

激光与光电子学进展

集成量子密钥分发研究进展(特邀)

张国威^{1,2}, 黄冠中^{1,2}, 王纺翔^{1,2*}, 陈巍^{1,2**}¹中国科学技术大学量子信息实验室, 安徽 合肥 230026;²中国科学技术大学量子网络安徽省重点实验室, 安徽 合肥 230026

摘要 量子密钥分发基于量子力学原理,为远程用户提供安全的密钥协同方法,是当前量子信息领域中实用化程度最高的技术之一。集成光学为量子密钥分发的实现提供了理想的技术平台,其成果已在系统规模、成本控制、集成度以及可扩展性等方面展现出显著优势。本文聚焦基于集成光学的量子密钥分发,首先对常用的集成光学材料平台和基础功能单元器件进行了概述;然后侧重系统实用化设计与实现,总结了集成量子密钥分发的代表性工作,并深入分析了集成量子密钥分发器件和系统的实际安全性问题;最后对基于集成器件的量子通信网络的发展进行了展望。

关键词 集成光学芯片; 量子密钥分发; 实际安全性

中图分类号 TN256

文献标志码 A

DOI: 10.3788/LOP250992

Research Progress of Integrated Quantum Key Distribution (Invited)

Zhang Guowei^{1,2}, Huang Guanzhong^{1,2}, Wang Fangxiang^{1,2*}, Chen Wei^{1,2**}¹Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, Anhui, China;²Anhui Province Key Laboratory of Quantum Network, University of Science and Technology of China, Hefei 230026, Anhui, China

Abstract Quantum key distribution (QKD), based on quantum mechanical principles, provides a secure key agreement method for remote users and represents one of the most practical technologies in quantum information science. Integrated photonics offers an ideal technological platform for implementing QKD, demonstrating significant advantages in system scale, cost control, integration density, and scalability. This study focuses on integrated optical QKD, providing an overview of commonly used integrated optical material platforms and fundamental functional devices. Emphasizing practical system design and implementation, we summarize representative achievements in integrated QKD and analyze in-depth security issues of integrated QKD devices and systems. Additionally, we present perspectives on the development of quantum communication networks based on integrated devices.

Key words integrated photonics chip; quantum key distribution; practical security

1 引言

量子密钥分发(QKD)以量子力学的基本原理而非计算复杂度为安全性基础,结合“一次一密”的加密手段,可以实现信息论安全的数据传输与通信,是应对量子计算等未来攻击手段的下一代信息安全技术^[1]。自1984年提出以来,QKD技术在理论安全性与实验研究方面均取得了显著进展,已经从实验室演示逐步迈向工程化与实用化,成为量子信息领域中最具产业化潜力的应用之一^[2]。但是,当前的QKD技术距离真

正走向大规模实际应用,还需要突破性能优化、成本控制、规模化生产以及标准化体系和测评等关键技术和工程难题。

集成光学为QKD技术的实现构建了一个理想的平台^[3-4]。与基于分立元件的光学系统相比,集成光学器件具有尺寸小、功耗低的优势,能够实现高密度集成与高稳定性封装,并且适合与各种复用方式相结合^[5],从而提升QKD系统的成码率和稳定性等核心性能。此外,集成光学中晶圆加工的高精度特性和批量生产能力可实现高一致性的器件制备,提高QKD网络化部

收稿日期: 2025-04-11; 修回日期: 2025-05-05; 录用日期: 2025-05-06; 网络首发日期: 2025-05-06

基金项目: 江苏省重点研发计划(BE2022071)、国家自然科学基金(62371437)

通信作者: *fxwung@ustc.edu.cn; **weich@ustc.edu.cn

署时的器件匹配性,同时显著降低 QKD 设备的成本,有助于实现大规模量子保密通信网络的部署,进而推进 QKD 技术的实用化进程^[6]。另一方面,集成光学的材料体系资源丰富,可以通过单片或异质集成方式制备不同种类的器件,实现各类功能单元^[7-10],提高协议的适用性和编码的兼容性,从而拓展 QKD 的应用场景。此外,集成光学器件可以通过亚波长量级的精细几何设计^[11-12]和丰富的操控机制^[13-14]对量子态进行精确操控,为实现高性能和新型的 QKD 方案提供支持。

本文首先从 QKD 的基本原理和常用集成材料平台出发,分析集成 QKD 的常用单元器件及其功能。随后,介绍集成 QKD 的发展现状,并重点关注其面向实用化的主要进展。此外,总结和分析了近期关于集成 QKD 实际安全性研究的代表性成果,梳理了实现高性能实用化量子通信系统所需的关键技术,为 QKD 系统的规模化部署提供技术路径和参考依据。在本文之外,读者也可参考集成 QKD 的相关综述文献^[15-18]。

2 量子密钥分发的基础集成器件

2.1 量子密钥分发

信息安全是国家安全的重要组成部分,加解密算法是保障信息安全的核心技术之一。现有加解密算法的安全性主要依赖于破译算法所需的计算复杂度,然而,随着算力的提升、算法的进步,特别是近年来量子计算等颠覆性技术的涌现和快速发展,传统加密算法正面临严峻挑战^[19-20]。QKD 提供了一条解决该问题的重要途径,可以保障两个远距离用户(通常称为 Alice 和 Bob)安全地共享信息。在量子力学基本原理的框架下,信道中的窃听者(通常称为 Eve)对信息的窃听操作,会不可避免地干扰承载信息的量子态,由此引入误码而被通信双方察觉。

QKD 的概念由 Bennett 和 Brassard^[1]在 1984 年提出,同时被提出的还有目前使用最广泛的 QKD 协议——BB84 协议。QKD 协议主要是指执行 QKD 的过程,即利用光量子等物理载体实现远程密钥协商的过程和数据处理方法。根据使用光量子态的物理资源的不同和信息加载提取方式的不同,研究者提出了不同类型的协议^[2],其中很多协议的理论安全性已经得到了严格的证明^[21],并已逐渐形成了较为成熟完整的安全性分析框架,例如:基于单光子粒子数态的 BB84 协议、B92 协议^[22]和 SARG04 协议等^[23],以及利用量子纠缠态特性保证通信双方获得相同的密钥信息的 QKD 协议,如 E91 协议^[24]、BBM92 协议^[25]和设备无关协议^[26]等。其中,设备无关协议的安全性由无漏洞 Bell 态测量保证,安全性不依赖于设备的可信度,但对性能要求较高,实用化仍存在很多技术挑战^[27]。Lo 等^[28]在 2012 年提出了测量设备无关(MDI)协议,它允许不受信任的第三方作为测量端对 Alice 和 Bob 发送的量子态进行 Bell 态测量,因此对测量设备的安全性不

作要求,完全保证了测量端的安全性^[29-30]。此外, Lucamarini 等^[31]在 2018 年提出的双场(TF)协议能够将 QKD 的密钥率与量子信道传输效率之间的关系由近似线性依赖关系变为平方根依赖关系,即 $R \sim O(\sqrt{\eta})$,显著延长了 QKD 的极限安全传输距离。还有一类利用相邻脉冲间的相对相位进行编码的分布式相位参考协议,主要包括差分相移(DPS)协议^[32]、相干态单路(COW)协议^[33]、环回差分相移(RRDPS)协议^[34]等。

上述协议将信息编码为经典的二进制比特,称为离散变量(DV)协议,也可将信息编码为连续分布的高斯随机数,加载于光场相空间的正则分量上,称为连续变量(CV)协议^[35]。其使用的零拍探测器从结构和使用条件上较为适合进行片上集成化设计。尽管 CV-QKD 系统在可组合安全性分析、长距离条件下的后处理和噪声抑制等方面仍面临一定的技术挑战,但该系统在短距离传输中展现出颇具优势的安全密钥生成能力,目前在 10 km 传输距离下已可实现超过 1 Gbit/s 的密钥率^[36]。通过各类噪声抑制和补偿方法,其远距离传输性能正持续获得提升^[37-38]。由于篇幅限制,本文重点讨论基于离散变量的集成 QKD 研究进展,而 CV-QKD 系统的进展可参考综述文献^[15, 18, 39]。

2.2 光子集成材料平台

近年来,集成光学飞速发展,发展出了硅基二氧化硅(Silica)^[40]、绝缘体上硅(SOI)^[41]、氮化硅(SiN)^[42]等硅基材料,以及 III-V 族半导体(III-V series)^[43]和铌酸锂(LN)^[44-45]等多种材料体系和工艺平台^[46]。

硅基二氧化硅(Silica)波导材料是 QKD 系统中最早实现芯片化集成的平台,它既可利用 CMOS 工艺进行加工制作,也可利用飞秒直写激光技术^[47]加工生产复杂的三维光路结构^[48]。其波导结构通过芯层与包层之间较小的折射率差($\Delta n \approx 0.01$)实现光场束缚,因此器件尺寸相对较大,但典型的传输损耗低于 0.1 dB/cm。该材料可利用热光效应实现 kHz 量级的调制,但难以实现 GHz 以上的快速调制^[49]。SOI 材料作为微电子工业的主流平台,凭借成熟的制备工艺和完备的产业链,在 QKD 芯片领域展现出规模化生产的优势^[50]。SOI 的强光场束缚特性($\Delta n \approx 2.0$)可实现亚微米级波导结构,因此集成度较高,但伴随较高的传输损耗(约为 2 dB/cm),需要特殊设计补偿。在调制方面,除可以利用热光效应实现低速相位调制^[51],也可以通过 PN 掺杂形成的载流子等离子体色散效应^[52]支持高性能 QKD 所需的 GHz 级高速调制。氮化硅(SiN)波导的光学透明窗口可覆盖可见光至中红外波段(400~2350 nm),其折射率($n \approx 2.0$)介于氧化硅和硅之间,因其在模场尺寸、非线性效应和传输损耗(约为 0.1 dB/cm)等关键参数间可以实现良好的平衡,成为非线性光子学和微波光子学研究的理想载体,也是研

究非线性光子学和微波光子学的良好平台^[53],但受其材料本征特性的限制,目前仅能利用热光效应进行调制,这在一定程度上限制了其在高性能 QKD 系统中的应用。

III-V 族半导体(如磷化铟 InP、砷化镓 GaAs 等)因其直接带隙特性,可在单一芯片上集成激光器、半导体光放大器(SOA)、电吸收调制器(EAM)和雪崩光电二极管(APD)等全系列有源器件^[54],为实现 QKD 发射端、量子随机数发生器等较为完整的片上模块和系统,提供了独特的材料平台优势。相较于 CMOS 工艺兼容的 SOI 等硅基材料,III-V 族半导体仍面临多重技术挑战:异质外延生长工艺复杂度高导致制备良率受限,波导与光纤耦合损耗普遍超过 1 dB,且需要特殊衬底导致制造成本增加。当前研究重点正转向 III-V/Si 异质集成技术,通过晶圆键合等先进工艺将 III-V 有源器件与硅基无源光路结合,有望在保持高性能的同时突破规模化生产的成本瓶颈。

铌酸锂材料以其优异的电光效应、宽光谱透明性和高折射率等特性,已成为光电集成领域的关键基础

材料之一^[55]。近年来,基于微纳加工技术制备的薄膜铌酸锂(TFLN)平台取得突破性进展,相较于传统体材料波导,其展现出集成度高、调制效率高、成本低等优势。但该材料的强化学惰性导致刻蚀选择比低、侧壁粗糙度控制难等问题,在产业化过程中仍面临工艺窗口窄、制程稳定性不足等方面的挑战。

表 1 给出了目前在光电集成领域的主流材料特性的总结。表中:Silica、SOI、SiN、III-V series、LN 分别代表硅基二氧化硅、绝缘体上硅、氮化硅、III-V 族半导体材料和铌酸锂;每种指标下★的个数越多,说明材料在该特性下的表现越优秀。由于各材料体系在折射率、非线性系数、传输损耗、调制效率等关键特性上存在着显著差异,单一材料体系难以满足 QKD 系统对光源生成、高速调制、低损传输和单光子探测等全功能集成的严苛要求。因此,有必要根据 QKD 发射端与接收端的具体性能要求,分别选择最适合的材料平台,通过异质集成或混合封装等技术手段^[56-57],充分发挥各材料的优势,并通过工艺解耦降低复杂器件的制备难度,从而有效提升集成化 QKD 系统的整体性能。

