
- [37] Lomonte E, Wolff M A, Beutel F, Ferrari S, Schuck C, Pernice W H P, Lenzini F **2021** *Nat. Commun.* **12** 6847
- [38] Xiong W J, Wang G L, Li J F, Zhao C, Wang W W, Radamson H H **2021** *J. Mater. Sci-Mater. El.* **32** 1
- [39] Wilmart Q, El Dirani H, Tyler N, Fowler D, Malhouitre S, Garcia S, Casale M, Kerdiles S, Hassan K, Monat C, Letartre X, Kamel A, Pu M, Yvind K, Oxenløwe L K, Rabaud W, Sciancalepore C, Szlag B, Olivier S **2019** *Appl. Sci.* **9** 255
- [40] Sacher W D, Huang Y, Lo G Q, Poon J K S **2015** *J. Lightw. Technol.* **33** 901
- [41] Gyger S, Zichi J, Schweickert L, Elshaari A W, Steinhauer S, Covre da Silva S F, Rastelli A, Zwiller V, Jöns K D, Errando Herranz C **2021** *Nat. Commun.* **12** 1408
- [42] Schuck C, Guo X, Fan L, Ma X, Poot M, Tang H X **2016** *Nat. Commun.* **7** 10352
- [43] Zhu C X, Chen Z Y, Li Y, Wang X Z, Wang C Z, Zhu Y L, Liang F T, Cai W Q, Jin G, Liao S K, Peng C Z **2022** *Phys. Rev. Appl.* **17** 064034
- [44] Beutel F, Brückhoff Plücker F, Gehring H, Kovalyuk V, Zolotov P, Goltsman G, Pernice W H P **2022** *Optica* **9** 1121
- [45] Dolphin J A, Paraíso T K, Du H, Woodward R I, Marangon D G, Shields A J **2023** *npj Quantum Inf.* **9** 84
- [46] Du Y Q, Zhu X, Hua X, Zhao Z G, Hu X, Qian Y, Xiao X, Wei K J **2023** *Chip* **2** 100039
- [47] Wei K J, Hu X, Du Y Q, Hua X, Zhao Z G, Chen Y, Huang C F, Xiao X **2023** *Photon. Res.* **11** 1364
- [48] Sax R, Boaron A, Boso G, Atzeni S, Crespi A, Grünenfelder F, Rusca D, Al Saadi A, Bronzi D, Kupijai S **2023** *Photon. Res.* **11** 1007
- [49] Lin Z H, Gao Y F, Zhou L, Yuan H H, Zhu Y T, Lin Z J, Zhang W, Huang Y D, Cai X L, Yuan Z L **2025** *Opt. Quantum* **3** 195
- [50] Heo H, Woo M K, Park C H, Jang H S, Hwang H, Lee H, Seo M K, Kim S, Kwon H, Jung H, Han S W **2025** *APL Photonics* **10** 031301
- [51] Li L, Wang T, Li X H, Huang P, Guo Y Y, Lu L J, Zhou L J, Zeng G H **2023** *Photon. Res.* **11** 504
- [52] Bian Y M, Pan Y, Xu X S, Zhao L, Li Y, Huang W, Zhang L, Yu S, Zhang Y C, Xu B J **2024** *Appl. Phys. Lett.* **124** 174001
- [53] Piétri Y, Trigo Vidarte L, Schiavon M, Vivien L, Grangier P, Rhouni A, Diamanti E **2024** *Opt. Quantum* **2** 428
- [54] Aldama J, Sarmiento S, Vidarte L T, Etcheverry S, Grande I L, Castelveto L, Hinojosa A, Beckerwerth T, Piétri Y, Rhouni A **2024** arXiv: 2412.03208 [quant-ph]
- [55] Hajomer A A, Bruynsteen C, Derkach I, Jain N, Bomhals A, Bastiaens S, Andersen U L, Yin X, Gehring T **2024** *Optica* **11** 1197
- [56] Hajomer A A, Bomhals A, Bruynsteen C, Sidhique A, Derkach I, Andersen U L, Yin X, Gehring T **2025** arXiv: 2504.09308 [quant-ph]
- [57] Ng S Q, Kanitschar F, Zhang G, Wang C **2025** arXiv: 2504.08298 [quant-ph]
- [58] Ma C X, Sacher W D, Tang Z Y, Mikkelsen J C, Yang Y S, Xu F H, Thiessen T, Lo H K, Poon J K S **2016** *Optica* **3** 1274
- [59] Bunandar D, Lentine A, Lee C, Cai H, Long C M, Boynton N, Martinez N, DeRose C, Chen C C, Grein M, Trotter D, Starbuck A, Pomerene A, Hamilton S, Wong F N C, Camacho R, Davids P, Urayama J, Englund D **2018** *Phys. Rev. X* **8** 021009
- [60] Cao L, Luo W, Wang Y X, Zou J, Yan R D, Cai H, Zhang Y, Hu X L, Jiang C, Fan W J, Zhou X Q, Dong B, Luo X S, Lo G Q, Wang Y X, Xu Z W, Sun S H, Wang X B, Hao Y L, Jin Y F, Kwong D L, Kwek L C, Liu A Q **2020** *Phys. Rev. Appl.* **14** 011001
- [61] Wang H, Li Y, Pi Y D, Pan Y, Shao Y, Ma L, Zhang Y C, Yang J, Zhang T, Huang W, Xu B J **2022** *Commun. Phys.* **5** 162
- [62] Zhang Y C, Chen Z Y, Chu B J, Zhou C, Wang X Y, Zhao Y J, Xu Y F, Xu C, Wang H J, Zheng Z Y, Huang Y D, Xu C C, Zhang X X, Shen T, Huang G, Zheng Y W, Fei Z X, Huang W N, Zhu M L, Huang L Y, Luo B, Yu S, Guo H **2020** *Bull. Am. Phys. Soc.* **65** 1
- [63] Zhang G, Haw J Y, Cai H, Xu F, Assad S M, Fitzsimons J F, Zhou X, Zhang Y, Yu S, Wu J, Ser W, Kwek L C, Liu A Q **2019** *Nat. Photonics* **13** 839
- [64] Wang C, Primaatmaja I W, Ng H J, Haw J Y, Ho R, Zhang J R, Zhang G, Lim C **2023** *Nat. Commun.* **14** 316
- [65] Chrysostomidis T, Roumpos I, Outerelo D A, Troncoso Costas M, Moskalenko V, Garcia Escartin J C, Diaz Otero F J, Vysokinos K **2023** *EPJ Quantum Technol.* **10** 5
- [66] Bruynsteen C, Gehring T, Lupo C, Bauwelinck J, Yin X **2023** *PRX Quantum* **4** 010330
- [67] Li L, Cai M L, Wang T, Tan Z C, Huang P, Wu K, Zeng G H **2024** *Photon. Res.* **12** 1379
- [68] Zhao Z G, Hua X, Du Y Q, Xu C Y, Xie F, Zhang Z R, Xiao X, Wei K J **2024** *Opt. Express* **32** 38793
- [69] Tanizawa K, Kato K, Futami F **2024** *J. Lightwave Technol.* **42** 1209
- [70] Wang X Y, Zheng T, Jia Y X, Huang J, Zhu X Y, Shi Y Q,

