

HAWK签名方案撤出NIST第三轮附加签名进程

39 篇 · 11 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	39
信息来源	11
阅读时长	约 11 分钟

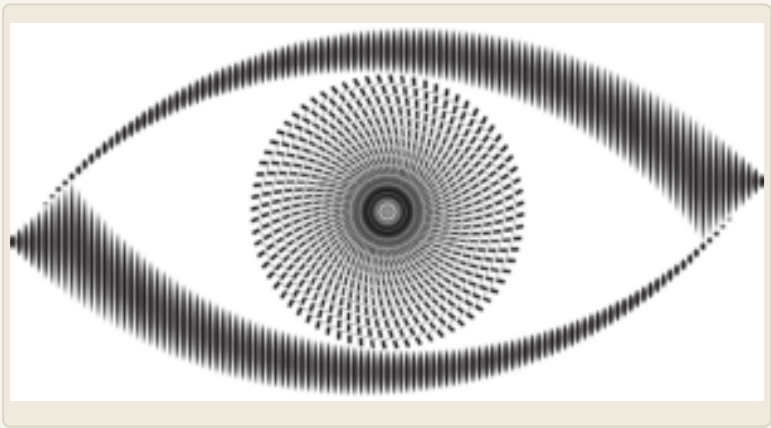
当前 S O T A

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

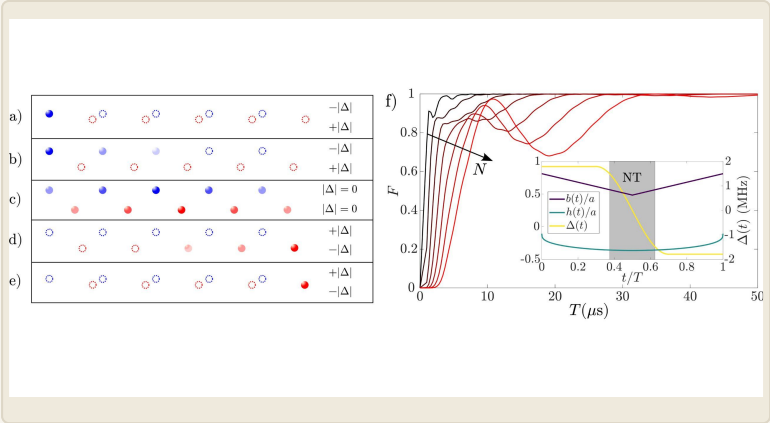


- HAWK签名方案撤回** 格基签名方案HAWK因改进版密钥恢复攻击（由Anthropic的Claude Mythos Preview主导发现）从NIST第三轮附加签名进程中撤回，公开披露后约17小时内完成^[39]——该攻击不影响已定稿标准ML-KEM与ML-DSA，但凸显加密敏捷性在后量子迁移规划中的现实必要性。
- 纽约州6000万美元RFP** 纽约州启动竞争性招标，拟建最多4个区域性量子技术商业化中心，资金来自2027财年预算^[14]——州级财政直接投向量子商业化基础设施。
- Xanadux阿尔伯塔大学** 合作开发光动力学癌症药物发现量子算法，聚焦肿瘤学与制药设计^[11]

——光量子计算切入药物发现方向的算法研发合作。

02 硬件

硬件前沿



超导

— 巴西物理学家开发出基于超导器件的连续变量通用计算构建块，成果发表于2026年8月13日 [16]。技术含义：在超导平台展示连续变量编码的通用计算基本单元，与主流离散变量超导量子比特路线形成互补。格局影响：若保真度与可扩展性验证通过，可能开辟超导量子计算新范式，但距离实用化仍缺错误纠正与多比特集成。

光子

— 伦敦玛丽女王大学开发出模块化光子量子计算架构Clavina，将量子模块设计为类似计算机组件 [26]。技术含义：以模块化方式构建光子量子计算系统，有望提升系统灵活性与可维护性。格局影响：光子路线长期受限于损耗与连接成功率，

模块化设计若配合高保真互连，可加速中等规模光子处理器落地。

- 量子芯片隔离器实现30分贝回反射抑制，演示了无磁、宽带行波隔离器用于光子集成电路^[23]。
技术含义：在光子集成电路上实现约30 dB峰值隔离度，且无需磁性材料。格局影响：为光子量子芯片的信号完整性提供关键组件，减少噪声源，向实用化光量子计算迈进。

