光电技术及应用

DOI：10.16818/j.issn1001－5868.20260324002

基于平面光波导的波长无关量子密钥分发解码器

周　雷[1]，陶　俊[1]，刘仁德[1,2]，李东东[1,3]*，马　龑[1]，杜先常[1]，肖道忠[1]，
何天宇[1]，赵于康[1]，蒋连军[1]，汤艳琳[1]，唐世彪[1]

（1. 科大国盾量子技术股份有限公司，合肥 230088；2. 中国科学技术大学 物理学院，合肥 230026；
3. 中国科学技术大学 网络空间安全学院，合肥 230027）

摘　要： 解码器是量子密钥分发接收端的关键组件，直接决定了系统的尺寸、成码率、量子比特误码率和安全性。文章基于平面光波导技术，面向BB84时间相位编码协议研制了一种紧凑型解码器芯片及组件。该组件通过混合集成法拉第旋转镜与热电制冷器，实现了一种非对称的法拉第-迈克尔逊干涉仪，能够对时间相位编码的光子对进行稳定干涉解码。实验结果表明，该器件具有超过170∶1的高干涉对比度、精确的时间延迟控制能力，尤为重要的是，其分束比在宽波长范围内随波长变化仅1.2 dB左右，表明其具备较强的抗波长调谐攻击能力。该工作为实际量子密钥分发应用提供了一种稳健、安全且实用的解码解决方案。

关键词： 量子密钥分发；平面光波导；解码器；时间相位编码；波长不敏感

中图分类号： TN256　**文章编号：** 1001－5868(2026)04－0709－07

Wavelength-Independent Quantum Key Distribution Decoder Based on Planar Lightwave Circuit

ZHOU Lei[1], TAO Jun[1], LIU Rende[1,2], LI Dongdong[1,3], MA Yan[1], DU Xianchang[1], XIAO Daozhong[1], HE Tianyu[1], ZHAO Yukang[1], JIANG Lianjun[1], TANG Yanlin[1], TANG Shibiao[1]

(1. QuantumCTek Co., Ltd., Hefei 230088, CHN; 2. School of Physical Sciences, University of Science and Technology of China, Hefei 230026, CHN; 3. School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230027, CHN)

Abstract: The decoder is a critical component in quantum key distribution receivers, directly governing the system size, key rate, quantum bit error rate, and security. In this study, we developed a compact decoder chip based on planar lightwave circuit technology for the BB84 time-bin phase-encoding protocol. The device implements an asymmetric Faraday－Michelson interferometer through the hybrid integration of a Faraday rotating mirror and thermoelectric cooler, enabling stable interference decoding of time-bin encoded photons. Experimental results demonstrate a high interference visibility exceeding 170∶1, precise temporal delay control, and, most notably, a nearly wavelength-insensitive beam-splitting ratio (1.2 dB) across a broad wavelength range, indicating its inherent resilience against wavelength-tuning attacks. The presented decoder provides a robust, secure, and practical solution for real-world quantum key distribution applications.

Key words: quantum key distribution; planar light-wave circuit; decoder; time-bin phase encoding; wavelength insensitive

收稿日期：2026－03－24.

*通信作者：李东东

0 引言

量子密钥分发(Quantum Key Distribution, QKD)基于量子力学基本原理,可在远程的通信双方之间实现基于信息理论安全的密钥交换[1-4]。这种独特的保密通信方式具备显著增强数据传输安全性的潜力,因此学界关注度持续攀升。近年来,QKD在政务、金融、电力等多个领域展现出广阔的应用前景,并且关于其与现有网络基础设施融合的报道也日益增多[5-15]。

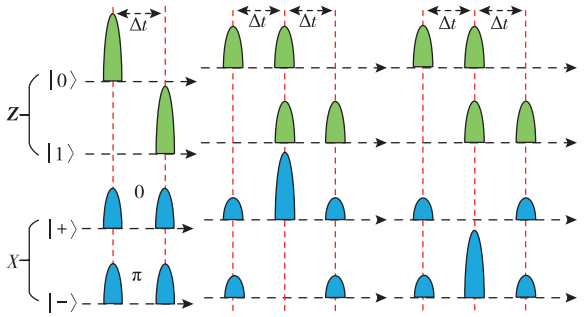
目前,大多数QKD系统采用诱骗态BB84协议,并广泛使用分立光学元件(如调制器、分束器、环行器和隔离器等)来实现编码和解码功能。此类分立架构通常导致编解码模块体积大、成本高,并且可靠性受限,从而制约了QKD终端的集成度、重量和长期稳定性[16-17]。随着集成光子学的快速发展,基于光学芯片开发编码器和解码器模块已成为推动QKD技术发展的关键趋势[18-21]。与分立器件相比,集成光子器件具有尺寸紧凑、重量轻、功耗低、稳定性高以及可规模化制造等优势,这些特性都有利于QKD系统的小型化和实际部署。