- Wang N, Lu Z G, Zou J, Li Y M 2024 *Photonics* **11** 468
- [71] Bian Y M, Yang J, Jiang H Y, Huang W, Su Q, Yu S, Zhang L, Zhang Y C, Xu B J 2025 *Opt. Lett.* **50** 1216
- [72] Bertapelle T, Avesani M, Santamato A, Montanaro A, Chiesa M, Rotta D, Artiglia M, Sorianello V, Testa F, De Angelis G, Contestabile G, Vallone G, Romagnoli M, Villoresi P 2025 *Opt. Quantum* **3** 111
- [73] Sun S H, Huang A Q 2022 *Entropy* **24** 260
- [74] Chen Y, Huang C F, Chen Z H, He W J, Zhang C X, Sun S H, Wei K J 2022 *Phys. Rev. A* **106** 022614
- [75] Zhang C, Hu X L, Jiang C, Chen J P, Liu Y, Zhang W J, Yu Z W, Li H, You L X, Wang Z, Wang X B, Zhang Q, Pan J W 2022 *Phys. Rev. Lett.* **128** 190503
- [76] Kang X, Ye P, Wang S, Zhang G W, Wang Z H, Chen J L, Yin Z Q, He D Y, Chen W, Fan Yuan G J, Guo G C, Han Z F 2025 *Phys. Rev. Appl.* **23** 024014
- [77] Tan H, Li W, Zhang L K, Wei K J, Xu F H 2021 *Phys. Rev. Appl.* **15** 064038
- [78] Li L, Huang P, Wang T, Zeng G H 2021 *Phys. Rev. A* **103** 032611
- [79] Ye P, Chen W, Wang Z H, Zhang G W, Ding Y Y, Huang G Z, Yin Z Q, Wang S, He D Y, Liu W, Guo G C, Han Z F 2022 *Opt. Express* **30** 39911
- [80] Curty M, Azuma K, Lo H K 2019 *npj Quantum Inf.* **5** 64
- [81] Zhu H T, Huang Y Z, Liu H, Zeng P, Zou M, Dai Y Q, Tang S B, Li H, You L X, Wang Z, Chen Y A, Ma X F, Chen T Y, Pan J W 2023 *Phys. Rev. Lett.* **130** 030801
- [82] Zeng P, Zhou H Y, Wu W J, Ma X F 2022 *Nat. Commun.* **13** 3903
- [83] Wang F X, Chen W, Yin Z Q, Wang S, Guo G C, Han Z F 2019 *Phys. Rev. Appl.* **11** 024070
- [84] Sekga C, Mafu M, Senekane M 2023 *Sci. Rep.* **13** 1229