表 1 集成光子学平台特性与功能

Table 1 Properties and functions of integrated photonic platforms

Property/function	Silica	SOI	SiN	III-V series	LN
Size	★	★★★★★	★★★	★★	★★
Loss	★★★★★	★★★	★★★★★	★★	★★
Polar independence	★★★★★	★★	★★★	★★★	★★
Source/detector	★	★★★	★★	★★★★★	★★★
Modulator	★	★★★	★	★★★★★	★★★★★
Passive device	★★★★★	★★★★★	★★★★★	★★	★★★

2.3 基于集成器件的量子通信光源

量子光源是 QKD 系统的核心组件,主要包括单光子源、弱相干态光源和纠缠光子源等。其中,弱相干态光源因其技术成熟度和实用性,成为当前 QKD 实验系统中最为常用的光源^[58]。尽管在大多数实验中,该光源通常作为独立组件,通过光纤与其他器件相连,然而,III-V 族半导体芯片的特性使其具备了直接在芯片上集成后续波导结构的潜力。此外,借助混合集成技术,弱相干态光源也可与其他材料平台结合,从而实现全片上发射端结构的构建。与此同时,研究者还在积极探索其他集成化光源结构,例如量子点、非线性纠缠光源和片上光频梳等,从而进一步提升 QKD 系统的性能、稳定性和集成化水平。

单光子源是 QKD 实验中的理想光源,能够在用户指定的任意时刻按需发射单个光子,并且每个光子具有不可区分性。2010 年, Takemoto 等^[59]利用砷化铟/磷化铟(InAs/InP)量子点首次成功实现了 1.5 μm 波段的单光子源,并完成了 50 km 的 QKD 实验,验证了其在 QKD 中的应用潜力[图 1(a)]。除量子点^[60]外,金刚石色心^[61]、碳化硅^[62]以及部分二维材料^[63]等也可

用于片上产生单光子源。但目前上述单光子源通常发光效率或重复频率仍然较低,难以满足 QKD 的高码率需求,对比目前使用弱相干光源(WCS)的 QKD 系统未能体现出优势,仍需进一步研究以提升其性能。

纠缠光子源可用于实现基于纠缠的 QKD 协议,或作为标记单光子源(SPS)用于 QKD 系统。集成化的纠缠光子源通常基于自发参量下转换和自发四波混频等非线性光学过程^[66]。得益于片上光场的紧密约束,结合周期极化^[67]、光学谐振腔^[64]、螺旋线^[68]等微纳结构,线性过程的效率可以得到显著提升,从而在小尺寸内高效地生成高质量的纠缠光子态。2015 年, Silverstone 等^[64]采用 SOI 微环谐振腔,通过四波混频过程产生纠缠光子对,并利用量子态层析等技术验证了光子对的高纠缠度,如图 1(b)所示。

近年来,集成光频梳光源也引起了一定关注。光学频率梳是一种在频域上具有等间距谱线的光源,通过锁定其中一条谱线和梳齿间距,可实现光频梳所有通道之间的互锁,对 QKD 的网络化应用具有重要意义。如图 1(c)所示, Wang 等^[65]利用氧化硅微环谐振腔产生了包含 200 条梳齿、频率范围达 3.2 THz 的耗散

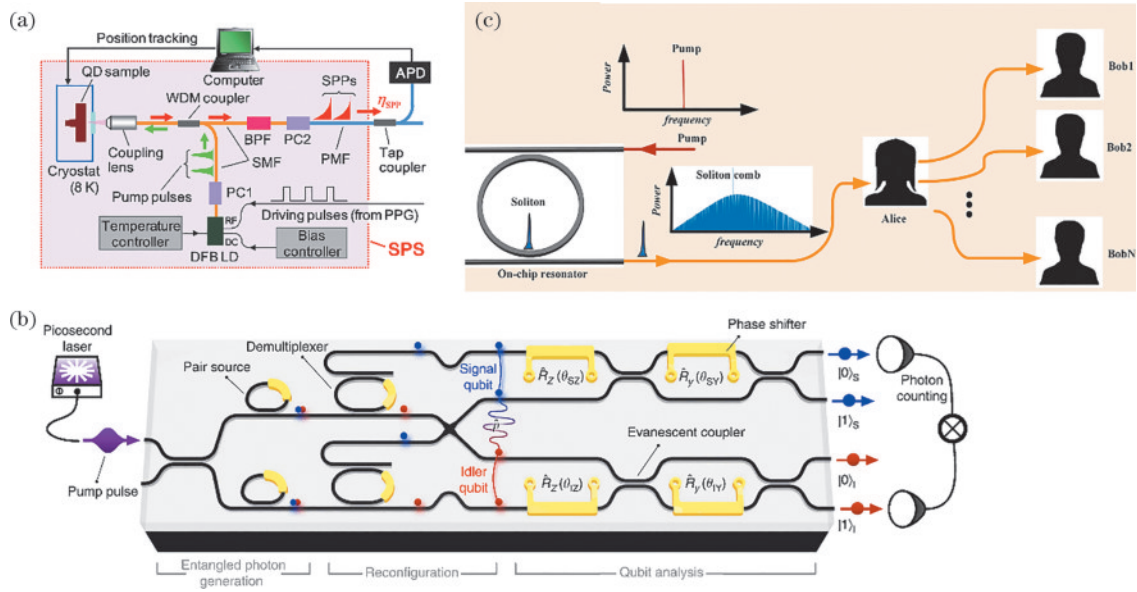


图1 基于集成光源的量子密钥分发系统。(a)基于量子点的单光子源装置图^[59]；(b)基于四波混频的片上纠缠光源及检测装置图^[64]；(c)基于光频梳的多通道量子密钥分发系统示意图^[65]

Fig. 1 Quantum key distribution systems based on integrated light source. (a) Experimental setup for single-photon source based on quantum dot^[59]; (b) experimental setup for on-chip entanglement source based on four-wave mixing^[64]; (c) schematic of a multichannel quantum key distribution system based on an optical frequency comb^[65]

Kerr 孤子频梳。实验中通过波分复用技术,首次演示了基于光频梳两个通道的 QKD 实验,验证了光频梳在多用户 QKD 网络中的可行性。

2.4 集成编解码器

在 QKD 过程中,编码信息的加载与读取依赖于对光量子态的高精度操作,因此,具备高速率和高精度操控的编码器是实现高性能片上 QKD 系统的基础组件。与光源或探测器不同,编解码器通常由光传输元件、分束器、调制器等多种基础功能器件组合而成。集成化 QKD 芯片需要利用各类片上单元器件来实现信息的调制和解调^[69-70]。例如:光栅耦合器、端面耦合器等器件可用于芯片与外部光纤系统的连接;光波导和螺旋形光延迟线可用于光量子信号的传输;定向耦合器、多模干涉仪等器件可实现光量子信号的路径分配和合并;基于热光效应、电光效应、等离子体色散效应等物理过程的调制器件可实现相位调制;基于电吸收效应或马赫-曾德尔干涉仪(MZI)、微环谐振腔等集成结构可实现光量子信号的强度调制。在偏振编码量子态操控中,还需要偏振分束器、偏振旋转器等偏振相关器件。

将上述集成单元器件根据系统需求进行组合,可以构建适用于多种编码方式和协议的编解码芯片,这已成为当前集成 QKD 系统研究的核心领域之一。2019年,Geng等^[71]利用 SOI 材料,设计并实现了较为成熟的时间戳-相位编解码器件,其结构如图 2(a)所示。该编解码器结构多次利用载流子耗尽型电光相位调制器,以及由它和波导、分束器组成的 MZI 强度调制器和不等臂 MZI 结构,实现了诱骗态调制、损耗平

衡、前后脉冲序列生成、相位基/时间基编解码等功能。该系统在 20 km 长的光纤信道中量子比特误码率为 0.84%,计算得到的渐进安全密钥率为 85.7 kbit/s,展示了集成相位编解码器在 QKD 系统中的高效性和实用性。

基于上述基础器件,也可构建用于偏振自由度的编解码器件。2016年,Ma等^[72]实现了首个基于偏振编码 BB84 协议的集成 QKD 编码器,其结构如图 2(b)所示。该编码芯片利用微环调制器作为强度调制器,分别用于光信号的斩波和诱骗态调制。通过级联的热光调制 MZI 型强度调制器将光强衰减至单光子量级,随后采用偏振分集方案进行偏振态调制。具体而言,该方案首先对不同路径的光进行相位和强度调制,随后通过偏振旋转分束器件将量子态从路径编码转换为偏振态编码输出。利用这一芯片,研究者在 5 km 光纤信道中成功开展了 QKD 验证实验,误码率和安全密钥率分别为 5.4% 和 0.95 kbit/s。在该实验系统中,接收端则仍使用了光纤器件。此后,集成偏振解码器件的相关成果也相继发表^[6,73-75]。这些解码器件同样基于将偏振态转化为路径编码的思想实现解码操作,并与编码端相匹配。图 2(c)给出了一种基于 SOI 的集成偏振解码器设计结构。

在 QKD 的集成化研究中,编解码方案主要基于路径、相位、时间戳和偏振等自由度。在路径编码方面,波导和多模干涉分束器等结构可支持高维量子态编码,但其性能仍可能受限于多路径之间的光程差精确调控和损耗均衡等关键技术。相位编码方案通过集成调制器实现相对简化的系统架构,但需重点解决相位

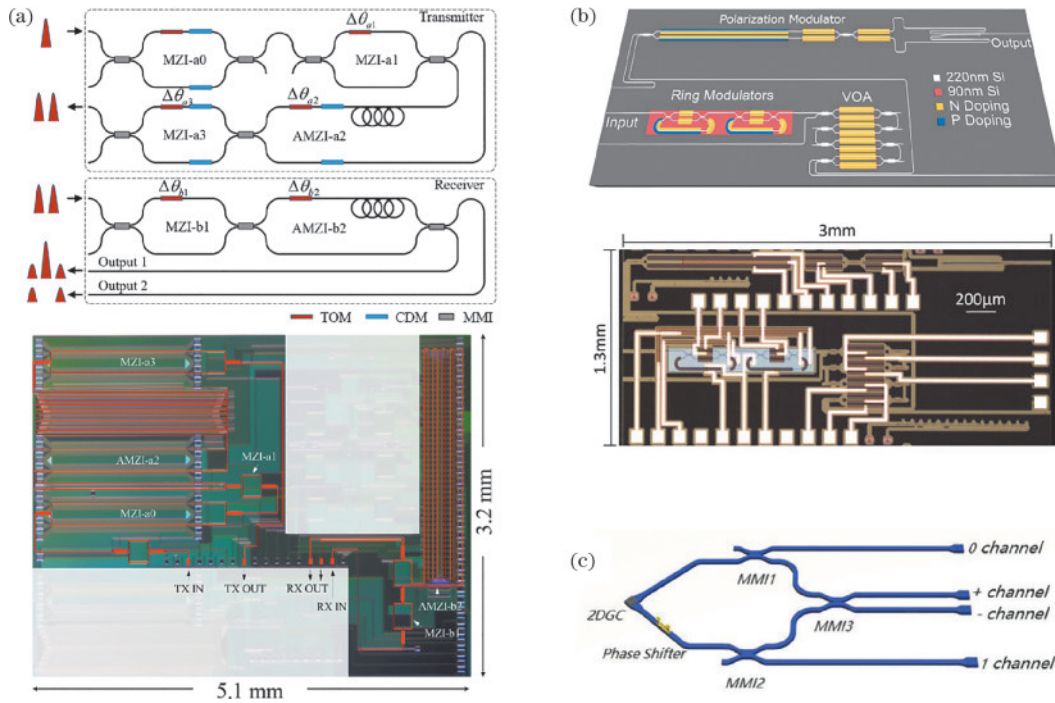


图 2 量子密钥分发编解码器。(a)相位编解码器^[71];(b)偏振编解码器^[72];(c)偏振解码器^[6]

Fig. 2 Codescs of quantum key distribution system. (a) Codec for phase degrees of freedom^[71]; (b) encoder for polarization degrees of freedom^[72]; (c) decoder for polarization degrees of freedom^[6]

漂移补偿和光子在光纤中传输时可能遇到的双折射扰动等问题。时间戳编码通常需要与精确的相位检测结合,其实现仍依赖于高精度的延迟线设计,特别在编解码器材料体系不同时,保证收发端干涉仪两臂延时值的精确匹配仍是一项颇具难度的技术挑战。对光量子偏振态的编解码通常采用路径-偏振转换器件来完成,通过偏振旋转分束器或二维光栅等片上器件,可以实现偏振向路径编码的自由度映射,这一方案可以避免在片上对光模式直接调制,但会相对地增加系统复杂度,并引入额外的损耗。

