2026 年 11 月 01 日 – 11 月 02 日 · 日报

量子保密通信曝漏洞一束弱蓝光即可窃取密钥

19 篇 · 6 个来源 | PDF | 本期汇总免费阅读

本 期 目 录

- 今日三件事
- 硬件前沿
- 算法与软件
- 产业与生态
- 学术前沿
- 今日影响
- 编辑点评

收录报道	19
信息来源	6
阅读时长	约 16 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**

01 亮点

今日三件事



1 **离子阱逻辑纠错手术误差破百分之一** 霍尼韦尔旗下Quantinuum在离子阱处理器上基于广义双环码完成七比特逻辑块操控，逻辑比特测量误差为0.72%，复用后二次测量误差为1.12%[16]——首次在双环码验证低误差格点手术，迈过容错实用门槛。

1 **美财政部将委内瑞拉移出量子投资受限名单** 美国财政部修订涉外投资规程，正式将委内瑞拉从涉及量子技术、超级计算及微电子领域的对外资本流动限制名单中移除[1]——边际松绑拉美涉量子资本流动，合规重心进一步聚焦。

1 **IBM携手边缘计算联盟共建先进计算生态** 下一代边缘联盟将于德克萨斯州弗里斯科星光体育场启

动，IBM量子副总裁约瑟夫·布罗兹将发表主题演讲推进算力下沉[12]——推动量子算力与边缘电信深度融合，加速算力下沉落地。

02 硬件

硬件前沿

离子阱

霍尼韦尔旗下Quantinuum科研团队在离子阱处理器上，利用广义双环码（一种高码率量子纠错码）实现了七比特逻辑块内部的独立测控，其逻辑量子比特测量误差为0.72%，且在复用相同物理比特进行二次测量时的误差为1.12%[16]。

该成果是国际上首次在广义双环码体系上验证格点手术（跨逻辑块信息交互技术）的有效性，其0.72%的单次测量误差跨过了1%的容错实用化公认门槛[16]。对照当前硬件SOTA（行业最佳水平）基线：在物理门层面，当前商用全比特对最高纪录为Quantinuum Helios保持的双比特门保真度99.921%（误差约0.079%），本次逻辑层测量的0.72%误差虽落后物理双比特门约一个数量级，但相较传统表面码大幅降低了物理比特开销[16]；在还差什么方面，离子阱技术路线仍受困于离子穿梭输运延迟与重复频率较低（典型值仅数十至百赫兹，较超导慢三个数量级以上）的硬瓶颈，距离百逻辑比特级容错机仍缺全芯片并行的超大规模实时解码验证[16]。

此进展直接巩固了Quantinuum在逻辑比特测控领域的领先地位，预计将在12至18个月内推动基于低密度奇偶校验码的离子阱容错架构从单块概念验证迈向多块逻辑拼接阶段[16]。

量子网络与通信

物理学研究人员实验证实，使用中等强度的外部连续蓝光照射连续变量QKD（量子密钥分发）发射机，会在其光学调制元器件恢复期引发暂态物理响应漂移，使攻击者在系统信道安全密钥率为零的无保护状态下成功截取并重构传输密钥[6]。

该工作首次在实验层面证实了连续变量QKD发射端复位阶段的物理层旁路漏洞，打破了该类协议依赖探测信道超额噪声即可判定绝对安全的前提假设[6]。

此漏洞直接冲击QKD设备集成商与通信运营商，迫使相关硬件厂商必须在6至12个月内针对光学发射前端增加光隔离硬件防护并升级设备故障恢复协议规范[6]。

量子传感

罗切斯特理工学院研究团队利用光力谐振器（微观光学与微机械振动耦合结构），在非厄米系统的奇异点（系统本征值与本征矢同时合并的退化点）处，通过定向优化外场探测方式，实现了在不牺牲精度的前提下缩短极弱外力信号观测时间的目标[14]。

该实验首次澄清了学界此前关于奇异点传感由于系统临界减慢而无法提升实际测量速度的长期理论争议，证明了特定探针动力学方案能够缩短外力探测响应时间（具体缩减比例未披露）[14]。

该方案为微纳级高灵敏度惯性制导陀螺仪与弱重力梯度测量仪的工程研制扫清了时延障碍，高精尖仪器制造商预计将在2至3年内将该拓扑探测技术导入下一代机载导航传感原型机[14]。

量子测控与多比特体系

物理实验团队在最长达12个量子比特的链状系统中利用主动重置技术测量量子纠缠态，发现不同物理观测量的响应出现分离，并通过詹森间隙（衡量统计凸性与纠缠保持度的数学量）直接量化出系统对历史操作信息的残留记忆[18]。

