2026 年 09 月 10 日 – 09 月 11 日 · 日报

量子加密芯片被发现偷偷发光 可能泄密

50 篇 · 8 个来源 | PDF | 本期汇总免费阅读

本 期 目 录

收录报道	50
信息来源	8
阅读时长	约 19 分钟

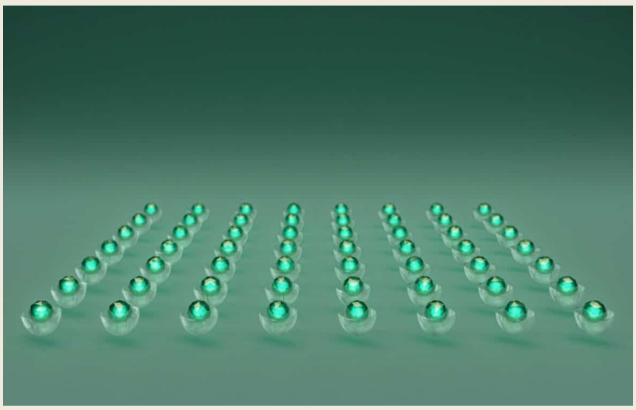
当 前 S O T A

物理比特	1, 180
2Q 保真度	99. 99%
逻辑比特	**96 LQ**

量子硬件 SOTA 对照表 →

01 亮点

今日三件事



1 **Quantinuum 把纠错码从存得住推到算得动** Helix 架构在 Helios 机器上同时跑通逻辑存储、Clifford 计算与码间接口，全程不做后选择[2]——纠错这次以整场成绩交卷，非 Clifford 门仍缺。

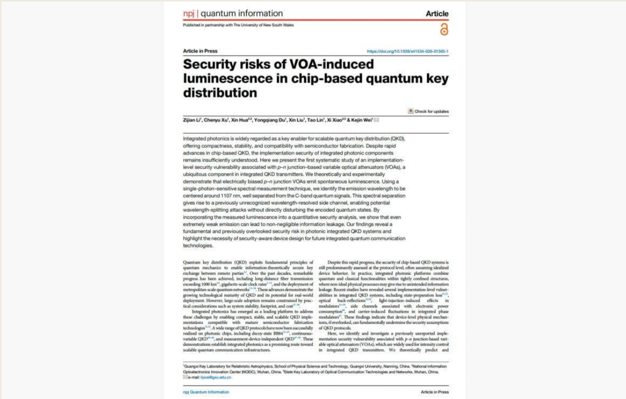
1 **SEALSQ 上半年营收增长 131%** 公司公布 2026 年上半年业绩，营收同比增长 131%，并给出 2026 全年指引[35]——不过通稿未拆分后量子芯片在其中贡献了多少。

1 **F1 赛车把量子求解器接进整车仿真** BWT Alpine 车队与 SEALSQ 扩大合作，引入 ColibriTD 的量子求解器处理赛车研发中的多物理场方程，同时用后量子技术保护设计数据[11]

——高预算工程仿真成为混合量子计算的新入口，合作金额与付费性质未披露。

02 硬件

硬件前沿


npj | quantum information　Article

Published in partnership with The University of New South Wales

Article in Press　https://doi.org/10.1038/s41534-026-01365-1

Security risks of VOA-induced luminescence in chip-based quantum key distribution

Check for updates

Zijian Li[1], Chenyu Xu[1], Xin Hua[2,3], Yongqiang Du[1], Xin Liu[1], Tao Lin[1], Xi Xiao[2,3] & Kejin Wei[1]

Integrated photonics is widely regarded as a key enabler for scalable quantum key distribution (QKD), offering compactness, stability, and compatibility with semiconductor fabrication. Despite rapid advances in chip-based QKD, the implementation security of integrated photonic components remains insufficiently understood. Here we present the first systematic study of an implementation-level security vulnerability associated with p–n junction-based variable optical attenuators (VOAs), a ubiquitous component in integrated QKD transmitters. We theoretically and experimentally demonstrate that electrically biased p–n junction VOAs emit spontaneous luminescence. Using a single-photon-sensitive spectral measurement technique, we identify the emission wavelength to be centered around 1107 nm, well separated from the C-band quantum signals. This spectral separation gives rise to a previously unrecognized wavelength-resolved side channel, enabling potential wavelength-splitting attacks without directly disturbing the encoded quantum states. By incorporating the measured luminescence into a quantitative security analysis, we show that even extremely weak emission can lead to non-negligible information leakage. Our findings reveal a fundamental and previously overlooked security risk in photonic integrated QKD systems and highlight the necessity of security-aware device design for future integrated quantum communication technologies.

