本 期 目 录

收录报道	39
信息来源	12
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

量子硬件 SOTA 对照表 →

2026 年 08 月 10 日 - 08 月 11 日 · 日报

Pasqal首次用光子集成电路囚禁中性原子

39 篇 · 12 个来源 | PDF | 本期汇总免费阅读

01 亮点

今日三件事

1 **Pasqal实现首个片上中性原子量子比特囚禁** 通过光子集成电路（PIC）替代自由空间光学，首次利用芯片上产生并导引的激光囚禁单个中性原子[10]——将中性原子量子计算从光学平台推向芯片级集成，但未披露门保真度。

2 **Intel宣布拟增发150亿美元普通股** 公司将其归因于客户对AI算力的强劲且可持续需求，以及物理AI、专用芯片、先进封装、外部晶圆等新兴领域的进展[5]——短期稀释现有股东权益，来源未提及量子部门或量子研发投入。

3 **Cloudflare获FedRAMP High认证，扩展量子安全政府平台** 将后量子密码学保护推向美国政府最

高安全级别数据[35]——加速量子安全加密在联邦机构的部署。

02 硬件

硬件前沿

中性原子

Pasqal首次通过光子集成电路囚禁中性原子量子比特

- 事实：Pasqal与其子公司Aeponyx合作，利用光子集成电路（PIC）产生的激光囚禁单个中性原子，替代了传统的自由空间光学平台[10]。
- 技术含义：这是中性原子量子计算首次实现片上囚禁，将大型光学平台微型化到固态芯片，有望大幅降低系统尺寸和复杂性。然而，该演示仅涉及囚禁，未报告任何门操作或保真度数据，距离实用化仍有显著差距；来源亦未给出与其他中性原子体系的保真度对照，片上囚禁是否影响门保真度仍是未知数。

— 格局影响：若该技术能扩展到门操作并保持保真度，可能改变中性原子量子计算机的工程化路径，降低制造成本和体积。短期内（1-2年）对产业格局影响有限，但长期可能威胁现有光学平台路线。

Q-CTRL在IBM硬件上运行100量子比特量子算法

— 事实：Q-CTRL在IBM量子硬件上执行了100量子比特的量子傅里叶变换（QFT），声称是迄今最大规模的QFT演示[15]。

— 技术含义：100量子比特的QFT演示展示了在含噪中等规模量子（NISQ）设备上运行实用算法的可能性，但QFT本身并非近期可带来量子优势的算法。来源仅称这是迄今规模最大的QFT演示，未披露算法执行的成功率或保真度，也未给出与其他硬件平台的对照数据。

— 格局影响：该成果强化了错误抑制软件在NISQ时代的价值，Q-CTRL作为量子软件公司，其技术可赋能多个硬件平台，可能吸引更多企业采用其错误缓解方案。

光子

Sizhen与中科大团队在硅基光子芯片上演示多量子比特量子态

— 事实：合肥Sizhen Chip Technology公司与中国科学技术大学量子信息重点实验室任希锋教授研究组联合报告了硅基光子芯片上的多量子比特光量子态[33]。

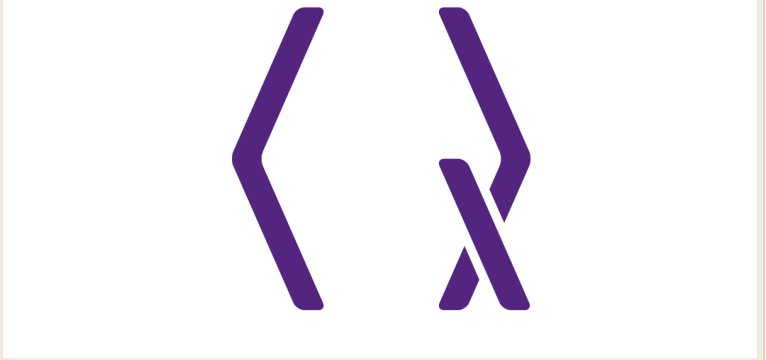
— 技术含义：光子量子计算在集成化方面取得进展，但报道未提供保真度或量子比特数量等具体指标，来源亦未给出可比的行业基线数据，该演示仍处早期阶段，距离实用化仍有很大差距。

— 格局影响：硅基光子技术是量子计算与经典半导体工艺结合的潜在路径，但该成果尚不足以影响全球竞争格局。

---

03 算法

算法与软件



Classiq提出空间搜索量子电路宽度对数增长

— 事实：Classiq提出基于离散时间量子行走的d维空间搜索量子电路，其宽度随网格大小对数增长；在所考察范围内，三维情况下的深度经验上服从某一依赖关系，来源未给出该关系的具体表达式[21]。