中性原子

- 理论框架实现里德堡阵列中长程相互作用下的鲁棒拓扑量子态转移^[29]。技术含义：提出一维长程耦合系统中快速、高保真拓扑态转移的理论框架，针对里德堡原子偶极-偶极相互作用优化。格局影响：中性原子路线在量子态传输与逻辑操作上获得新工具，但尚未有实验验证，时间尺度预计2-3年。

算法与软件



- 催化z旋转实现恒定T深度：研究显示利用特定催化态，任意单比特z旋转的T深度可降至3，且催化态大小随精度对数多项式增长^[28]。技术含义：在催化态可用的前提下将单比特z旋转的T深度压缩至常数3，T门是容错计算中成本最高的操作之一。格局影响：该结果可显著降低容错量子电路的门开销，对量子编译器和纠错架构设计有直接指导意义。
- 线性光学中高效图态生成：提出在光子系统中高效生成图态的方法，图态是量子计算、通信和纠错的核心资源^[30]。技术含义：绕开传统的概率性融合门，仅用单光子源、线性光学与预报测量直接生成毛虫图态（CGS），降低光子数与成功率带来的开销。格局影响：光子量子计算的关键瓶颈之一是大规模纠缠态制备，该方案若实验验证可推动光子路线实用化。
- 贝叶斯多参数量子估计中的测量不相容性：系统阐述了贝叶斯框架下多参数量子估计的理论，并量化了测量不相容性对可达精度的影响^[27]。技术含义：给出测量不相容性对多参数估计精度的定量界限，作者自述为一次全面且具教学性的表

述，并将结论与局域估计理论的多拷贝情形类比。格局影响：为量子计量与传感设计提供理论指导，影响量子增强测量方案的优化。

04 产业

产业与生态



融资与政策

- 纽约州州长Kathy Hochul宣布启动竞争性RFP，建立最多4个区域性量子技术商业化中心，总资金6000万美元，由Empire State Development的NYSTAR部门管理^[14]。商业含义：州政府直接注资量子商业化基础设施，吸引企业落地并形成区域集群。格局影响：纽约州意图成为美国量子产业核心地带，其他州可能跟进，时间尺度1-2年。
- SEALSQ与Quobly达成500万美元商业协议，将后量子安全技术集成到Quobly的硅基量子计算平台^[18]。商业含义：量子计算硬件厂商开始内置后量子安全模块，为未来量子-经典混合系统提

供安全保障。格局影响：硅基量子计算路线获得安全层支持，推动商业部署进程。

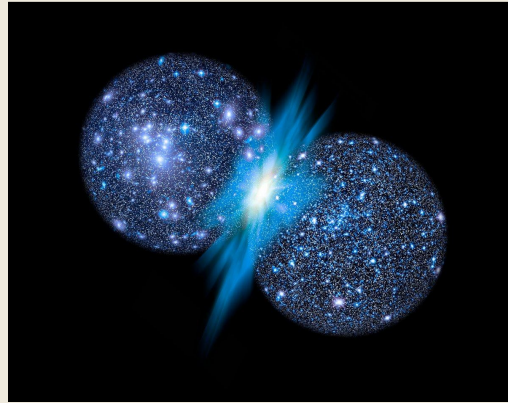
合作与部署

- Xanadu与阿尔伯塔大学合作开发光动力学癌症药物发现量子算法，由Xanadu算法团队与阿尔伯塔大学化学系主任Alex Brown教授领导^[11]。商业含义：光量子计算公司切入药物研发垂直领域，验证算法在真实化学问题上的优势。格局影响：若项目产出可行算法，将吸引制药行业投资，时间尺度2-3年。
- BTQ Technologies与ITCENGLOBAL子公司ITCEN PNS签署MOU，在韩国部署后量子安全解决方案，包括PQC、量子安全认证与硬件根信任^[12]。商业含义：韩国市场对后量子安全需求增长，BTQ通过本地伙伴进入。格局影响：亚洲后量子安全部署加速，韩国金融与政府机构或率先采用。
- 加拿大非营利组织Open Quantum Design与韩国SDT达成制造合作，SDT将把开源硬件蓝图转化为物理离子阱量子处理单元^[13]。商业含义：开源量子硬件设计获得主要商业化制造伙伴，降低离子阱量子计算机的进入门槛。格局影响：若开源模式成功，将催生更多中小型量子硬件厂商，时间尺度2-4年。
- Qunnect获DARPA合同，推进量子网络实时偏振补偿技术，属于QuANET项目与SBIR计划^[8]。商业含义：量子网络硬件初创公司获得国防资金，验证纠缠分发在电信光纤中的稳定性。格局