SPECIAL TOPIC—Quantum information processing

Recent progress on photon-integrated quantum key distribution and quantum random number generator^{*}YU Jingchun¹⁾²⁾ LU Wenbin³⁾⁴⁾ CHEN Bin¹⁾²⁾ DU Yongqiang¹⁾
XIE Feng¹⁾ LI Wei³⁾⁴⁾† WEI Kejin^{1)‡}¹⁾ (*Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning 530004, China*)²⁾ (*School of Computer, Electronics and Information, Guangxi University, Nanning 530004, China*)³⁾ (*School of Artificial Intelligence Science and Technology, University of Shanghai for Science and Technology, Shanghai 200093, China*)⁴⁾ (*Institute of Photonic Chips, University of Shanghai for Science and Technology, Shanghai 200093, China*)

(Received 18 June 2025; revised manuscript received 17 July 2025)

Abstract

Quantum key distribution (QKD) relies on the fundamental principles of quantum mechanics and can theoretically achieve unconditionally secure communication that is provable by information theory. Quantum random number generators, on the other hand, utilize the inherent randomness of quantum phenomena and are capable of generating a truly random entropy source that is unpredictable, unbiased and unrepeatable. These two technologies are crucial for building highly trustworthy and secure communication systems resistant to quantum attacks. However, their large-scale deployment still faces challenges such as system performance optimization, cost control and scale production.

Relying on wafer-level fabrication platforms and micro-nanometer processing, integrated photonics technology integrates the core devices of traditional QKD systems (e.g., light source, modulator, and detector) in a single chip at high density. It significantly improves the miniaturization, operational stability and cost-effectiveness of the system, and enhances the intrinsic security, and becomes a key enabling platform to drive QKD and QRNG from laboratory to engineering applications.

In this paper, we systematically review the recent breakthroughs of photonic integrated QKD based on different material platforms (SOI/InP/TFLN/Si₃N₄) in terms of core metrics, such as transmission distance and key rate, as well as the significant breakthroughs of integrated QRNG in terms of random number generation rate and system integration. Finally, the future development direction of this field is discussed and outlooked from the four dimensions of practical security of QKD systems, on-chip implementation of cutting-edge QKD protocols, practical fully-integrated QKD systems, and synergistic optimization of high performance and high integration of integrated QRNG.

Keywords: quantum key distribution, quantum random number generators, integrated photonics**PACS:** 03.67.Hk, 03.67.-a, 42.82.-m**DOI:** 10.7498/aps.74.20250791**CSTR:** 32037.14.aps.74.20250791

* Project supported by the National Natural Science Foundation of China (Grant Nos. 62171144, 62031024), the Guangxi Natural Science Foundation, China (Grant Nos. 2025GXNSFAA069137, GXR-1BGQ2424005), and the Innovation Project of Guangxi Graduate Education, China (Grant No. YCBZ2024002).

† Corresponding author. E-mail: weil@usst.edu.cn

‡ Corresponding author. E-mail: kjwei@gxu.edu.cn



光子集成的量子密钥分发和量子随机数生成器研究进展

于景春 芦文斌 陈宾 杜永强 谢锋 李蔚 韦克金

Recent progress on photon-integrated quantum key distribution and quantum random number generator

YU Jingchun LU Wenbin CHEN Bin DU Yongqiang XIE Feng LI Wei WEI Kejin

引用信息 Citation: *Acta Physica Sinica*, 74, 160304 (2025) DOI: 10.7498/aps.74.20250791

CSTR: 32037.14.aps.74.20250791

在线阅读 View online: <https://doi.org/10.7498/aps.74.20250791>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

您可能感兴趣的其他文章

Articles you may be interested in

标记单光子源在量子密钥分发中的应用

Overview of applications of heralded single photon source in quantum key distribution

物理学报. 2022, 71(17): 170304 <https://doi.org/10.7498/aps.71.20220344>

基于监控标记单光子源的量子密钥分发协议

Source monitoring quantum key distribution protocol based on heralded single photon source

物理学报. 2024, 73(24): 240302 <https://doi.org/10.7498/aps.73.20241269>

改进的关联源量子密钥分发

Improved source-correlated quantum key distribution

物理学报. 2025, 74(14): 140302 <https://doi.org/10.7498/aps.74.20250268>

一种基于标记单光子源的态制备误差容忍量子密钥分发协议

State preparation error tolerant quantum key distribution protocol based on heralded single photon source

物理学报. 2022, 71(3): 030301 <https://doi.org/10.7498/aps.71.20211456>

非对称信道相位匹配量子密钥分发

Asymmetric channel phase matching quantum key distribution

物理学报. 2023, 72(14): 140302 <https://doi.org/10.7498/aps.72.20230652>

实时熵源评估二重并行连续变量量子随机数发生器

Real-time entropy source evaluated dual-parallel continuous variable quantum random number generator

物理学报. 2025, 74(12): 124202 <https://doi.org/10.7498/aps.74.20250333>