多种材料平台已被探索用于实现芯片化QKD,如绝缘体上硅(SOI)、III-V族化合物、铌酸锂和平面光波导(PLC)[22-26]。其中,硅基衬底SOI工艺平台具有器件尺寸小、集成度高且与CMOS工艺兼容等优点,在QKD系统尤其是集成QKD发送方芯片被广泛研究。以磷化铟(InP)为代表的III-V族化合物平台为直接带隙材料,适合集成光源和调制器等。铌酸锂具有电光系数大、非线性效应强等优点,适用于高速调制器芯片。基于SiO_2材料的PLC芯片因具有传输和耦合损耗低、工艺成熟可靠等特点,在集成化QKD设备,特别是解码端的应用备受关注。文献[27]报道了一种基于标准硅光平台制造的偏振编码QKD发送方芯片,能够实现片上制备BB84偏振态和诱骗态强度调制。文献[24]演示了在InP平台上单片集成的QKD发送方,通过集成激光器、强度和相位调制器以及相位编码器,实现了完整的片上QKD功能。在接收端,文献[28]利用片上偏振分束器实现了一种基于PLC的偏振解码器。文献[29-30]进一步提出基于混合集成PLC芯片的偏振不敏感非对称干涉仪,用于解码相位或时间相位编码的光子对。此外,文献[31]介绍了一种支持时间相位编码等多种协议的PLC解码器。这些成果均标志着芯片化QKD研究取得了重要进展,但多数工作仍以实验室功能性演示为主,在工程化应用中仍需在提高器件的鲁棒性方面做进一步探索。值得注意的是,解码器作为QKD接收端的重要部件,除需具备基础解码功能外,还必须能够抵抗波长调谐相关的量子攻击,这是既有集成化研究中鲜有关注的安全性方面的内容。

本文设计并制造了一款基于PLC工艺、面向BB84时间相位QKD协议的解码器芯片。该解码器芯片包含两个主要功能单元:用于相位干涉解码的片上非对称法拉第-迈克尔逊干涉仪(AFMI)和用于基矢选择的7:3分束器(BS)。该干涉仪由一个5:5 BS、片上光波导延迟线和两个法拉第旋转镜(FRM)组成。除FRM外,解码器的所有光学功能单元均在单片SiO_2基PLC芯片上制造。FRM作为微光学元件,与PLC芯片通过光耦合,并进行混合封装。完整的组件还封装了用于实现相位稳定的热电制冷器(TEC)和热敏电阻,形成了结构紧凑且环境鲁棒高的解码器。此外,7:3的BS经过优化设计,在宽波长范围内表现出极小的波长相关性,能够有效抵御波长相关攻击。本工作有助于开发基于PLC芯片技术、安全性和稳定性高的实用化QKD接收端。

1 时间相位编码QKD基本原理

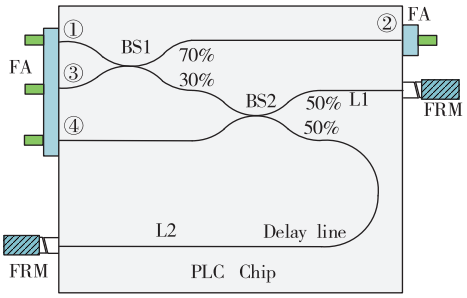
基于BB84时间相位编码协议的QKD系统利用光脉冲的时间和相位信息进行编码,在发送方通过光源和编码器实现光量子信号产生与编码。编码器为非对称的干涉仪,对光源产生的光脉冲进行分束和延时,产生在时序上一前一后的光子脉冲对,脉冲时间间隔Δt取决于干涉仪的臂长差。通过随机驱动信号对光子脉冲对进行调制,产生时间相位(time-bin)编码信息。根据调制信号的不同,可能出现下列几种情形:QKD系统周期内只发前一个光脉冲,对应$|0\rangle$态,或只发后一个光脉冲,对应$|1\rangle$态,称之为时间态(Z基矢);在系统周期内同时发前后两个光脉冲,且脉冲光子之间受到的调制相位差分别为0和π,对应$|+\rangle$和$|-\rangle$态,称之为相位态(X基矢)。几种量子态发光编码示意图如图1(a)所示。在QKD接收端,经发送方编码的量子态进入解码器首先进行解码,其过程如图1(b)所示。