影响：量子网络基础设施向实用化迈进，国防应用可能率先部署。

- T-SQUARED开始为Infleqtion在牛津科技园建设量子创新中心，该设施将使Infleqtion英国运营能力扩大三倍^[9]。商业含义：中性原子量子技术公司扩大研发与制造规模，为商业化量产做准备。格局影响：英国量子供应链获得制造能力提升，中性原子路线竞争加剧。
- 圭尔夫大学与Xanadu签署MOU，合作量子计算教育与人才发展，合作期至2028年^[10]。商业含义：光量子计算公司投资教育生态，培养潜在客户与人才。格局影响：量子人才管道从研究向产业延伸，长期利好行业。
- CO.LAB Q提供12个月商业化工作室，帮助量子初创企业在查塔努加扩展，现已开放申请^[21]。商业含义：加速器模式进入量子领域，提供创业指导与资源对接。格局影响：量子创业生态进一步丰富，可能催生新一批应用型公司。

学术前沿



- 单杂质束缚激子产生相干量子光：npj Quantum Information发表研究，展示从单杂质束缚激子产生相干量子光^[3]。技术含义：展示基于单杂质束缚激子的相干光源（来源仅提供论文标题与DOI，未见摘要），为固态量子光学提供新途径。格局影响：若可集成到芯片，将推动片上量子光源发展，影响量子通信与计算。
- BBM哈密顿量的度量补全中缺失本征态：分析Bender–Brody–Müller哈密顿量作为Hilbert–Pólya算子时，某些候选本征函数在补全空间中不存在^[20]。技术含义：澄清了非厄米哈密顿量在量子力学中的数学结构。格局影响：对量子力学基础与量子混沌研究有理论意义，短期无产业影响。
- 哈马德·本·哈利法大学团队设定量子预测界限：研究自指涉预测极限在量子控制、资源界限与Gödel安全架构中的构造性实现^[17]。技术含义：构造性展示量子预测的极限与Gödel安全架构。格局影响：为量子机器学习与量子控制理论提供边界条件。

- 远距离超扩散星系中的球状星团流揭示暗物质新线索：Nature发表研究，利用遥远超扩散星系中的恒星流绘制暗物质分布^[25]。技术含义：在遥远超扩散星系中发现的恒星流，为测绘暗物质提供了一次罕见机会。格局影响：暗物质研究获得新探针，与量子传感技术潜在交叉。
- 物理学家确定重子数，解物质最大谜团之一：研究精确确定重子数，可能解释宇宙中物质与反物质的不对称性^[31]。技术含义：确定了重子数这一难以捉摸的量，来源未披露精度数值，也未说明该结果为实验还是理论工作。格局影响：基础物理突破可能启发新量子模拟方向。
- 神经科学家低估脑细胞计算能力：新研究显示每个神经元可同时进行多项计算，得益于数百个分支^[33]。技术含义：对神经计算模型提出修正。格局影响：可能影响神经形态计算与量子-经典混合架构设计。

今日影响



- 1 NIST后量子标准化进程受挫：** HAWK撤回表明即使进入第三轮的方案也可能存在致命漏洞，该攻击不影响已定稿标准ML-KEM与ML-DSA，但企业与政府需将加密敏捷性纳入后量子迁移规划[39]。
- 2 纽约州量子商业化加速：** 6000万美元RFP将吸引量子公司落户纽约，形成区域集群，投资者可关注中标企业与相关供应链机会[14]。
- 3 韩国后量子安全市场启动：** BTQ与ITCEN PNS签署MOU建立商业框架（尚未部署交付），韩国金融与政府机构可能率先采购后量子安全产品，为其他亚洲国家提供模板[12]。
- 4 光量子计算切入药物研发：** Xanadu与阿尔伯塔大学合作若产出有效算法，将吸引制药行业投资，并加速光量子计算在垂直领域的应用[11]。
- 5 量子网络基础设施获得国防资金：** Qunnect获DARPA合同，实时偏振补偿技术若成功，将推动量子网络在国防通信中的部署，并带动相关硬件供应链[8]。