Quantum key distribution (QKD) exploits fundamental principles of quantum mechanics to enable information-theoretically secure key exchange between remote parties. Over the past decades, remarkable progress has been achieved, including long-distance fiber transmission exceeding 1000 km, gigahertz-scale clock rates, and the deployment of metropolitan-scale quantum networks. These advances demonstrate the growing technological maturity of QKD and its potential for real-world deployment. However, large-scale adoption remains constrained by practical considerations such as system stability, footprint, and cost.

Integrated photonics has emerged as a leading platform to address these challenges by enabling compact, stable, and scalable QKD implementations compatible with mature semiconductor fabrication technologies. A wide range of QKD protocols have now been successfully realized on photonic chips, including decoy-state BB84, continuous-variable QKD, and measurement-device-independent QKD. These demonstrations establish integrated photonics as a promising route toward scalable quantum communication infrastructures.

Despite this rapid progress, the security of chip-based QKD systems is still predominantly assessed at the protocol level, often assuming idealized device behavior. In practice, integrated photonic platforms combine quantum and classical functionalities within tightly confined structures, where non-ideal physical processes may give rise to unintended information leakage. Recent studies have revealed several implementation-level vulnerabilities in integrated QKD systems, including state-preparation loss, optical back-reflections, light-injection-induced effects in modulators, side channels associated with electronic power consumption, and carrier-induced fluctuations in integrated phase modulators. These findings indicate that device-level physical mechanisms, if overlooked, can fundamentally undermine the security assumptions of QKD protocols.

Here, we identify and investigate a previously unreported implementation security vulnerability associated with p–n junction-based variable optical attenuators (VOAs), which are widely used for intensity control in integrated QKD transmitters. We theoretically predict and

[1]Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning, China. [2]National Information Optoelectronics Innovation Center (NOEIC), Wuhan, China. [3]State Key Laboratory of Optical Communication Technologies and Networks, Wuhan, China. e-mail: kjwei@gxu.edu.cn

npj Quantum Information　Article in Press

离子阱

Quantinuum 补上了纠错的计算那一环

Quantinuum 公布 Helix 架构在 Helios 上的实测：同一套紧凑纠错码上同时实现逻辑存储、Clifford 计算（一类可被经典高效模拟的基础门集）与码间接口，全过程不依赖后选择[2]。

技术含义：后选择指事后丢掉失败运行、只统计成功数据，它一直是逻辑比特演示最受质疑的口径问题；取消这一步，报出的逻辑错误率才是整场比赛的成绩而非精选集锦。对照当前基线，该报道只说明这是一套紧凑纠错码，Helios 的比特数、双比特门保真度与物理 / 逻辑编码比均未在其中披露（相关数字多见于公司自身发布，尚待独立核对）——此次不是刷新保真度纪录，而是在同一套硬件上把

能力维度补齐一格。还差什么：非 Clifford 门（魔法态注入那一类，决定能否做通用计算）与长时间持续运行，报道也把这道缝定义为下一步。

格局影响：离子阱阵营继续以逻辑比特的质量，对抗中性原子路线在比特数量上的规模优势；对采购方而言，是否后选择正在变成尽调表上的必填栏，时间尺度以季度计。

Clarendon 实验室提出每秒 20 万对的原子间纠缠方案

基于腔辅助光子散射的时间与波长复用协议，预测每秒可生成 2×10^5 对原子-原子贝尔对（最基本的两体纠缠态），预报的预示保真度 0.999，且不需要腔内比特重置[22]。

技术含义：这是方案与数值预测，尚未上机验证；来源也未给出可比的现有实验速率基线，兑现与否要等实验组接手。格局影响：远程纠缠速率是把多台小机器拼成一台大机器的硬瓶颈，也是量子网络中继的限速环节；该协议若被实验组接手复现，受影响最快的是模块化架构路线，时间尺度以年计。