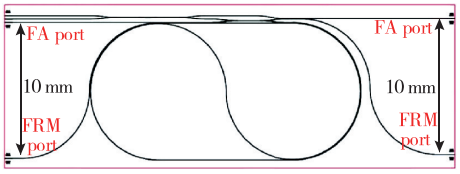
（a）编码量子态　　（b）解码输出 1　解码输出 2

图 1　BB84 时间相位 QKD 的编解码原理示意图

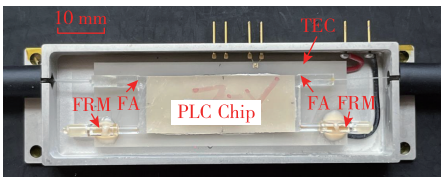
典型的时间相位 QKD 解码器的光路原理如图 2(a)所示，包括基矢分束器(BS1)和 AFMI。其中 AFMI 由等比分束器(BS2)、片上延迟线和和匹配臂长差构成，其臂长差设计值与发送方干涉仪相同，具有干涉结果互补的两个输出端，可输出脉冲对的相位干涉结果信息。时间态 Z 基矢经解码器的基矢分束器的其中一个输出端口后进入探测器直接探测，相位态 X 基矢经分束器另一输出端口后再进入 AFMI 进行干涉。时间态经 AFMI 之后分成的两束光脉冲在时间上不重叠，因此不会发生干涉。相位态编码存在前后两个光脉冲，由于编解码干涉仪臂长差相等，在 AFMI 中，先到达的光脉冲经长臂传输的一束与后到达的光脉冲经短臂传输的一束同时到达输出合束端口并发生干涉，形成干涉峰。干涉的结果取决于其相位差为 0 或 π，分别出现相干相涨或相消，AFMI 的两输出端的光强是互补的。此外，先到达且经短臂传输的光脉冲以及后到达且经长臂传输的光脉冲，在时间上分别处在干涉峰之前和之后的位置，不会发生干涉，称为非干涉峰。经过上述过程即可完成量子态的解码，解码后光信号分别由相应的单光子探测器探测输出电信号。单光子探测器为门控型探测器，其门控周期与干涉峰的时间间隔保持一致。



（a）光路原理图



（b）芯片版图



（c）封装实物图

图 2　PLC 时间相位解码器(FA：光纤阵列)

2　PLC 解码器的设计与制造

在前述各种集成光子平台中，基于 SiO_2 的 PLC 因具有低传输损耗和耦合损耗、偏振不敏感性以及技术成熟度[30,32]等优点，特别适用于作为 QKD 解码器的工艺平台。本文设计的 PLC 解码器是在基于标准的 PLC 工艺平台上进行加工制造。

PLC 芯片在基于 SiO_2 材料工艺平台上制造。芯片设计的工作波长为 1 310 nm，波导的包层为纯 SiO_2 材料。为提高芯层的折射率，在其中掺入少量折射率相对较高的 GeO_2，使芯层与包层的折射率差为 0.75%。波导的最小弯曲半径为 5 mm，芯层的截面为 6 μm×6 μm，因此与单模光纤耦合时损耗较低。为最小化背向光反射，芯片的端面和 FRM 端面设计为斜 8°角。FRM 可以抑制光纤中可能存在的双折射效应所引起两正交偏振分量在往返时的光程差。在每一臂中，水平和垂直偏振态分量在往返 FRM 时偏振态旋转 90°，实现偏振态交换，总效应是各分量经过的光程一致，消除了同一段光纤双折射效应引起的水平和垂直分量之间的相位差，因而每一臂中的反射光在返回分束器时的偏振态是稳定的，消除了偏振态变化对干涉结果的影响。最终芯片版图尺寸为 34 mm×12 mm(图 2(b))，封装后解码器尺寸为 85 mm×25 mm×12 mm(图 2(c))。

SiO_2 材料具有较高的热光系数，其相位对环境温度敏感性高。为了使器件稳定工作，模块在芯片与封装底板之间集成了一个 TEC 和一个热敏电阻。通过比例-积分-微分(PID)控制器将芯片保持在恒定的工作温度，可保证解码器在环境温度变化环境条件下的长期相位稳定性。