相较于分立器件,集成化编解码器在结构稳定性、工艺一致性、器件加工精度和规模可拓展性等方面具有天然优势,然而 QKD 系统中所需的单光子级探测灵敏度、亚纳秒级时序操控精度、低插损、精确操控和抗信道扰动等特性,对集成器件的工作带宽、插损、偏振无关等性能提出了严苛的要求。因此,面向 QKD 实用化和规模化部署需求的集成光子器件优化,特别是高带宽、高精度的编码器件与低插损、低误码和抗干扰解码器的设计,仍是该领域的重要研究方向。

2.5 解码器与单光子探测器的集成

在 QKD 系统中,接收方 Bob 需要使用单光子探测器对 Alice 发送的量子态进行测量。当前常用的单光子探测器主要包括单光子雪崩二极管 (SPAD)^[76] 和超导纳米线单光子探测器 (SNSPD)^[77]。因其在用于 QKD 系统时,通常需要工作在低于室温的环境下,因此通常作为独立设备或模块,通过光纤与系统的解码器相连。

近年来,随着技术的不断进步, SNSPD 与其他光学器件的集成化研究取得了突破。2021 年, Beutel 等^[10]在氮化硅芯片上成功实现了 SNSPD 与基于不等臂 MZI 的解码器的集成[图 3(a)],构建了光学器件全集成的接收端芯片。基于该芯片,他们成功开展了重复频率高达 2.6 GHz 的时间戳-相位编码 QKD 实验。2022 年,该研究团队进一步拓展了集成规模,实现了支持四通道波分复用的 QKD 全集成接收端芯片^[78],如图 3(b)所示。

与此同时, Zheng 等^[79]在 2021 年将 MDI 协议所需的接收端器件与 SNSPD 集成在一起[图 3(c)],实现了在 24 dB 信道损耗下 6.166 kbit/s 的安全码率。这些研究工作展示了 SNSPD 的集成化潜力,为实现高性能、小型化的量子通信系统奠定了重要的技术基础。

3 集成量子密钥分发系统

3.1 量子密钥分发系统的集成化

集成光学技术的持续发展为 QKD 系统的大规模应用提供了理想的平台支持。研究者们迅速将其应用于 QKD 系统中,极大地推动了 QKD 的小型化和实用化进程。早在 2004 年, Honjo 等^[48]就基于 Silica 波导设计并实现了不等臂 MZI,并将其应用于实现基于 DPS 协议的 QKD 系统。此后,研究者相继基于 Silica 波导实现了 DPS 协议^[48,80]和相位编码 BB84 协议^[81-83]的集成化 QKD 方案。这些研究利用 Silica 波导的低损耗、高稳定性以及低偏振相关性等特性,通过不等臂干涉仪实现光脉冲的前后波包分离与干涉,但仍需结合铌

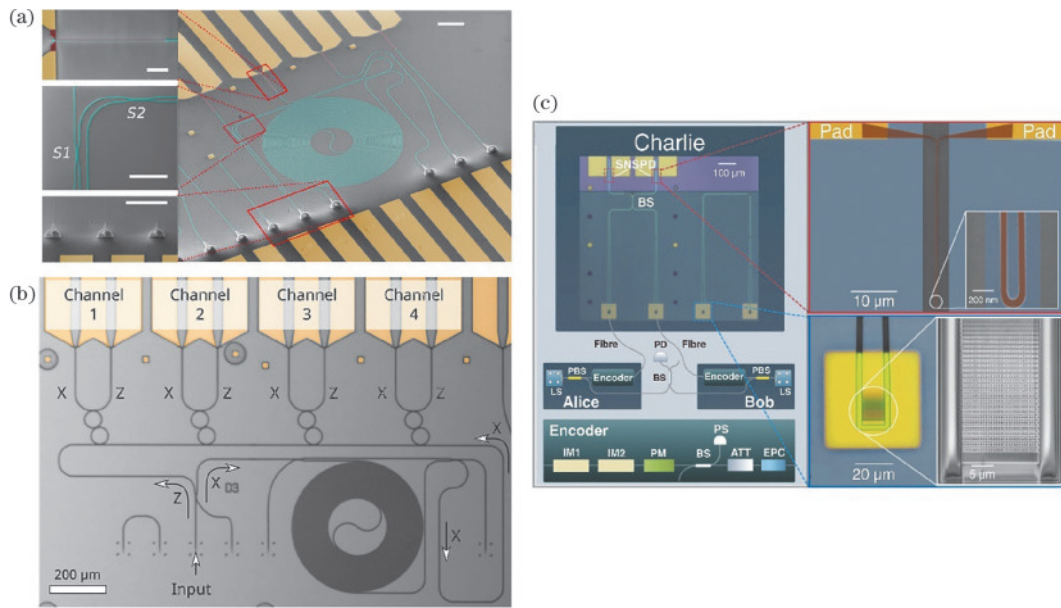


图 3 基于集成超导纳米线单光子探测器的量子密钥分发系统。(a)接收端芯片扫描电镜(SEM)图^[10]; (b)四通道接收端芯片显微镜图^[78]; (c) MDI协议实验装置和器件SEM图^[79]

Fig. 3 Quantum key distribution systems based on integrated superconducting nanowire single-photon detectors. (a) Scanning electron microscope (SEM) image of receiver chip^[10]; (b) microscope image of the receiver chip for four-channel systems^[78]; (c) schematic of the experiment setup for MDI protocols and the SEM image of the chip device^[79]

酸锂等外置的相位调制器件完成 QKD 过程中的信息编码。与传统分立器件相比,集成干涉仪已经在精度和稳定性等方面表现出显著优势。然而,由于 Silica 波导的尺寸较大且缺乏高速调制能力,限制了其在 QKD 系统中的应用。

随着集成光学技术的持续进步,集成材料体系愈发多样化,微纳加工工艺也日益成熟,为 QKD 系统的

小型化和高性能化提供了更强大的技术平台。在此背景下,集成 QKD 系统的研究进入了快速发展阶段。研究者们基于多种材料体系,实现了多种 QKD 协议的集成化方案。表 2、表 3 分别梳理了基于离散变量和连续变量协议的集成化 QKD 的主要研究成果,重点关注利用集成器件操控光量子态,完成 QKD 实验并成功获得密钥率的研究成果。

表 2 基于离散变量协议的集成化量子密钥分发系统的主要研究成果

Table 2 Main research results of the integrated QKD system based on discrete variable protocols

Reference	Year	Platform Tx	Platform Rx	Encoding way	Protocol	Clock rate	Distance (loss)	Key rate / (kbit/s)
[48]	2004	-	SiO ₂	-	DPS	1 GHz	20 km	3.08
[80]	2005	-	SiO ₂	-	DPS	1 GHz	105 km	0.21
[84]	2008	SiO ₂	SiO ₂	Phase	BB84	625 MHz	97 km	0.82
[72]	2016	Si	-	Polarization	BB84	10 MHz	5 km	0.95
[54]	2017	InP	SiO _x N _y	Time-bin	BB84	560 MHz	4 dB	345
				-	COW	860 MHz	4 dB	311
				-	DPS	1.72 GHz	4 dB	565
[50]	2017	Si	SiO _x N _y	-	COW	1.72 GHz	20 km	916
		Si	-	Polarization	BB84	1 GHz	20 km	329
[5]	2017	Si	Si	Path	HD-QKD	5 kHz	4 dB	7.5 × 10 ⁻³
[85]	2018	-	SiO ₂	Polarization	BB84	100 MHz	2 m	415
[86]	2018	Si	-	Polarization	BB84	625 MHz	43 km	157
[87]	2019	InP	Si	Phase	BB84	1 GHz	20 dB	270
				-	DPS	2 GHz	20 dB	400
[71]	2019	Si	Si	Time-bin	BB84	100 MHz	4 dB	85.7
[88]	2020	InP	-	Time-bin	MDI	250 MHz	20 dB	1.0
[89]	2020	Si	Si	-	COW	1.27 GHz	4 dB	792

表 2 (续)

Reference	Year	Platform Tx	Platform Rx	Encoding way	Protocol	Clock rate	Distance (loss)	Key rate / (kbit/s)
				-	DPS	2.54 GHz	4 dB	940
[6]	2020	-	Si	Polarization	BB84	10 MHz	4 dB	13.68
[90]	2020	Si	Si	Polarization	MDI	0.5 MHz	10 dB	1.46×10^{-3}
[30]	2020	Si	-	Polarization	MDI	1.25 GHz	36 dB	0.031
[10]	2021	-	Si ₃ N ₄	Time-bin	BB84	2.6 GHz	2.5 dB	2500
[91]	2021	Si	-	Polarization	MDI	1.25 GHz	24 dB	0.137
[92]	2021	Si	-	Polarization	BB84	50 MHz	145 m	30
[93]	2021	Si	-	Polarization	MDI	1.25 GHz	24 dB	0.4
[94]	2021	InP	SiO _x N _y	Phase	BB84	2 GHz	14 dB	500
				-	DPS	2 GHz	14 dB	400
				-	COW	2 GHz	14 dB	2500
[79]	2021	-	Si	Time-bin	MDI	125 MHz	24 dB	6.166
[95]	2021	InP	SiO _x N _y	Phase	T12	1 GHz	50 km	28
[74]	2022	Si	Si	Polarization	BB84	2 GHz	4 dB	868
[96]	2022	Si	-	Polarization	BB84	312.5 MHz	100 km	42.7
[97]	2022	SiO ₂	SiO ₂	Time-bin	BB84	1.25 GHz	50 km	1340
[78]	2022	-	Si ₃ N ₄	Time-bin	BB84	3.35 GHz	10 dB	1.217×10^4
[75]	2023	Si	Si	Polarization	BB84	50 MHz	100 km	0.24
[98]	2023	Si	-	Polarization	BB84	2.5 GHz	10 km	1.158×10^5
[99]	2023	Si	SiO ₂	Time-bin	BB84	2.5 GHz	202 km	9.4
[100]	2023	Si	Si	Polarization	BB84	50 MHz	150 km	0.866
[101]	2023	InP/ Si ₃ N ₄	InP/ Si ₃ N ₄	Time-bin	BB84	1 GHz	10 dB	1820
[102]	2024	Si	-	Polarization	BB84	2.5 GHz	21 dB	1018
[103]	2024	InP	-	SNS	TF	1 GHz	74.88 dB	8.53×10^{-3}
[104]	2025	SiO ₂	SiO ₂	Time-bin	BB84	625 MHz	18 dB	1.85

Notes: Tx is transmitter, Rx is receiver.

表 3 基于连续变量协议的集成化 QKD 系统的主要研究成果

Table 3 Main research results of the integrated QKD system based on continuous variable protocols

Reference	Year	Platform Tx	Platform Rx	Encoding way	Distance (loss)	Key rate / (kbit/s)
[105]	2019	Si	Si	Gaussian-modulated	2.0 m	250
[106]	2023	III-V/Si ₃ N ₄	III-V/Si ₃ N ₄	Gaussian-modulated	50.0 km	750
[107]	2024	-	Si	Gaussian-modulated	28.6 km	1380
[108]	2024	-	Si	Discrete-modulated	5.0 km	737 000
[109]	2024	-	Si	Gaussian-modulated	4.6 dB	220
[110]	2025	InP	-	Gaussian-modulated	11.0 km	78

Notes: Tx is transmitter, Rx is receiver.