光子与量子通信

QKD 芯片里的衰减器自己在发光

一项同行评审研究发现，集成 QKD（量子密钥分发，用光子分发密钥的加密方式）芯片中的可变光衰减器会在 1107 纳米附近发出非预期的光，这束光形成一条按波长可分辨的旁路信道，而标准 BB84 安全性分析并不把它计入[3]。

技术含义：QKD 的卖点是安全性由物理定律保证，但这个保证只覆盖安全证明写进去的那些自由度；衰减器的发光属于器件层面的意外辐射，证明里根本没有这一项，属于典型的实现漏洞而非协议漏洞。这不是理论推演，而是在实际芯片上测到的发射谱。

格局影响：所有走片上集成路线的 QKD 厂商与正在做 QKD 采购认证的电信、政务客户直接受影响——安全证明需要补充器件建模，认证流程要加波长扫描项；对已部署系统而言，这是一轮补丁而非推倒重来，时间尺度以月计。

超导

一种量子存储方案把信号存到 620 微秒

研究者用新的量子存储手段提升超导比特的相干表现，信号最长存储 620 微秒[24]。

对照基线：来源只给出 620 微秒这一个数字，未提供同类超导器件的相干时间对照；而且存储器件的保存时长与比特自身的 T1（能量弛豫时间，比特忘掉自身状态的快慢）不是同一口径，不可直接并列为纪录。还差什么：超导的老问题是缺陷引起的时序漂移，单次最好值之外必须看长期稳定性分布。

格局影响：同步与缓存能力决定多比特调度的效率，超导大厂的编译层可直接吸收这类组件，属渐进改良而非路线变更。

中性原子

管住原子掉在哪，现实条件下逻辑错误率改善 5.3 倍

新的优化方法把原子丢失（中性原子阵列特有的错误：原子从光镊中跑掉）纳入纠错码的设计变量，在最多 73% 的测试场景中改善逻辑错误率，现实条件下增益 5.3 倍[23]。

技术含义：此前该路线主要关心丢了几个原子，这项工作把丢在码的哪个位置变成可主动管理的量。对照基线：中性原子的长处一向是阵列规模，短板在循环重复率（典型 1–10 赫兹）与中路测量；原子丢失属于后者的衍生问题，这次改善的是纠错层策略，不触碰重复率的硬约束。

格局影响：QuEra、Pasqal、Atom Computing 的纠错栈可在不换硬件的前提下吸收这类编译期优化，见效以季度计。

材料与器件

维也纳大学在白石墨烯上刻出原子级孔洞

Jani Kotakoski 带领的团队用电子辐照配合氧气，在六方氮化硼（俗称白石墨烯的二维绝缘材料）上精确成形原子尺度孔洞[19]。技术含义：孔洞位置与尺寸可控，是把单光子发射体做成可复制器件的前提，此前该类缺陷多靠偶然生成。格局影响：影响单光子源与量子传感的材料供给端，距器件产品尚有数年。

金刚石里拖累传感器的氢缺陷被完整追踪

DEER 谱学揭示出一个 X 系综缺陷，其中的空位与间隙原子成分在 650°C 前消失，而空位团簇可存续到 1000°C[13]。技术含义：过去评估辐照对金刚石量子传感的影响，必须把加工阶段与生长阶段分开分析，这次把缺陷从产生到退火的演化连成一幅完整图景。格局影响：金刚石量子传感器厂商的退火工艺窗口有了可依据的温度分界，属工艺参数级改进。

03 算法

算法与软件

BB84 被证明达到不可克隆加密的最高安全等级

此前的不可克隆加密方案只做到搜索安全，即攻击者难以找出正确密钥；新结果把它提升到不可克隆不可区分性，保证攻击者无法分辨两条被加密消息的差别，并用成熟的 BB84 协议完成了实现[12]。

技术含义：从找不到答案升级为看不出区别，是密码学安全定义里的一次级别跳变，后者才是现代加密方案的标准门槛。格局影响：不可克隆加密的理论地基被夯实，但落地仍受限于光子分发的实际信

道；受益的是长期做量子密码证明的学术与标准化圈子，产品化尺度以年计。

200 比特态制备的门数从四万压到五千五

一个此前需要四万多次量子操作的复杂概率分布制备任务，改用优化的张量网络方法后仅需约 5500 个受控非门，来源给出的目标态指标为 7.44×10^{-9}（原文用词为 fidelity，具体口径需核对论文）[14]。