该研究首次在12比特真实物理尺度上证实，测量并主动重置部分比特所产生的动力学轨迹能够直接提取非马尔可夫历史关联，省去了全态层析所需的指数级测量次数[18]。

该研究展现了构建可扩展量子存储器的潜力，但对多比特硬件环境噪声表征时间的优化效果未披露[18]。

算法与软件

纠错码与编译优化

针对中性原子量子计算平台的物理特性，科研人员发布了名为NAKO的专用基准测试框架，利用配套的Enola编译器在标准测试线路上将中性原子量子比特的平均物理移动距离减少了78.9%，同时最小化了纠缠门操作数量[10]。

这是量子编译领域首次建立针对中性原子穿梭调度的全流程诊断与优化标准，将原子在光镊阵列中移动导致的退相干加热损耗压减至原基准水平的五分之一左右[10]。对照中性原子SOTA基线：目前中性原子物理比特规模已达1180个，但循环重复率受限于原子穿梭加热，长期卡在1至10赫兹的低频瓶颈；本次78.9%的位移缩减精准击中该短板，但要实现深层电路仍缺极低温原位连续装载与高保真中路测量的全面闭环[10]。此编译框架预计将在6个月内被QuEra、Pasqal等中性原子整机团队吸收进底层云端驱动堆栈[10]。

理论物理团队收紧了量子数据存储中纠错恢复性能的数学上界，证明当纠错距离参数δ等于2时，其性能极限严格匹配经典的戈洛维奇-古鲁斯瓦米（Golowich-Guruswami）单擦除上界，并通过显式余项修正改进了现存纠错恢复理论界限[8]。该成果首次消除了此前理论评估对特定纠错码拓扑设计的强假设依赖，为表面码与qLDPC（量子低密度奇偶校验码）架构师在设计新型低开销解码算法时提供了严密的性能判定锚点[8]。

量子模拟与算法复杂度

研究团队提出基于Mamba序列状态空间架构的量子特征求解器（Mamba Quantum Eigensolver），在氢气分子基态模拟测试中实现了低于3×10^{-6}哈特里（Ha，原子能量单位）的能量误差，并将传统量子化学模拟从二次计算复杂度降至线性复杂度[5]。该算法首次利用高效序列建模架构实现了分子势能面的直接端到端预测，摆脱了传统参数化变分算法在处理复杂多电子体系时计算开销随体系规模二次方膨胀的严重瓶颈[5]。该方案为计算化学与药物靶点筛选提供了高精度新范式，预计将在2至3年内推动制药巨头材料计算管线向新型状态空间算法底座迁移[5]。

理论计算团队针对图论锦标赛问题开发出新型量子搜索算法，将判定竞赛图优胜集合（Top Cycle）的计算复杂度从经典算法的$\Theta(N^2)$降低至量子查询复杂度$\Theta(N)$，并将寻找击败所有对手的孔多塞优胜者（Condorcet Winner）查询次数由$\Theta(N)$降至$\Theta(\sqrt{N})$[9]。该成果首次证明了图论排序决策问题存在严格的二次级量子加速，扩充了平方加速算子的应用边界，为未来分布式共识协议与复杂金融博弈论模拟奠定了理论基石[9]。

针对变分量子算法中普遍存在的训练停滞难题，科研人员提出将变分线路与绝热量子计算相结合的优化路径，利用QUBO（无约束二次二值优化）数学表述完成算法绝热训练，成功实现了对多体量子纠缠态的高效识别[15]。该方案首次将连续绝热演化引入变分参数求解，初步测试表明其为可扩展纠缠验

证提供了新途径，但更广泛的性能对比尚未完成[15]。

在混合数字-模拟量子网络研究中，科研团队证实通过引入长程量子相互作用链路，仅需单层物理连接即可学习传统方案需要6层标准最近邻连接才能提取的数据模式，将训练耗时与电路深度均缩减至原有水平的六分之一[17]。该发现首次量化了长程模拟相互作用对多层离散量子门的替代比例，大幅降低了硬件相干时间不足对深层线路的制约，利好超导腔与离子阱硬件在1至2年内承接更复杂的拓扑数据学习任务[17]。

04 产业

产业与生态



政策与资本规程

美国财政部正式发布法规修订通知，将委内瑞拉从涉及量子信息技术、超级计算及先进半导体领域的对外资本流动限制名单中移除[1]。

该举措表明美方基于第14105号行政令框架设立的对外投资国家安全审查体系，正在收缩次要地缘风

险区域的合规防线，将执法资源与跨境资本监控重心进一步聚焦于主要竞争对手[1]。

此项调整为跨国资本在拉美特定市场的电信级抗量子加密网络与半导体供应链布局扫清了合规障碍，但全球顶尖量子芯片及核心制冷设备的出口管制高墙并未发生松动[1]。

网络安全与公钥基础设施

数字证书颁发机构（CA）与自动化证书管理服务商Sectigo针对全球500位企业信息技术与网络安全负责人开展的年度调研显示，38%的企业已经全面评估了自身的量子密码风险敞口（较2025年增加），但仅有4%的企业实现了数字证书的完全自动化生命周期管理[3]。