2015 年, Sibson 等^[54,111]首次在会议中展示了多协议兼容的编解码端芯片,其结构如图 4 所示。发射端芯片基于 InP 材料平台,能够实现激光产生、快速调制和光强监测等功能。接收端采用硅基氮氧化硅(SiO_xN_y)材料,以降低插入损耗。整个系统仅需外接单光子探测器和控制驱动设备即可完成 QKD 过程。通过调整编解码端芯片上的驱动信号,研究者成功实现了基于时间戳-相位编码 BB84、DPS 和 COW 三种协议的 QKD 实验。在 4 dB 信道衰减下,估算得到的三种协议的安全码率分别为 345 kbit/s、311 kbit/s 和

565 kbit/s。

此外,该研究团队还基于 SOI 材料平台,设计并制作了适用于 COW、偏振编码和时间戳-相位编码 BB84 三种协议的编码器芯片^[50],其结构如图 5 所示。与文献[72]不同的是,偏振编码结构中采用二维光栅结构作为路径-偏振转换器件,将不同路径输入的光转换为不同的偏振态输出。实验结果显示,COW 协议和偏振编码 BB84 协议中的估算安全密钥率分别为 916 kbit/s 和 329 kbit/s,而时间戳-相位编码误码率为 2.1%,但未给出安全密钥率。

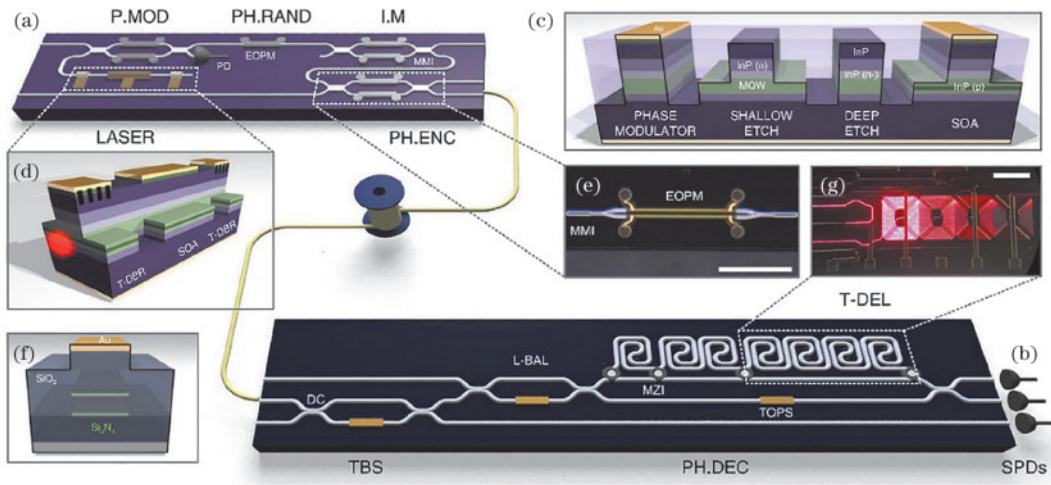


图 4 兼容多种 QKD 协议的集成光学芯片^[54]。(a)磷化铟集成发射端;(b)氮氧化硅集成接收端;(c)磷化铟波导横截面;(d)波长可调连续激光器;(e)MZI 显微镜图;(f)氮氧化硅波导横截面;(g)接收端延时线显微镜图

Fig. 4 Integrated photonic chips compatible with multiple QKD protocols^[54]. (a) Integrated InP transmitter; (b) integrated SiO_xN_y receiver; (c) InP waveguide cross-section; (d) wavelength tunable continuous wave laser; (e) microscopic image of the MZI; (f) SiO_xN_y waveguide cross-section; (g) microscopic image of the receiver delay lines

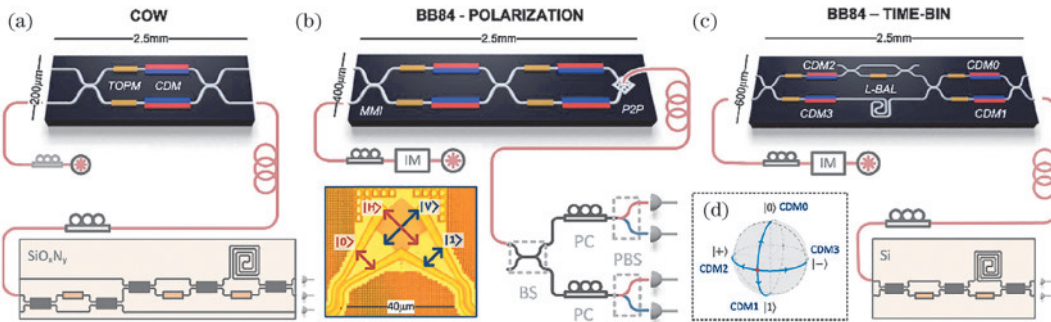


图 5 硅基光电子学 QKD 芯片^[50]。(a) COW 协议;(b)偏振编码 BB84 协议;(c)时间戳-相位编码 BB84 协议;(d) Bloch 球示意图

MDI 协议能够有效抵御针对探测器端的攻击,显著提升 QKD 系统的实际安全性。因此,MDI-QKD 的集成化方案研究受到了广泛关注,并迅速发展。2020 年, Semenenko 等^[88]基于 InP 材料平台,研制出时间戳-相位编码 MDI-QKD 的全集成发射端。如图 6(a)所示,该芯片集成了激光光源、斩波、相位调制和强度调制等多种功能器件。在 250 MHz 的系统重复频率下,研究组在 20 dB 信道衰减条件下获得了 1 kbit/s 的安全密

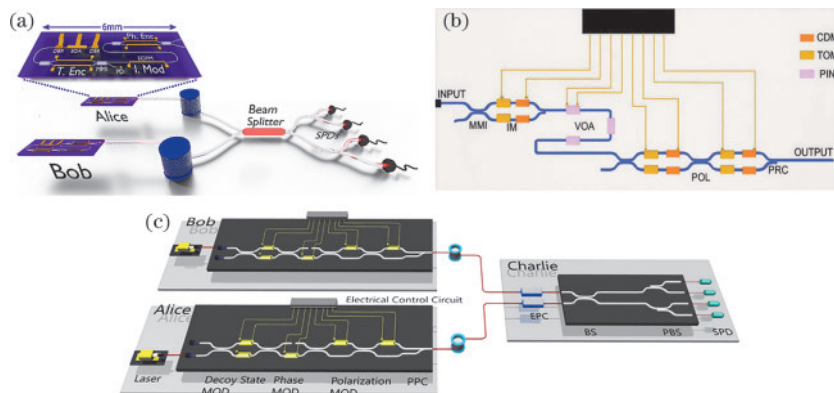


图 6 集成化 MDI-QKD 方案示意图。(a)基于 InP 材料的发射端芯片^[88];(b)基于 SOI 材料的高速量子态制备芯片^[30];(c)基于 SOI 材料的制备+测量芯片^[90]

Fig. 6 Schematic diagram of the integrated MDI-QKD schemes. (a) Transmitter chip based on InP material^[88]; (b) high-speed quantum state preparation chip based on SOI material^[30]; (c) preparation and measurement chip based on SOI material^[90]

钥率。同年,Wei等^[30]基于SOI材料平台,研制了兼容片上高速调制的偏振编码MDI-QKD量子态制备芯片。如图6(b)所示,该芯片在1.25 GHz的重复频率下,实现了36 dB信道衰减下31 bit/s的安全密钥率。同年,Cao等^[90]同样基于SOI材料平台,设计并制备了偏振编码MDI-QKD的制备端和测量端芯片,如图6(c)所示。该芯片在0.5 MHz的重复频率下实现了10 dB信道衰减下每脉冲 2.9×10^{-6} 的安全密钥率。尽管制备端的激光器需要外置且无法实现高速调制,但该方案成功将接收端(除单光子探测器外)的其他组件集成化,展示了全集成化系统的潜力。2021年,Zheng等^[79]将超导纳米线单光子探测器与MDI-QKD测量端异质集成,验证了MDI-QKD测量端全集成的可行性[图3(c)]。

除上述常见协议的集成化研究外,研究者还广泛拓展了多种QKD协议的集成化。这些协议包括路径编码的BB84协议^[112]、T12协议^[95]、基于纠缠的协议(如BBM92协议^[113-114]),以及高维编码QKD系统^[5,115]等。此外,连续变量QKD因其无需单光子探测器,在集成化过程中展现出独特的优势,成为近年来的研究热点之一,并取得了多项重要成果^[105-110]。

3.2 面向应用的集成量子密钥分发系统

作为一项朝着网络化和大规模部署方向发展的量子信息技术,QKD的集成化过程不仅需要关注技术的实现和性能的提升,还必须充分考虑系统的实用化特性。例如,此前介绍的多协议兼容芯片^[54]基于QKD系统中共通的基本功能器件,利用集成光器件的可重构性和可拓展性,通过优化功能结构设计,实现了面向实际应用需求的片上器件结构。该方案增强了系统的灵活性和兼容性,拓展了QKD系统的适用场景。

小型化是集成光学器件的固有优势,而逐渐成熟的工艺和封装能力进一步提升了QKD的集成度和系统性。近年来,激光器和单光子探测器已能够在多种平台上与编解码结构集成,实现了全片上的发射端或接收端结构^[54,87,95,101,106]。2019年,Paraiso等^[87]基于光源相位直接调制方法,开发出无调制器的InP发射端芯片,并结合基于硅基干涉仪结构的集成解码器,成功实现了time-bin编码的BB84协议和DPS协议,如图7(a)所示。2021年,该研究组进一步完成了QKD发射端、接收端以及量子随机数发生器等一系列QKD系统组件的封装,如图7(b)^[95]所示。2023年,该研究组通过将InP和SiN材料混合封装,实现了收发双工的QKD集成化芯片,其结构如图7(c)^[101]所示。这一系列工作极大地推进了QKD的实用化进程。

稳定性是影响QKD系统性能的关键因素之一。QKD的安全性要求通信双方准确评估泄露至窃听者的信息量,这一过程高度依赖于QKD系统的稳定性。温度涨落、振动等环境因素对光纤线路和光学器件不可避免地存在扰动,并引起双折射等特性的变化,从而

带来光量子偏振态的变化。尽管集成器件在稳定性上相较于分立器件具有一定的优势,但对量子态的编解码与探测仍可能因为这些扰动而产生误码,因此必须对其进行抵御或补偿。

为抵御这些扰动,研究者提出了多种解决方案,大致可以分为主动和被动两类。主动方法通过使用偏振调节器件并结合系统根据测量信号的反馈机制进行动态补偿。目前,大多数的集成QKD实验仍依赖外置偏振补偿器件。2023年,Du等^[75]在SOI平台上首次实现了可片上补偿信道偏振变化的集成偏振解码器件,其结构如图8(a)所示。研究者在考虑有限长效应的前提下,在100 km单模光纤信道中实现了240 bit/s的安全密钥率。随后,该研究组进一步结合SOI偏振编码芯片,成功实现150 km光纤信道下866 bit/s的安全密钥率,进一步提升了系统集成度和性能^[100]。

然而,无论是分立器件还是集成器件,主动补偿方案往往会增加系统复杂度并消耗额外的系统资源。通过协议和方案设计实现系统对偏振扰动的自动补偿,则是一种更为根本且高效的解决方案。Nambu等^[82]和Li等^[116]基于MZI结构提出了一种通过精确控制芯片温度最小化准TE和准TM模式的有效折射率差以消除偏振相关性的解决方案。不过,该方法要求芯片在宽温度范围内寻找工作点,对温度控制单元提出了严格的要求,同时还会增加系统能耗,有待进一步优化。2022年,Zhang等^[97]利用硅基二氧化硅材料与法拉第反射镜混合封装的方法,实现了基于不等臂法拉第-迈克耳孙干涉仪的时间戳-相位编码BB84协议QKD实验,其实验方案如图8(b)所示。该干涉仪能够自动补偿环境引起的偏振扰动。实验结果表明,在额外随机扰偏的条件下,干涉可见度可长期保持在98.5%以上^[117]。在考虑有限长效应的前提下,研究者在50 km单模光纤信道中获得了1.34 Mbit/s的安全密钥率。

实际环境部署是验证QKD系统性能的重要手段。2018年,Bunandar等^[86]首次报道了集成QKD系统的外场部署研究。如图9(a)所示,他们在学校与林肯实验室之间部署了一套基于SOI偏振编解码器的BB84协议QKD实验系统,在43 km光纤信道中获得了157 kbit/s的安全密钥率。2021年,Avesani等^[92]利用SOI偏振编码器实现了日光条件下的自由空间BB84协议集成QKD外场测试实验,如图9(b)所示。研究者利用快反镜构建反馈结构以修正低阶像差,从而在含有日光的条件下,在9 h内通过145 m长的自由空间信道,获得了平均30 kbit/s的安全密钥率。这些外场测试结果表明,集成QKD系统不仅在实验室环境中表现出色,还能在实际复杂环境下稳定运行,为未来量子通信网络的部署提供了重要参考。