技术含义：态制备是几乎所有实用量子算法的第一步，也是最常被忽略的隐性开销；门数降到约七分之一，等于把这道前置成本从算法的主要负担降为次要项。格局影响：金融衍生品定价、蒙特卡洛类量子算法的资源估算基数需要重算，直接影响所有对外发布量子优势时间表的团队。

量子态层析的开销从指数降到线性

通过把密度矩阵表示为收缩块张量列，表征量子系统所需的内存与计算时间随比特数从指数缩放降到线性缩放[15]。

技术含义：量子态层析（把量子态完整测量重建出来）的指数开销，长期把可验证系统规模卡在十几个比特；线性缩放意味着验证工具终于能追上硬件的比特数增长。格局影响：硬件厂商的验收与验证环节最先受益——没有可扩展的层析手段，逻辑比特的质量声明就只能靠抽样对；工具链落地以季度计。

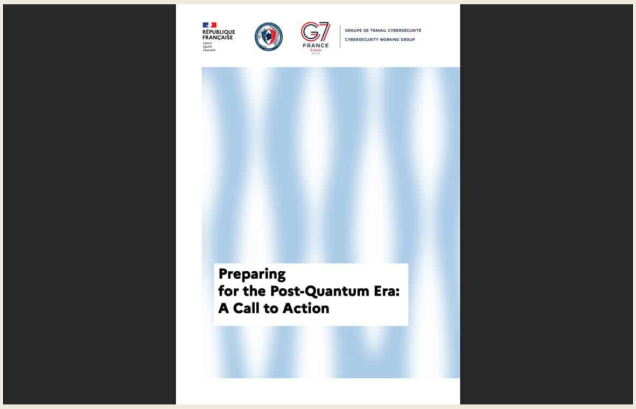
Jolt 零知识虚拟机换用格密码

开源 zkVM 项目 Jolt 推出 LatticeJolt 版本，用格密码替换椭圆曲线，既提速也顺带抗量子[21]。

技术含义：这是后量子迁移里少见的正向案例——换成抗量子原语不是付出性能代价，而是换来了性能；多数迁移场景中格密码意味着更大的密钥与签名体积。格局影响：区块链与零知识证明基础设施的后量子迁移动机从合规变成性能，迁移速度会明显快于传统 IT 领域，时间尺度以季度计。

04 产业

产业与生态



G7 喊话所有机构启动后量子迁移，真正有牙齿的是采购条款

G7 网络安全工作组在 2026 年 9 月发布行动倡议，敦促所有组织启动 PQC（后量子密码，能抵抗量子计算机破解的加密算法）迁移[1]。文件属于指引而非法规，但其中关于采购与供应链的措辞对企业及其供应商有实质约束力[1]。

商业含义：监管的软硬不在于文件本身是否有罚则，而在于它会不会被写进招标文件；采购语言一

旦落地，中小供应商的迁移窗口就由客户的合同周期决定，而不是自己的技术规划。

格局影响：受影响最直接的是向 G7 国家政府与金融机构供货的软硬件厂商，下一轮合同续签就会碰到这道门槛，时间尺度以年计；密码资产盘点与证书管理类厂商是明确的收入侧受益方。

Cloudflare 的 1.1.1.1 开始验证后量子 DNSSEC 签名

Cloudflare 在其 1.1.1.1 公共解析器上启用 ML-DSA-44 的 DNSSEC 签名验证，目前尚无其他主流公共解析器宣布同等支持[4]。

技术含义：DNSSEC（给域名解析结果加数字签名，防止被篡改）的签名体积在后量子算法下大幅膨胀，直接撞上 DNS 报文的传输限制；这次部署把传输、降级攻击与信任链三类问题从纸面推到线上，暴露出后量子迁移是系统工程而非换个算法库。

格局影响：域名注册商、权威 DNS 服务商与递归解析运营方被迫跟进测试，互联网基础设施的后量子迁移由此有了第一个可观测的真实样本，时间尺度以年计。

SEALSQ 上半年营收增长 131%

SEALSQ 公布 2026 年上半年业绩，营收同比增长 131%，并给出 2026 全年指引[35]。

商业含义：后量子安全长期是叙事强、收入弱的赛道，这是少见的收入侧证据；不过公司未拆分后量子芯片的收入贡献，增长起点基数与产品结构也决

定了它离规模化验证还有距离。格局影响：同期该公司还在首尔与市政方共建后量子芯片安全中心，把抗量子密钥直接嵌入半导体芯片[20]，并与 BWT Alpine F1 车队扩大合作、用后量子技术保护赛车设计资产[11]——三条线共同指向同一个打法：不卖算法，卖带密钥的芯片与合规入口。