3 实验结果与讨论

3.1 器件性能表征

作为面向时间相位QKD系统的解码器，本文系统表征了其关键性能参数——插入损耗、脉冲延时差和幅度一致性，其中插入损耗直接影响QKD系统的安全成码率。如图2(a)所示，测试时激光脉冲从端口①输入，分别在端口②、③和④测量输出功率，对应时间基矢和两个相位基矢的插入损耗。实际测得的插入损耗为：①→②为2.49 dB，①→③和①→④分别为12.88 dB和11.33 dB。这些数值与分立解码器相当，满足时间相位QKD系统的要求。端口③比端口④高出约1.5 dB的损耗，这源于其额外通过了BS1的直通臂引入的固有损耗。

延时差是非对称干涉仪的关键参数，决定了前后脉冲对能否精确在同一时刻到达并干涉。从解码器的端口①输入脉冲激光，在端口④衰减后通过单光子探测器(SPD)和时间数字转换器(TDC)进行测量，TDC的时间分辨率约为4 ps，扫描得出前后脉冲光子对的计数值随时间变化如图3所示，横坐标之差(800 ps)即为脉冲往返延时差，与设计值一致。因此，通过精确的波导折射率和长度等参数控制，解码组件可实现精准的延时差。

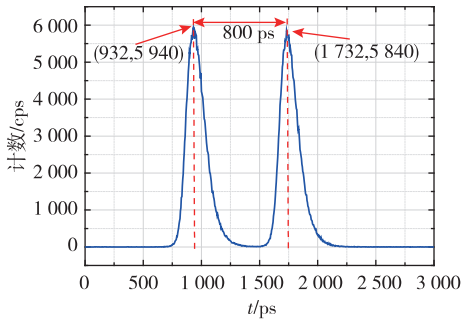


图3 PLC光芯片延时差和脉冲幅值一致性测试结果

测试所用脉冲激光器的脉宽为50 ps，中心波长为1 310 nm，与PLC光芯片的设计工作波段一致。单光子探测器在1 310 nm的探测效率约为28%，门控频率为1.25 GHz。

除延时差以外，影响解码器干涉对比度的另一重要因素是非对称干涉仪延时形成的前后脉冲幅值一致性。在解码器组件的制作过程中，当FRM与PLC芯片耦合时，两者之间加入折射率匹配液，以减少端面反射。通过监测前后光脉冲的幅值，并不断微调FRM的耦合角度和位置，保证前后脉冲的幅值接近一致，此时再通过胶水将其固化。幅值一致性的测量可与延时差指标测量同步进行，图3的两个脉冲峰值计数即为幅值，分别为5 940和5 840 cps，相对差异在0.1 dB以内，实现了良好的脉冲幅度一致性。

3.2 干涉对比度

干涉对比度是直接关系到QKD系统量子比特误码率(QBER)的关键指标。使用一对相同的解码器(#1和#2)分别作为发送方和接收方干涉仪来评估干涉对比度。如图4所示，将脉冲激光器连接至#1解码器的端口①，随后经过可调光衰减器和#2解码器，其端口④的输出计数由SPD和TDC进行测量。