集成光子学器件因其低成本和可拓展性,在量子通信网络化方面展现出巨大的应用潜力,相关研究持

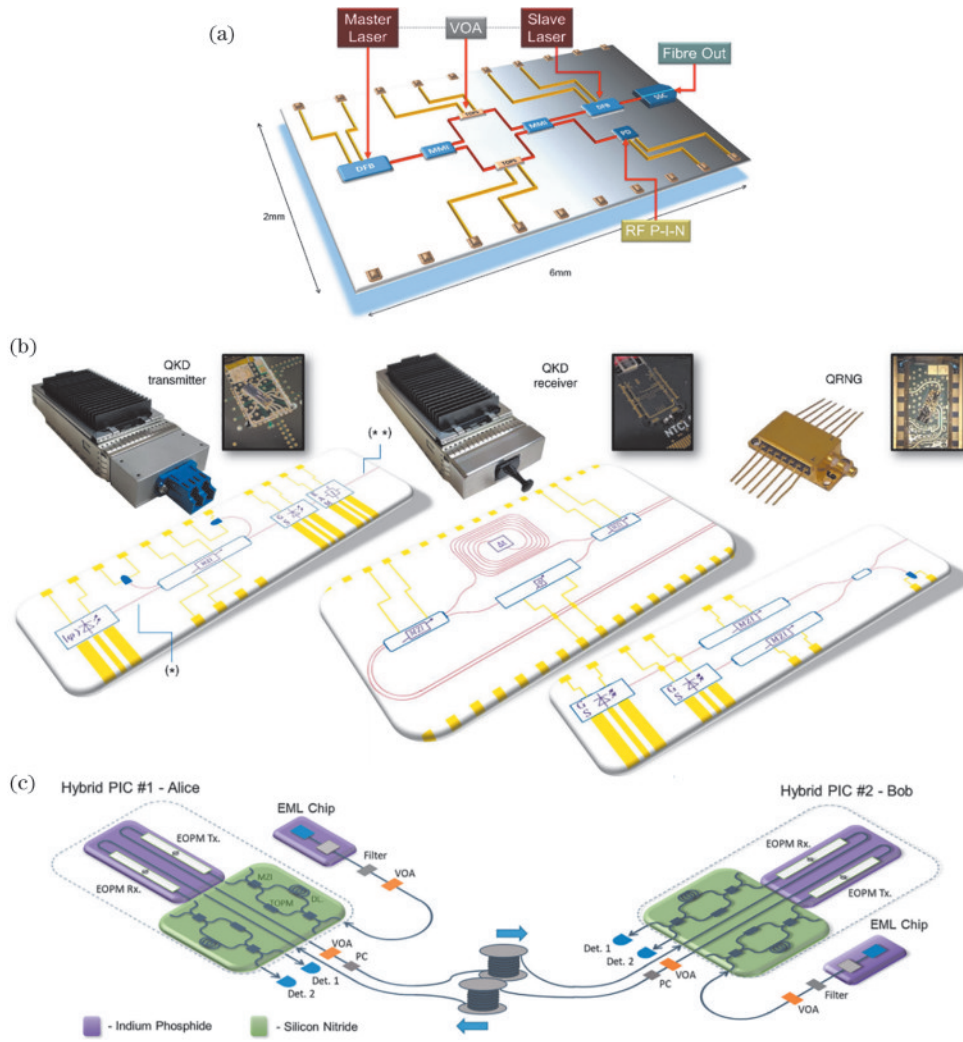


图 7 小型化和高集成度的 QKD 方案。(a)无调制器发射端芯片^[87]；(b) QKD 模组和芯片^[95]；(c)混合集成的 QKD 收发芯片和系统^[101]
 Fig. 7 QKD schemes with miniaturization and high integration. (a) Modulator-free transmitter chip^[87]; (b) QKD modules and chips^[95];
 (c) hybrid integrated QKD transceiver and system^[101]

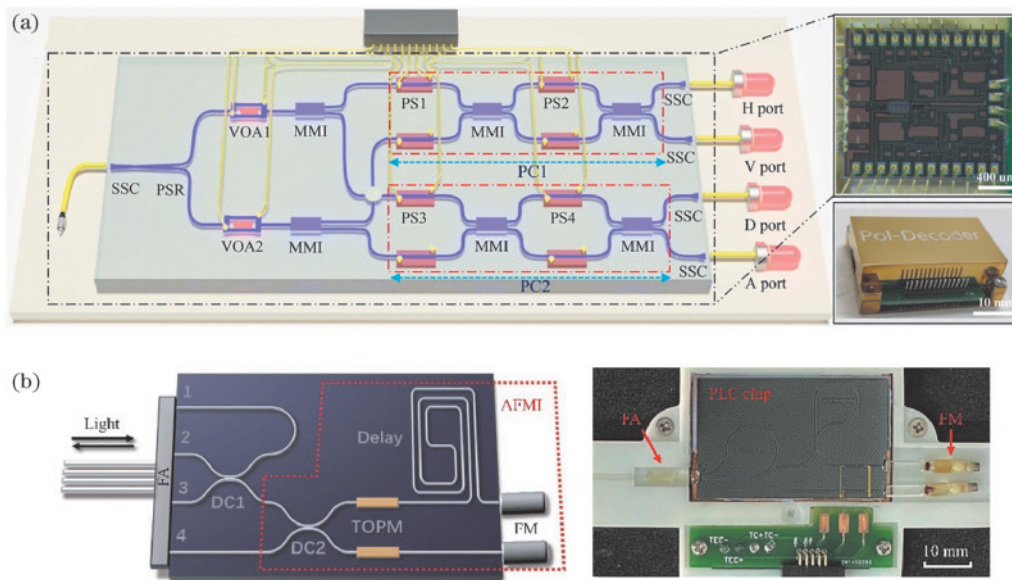


图 8 可抵御偏振扰动的集成 QKD 方案。(a)可主动反馈偏振变化的解码器芯片^[75]；(b)可自动补偿偏振变化的解码器芯片^[97]
 Fig. 8 Integrated QKD schemes resistant to polarization disturbance. (a) Decoder chip with active feedback for polarization variations^[75];
 (b) decoder chip of automatically compensating for polarization variations^[97]

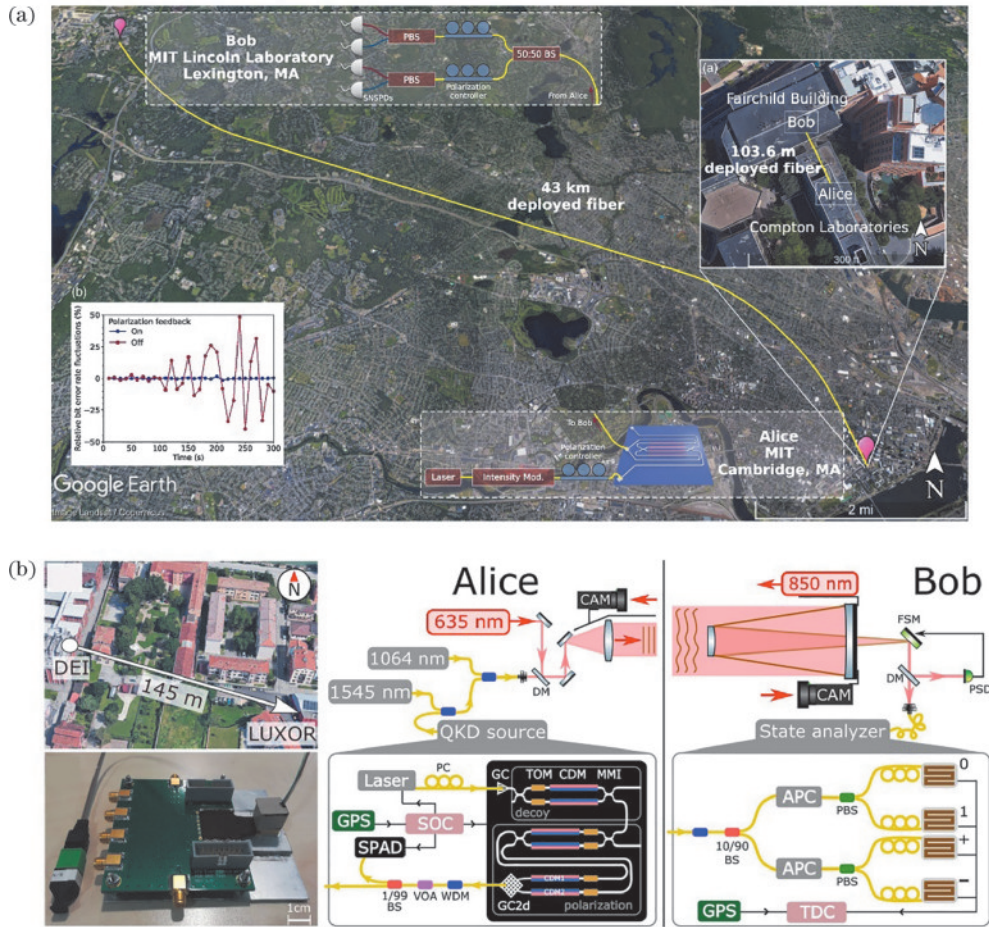


图 9 集成化 QKD 实地测试实验系统。(a) 43 km 暗光纤实验系统鸟瞰图^[86]；(b) 145 m 自由空间实验系统鸟瞰图和实验装置^[92]
 Fig. 9 Integrated QKD field trial experimental systems. (a) Aerial view of the 43 km dark fiber link experimental system^[86]; (b) aerial view and setups of the 145 m free space experimental system^[92]

续涌现。例如,研究者开发了可供多用户使用的片上纠缠光子源^[113-114]和片上 Kerr 光孤子源^[65],这些光源能够高效地为多用户 QKD 系统提供量子态。此外,时分复用^[6]、波分复用^[78]、空分复用^[112]等技术也被应用于集成 QKD 系统中,显著提升了系统的用户容量。这些成果为构建大规模量子通信网络奠定了坚实基础,推动了量子通信技术向实用化和网络化方向发展。

4 集成量子密钥分发系统的实际安全性

QKD 系统的实际安全性一直是该领域的核心研究方向之一。随着集成 QKD 系统的不断发展,器件结构尺寸的减小、材料体系的变化以及器件工作机理的差异,集成化既可以提升 QKD 系统的安全性,也可能引入新的安全隐患。因此,针对集成量子器件在 QKD 实际安全性方面的研究显得尤为重要。

4.1 激光损伤攻击

在 QKD 系统中,光衰减器是将相干光脉冲的平均光子数衰减至单光子量级的关键器件。在系统运行过程中,如果光衰减器的衰减量发生预期之外的变化,通信双方对误码率的估计将变得不准确,从而导致安全

密钥率估计错误,引入安全性问题。

2020 年, Huang 等^[118]提出了一种利用高功率激光器对光衰减器进行损伤的攻击方案,并在实际光纤 QKD 系统中进行了验证。实验结果表明,被测试的常用光纤衰减器几乎都无法抵御这种攻击。因此,需要在实验系统中额外增加类似于“光保险丝”的装置,该装置仅允许一定功率内的激光通过,一旦注入功率超过阈值,装置将永久断开。该研究团队进一步研究发现^[119],现有的光纤隔离器和环形器具有类似的保护特性,可用于防止高功率光注入攻击,从而保护光纤 QKD 系统。

同年,该研究团队还分析了集成 QKD 系统在面对高功率激光损伤攻击时的性能表现^[120]。他们对基于 InP 材料平台的 QKD 发射端芯片进行了相关测试,如图 10 所示。实验结果表明,模斑转换器(用于匹配芯片与光纤之间的光场模式,以最大化端面耦合效率)首先出现烧毁现象。一旦模斑转换器被烧毁,该处耦合相当于断路,从而起到“光保险丝”的作用,防止芯片内部器件受到更高功率激光的进一步损伤。

对于通信双方而言,一旦集成 QKD 系统遭受窃听者发起的激光损伤攻击,系统将立即终止运行,从而及

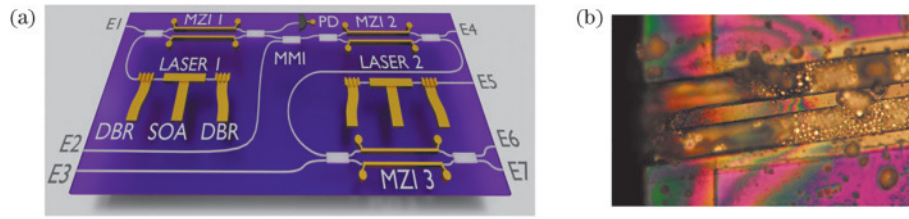


图 10 集成 QKD 芯片激光损伤攻击^[120]。(a) InP 材料 QKD 发射端芯片示意图；(b) 损伤的模斑转换器

Fig. 10 Laser damage attack on an integrated QKD chip^[120]. (a) Schematic diagram of the InP QKD transmitter chip; (b) damaged spot size converter