Qubic 在 350 万美元种子轮后拿下 150 万加元政府合同

Qubic 与加拿大政府签下 150 万加元的量子低温放大器合同，此前该公司刚完成 350 万美元种子轮[16]。

商业含义：低温放大器是超导与自旋量子比特读出链路的必需件，属于典型的卖铲子生意，收入确定性高于整机厂商。格局影响：政府订单为早期硬件供应链公司提供了种子轮到 A 轮之间的过桥收入，这一模式在北美与欧洲正在成为常态。

Qilimanjaro 入选 EuroHPC 量子大挑战一期

西班牙公司 Qilimanjaro 从 27 份合格提案中选出的 13 家欧洲量子公司里入选，是唯一的西班牙企业，其 EuroQ-Stack 项目同时获得 STEP 认证印章[17]。

商业含义：STEP 印章是欧盟给战略技术项目的背书标签，此次认定 EuroQ-Stack 属于关乎欧洲技术主权与竞争力的高质量战略技术项目。格局影响：欧洲的量子资金分配正从撒网转向筛选，13 家入围名单基本划定了未来数年欧洲本土供应商的短名单。

生态简讯

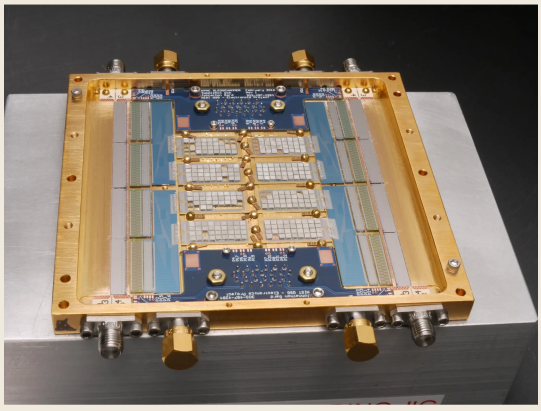
The Quantum Insider 推出经分析师核验的量子市场数据集产品[36]——量子行业的数据本身开始被当作商品出售。Qtonic Quantum 发布 2026 年第四季度量子网络安全报告[40]。QClairvoyance 与 Samgnya 签署量子技术研究谅解备忘录[39]。Quip Network 将推出 Quantum Echoes QFT 系列[41]。Bull 被选中承建西班牙国家气象预报基础设施的现代化升级[37]，属于量子邻接的高性能计算订单。

一篇面向从业者的分析开始系统梳理四类核心量子算法在美国法下的专利适格性问题[10]——量子软件的知识产权边界至今没有判例定型，这是估值模型里最少被定价的一项风险。

人才侧，斯德哥尔摩大学同期放出三个离子阱方向岗位，分别针对开放量子系统模拟、二维里德堡离子模拟与囚禁离子集体量子现象[7][8][9]；博洛尼亚大学开放经典与量子复杂系统数学物理方向的博士名额[6]。

05 学术

学术前沿



一种新测量方案逼近量子传感的终极精度界

利用玻色辅助模的物理测量方案，把多参数估计精度推到接近 Holevo–Nagaoka 界（量子测量精度的理论上限）[18]。

技术含义：此前该界限多被视为数学上的存在性结果，缺少可在实验室搭出来的对应方案；把它落到具体物理装置上，等于给传感精度划出了一条可实测的天花板。格局影响：量子传感的性能宣称从此有了统一标尺，磁力计、原子钟与重力仪厂商的对比口径会被逐步规范，时间尺度以年计。

时间本身可能带着一个最小的不确定度

非常规量子理论推出的结果显示，时间自身可能存在一个基本的不确定度，为任何时钟的测量精度设下终极上限；该效应远低于当前探测能力，但可能牵出量子力学、引力与时空之间的隐藏联系[25]。