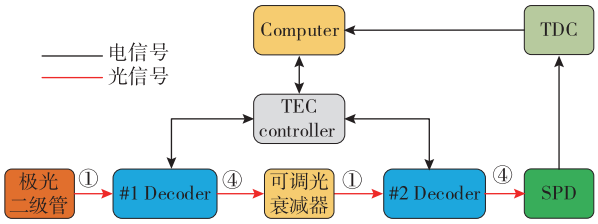


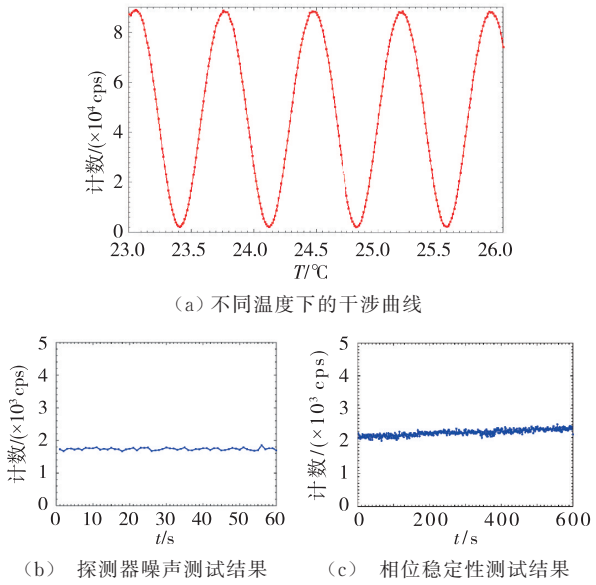
图4 干涉对比度测量实验装置

在干涉对比度测试时，#2解码器的芯片温度以0.01 ℃/s的步进从23℃扫描至26℃，#1解码器的芯片通过TEC控制器将温度稳定在25℃。从扫描的干涉曲线(图5(a))可得出最大干涉计数C_{max}和最小干涉计数C_{min}。由于探测器的暗计数和后脉冲等噪声计数的存在，在计算干涉对比度时需进行扣除。具体方法如下：去除解码器组件，激光器经可调光衰减器衰减后直接接入单光子探测器，调节衰减值使单光子探测器的非干涉峰计数与之前保持一致，此时门控探测器的干涉峰内没有光脉冲进入，测得的计数仅包含后脉冲和暗计数，持续监测60 s，如图5(b)所示，取平均值作为噪声，$C_{noise}\approx 1\,700$。由公式(1)算得的干涉对比度$V\approx 176$：

$$V=\frac{C_{max}-C_{noise}}{C_{min}-C_{noise}} \tag{1}$$

另外从干涉扫描曲线可得出，产生π相移所需温度变化仅为0.35℃左右，因此芯片对温度敏感性较高，需要进行精确温控。在相位稳定性测试时，一个芯片的工作温度保持恒定，通过调节另一个芯片的工作温度，使这对解码器组件干涉输出稳定在最小值C_{min}附近，并持续10 min监测TDC输出计数变化来评估相位稳定性(图5(c))。输出计数仅在2 000～2 500计数之间波动，得出的相位干涉对比度变化范围为286∶1到106∶1，对应的QBER约处在

0.35%～1% 之间，验证了所研制的 PLC 解码器在工作时具有较高的稳定性。



（a）不同温度下的干涉曲线

（b） 探测器噪声测试结果　　（c） 相位稳定性测试结果

图 5　测试结果

3.3　波长相关安全性

QKD 的安全性是由信息理论上所保证的，然而实际系统可能因器件缺陷而存在安全隐患。在通常的安全性分析里，分束器的分束比被看作是固定不变的。但是理论计算和实验测试表明，常规的分束器的分束比是会随输入光波长不同而发生改变。虽然设定的工作波长分束比特性十分理想，但是当输入光波长发生偏离时，分束比大小也随之发生改变。尤其是当全波段的分束比偏差显著（如 12 dB 及以上）时，一个输入波长几乎从其中一个输出端口输出，而另一个输入波长几乎完全从另一个输出端输出。此时，分束器几乎演变为一个“波长选择器”。攻击者可以利用分束器的这种特性，发送不同波长的伪造态来控制测量基选择，从而得到与窃听者相同的选基和探测结果，窃听者便可以在引入极少额外误码的情况下窃取到全部安全密钥信息。基矢分束器这种分束比随波长而出现显著变化的现象在光纤分束器或常规 PLC 型光分路器中较为常见，这可能为基于波长调谐的相关攻击留下安全漏洞[33-35]。

因此，本文在设计 PLC 光芯片时，对其中的基矢分束器 BS1 进行了基于严格仿真的优化设计。通常，PLC 中的分束器主要基于单个定向耦合器（DC）设计，其分光比对波长极为敏感，波长变化会导致耦合长度发生显著改变，从而使分光比大幅偏离设计值。相比之下，基于级联 MZI 的结构可以通过引入额外的相位延迟来抵消这种色散效应。通过精确设计 MZI 两臂的相位差，可以在宽波长范围内将分光比的波动控制在很小的范围。

如图 6 显示了所设计的 PLC 光芯片中的基矢分束器（BS1）在 1 250～1 650 nm 波长范围内分束比波长相关性。作为对照，同时给出常规的 7∶3 光分束器的分束比波长相关性。可见，常规 PLC 分束器在 1 250～1 650 nm 范围内的分束比波动通常会超过 12 dB，而本文优化的 7∶3 分束器在相同波段内分束比波动极低，仅为 1.2 dB 左右。这显著降低了解码器在基矢选择时对波长的依赖性，从而增强了对波长调谐攻击的抵抗力，提升了 QKD 系统的实际安全性。