时保证密钥的安全。因此,基于 InP 材料平台的集成 QKD 系统在应对激光损伤攻击时具有天然的安全优势。然而,对 SOI、LNOI 等其他平台以及其他封装方式的相关研究仍需进一步开展,以评估其在类似攻击下的安全性。

4.2 特洛伊木马攻击

特洛伊木马攻击(TPA)是一种针对 QKD 系统发射端的攻击方法。在实施 TPA 时,攻击者向发射端反向注入大量特洛伊光子,这些光子与信号光子一起在发射端被调制,从而携带量子态的编码信息。同时,特洛伊光子在经过发射端的各个器件时会发生反射,窃听者可以通过测量这些反射光子来获取量子态的编码信息。研究表明^[121],QKD 系统中反射回来的特洛伊

光子数量与系统的隔离度和反射率密切相关,并直接决定了窃听者可能获取的信息量。因此,评估实际 QKD 系统对 TPA 的安全性,关键在于评估系统对特洛伊光子的反射特性。

2021 年, Tan 等^[93]对 SOI 材料的偏振编码 QKD 集成芯片进行了 TPA 相关测试,如图 11 所示。在该芯片中,强度调制器和偏振调制器包含重要的编码信息,是窃听者实施攻击的主要目标。测试结果显示,芯片的反射峰主要来自芯片三种内部组件:多模干涉耦合器、监控用光电二极管和光栅耦合器。具体而言,能泄露偏振调制器和强度调制器调制信息的反射峰的总反射率分别为 -64.45 dB 和 -86.10 dB,分别对应图 11(b) 中的虚线方框和实线方框内的反射峰。

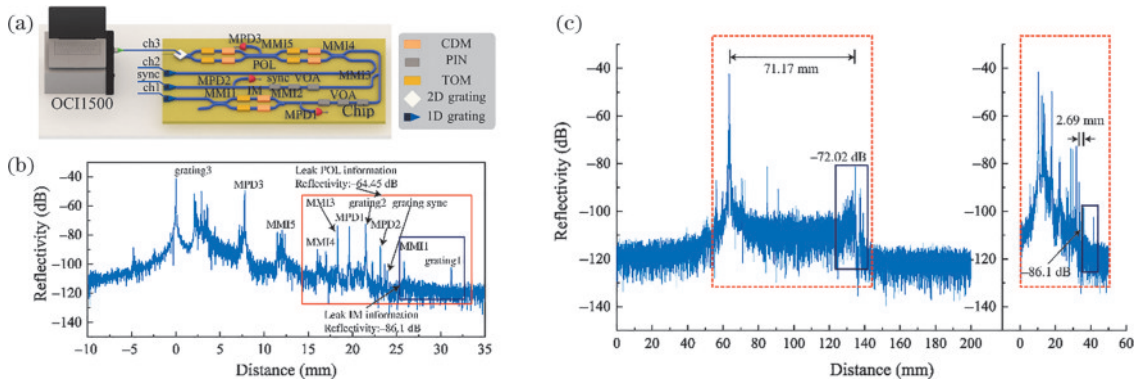


图 11 硅基 QKD 芯片反射率测试^[93]。(a) 硅基发射器芯片和反射率测试实验示意图；(b) 硅芯片内的反射率；(c) 光纤调制器和硅基芯片的反射率对比

Fig. 11 Reflectivity experiments on a silicon-based QKD chip^[93]. (a) Schematic of the silicon-based transmitter chip and reflectivity measurement experiment; (b) reflectivity inside the silicon chip; (c) comparison of reflectivity between the fiber optic modulator and silicon-based chip

作为对比,该研究组还测试了光纤 QKD 系统中常用的铌酸锂体波导强度调制器,其反射峰主要来自光纤与铌酸锂芯片的两个端面连接处。仅有反射经过调制器波导的光子才会携带调制信息,其反射率为 -72.02 dB,对应图 11(c) 中的实线方框。

因此,在 TPA 下,集成 QKD 发射端的反射率明显低于在光纤 QKD 系统中所用的铌酸锂调制器的反射率(约低 14.08 dB)。此外,由于芯片尺寸较小,其内部的反射峰间隔更小(集成器件中的 2.69 mm 相比于光纤系统中的 71.17 mm)。这意味着窃听者需要注入更多的特洛伊光子来进行攻击。然而,集成 QKD 芯片允

许注入的最大光强更低,从而限制了窃听者所能够注入的最大光子数。尽管集成和光纤 QKD 系统都需要额外增加隔离器以保证 TPA 下的安全性,但相对而言,集成 QKD 芯片对 TPA 具有更高的容忍度。

4.3 调制相关损耗的影响

SOI 和 InP 是目前工艺水平较为成熟的材料平台,因此现有高速调制 QKD 发射端芯片大多基于这两种材料制备。InP 材料平台中的高速相位调制器主要基于 Franz-Keldysh 效应和量子限制斯塔克效应,而 SOI 平台中的高速相位调制器主要基于等离子体色散效应。这两种机制均属于电致吸收效应^[122],即在调制

波导折射率实部的同时,也会改变折射率的虚部。折射率虚部的改变意味着传输损耗的变化,从而导致量子态在相位调制时存在调制相关损耗。此外,片上的强度和偏振调制器通常基于相位调制器制备,调制相关损耗的存在会导致量子态的强度、相位以及偏振信息产生关联。这种非理想特性违背了 QKD 协议的安全性假设,可能会成为侧信道并引入潜在的安全性问题。

为解决这一问题,研究者们从 QKD 协议设计和片上器件设计两个层面提出了相应的解决方案。在协议设计层面, Li 等^[123]提出了一种通过抛弃强度过大的量子态来实现可容忍偏振相关损耗的协议。虽然该方案可以降低偏振相关损耗的影响,但抛弃部分信号态也会导致安全密钥率的降低。

在器件设计层面,目前存在多种解决方案。从机理上来说,相位调制器的透过率变化程度与调制相位成正比。因此,减小相位调制器的调制范围可以在一定程度上解决这一问题。Sibson 等^[50]利用额外的热光相位调制器将干涉仪两臂设置到合适的偏置工作点,

将基于等离子体色散效应的高速相位调制器的调制范围限制在 $\pi/2$ 以内。但即使在这种情况下,仍然存在约 20% 的透过率变化。Dai 等^[89]则采用了一种名为 Pass-Block 的结构来实现理想的 0 和 π 相位的调制。然而,这种结构仅能实现这两个相位点的调制,无法灵活调节相位。Dupuis 等^[124]设计了一种名为 Shift-and-Dump 相位调制器的结构。该结构基于载流子注入型相位调制器的透过率变化与相位的关系,通过求解特定相位点的方程组来确定所需的结构参数。它可以实现任意两个相位点的透过率不变相位调制,但相位点在设计时已固定,无法灵活调节,且对加工误差的容忍度较低。

2022 年, Ye 等^[125]设计了一种透过率恒定相位调制器,如图 12 所示。该结构基于 SOI 材料平台的 MZI 结构,能够实现 $[0, 2\pi]$ 全相位范围内的透过率恒定相位调制。此外,该结构还具有工艺容差大和普适性好的优点,能够基于现有调制深度不足的相位调制器实现更大的相位调制深度,拓展现有器件的应用场景,满足 QKD 对相位调制器的安全性要求和调制需求。

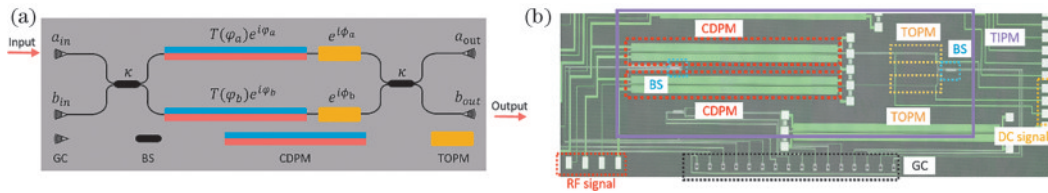


图 12 透过率恒定相位调制器^[125]。(a)调制器示意图;(b)调制器显微镜图

Fig. 12 Transmittance-invariant phase modulator^[125]. (a) Schematic diagram of the modulator; (b) microscope image of the modulator

4.4 光折变效应可能引起的潜在安全性问题

基于铌酸锂体波导的高速调制器件在光纤 QKD 系统中得到了广泛应用。近年来,薄膜铌酸锂凭借其在调制效率和集成度方面的优势,逐渐成为研究热点。与 SOI 平台相比,薄膜铌酸锂能够在更低功耗下实现更高的调制效率和带宽。此外,基于线性电光效应的铌酸锂调制器不存在调制相关损耗问题。

然而,研究发现铌酸锂材料中的光折变效应可能对 QKD 系统的实际安全性构成严重威胁。光折变效应是指电光材料在辐照光作用下,折射率随光强空间分布发生变化的现象^[126]。其过程如图 13^[127]所示,随着辐照光的注入,铌酸锂波导的折射率会发生改变,进

而影响相位、振幅、偏振等调制结果。若窃听者向发射端反向注入辐照光,可能改变铌酸锂器件的工作状态,从而实施攻击并窃取安全密钥。

Ye 等^[127-128]研究发现,光折变效应可被窃听者利用,作为一种针对 QKD 系统源端的攻击机制。窃听者使用短波长攻击光,能够穿透部分隔离器件,并利用光折变效应以极低的注入光能量控制 QKD 用户的源端,诱导收发双方在不被察觉的情况下生成不安全的密钥。该研究团队设计了一种最优攻击策略,并针对未加设防的 MDI-QKD 系统进行了攻击演示实验,成功获取了几乎全部密钥。同时提出了防御措施,如状态监控、器件合理布局和及时校准等,可有效抵御此类攻击。Han 等^[129]进一步研究了多种铌酸锂体波导相位和强度调制器件在光折变攻击下的性能表现,并系统分析了相关的攻击机制与防御策略。这些研究为 QKD 系统的安全性分析提供了新的视角,为该技术的实用化和标准化发展奠定了重要基础。

除上述攻击方法外, Li 等^[91]利用 SOI 编码端芯片,针对恶意设备攻击的安全性进行了研究。Chen 等^[130]则针对太空辐射环境对 QKD 芯片的影响进行了研究,结果表明,在低剂量辐照下,芯片的基本功能和性能未发生显著变化,仅插入损耗略有降低。这些研究以

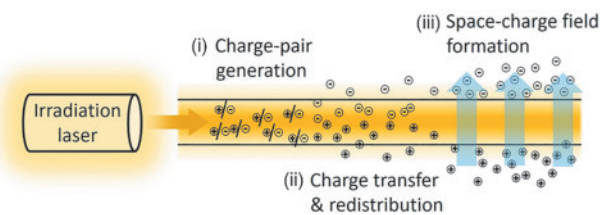


图 13 光折变效应过程示意图^[127]

Fig. 13 Schematic diagram of the photorefractive effect procedure^[127]

QKD 芯片为基础,为其实用化场景下的安全性分析和防护措施设计提供了重要参考。

虽然针对集成 QKD 的实际安全性研究已获得关注并取得了多项研究成果,但现有工作仍主要聚焦在集成器件的材料本征特性(如器件的激光损伤阈值、基于电致吸收效应的高速调制方法、铈酸锂材料光折变特性等)对系统安全性的影响机制。后续仍需系统地加强对集成 QKD 的实际安全性研究,可能的研究方向包括:1)挖掘集成器件的潜在安全性漏洞,并提出相应防护措施;2)研究具备更优安全特性和抗干扰能力的集成器件,构建主动防御机制;3)结合器件特性和实际安全性问题,优化协议并修正码率计算方法,提升系统容忍非理想特性的能力和判别的准确性;4)完善对集成 QKD 系统的安全评估体系和测评技术,推动集成器件的标准化进程。