技术含义：这是理论层面的可证伪命题，而非工程指标；其价值在于它把一个形而上的问题转换成了原子钟精度竞赛的长期靶子。格局影响：短期对产业没有影响，但为下一代光钟的精度目标提供了一个物理动机而非纯粹的工程惯性。

谷歌的多重宇宙主张：论证是认真的，实验挂错了

有评论指出，谷歌把一套严肃的量子力学诠释论证，绑在了一个所有标准诠释都能预测同样结果的基准测试上，而该测试的头条数据从未被直接验证；十个月后同一实验室保留了干涉部分[5]。

技术含义：判别不同量子力学诠释需要能区分它们的实验，而谷歌挂靠的那个基准恰恰不具备这种区

分力——所有标准诠释都预测同样的结果；论证有效性与实验设计的匹配失败，是量子计算宣传中反复出现的结构性问题。格局影响：受影响的是整个行业的可信度账户；对投资者而言，实用的检验方法是问一句这个实验能否证伪相反结论，而不是看结论有多惊人。

06 影响

今日影响

1 **走片上集成路线的 QKD 厂商要重跑安全评估。** 衰减器在 1107 纳米附近的意外发光构成了标准 BB84 分析没有覆盖的旁路信道[3]，这意味着安全证明需要补进器件辐射模型，认证流程要增加波长扫描项。下一步值得盯：是否有厂商公布器件级屏蔽方案，以及标准化组织会不会把光谱测试写进 QKD 认证规范。

1 **评估逻辑比特的尽调问题清单变了。** Helix 在 Helios 上的演示全程不做后选择[2]，把是否后选择从论文脚注抬到了首要口径问题；今后任何厂商报出逻辑错误率，第一问都应该是有没有丢数据。下一步值得盯：非 Clifford 门与魔法态注入

何时出现在同一套硬件上——那才是通用逻辑计算的临界点。

1 **后量子迁移的成本账被两头改写。** 一头是 G7 把迁移压力通过采购条款传导给供应链[1]，另一头是 Cloudflare 在 1.1.1.1 上的实际部署暴露出传输、降级与信任链的系统性难题[4]。对企业安全负责人而言，迁移预算里真正的大头不是换算法库，而是排查那些会被更大签名撑爆的协议。下一步值得盯：是否有第二家主流公共解析器跟进后量子 DNSSEC 验证。

1 **量子软件的资源估算基数集体下修。** 200 比特态制备的门数从四万多降到约 5500[14]，态层析开销从指数降到线性缩放[15]，两项都作用在算法的前置与验证环节。任何在过去一年做过量子优势时间表测算的团队，其分母都需要重算。下一步值得盯：这两项方法能否在真实硬件上跑通，而不只停留在模拟基准。

1 **后量子安全开始出现收入侧证据。** SEALSQ 上半年营收增长 131%[35]，同期在首尔落地芯片安全中心[20]、在 F1 赛车研发中扩大合作并以后量子技术保护设计数据[11]，卖芯片而非卖算法的路径开始有账面回报。下一步值得盯：全年指引能否兑现，以及增长中有多大比例真正来自后量子迁移而非传统安全芯片业务。

07 编辑

编辑点评

这两天最值得记下的，不是哪个数字又刷了纪录，而是几处口径在同时收紧。纠错演示开始强调不做后选择，测量精度开始对标理论上限，量子态验证的工具终于能跟上比特数的增长，连诠释性主张也被公开追问实验设计能否支撑结论。这些都指向同一件事：这个行业正在从比谁的数字大，转向比谁的数字经得起追问。对做尽调的人来说，这是好消息——可比性变强了；对靠单点最优值做估值的人来说，这是坏消息——单对最优、后选择后的成绩、条件保真度这类说法的折价会越来越明显。

另一条线索在安全侧。抗量子加密长期被当成一个未来问题，而这两天它同时从三个方向变成当下问题：采购条款让它成为合同义务，基础设施部署让它暴露出系统性摩擦，而集成器件里的意外发光提醒人们，物理定律保证的安全只覆盖证明里写进去的那些自由度，写不进去的部分照样会漏。值得注意的是，这三件事的推进速度并不由技术决定——密码迁移的节奏由合同周期、认证流程和供应链替换周期决定，通常以年计。真正的风险不在于量子计算机哪年造出来，而在于迁移的组织成本被持续低估，而窗口正在被采购条款一格格收窄。