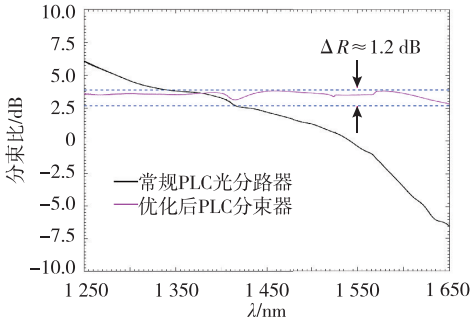


图 6　常规 PLC 光分路器与本文优化后 PLC 分束器的分束比波长相关性对比

光分束器波长相关性攻击引入的额外错误率可以通过以下公式计算[33]：

$$Err=\frac{1}{4}\left(\frac{1-r_1}{2-r_1-r_2}+\frac{r_2}{r_1+r_2}\right) \tag{2}$$

式中，r_1 和 r_2 分别为分束器在工作波长 λ_1 和 λ_2 的耦合比，定义如下：

$$r=\frac{I_{\text{port1}}}{I_{\text{port1}}+I_{\text{port2}}} \tag{3}$$

式中，I_{port1} 和 I_{port2} 分别是分束器输出端口 1 和 2 的输出光功率。对于时间相位 QKD 系统中的非平衡基矢，在理想分束比下，$r_1=r_2\approx0.7$，此时对应的错误率 $Err\approx25\%$。对于本文所研制的 PLC 芯片中的基矢分束器，分束比在 1 250～1 650 nm 波段范围内仅波动 1.2 dB，对应 $r_1\approx0.728$，$r_2\approx0.67$，预估带来的错误率约为 23.2%，远大于安全阈值 11%[36]。若此时采用波长攻击，则无法生产安全密钥，窃听行为极易被发现。而图 6 显示的常规分束器在此波段范围内分束比波动大于 12 dB。按 12 dB 波动预估，

$r_1 \approx 0.905$，$r_2 \approx 0.37$，所得 $Err \approx 10.5\%$。此时，窃听者引起的错误率已低于11%的安全阈值[36]，为攻击者掩盖自身的攻击行为提供了可能性。综上，本文研制的PLC芯片中，分束比在全波段的高一致性显著降低了波长相关攻击的可能性，进而关闭了该安全漏洞，对提高QKD的实际安全性具有现实意义。

4 结论

本文面向BB84时间相位编码协议的QKD系统，设计并制作了一款基于PLC工艺平台的量子密钥解码器，且系统评估了解码器的关键性能指标和安全特性。实验结果表明，该器件具有尺寸紧凑、插入损耗低、时间延迟准确以及脉冲幅度一致性高等优点。通过解码器（干涉仪）配对测试，实现的光脉冲干涉对比度可达170∶1以上，且具备较高的稳定性，能够满足QKD系统的功能性要求。此外，针对之前相关工作所有提及的解码器安全性要求，对器件的基矢分束单元的分束比波长相关性进行了优化，在1 250～1 650 nm宽波长范围内，分束比波动仅为1.2 dB左右，能够有效抵御窃听者对QKD接收端的进行波长相关攻击。所研制的解码器不仅满足功能性和安全性要求，还具有高集成度和鲁棒性，有望替代QKD系统由传统分立器件所组成的解码器。本工作为开发小型化、高可靠、实际安全性高的QKD接收端奠定了基础。

参考文献：

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

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

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

[4] Lu C Y, Cao Y, Peng C Z, et al. Micius quantum experiments in space [J]. Reviews of Modern Physics, 2022, 94(3): 035001.

[5] Peev M, Pacher C, Alléaume R, et al. The SECOQC quantum key distribution network in Vienna [J]. New Journal of Physics, 2009, 11(7): 075001.

[6] Chen T Y, Wang J, Liang H, et al. Metropolitan all-pass and inter-city quantum communication network [J]. Optics Express, 2010, 18(26): 27217.

[7] Sasaki M, Fujiwara M, Ishizuka H, et al. Field test of quantum key distribution in the Tokyo QKD Network [J]. Optics Express, 2011, 19(11): 10387.

[8] Li D D, Gao S, Li G C, et al. Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback [J]. Optics Express, 2018, 26(18): 22793.