5 结束语

本文系统介绍了集成 QKD 的相关内容。从集成材料和工艺平台、QKD 基础功能器件、典型的集成 QKD 系统及其实用化进展等维度进行了总结和分析,同时探讨了集成光子平台对 QKD 实际安全性带来的影响,梳理了分析的新角度和新案例。总体而言,集成化 QKD 技术已经完成了从 BB84 协议到测量设备无关协议等多种通信协议在不同材料平台上的原理验证,并成功实现了芯片级 QKD 系统的演示验证,未来的研究需要在性能、实用性和安全性等方面开展更深入的探索。具体而言,在提升集成化 QKD 系统性能方面,可通过优化各材料体系下的集成器件参数,结合 RRDPS 协议、TF 协议和高维编码等新型 QKD 协议,同时面向量子保密通信网络的规模化、智能化需求开展集成化设计。在实用化方面,突破隔离器、环形器、法拉第反射镜等关键无源器件的片上集成,发展先进的混合集成封装技术,以实现系统在偏振不敏感性、长期稳定性、低功耗和小型化等方面的实用化需求。此外,亟需加快发展集成化 QKD 系统的安全评估体系和测评技术,重点研究集成器件在材料、工艺等方面的特性及其对安全性可能产生的影响,并提出相应的防护措施,以此提升集成化 QKD 系统的实际安全性,为其大规模部署和应用奠定基础。

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] Xu F H, Ma X F, Zhang Q, et al. [Secure quantum key distribution with realistic devices](#)[J]. *Reviews of Modern Physics*, 2020, 92(2): 025002.
- [3] Yan J B, Fang L, Sun Z H, et al. [Complete active-passive photonic integration based on GaN-on-silicon platform](#)[J]. *Advanced Photonics Nexus*, 2023, 2(4): 046003.
- [4] Cherchi M, Bera A, Kemppinen A, et al. [Supporting quantum technologies with an ultralow-loss silicon photonics platform](#)[J]. *Advanced Photonics Nexus*, 2023, 2(2): 024002.
- [5] Ding Y H, Bacco D, Dalgaard K, et al. [High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits](#)[J]. *NPJ Quantum Information*, 2017, 3: 25.
- [6] Kong L W, Li Z H, Li C X, et al. [Photonic integrated quantum key distribution receiver for multiple users](#)[J]. *Optics Express*, 2020, 28(12): 18449-18455.
- [7] He M B, Xu M Y, Ren Y X, et al. [High-performance hybrid silicon and lithium niobate Mach-Zehnder modulators for 100 Gbit s⁻¹ and beyond](#)[J]. *Nature Photonics*, 2019, 13(5): 359-364.
- [8] Bonaccorso F, Sun Z, Hasan T, et al. [Graphene photonics and optoelectronics](#)[J]. *Nature Photonics*, 2010, 4(9): 611-622.
- [9] Feng L T, Guo G C, Ren X F. [Progress on integrated quantum photonic sources with silicon](#)[J]. *Advanced Quantum Technologies*, 2020, 3(2): 1900058.
- [10] Beutel F, Gehring H, Wolff M A, et al. [Detector-integrated on-chip QKD receiver for GHz clock rates](#)[J]. *NPJ Quantum Information*, 2021, 7: 40.
- [11] Halir R, Bock P J, Cheben P, et al. [Waveguide sub-wavelength structures: a review of principles and applications](#)[J]. *Laser & Photonics Reviews*, 2015, 9(1): 25-49.
- [12] Cheben P, Halir R, Schmid J H, et al. [Subwavelength integrated photonics](#)[J]. *Nature*, 2018, 560(7720): 565-572.
- [13] Yu Z J, Xi X, Ma J W, et al. [Photonic integrated circuits with bound states in the continuum](#)[J]. *Optica*, 2019, 6(10): 1342-1348.
- [14] Bütow J, Eismann J S, Sharma V, et al. [Generating free-space structured light with programmable integrated photonics](#)[J]. *Nature Photonics*, 2024, 18(3): 243-249.
- [15] Kwek L C, Cao L, Luo W, et al. [Chip-based quantum key distribution](#)[J]. *AAPPS Bulletin*, 2021, 31(1): 15.
- [16] Aldama J, Sarmiento S, Grande I H L, et al. [Integrated QKD and QRNG photonic technologies](#)[J]. *Journal of Lightwave Technology*, 2022, 40(23): 7498-7517.
- [17] Liu Q, Huang Y M, Du Y Q, et al. [Advances in chip-based quantum key distribution](#)[J]. *Entropy*, 2022, 24(10): 1334.
- [18] Luo W, Cao L, Shi Y Z, et al. [Recent progress in quantum photonic chips for quantum communication and Internet](#)[J]. *Light: Science & Applications*, 2023, 12: 175.
- [19] Benioff P. [The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines](#)[J]. *Journal of Statistical Physics*, 1980, 22(5): 563-591.
- [20] Shor P W. [Algorithms for quantum computation: discrete logarithms and factoring](#)[C]//*Proceedings 35th Annual Symposium on Foundations of Computer Science*, November 20-22, 1994, Santa Fe, NM, USA. New

- York: IEEE Press, 1994: 124-134.
- [21] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050-2056.
- [22] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121-3124.
- [23] Scarani V, Acín A, Ribordy G, et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations[J]. Physical Review Letters, 2004, 92(5): 057901.
- [24] Ekert A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661-663.
- [25] Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell's theorem[J]. Physical Review Letters, 1992, 68(5): 557-559.
- [26] 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.
- [27] Masanes L, Pironio S, Acín A. Secure device-independent quantum key distribution with causally independent measurement devices[J]. Nature Communications, 2011, 2: 238.
- [28] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.
- [29] 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.
- [30] Wei K J, Li W, Tan H, et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics[J]. Physical Review X, 2020, 10(3): 031030.
- [31] Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557(7705): 400-403.
- [32] Inoue K, Waks E, Yamamoto Y. Differential phase shift quantum key distribution[J]. Physical Review Letters, 2002, 89(3): 037902.
- [33] Stucki D, Brunner N, Gisin N, et al. Fast and simple one-way quantum key distribution[J]. Applied Physics Letters, 2005, 87(19): 194108.
- [34] Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance[J]. Nature, 2014, 509(7501): 475-478.
- [35] Cerf N J, Lévy M, Assche G V. Quantum distribution of Gaussian keys using squeezed states[J]. Physical Review A, 2001, 63(5): 052311.
- [36] Ng S Q, Kanitschar F, Zhang G, et al. Gigabit-rate quantum key distribution on integrated photonic chips [EB/OL]. (2025-04-11)[2025-05-04]. <https://arxiv.org/abs/2504.08298v1>.
- [37] Pi Y D, Wang H, Pan Y, et al. Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100 km fiber[J]. Optics Letters, 2023, 48(7): 1766-1769.
- [38] Hajomer A A E, Derkach I, Jain N, et al. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator[J]. Science Advances, 2024, 10(1): eadi9474.
- [39] Zhang Y C, Bian Y M, Li Z Y, et al. Continuous-variable quantum key distribution system: past, present, and future[J]. Applied Physics Reviews, 2024, 11(1): 011318.
- [40] Doerr C R, Okamoto K. Advances in silica planar lightwave circuits[J]. Journal of Lightwave Technology, 2006, 24(12): 4763-4789.
- [41] Silverstone J W, Bonneau D, O'Brien J L, et al. Silicon quantum photonics[J]. IEEE Journal of Selected Topics in Quantum Electronics, 2016, 22(6): 390-402.
- [42] Blumenthal D J, Heideman R, Geuzebroek D, et al. Silicon nitride in silicon photonics[J]. Proceedings of the IEEE, 2018, 106(12): 2209-2231.
- [43] Augustin L M, Santos R, den Haan E, et al. InP-based generic foundry platform for photonic integrated circuits [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2018, 24(1): 6100210.
- [44] Qi Y F, Li Y. Integrated lithium niobate photonics[J]. Nanophotonics, 2020, 9(6): 1287-1320.
- [45] Luo Q, Bo F, Kong Y F, et al. Advances in lithium niobate thin-film lasers and amplifiers: a review[J]. Advanced Photonics, 2023, 5(3): 034002.
- [46] Bogdanov S, Shalaginov M Y, Boltasseva A, et al. Material platforms for integrated quantum photonics[J]. Optical Materials Express, 2017, 7(1): 111-132.
- [47] Davis K M, Miura K, Sugimoto N, et al. Writing waveguides in glass with a femtosecond laser[J]. Optics Letters, 1996, 21(21): 1729-1731.
- [48] Honjo T, Inoue K, Takahashi H. Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer[J]. Optics Letters, 2004, 29(23): 2797-2799.
- [49] Su Y K, Zhang Y, Qiu C Y, et al. Silicon photonic platform for passive waveguide devices: materials, fabrication, and applications[J]. Advanced Materials Technologies, 2020, 5(8): 1901153.
- [50] Sibson P, Kennard J E, Stanisc S, et al. Integrated silicon photonics for high-speed quantum key distribution [J]. Optica, 2017, 4(2): 172.
- [51] Kim S H, You J B, Rhee H W, et al. High-performance silicon MMI switch based on thermo-optic control of interference modes[J]. IEEE Photonics Technology Letters, 2018, 30(16): 1427-1430.
- [52] Reed G T, Mashanovich G, Gardes F Y, et al. Silicon optical modulators[J]. Nature Photonics, 2010, 4(8): 518-526.
- [53] Baets R, Subramanian A Z, Clemmen S, et al. Silicon photonics: silicon nitride versus silicon-on-insulator[C]// Optical Fiber Communication Conference, March 20-22, 2016, Anaheim, California. Washington, DC: OSA,