参考资料

[1] G7 Tells Every Organization to Start PQC Migration – But the Procurement Signal Matters More Than the Headline

[2] Quantinuum’s Helix Demonstrates How a Compact Error-Correcting Code Can Compute

[3] Chip-Based QKD Has a Glow Problem: VOA Luminescence Creates a Side Channel That Standard Security Analyses Miss

[4] Cloudflare’s 1.1.1.1 Now Validates Post-Quantum DNSSEC Signatures – And Shows Why PQC Migration Is a Systems Problem

[5] Google’s Multiverse Claim Was a Serious Argument Attached to the Wrong Experiment

[6] PhD fellowship in Mathematics @University of Bologna on Mathematical physics of classical and quantum complex systems

[7] PhD position in open quantum system simulations with trapped ions at Stockholm University

[8] PhD position in 2D quantum simulations with trapped Rydberg ions at Stockholm University

[9] Postdoc position in investigation of collective quantum phenomena with trapped ions at Stockholm University

[10] Patenting Quantum Computing Innovations: Lessons from Four Core Quantum Algorithms – Part 1

[11] LUMI AI Factory Selects IQM’s Halocene Roadmap for Europe’s First Superconducting Logical Qubit System

[12] Infleqtion and Cisco Partner to Advance Distributed Neutral-Atom Quantum Networking Architectures

[13] Altera and Riverlane Partner on QEC Interfaces for Agilex FPGAs Following Post-Quantum Security Rollout

[14] Chalmers Researchers Accelerate Bosonic Quantum Operations by 1,000x Using Quantum Lattice Gates

[15] BWT Alpine Formula One Team and SEALSQ Expand Quantum Partnership into Multiphysics Simulation

[16] Researchers Prove BB84 Encryption Achieves Top Security Level

[17] Researchers Map Hydrogen Defects Limiting Diamond Qubit Coherence

[18] NIST quantum sensors help verify nuclear safeguards internationally

[19] Researchers Achieve 7.44e-9 Fidelity for 200-Qubit States

[20] Xanadu and AMD speed up quantum computing with Backline link

[21] Researchers Cut Complexity of Quantum State Estimation

[22] $1.5M contract follows $3.5M seed for Qubic’s quantum hardware

[23] Spanish Firm Qilimanjaro Joins EuroHPC Quantum Push

[24] A new measurement scheme nears the ultimate precision for quantum sensing

[25] Vienna team sculpts quantum atomic-scale pores in ‘white graphene’

[26] Seoul and SEALSQ build center for post-quantum chip security

[27] Jolt zkVM switches to lattices for faster, post-quantum proofs

[28] Clarendon Laboratory boosts atom-atom entanglement with cavity design

[29] Researchers Cut Quantum Error Rates with Optimised Atom Loss

[30] Researchers synchronize qubits using a new quantum memory trick

[31] Physicists just found a tiny glitch in time itself

[32] AI researcher Jacob Coxon quit, fearing extinction. Security experts see a familiar fight

[33] Unique, mathematical 60-sided "Go First Dice" go on display

[34] The Atlantic hurricane season just quietly broke a new weather record

[35] Giant armored crustaceans survive thanks to a gene stolen from bacteria

[36] ‘Odd couple’ black holes can find each other in space

[37] Why the Swift telescope was so special

[38] Are AI chatbots making us less human?

[39] 25 years after 9/11, survivors are still getting sick—here are the numbers

[40] 9/11 in Berkeley

[41] SEALSQ Reports 131% Revenue Growth in H1 2026

[42] Stevens Researchers Take Step Toward More Precise, Practical Quantum Technologies

[43] The Quantum Insider Launches Datasets, Analyst-Verified Quantum Market Information

[44] Bull Selected to Modernize Spain’s National Weather Forecasting Infrastructure

[45] Quantum Cybersecurity Explained: Preparing for Quantum Computing

[46] Qubic Secures $1.5 Million Canadian Government Contract for Cryogenic Amplifiers

[47] BWT Alpine and SEALSQ Explore Quantum-Classical Simulation for Formula One

[48] QClairvoyance and Samgnya Sign MoU on Quantum Technology Research

[49] Qtonic Quantum Publishes Q4 2026 Quantum Cybersecurity Report

[50] Quip Network to Launch Quantum Echoes QFT Collection