[9] Li D D, Shen Q, Chen W, et al. Proof-of-principle demonstration of quantum key distribution with seawater channel: towards space-to-underwater quantum communication [J]. Optics Communications, 2019, 452: 220-226.

[10] Tang Y L, Zhou C, Li D D, et al. Time-bin phase-encoding quantum key distribution using Sagnac-based optics and compatible electronics [J]. Optics Express, 2023, 31(16): 26335.

[11] Tang Y L, Xie Z L, Zhou C, et al. Field test of quantum key distribution over aerial fiber based on simple and stable modulation [J]. Optics Express, 2023, 31(16): 26301.

[12] Chen Y A, Zhang Q, Chen T Y, et al. An integrated space-to-ground quantum communication network over 4 600 kilometres [J]. Nature, 2021, 589(7841): 214-219.

[13] Chen T Y, Jiang X, Tang S B, et al. Implementation of a 46-node quantum metropolitan area network [J]. npj Quantum Information, 2021, 7: 134.

[14] Dynes J F, Wonfor A, Tam W W S, et al. Cambridge quantum network [J]. npj Quantum Information, 2019, 5: 101.

[15] Ma C L, Li D D, Li Y, et al. Quantum-secure fault-tolerant distributed cloud storage system [J]. AIP Advances, 2023, 13(11): 115309.

[16] Orieux A, Diamanti E. Recent advances on integrated quantum communications [J]. Journal of Optics, 2016, 18(8): 083002.

[17] Pittaluga M, Minder M, Lucamarini M, et al. 600-km repeater-like quantum communications with dual-band stabilization [J]. Nature Photonics, 2021, 15(7): 530-535.

[18] Luo W, Cao L, Shi Y, et al. Recent progress in quantum photonic chips for quantum communication and Internet [J]. Light: Science & Applications, 2023, 12: 175.

[19] Liu Q, Huang Y, Du Y, et al. Advances in chip-based quantum key distribution [J]. Entropy, 2022, 24(10): 1334.

[20] Wang Q, Zheng Y, Zhai C, et al. Chip-based quantum communications [J]. Journal of Semiconductors, 2021, 42(9): 091901.

[21] Wang J, Sciarrino F, Laing A, et al. Integrated photonic quantum technologies [J]. Nature Photonics, 2020, 14(5): 273-284.

[22] Du Y, Li B H, Hua X, et al. Chip-integrated quantum signature network over 200 km [J]. Light: Science & Applications, 2025, 14: 108.

[23] Ma C, Sacher W D, Tang Z, et al. Silicon photonic transmitter for polarization-encoded quantum key distribution [J]. Optica, 2016, 3(11): 1274.

[24] Sibson P, Erven C, Godfrey M, et al. Chip-based quantum

key distribution [J]. Nature Communications, 2017, 8: 13984.

[25] 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.

[26] Dolphin J A, Paraïso T K, Du H, et al. A hybrid integrated quantum key distribution transceiver chip [J]. npj Quantum Information, 2023, 9: 84.

[27] Zhang G, Zhao Z, Dai J, et al. Polarization-based quantum key distribution encoder and decoder on silicon photonics[J]. Journal of Lightwave Technology, 2022, 40(7): 2052-2059.

[28] Choe J S, Ko H, Choi B S, et al. Silica planar lightwave circuit based integrated 1 × 4 polarization beam splitter module for free-space BB84 quantum key distribution [J]. IEEE Photonics Journal, 2018, 10(1): 7600108.

[29] 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.

[30] 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.

[31] Zhang C X, Li J G, Wang Y, et al. Multi-protocol quantum key distribution decoding chip[J]. Chinese Physics B, 2025, 34(5): 050303.

[32] 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.

[33] Li H W, Wang S, Huang J Z, et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources [J]. Physical Review A, 2011, 84(6): 062308.

[34] Li D D, Tang Y L, Zhao Y K, et al. Security of optical beam splitter in quantum key distribution [J]. Photonics, 2022, 9(8): 527.

[35] Zhou F, Zhao M S, Wang X B. Security of quantum key distribution under the wavelength-dependent quantum hack[J]. Science China Information Sciences, 2014, 44(3): 322.

[36] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Physical Review Letters, 2000, 85(2): 441-444.

作者简介：

周　雷(1981—)，男，高级工程师，主要从事量子通信方面的研究；

李东东(1989—)，男，高级工程师，主要从事量子通信和超导量子计算方面的研究。