- 2016: Th3J.1.
- [54] Sibson P, Erven C, Godfrey M, et al. [Chip-based quantum key distribution](#)[J]. *Nature Communications*, 2017, 8: 13984.
- [55] Chen G Y, Li N X, Ng J D, et al. [Advances in lithium niobate photonics: development status and perspectives](#) [J]. *Advanced Photonics*, 2022, 4(3): 034003.
- [56] Wang C, Zhang M, Chen X, et al. [Integrated lithium niobate electro-optic modulators operating at CMOS-compatible voltages](#)[J]. *Nature*, 2018, 562(7725): 101-104.
- [57] Crosnier G, Sanchez D, Bouchoule S, et al. [Hybrid indium phosphide-on-silicon nanolaser diode](#)[J]. *Nature Photonics*, 2017, 11(5): 297-300.
- [58] Semenenko H, Sibson P, Thompson M G, et al. [Interference between independent photonic integrated devices for quantum key distribution](#)[J]. *Optics Letters*, 2019, 44(2): 275-278.
- [59] Takemoto K, Nambu Y, Miyazawa T, et al. [Transmission experiment of quantum keys over 50 km using high-performance quantum-dot single-photon source at 1.5 \$\mu\text{m}\$ wavelength](#)[J]. *Applied Physics Express*, 2010, 3(9): 092802.
- [60] Zeng H Z J, Ngyuen M A P, Ai X Y, et al. [Integrated room temperature single-photon source for quantum key distribution](#)[J]. *Optics Letters*, 2022, 47(7): 1673-1676.
- [61] Lenzini F, Gruhler N, Walter N, et al. [Diamond as a platform for integrated quantum photonics](#)[J]. *Advanced Quantum Technologies*, 2018, 1(3): 1800061.
- [62] Castelletto S, Johnson B C, Ivády V, et al. [A silicon carbide room-temperature single-photon source](#)[J]. *Nature Materials*, 2014, 13(2): 151-156.
- [63] He Y M, Clark G, Schaibley J R, et al. [Single quantum emitters in monolayer semiconductors](#)[J]. *Nature Nanotechnology*, 2015, 10(6): 497-502.
- [64] Silverstone J W, Santagati R, Bonneau D, et al. [Qubit entanglement between ring-resonator photon-pair sources on a silicon chip](#)[J]. *Nature Communications*, 2015, 6: 7948.
- [65] Wang F X, Wang W Q, Niu R, et al. [Quantum key distribution with on-chip dissipative Kerr soliton](#)[J]. *Laser & Photonics Reviews*, 2020, 14(2): 1900190.
- [66] Caspani L, Xiong C L, Eggleton B J, et al. [Integrated sources of photon quantum states based on nonlinear optics](#)[J]. *Light: Science & Applications*, 2017, 6(11): e17100.
- [67] Arahira S, Murai H, Sasaki H. [Generation of highly stable WDM time-bin entanglement by cascaded sum-frequency generation and spontaneous parametric downconversion in a PPLN waveguide device](#)[J]. *Optics Express*, 2016, 24(17): 19581-19591.
- [68] Harada K I, Takesue H, Fukuda H, et al. [Indistinguishable photon pair generation using two independent silicon wire waveguides](#)[J]. *New Journal of Physics*, 2011, 13(6): 065005.
- [69] Subbaraman H, Xu X C, Hosseini A, et al. [Recent advances in silicon-based passive and active optical interconnects](#)[J]. *Optics Express*, 2015, 23(3): 2487-2511.
- [70] Parra J, Navarro-Arenas J, Sanchis P. [Silicon thermo-optic phase shifters: a review of configurations and optimization strategies](#)[J]. *Advanced Photonics Nexus*, 2024, 3(4): 044001.
- [71] Geng W, Zhang C, Zheng Y L, et al. [Stable quantum key distribution using a silicon photonic transceiver](#)[J]. *Optics Express*, 2019, 27(20): 29045-29054.
- [72] Ma C X, Sacher W D, Tang Z Y, et al. [Silicon photonic transmitter for polarization-encoded quantum key distribution](#) [J]. *Optica*, 2016, 3(11): 1274-1278.
- [73] Cai H, Long C M, DeRose C T, et al. [Silicon photonic transceiver circuit for high-speed polarization-based discrete variable quantum key distribution](#)[J]. *Optics Express*, 2017, 25(11): 12282-12294.
- [74] Zhang G L, Zhao Z Z, Dai J C, et al. [Polarization-based quantum key distribution encoder and decoder on silicon photonics](#)[J]. *Journal of Lightwave Technology*, 2022, 40(7): 2052-2059.
- [75] Du Y Q, Zhu X, Hua X, et al. [Silicon-based decoder for polarization-encoding quantum key distribution](#)[J]. *Chip*, 2023, 2(1): 100039.
- [76] Ribordy G, Gautier J D, Zbinden H, et al. [Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters](#)[J]. *Applied Optics*, 1998, 37(12): 2272-2277.
- [77] Gol'tsman G N, Okunev O, Chulkova G, et al. [Picosecond superconducting single-photon optical detector](#) [J]. *Applied Physics Letters*, 2001, 79(6): 705-707.
- [78] Beutel F, Brückerhoff-Plückelmann F, Gehring H, et al. [Fully integrated four-channel wavelength-division multiplexed QKD receiver](#)[J]. *Optica*, 2022, 9(10): 1121-1130.
- [79] Zheng X D, Zhang P Y, Ge R Y, et al. [Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution](#)[J]. *Advanced Photonics*, 2021, 3(5): 055002.
- [80] Takesue H, Diamanti E, Honjo T, et al. [Differential phase shift quantum key distribution experiment over 105 km fibre](#)[J]. *New Journal of Physics*, 2005, 7: 232.
- [81] Nambu Y, Yoshino K, Tomita A. [One-way quantum key distribution system based on planar lightwave circuits](#) [J]. *Japanese Journal of Applied Physics*, 2006, 45(6R): 5344.
- [82] Nambu Y, Yoshino K, Tomita A. [Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit](#)[J]. *Journal of Modern Optics*, 2008, 55(12): 1953-1970.
- [83] Tomita A, Yoshino K I, Nambu Y, et al. [High speed quantum key distribution system](#)[J]. *Optical Fiber Technology*, 2010, 16(1): 55-62.
- [84] Tanaka A, Fujiwara M, Nam S W, et al. [Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization](#)[J]. *Optics Express*, 2008, 16(15): 11354-11360.
- [85] Choe J S, Ko H, Choi B S, et al. [Silica planar lightwave circuit based integrated 1 \$\times\$ 4 polarization beam splitter](#)

- module for free-space BB84 quantum key distribution[J]. *IEEE Photonics Journal*, 2018, 10(1): 7600108.
- [86] Bunandar D, Lentine A, Lee C, et al. Metropolitan quantum key distribution with silicon photonics[J]. *Physical Review X*, 2018, 8(2): 021009.
- [87] Paraíso T K, De Marco I, Roger T, et al. A modulator-free quantum key distribution transmitter chip[J]. *NPJ Quantum Information*, 2019, 5: 42.
- [88] Semenenko H, Sibson P, Hart A, et al. Chip-based measurement-device-independent quantum key distribution [J]. *Optica*, 2020, 7(3): 238-242.
- [89] Dai J C, Zhang L, Fu X, et al. Pass-block architecture for distributed-phase-reference quantum key distribution using silicon photonics[J]. *Optics Letters*, 2020, 45(7): 2014-2017.
- [90] Cao L, Luo W, Wang Y X, et al. Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems[J]. *Physical Review Applied*, 2020, 14(1): 011001.
- [91] Li W, Zapatero V, Tan H, et al. Experimental quantum key distribution secure against malicious devices[J]. *Physical Review Applied*, 2021, 15(3): 034081.
- [92] Avesani M, Calderaro L, Schiavon M, et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics[J]. *NPJ Quantum Information*, 2021, 7: 93.
- [93] Tan H, Li W, Zhang L K, et al. Chip-based quantum key distribution against Trojan-horse attack[J]. *Physical Review Applied*, 2021, 15(6): 064038.
- [94] de Marco I, Woodward R I, Roberts G L, et al. Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter[J]. *Optica*, 2021, 8(6): 911-915.
- [95] Paraíso T K, Roger T, Marangon D G, et al. A photonic integrated quantum secure communication system[J]. *Nature Photonics*, 2021, 15(11): 850-856.
- [96] Zhu C X, Chen Z Y, Li Y, et al. Experimental quantum key distribution with integrated silicon photonics and electronics[J]. *Physical Review Applied*, 2022, 17(6): 064034.
- [97] Zhang G W, Chen W, Fan-Yuan G J, et al. Polarization-insensitive quantum key distribution using planar lightwave circuit chips[J]. *Science China Information Sciences*, 2022, 65(10): 200506.
- [98] Li W, Zhang L K, Tan H, et al. High-rate quantum key distribution exceeding 110 Mb s⁻¹[J]. *Nature Photonics*, 2023, 17(5): 416-421.
- [99] Sax R, Boaron A, Boso G, et al. High-speed integrated QKD system[J]. *Photonics Research*, 2023, 11(6): 1007-1014.
- [100] Wei K J, Hu X, Du Y Q, et al. Resource-efficient quantum key distribution with integrated silicon photonics [J]. *Photonics Research*, 2023, 11(8): 1364-1372.
- [101] Dolphin J A, Paraíso T K, Du H, et al. A hybrid integrated quantum key distribution transceiver chip[J]. *NPJ Quantum Information*, 2023, 9: 84.
- [102] Luo W, Cao L, Cai H, et al. A silicon photonic chip-based system for 2.5-GHz quantum key distribution (QKD) [C]//Optical Fiber Communication Conference (OFC) 2024, March 24-28, 2024, San Diego California. Washington, DC: Optica Publishing Group, 2024: Th2A.9.
- [103] Du H, Paraíso T K, Pittaluga M, et al. Twin-field quantum key distribution with optical injection locking and phase encoding on-chip[J]. *Optica*, 2024, 11(10): 1385-1390.
- [104] Zhu J L, Zhou X Y, Ding H J, et al. One-decoy-state quantum key distribution with advantage distillation based on planar-lightwave-circuit-integration modules[J]. *Physical Review A*, 2025, 111(1): 012608.
- [105] Zhang G, Haw J Y, Cai H, et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution[J]. *Nature Photonics*, 2019, 13(12): 839-842.
- [106] Li L, Wang T, Li X H, et al. Continuous-variable quantum key distribution with on-chip light sources[J]. *Photonics Research*, 2023, 11(4): 504-516.
- [107] Bian Y M, Pan Y, Xu X S, et al. Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip[J]. *Applied Physics Letters*, 2024, 124(17): 174001.
- [108] Hajomer A A E, Bruynsteen C, Derkach I, et al. Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver [J]. *Optica*, 2024, 11(9): 1197-1204.
- [109] Piétri Y, Trigo Vidarte L, Schiavon M, et al. Experimental demonstration of continuous-variable quantum key distribution with a silicon photonics integrated receiver[J]. *Optica Quantum*, 2024, 2(6): 428-437.
- [110] Aldama J, Sarmiento S, Trigo Vidarte L, et al. Integrated InP-based transmitter for continuous-variable quantum key distribution[J]. *Optics Express*, 2025, 33(4): 8139-8149.
- [111] Sibson P, Godfrey M, Erven C, et al. Integrated photonic transmitter and receiver for quantum key distribution[C]//2015 European Conference on Lasers and Electro-Optics-European Quantum Electronics Conference, June 21-25, 2015, Munich, Germany. Washington, DC: OSA, 2015: JSV45.
- [112] Bacco D, Ding Y H, Dalgaard K, et al. Space division multiplexing chip-to-chip quantum key distribution[J]. *Scientific Reports*, 2017, 7: 12459.
- [113] Autebert C, Trapateau J, Orioux A, et al. Multi-user quantum key distribution with entangled photons from an AlGaAs chip[J]. *Quantum Science and Technology*, 2016, 1(1): 01LT02.
- [114] Appas F, Baboux F, Amanti M I, et al. Flexible entanglement-distribution network with an AlGaAs chip for secure communications[J]. *NPJ Quantum Information*, 2021, 7: 118.
- [115] Zahidy M, Liu Y X, Cozzolino D, et al. Photonic integrated chip enabling orbital angular momentum multiplexing for quantum communication[J]. *Nanophotonics*,

- 2022, 11(4): 821-827.
- [116] Li X, Ren M Z, Zhang J S, et al. Interference at the single-photon level based on silica photonics robust against channel disturbance[J]. *Photonics Research*, 2021, 9(2): 222-228.
- [117] Zhang G W, Ding Y Y, Chen W, et al. Polarization-insensitive interferometer based on a hybrid integrated planar light-wave circuit[J]. *Photonics Research*, 2021, 9(11): 2176-2181.
- [118] Huang A Q, Li R P, Egorov V, et al. Laser-damage attack against optical attenuators in quantum key distribution[J]. *Physical Review Applied*, 2020, 13(3): 034017.
- [119] 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.
- [120] Ruzhitskaya D, Jöhlinger F, Ponosova A, et al. Laser damage attack on an integrated optics chip for quantum key distribution[EB/OL]. (2020-03-01) [2025-04-04]. <http://qutes.org/wp-content/uploads/2020/02/RuzhitskayaDD.pdf>.
- [121] Gisin N, Fasel S, Kraus B, et al. Trojan-horse attacks on quantum-key-distribution systems[J]. *Physical Review A*, 2006, 73(2): 022320.
- [122] Liu K, Ye C R, Khan S, et al. Review and perspective on ultrafast wavelength-size electro-optic modulators[J]. *Laser & Photonics Reviews*, 2015, 9(2): 172-194.
- [123] Li C Y, Curty M, Xu F H, et al. Secure quantum communication in the presence of phase- and polarization-dependent loss[J]. *Physical Review A*, 2018, 98(4): 042324.
- [124] Dupuis N, Proesel J E, Ainspan H, et al. Nanosecond-scale shift-and-dump Mach-Zehnder switch[J]. *Optics Letters*, 2019, 44(18): 4614-4616.
- [125] Ye P, Chen W, Wang Z H, et al. Transmittance-invariant phase modulator for chip-based quantum key distribution[J]. *Optics Express*, 2022, 30(22): 39911-39921.
- [126] Ashkin A, Boyd G D, Dziedzic J M, et al. Optically-induced refractive index inhomogeneities in LiNbO_3 and LiTaO_3 [J]. *Applied Physics Letters*, 1966, 9(1): 72-74.
- [127] Ye P, Chen W, Zhang G W, et al. Induced-photorefractive attack against quantum key distribution[J]. *Physical Review Applied*, 2023, 19(5): 054052.
- [128] Lu F Y, Ye P, Wang Z H, et al. Hacking measurement-device-independent quantum key distribution[J]. *Optica*, 2023, 10(4): 520-527.
- [129] Han L Y, Li Y, Tan H, et al. Effect of light injection on the security of practical quantum key distribution[J]. *Physical Review Applied*, 2023, 20(4): 044013.
- [130] Chen Z Y, Liu Y F, Chen C, et al. Radiation effect on silicon photonics chips for space quantum key distribution[J]. *Optics Express*, 2024, 32(2): 2015-2028.