编辑点评

本期最引人注目的不是某个技术突破，而是HAWK从NIST第三轮附加签名进程中的撤回。HAWK的撤回并非因为量子计算机变得更强大，而是因为经典攻击借助更彻底的分析方法（包括来自Anthropic的Claude Mythos Preview）发现了漏洞。这提醒产业界：后量子安全不能仅仅依赖标准化流程，还需持续的安全审计与快速响应机制。对投资者而言，PQC领域的风险与机遇并存，那些能够快速迭代并验证安全性的公司更可能获得信任。

同时，纽约州的6000万美元RFP和韩国市场的后量子安全部署表明，量子技术正在从实验室走向区域经济竞争与地缘安全博弈。州政府与国防机构的资金注入，将加速量子商业化进程，但也可能导致市场碎片化。未来12-18个月，关注哪些区域能形成可持续的量子产业生态，而非仅仅依赖一次性拨款。

参考资料

[1] Industry Opportunities for Advancing Non-Military Drone Computing	[4] Google Cloud Put Dates on Its PQC Migration. Signatures Trail Confidentiality by a Year.
[2] Three Regional Quantum Finance Strategies Differ	[5] I Set Five Tests for Silicon Spin in March. One of Them Was Too Weak.
[3] Generation of coherent quantum light from a single impurity-bound exciton	[6] Six Teams Shipped the Same ZK Verifier Bug.

Quantum Doesn't Get a Patch.

- [7] Ph.D Positions in Post Quantum Cryptography, VIT vellore
- [8] DARPA Awards Contract to Qunnect to Advance Real-Time Polarization Compensation for Quantum Networks
- [9] T-SQUARED Begins Construction on Inflection's Quantum Innovation Centre in Oxford
- [10] University of Guelph and Xanadu Sign MOU to Advance Quantum Education and Talent Development
- [11] Xanadu and University of Alberta Partner to Accelerate Photodynamic Cancer Drug Discovery
- [12] BTQ Technologies Signs MOU with ITCENGLOBAL Subsidiary ITCEN PNS to Deploy Post-Quantum Security in South Korea
- [13] SDT Joins Canadian Non-Profit Open Quantum Design as Official Manufacturing Partner
- [14] New York State Launches \$60M RFP for Regional Quantum Technology Commercialization Hubs
- [15] WarpSpeed Says its AI cuts quantum encryption cracking cost sharply
- [16] Superconducting device develops continuous-variable quantum computing

- [17] Hamad Bin Khalifa University team sets bounds on quantum prediction
- [18] SEALSQ & Quobly Seal \$5 Million Post-Quantum Security Deal
- [19] Gemma models surpass 900 million downloads, Google says
- [20] Hilbert-Pólya Finds Missing Eigenstates in BBM Hamiltonian's Metric Completion
- [21] CO.LAB Q offers 12 months to build a quantum business in Chattanooga
- [22] Kagome metal's quantum effects yield strong heat-to-power at zero field
- [23] Quantum chip isolator cuts back-reflections by 30 decibels
- [24] Neuromorphic Labs builds a 'trust layer' for business AI
- [25] Globular cluster stream in distant galaxy offers new dark matter insights
- [26] Queen Mary University of London builds quantum modules like computer components
- [27] Measurement incompatibility in Bayesian multiparameter quantum estimation
- [28] Catalytic $\$z\$$ -rotations in constant $\$T\$$ -depth
- [29] Robust topological quantum state transfer with long-range interactions in Rydberg arrays
- [30] Efficient Graph State Generation in Linear Optics

- [31] Physicists find major clue to matter's biggest mystery
- [32] Rare Tropical Storm Lala on course for Hawaii, with hurricane conditions possible
- [33] Neuroscientists have vastly underestimated brain cells' computing power
- [34] Popular drug metformin transforms your gut into a sugar sink
- [35] Squishies are everywhere—but what are they made of?
- [36] Guest Post: Why Quantum Readiness Is Becoming a Venture Capital Question
- [37] Guest Post — Quantum Strategy Demands a New Operating Model: From Uncertainty to Readiness.
- [38] Kartik Srinivasan Appointed Editor-in-Chief of Optica Quantum
- [39] HAWK Lattice Signature Scheme Withdrawn from NIST Round 3 After AI-Assisted Key-Recovery Attack

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。