该调研揭示了当前企业抗量子防御中严重的“能力脱节”——虽然风险意识大幅攀升，但96%的系统仍依赖人工或半自动化运维，在应对未来PQC（后量子密码）公钥体积膨胀与高频轮换时极易发生配置崩溃[3]。

随着谷歌Chrome浏览器加快在公钥基础设施中强制推行抗量子数字证书，金融支付网络与大型云服务商面临巨大的业务中断风险，此矛盾将在未来24个月内倒逼全球百亿美元级网络安全运维市场全面转向自动化加密敏捷性架构[3]。

跨界联盟与生态拓展

下一代边缘计算联盟（Next Edge Alliance）将于2026年11月3日在德克萨斯州弗里斯科星光体育场

启动，IBM量子业务副总裁兼全球生态负责人约瑟夫·布罗兹（Joseph Broz）将受邀发表开幕主题演讲[12]。

该合作意味着顶级量子硬件厂商正在主动突破传统云端集中机房形态，将量子算力接口向5G/6G边缘基站、工业物联网节点及分布式边缘微数据中心生态渗透[12]。

此联盟的成立加速了量子计算与电信运营商基础网络的协议对齐，预计将在2年内催生多模态分布式算力调度体系，推动量子启发式算法在智能电网调度与车路协同边缘节点中的早期商用试跑[12]。

05 学术

学术前沿

计算复杂性与验证理论

理论计算机科学家在相对经典预言机框架下，成功证明了处于多项式层次结构（PH）之外、可在量子多项式时间（BQP）内判定的语言，能够被经典验证者以仅四分之一的极低错误率进行经典交互验证，且交互信息传输报文数量达到了理论最优值[7]。

该成果是国际上首次证明经典交互式证明系统有能力监督超越经典计算能力极限的复杂量子任务，确立了经典计算机对超常量子计算能力的有效监督范式[7]。

这一结论重塑了密码学中零知识证明与可验证外包量子计算的底层理论防线，为未来金融机构租用不可信第三方量子云进行私密资产运算提供了可落地的经典验证框架[7]。

连续变量与存储理论

物理学者提出由(2r+2)个波包组成的连续变量玻色纠错编码架构，证明量子存储保真度误差随阻尼率γ按O(γ^(r+1))多项式阶缩减，且采用6个及以上波包编码时可完全消除光子数退相干引起的一阶物理误差，首次实现了在不破坏所编码逻辑量子比特的前提下同时高灵敏度感知外部微弱力场[11]。

该工作从理论上打破了“纠错保护”与“外场传感”在单模物理体系中不可兼得的长期认知，将量子存储器与高灵敏度探测器合二为一[11]。

该设计直接利好连续变量量子中继节点与超导微波腔存储器件的研发，预计将在3年内推动兼具长寿命量子中继与极弱雷达信号探测功能的新型集成量子节点问世[11]。

统计物理研究团队证明，在二维与三维空间中的“R压缩”拓扑纠错体系下，即使完全摒弃全局时钟同步脉冲，仅依靠系统各组件完全独立的随机局部更新，量子存储器依然能够展现出长效稳定的纠错保护能力[13]。

该理论首次在非互斥动力学系统中确立了异步纠错的稳定性边界，证明了大规模量子纠错计算机无需在整芯片数百个区域维持严格的纳秒级同步时钟[13]。

该结论显著降低了超导芯片内部低温同轴布线与多通道同步微波发生器的工程负担，有助于稀释制冷机内部极低温布线热负荷问题的解决[13]。

量子态估计公理化

《自然·量子信息》（npj Quantum Information）发表最新理论论文，研究人员借助扩展逆向回溯态估计框架，将历史上各自独立的连续时间量子平滑理论统一在同一数学体系下[2]。

该成果消除了此前学界在处理开系统量子动力学中过去、现在与未来时间序列联合推断时的公理化割裂，提供了标准化的轨迹平滑后验概率推断工具[2]。

此数学引擎直接适用于高保真度连续微弱测量信号的在线降噪[2]。

06 影响

今日影响

1 **企业首席信息安全官与网络架构师**：Sectigo调研显示38%的企业虽已明确量子解密威胁，但仅4%具备全自动化证书管理能力[3]。随着主流浏览器即将强制推行后量子证书，96%依赖人工维护的企业极易爆发业务中断，倒逼技术团队必须在未来12个月内将证书生命周期管理（CLM）工具由可选外挂升级为P0级基础设施。

1 **量子保密通信设备制造商与电网政企专网用户**：研究证实连续变量QKD发射机在弱蓝光照射下的

复位阶段可被隐蔽绕过安全防线并泄露密钥[6]。依赖该类设备保护高敏感资产的金融与电力专网机构，需立即督促设备供应商复测物理层防光注入隔离机制，并要求在采购标准中加入暂态复位状态的异常自毁与报警规范。

1 **中性原子量子硬件研发团队与编译工具链厂商**：NAKO基准与Enola编译器将原子物理穿梭平均距离缩减78.9%[10]，直接针对中性原子路线核心痛点——原子穿梭加热与退相干耗时。这将大幅减轻中性原子整机团队对高功率激光光镊控制系统的硬件设计冗余压力，预计6个月内将引发中性原子编译软件层的新一轮算子重构竞赛。

1 **容错通用量子计算投资机构与软硬件团队**：Quantinuum在广义双环码体系上实现0.72%的格点手术测量误差[16]，标志着低物理比特开销的qLDPC编码在离子阱上跨过了首个逻辑拼接门槛。资本市场对多逻辑比特芯片的估值逻辑正从“单个芯片上拼凑物理比特数量”向“低编码开销下能否完成模块化逻辑手术”深度切换。

07 编辑

编辑点评

从今日盘面的技术脉络观察，量子硬件与应用生态正在呈现鲜明的“工程化深化”与“现实碰撞”双轨特征。在计算硬件端，竞争重心已彻底告别早年单比特保真度刷榜的单一叙事，转向多物理维度的系统级折中：无论是离子阱平台跨过1%误差门槛的广义双环码格点手术，还是中性原子编译器将原子

移动距离压减近八成的精准调度，都表明行业正在以前所未有的工程严谨度，正面攻坚穿梭延迟、加热退相干与逻辑块互联这些决定容错机器能否真正落地的硬核工程屏障。

然而，当我们将视线移至通信与产业防御端，理论模型的完美性正遭遇物理工程实现的严酷现实。一方面，声称基于物理规律不可破解的连续变量量子通信系统，却因为发射端复位阶段的一束弱蓝光而暴露出旁路密钥泄露通道；另一方面，面对迫在眉睫的量子解密风险，全球高达96%的企业由于缺乏自动化工具而无法有效更迭传统加密证书。这深刻警示着行业：量子安全防御绝非在白皮书上更新一套抗量子加密算法或架设一套QKD设备即可一劳永逸，其真正的胜负手在于物理层硬件抗物理篡改的工程鲁棒性，以及企业IT基础设施抵御高频轮转冲击的自动化运维韧性。

参考资料

[1] IQT Sunday Edition

[2] Unifying quantum smoothing theories with extended retrodiction

[3] Sectigo Reports 38% Have Fully Assessed Their Quantum Exposure, but Only 4% Say Their Certificate Management Is Fully Automated

[4] Two fully funded 3-year PhD positions in coupled-cluster theory development

[5] Researchers Predict Stable Electronic Structures Using Mamba

[6] Researchers Find Attack Exploiting QKD Transmitter Recovery

[7] Researchers Verify Quantum Computation Beyond Polynomial Hierarchy

[8] Researchers Bound Performance of Quantum Error Recovery

[9] Researchers Cut Quantum Search Time for Tournament Solutions

[10] Meet NAKO, A Benchmarking Framework for Evaluating and Diagnosing Neutral-Atom Quantum Compilers

[11] Researchers Bound Memory Error to Gamma Raised to R Plus One

[12] IBM Quantum’s Joseph Broz to keynote Next Edge Alliance launch

[13] Researchers Stabilise Quantum Memory with Random Updates

[14] Rochester Institute of Technology Detects Weak Forces Faster Using Quantum Points

[15] Researchers Train Algorithms to Detect Entanglement Using Quantum Computing

[16] Researchers Measure Logical Qubit with 0.72% Error Using Quantum Surgery

[17] Researchers Cut Training Time Using Longer-Range Quantum Links

[18] Researchers Measure Entanglement on 12-Qubit System Via Resets

[19] These tattoos can magically' disappear—here’s how they work

量子研究内参

全部期数 · 周刊深度解析 · 每日快报 → qbitbrief.com

FOR RESEARCH REFERENCE ONLY

配图源自所引论文与新闻稿；如引用不规范，请联系编辑部删除。