— 技术含义：该设计显著降低了空间搜索算法的电路宽度，使大规模搜索问题可能更早地在有限量子比特上实现。但深度的具体增长形式未披露，且未与现有经典算法进行性能对比。

- 格局影响：若该算法在近期量子硬件上验证有效，可能影响物流、路径优化等领域的量子应用开发，但时间尺度在3-5年以上。

Quantum期刊比较两种表面码晶格手术方法的量子资源

- 事实：发表于Quantum期刊的研究比较了两种领先的表面码晶格手术方法在哈密顿量模拟中的资源需求，提供了端到端资源估算[22]。
- 技术含义：该研究为容错量子计算的实际资源需求提供了定量对比框架。来源摘要止于对表面码编译假设（通过消除Clifford门实现电路串行化）的描述，两种方法在逻辑比特数与操作数上的具体差异未在摘要中给出，需查阅原文确认。
- 格局影响：对量子硬件开发者而言，该研究明确了不同纠错方案的资源开销，可能影响未来硬件架构设计，但短期内不会改变产业路线。

Szegedy量子行走的转移矩阵扰动谱范数为1/N

- 事实：一项分析证明，在完全图上移除单条边对Szegedy量子行走的转移矩阵扰动谱范数为1/N[16]。
- 技术含义：该结果量化了量子行走对图结构变化的鲁棒性，对基于量子行走的算法设计有理论指导意义。
- 格局影响：纯理论成果，短期无产业影响。

经典可模拟测量（CSM）的模拟成本上下界被推导

- 事实：一项研究推导了提升经典可模拟测量（CSM）鉴别能力所需模拟成本的下界和上界，并将该成本与魔法资源相关联[20]。
- 技术含义：该工作为量子优势的验证提供了更精细的理论工具，有助于界定量子计算超越经典模拟的边界。
- 格局影响：理论进展，可能影响未来量子优势实验的设计，但无直接商业影响。

---

04 产业

产业与生态

Intel宣布拟增发150亿美元普通股

- 事实：Intel宣布拟进行150亿美元普通股包销公开发行，尚未完成定价与交割；公司称客户持续释放强劲且可持续的需求信号，由AI算力的空前投资驱动，物理AI、专用芯片、先进封装和外部晶圆等新兴领域的进展亦是原因[5]。

— 商业含义：来源将增发归因于承接AI算力需求与新兴领域投资机会，全文未提及财务压力；大规模增发将稀释现有股东权益。

— 格局影响：来源未提及Intel的量子计算部门或硅自旋量子比特路线，本次拟增发对其量子研发投入的影响尚未披露。投资者可关注Intel后续披露的量子部门投入变化。

Cloudflare获FedRAMP High认证，扩展量子安全政府平台

— 事实：Cloudflare宣布其政府安全平台获得FedRAMP High授权，将后量子密码学保护能力扩展到美国联邦政府最高安全级别的工作负载[35]。

— 商业含义：FedRAMP High是服务美国政府最敏感数据的必要认证。需注意来源为公司新闻稿，仅说明Cloudflare for Government取得该授权；至于Cloudflare在量子安全云服务中的相对位次及所谓先发优势，来源未提供依据。

— 格局影响：联邦政府加速向后量子密码学迁移，将带动其他云服务商跟进，并刺激量子安全加密市场的增长。短期内（1-2年），Cloudflare的竞争对手如AWS、Azure可能加快类似认证。

美国立法者推动增加量子国防支出

— 事实：据报道，美国国会议员正推动在国防预算中增加量子技术支出，以应对与中国在量子领域的竞争[37]。

- 商业含义：增加的国防资金将直接流向量子计算、量子传感和量子通信的研发与采购，利好国防承包商和量子初创公司。
- 格局影响：量子技术的地缘政治竞争加剧，可能加速美国量子技术的军事应用，并促使盟国同步投资。投资者应关注国防相关量子合同的流向。

Infleqtion与Eaton合作推进量子计算用于美国电网韧性

- 事实：继此前报道后，本次通稿明确该合作为多年期、数百万美元规模的项目，Eaton选定Infleqtion支持相关研究，目标是利用量子计算增强美国电网韧性并减少停电的经济损失[2]。
- 商业含义：该合作是量子计算在能源领域的早期案例，但目前仍处研究支持阶段，来源未公布任何结果，量子优化在电网管理中的价值尚待验证。
- 格局影响：若项目成功，可能吸引更多公用事业公司投资量子解决方案，但实用化时间可能在5年以上。

Qunnect与Monarch Quantum合作商业化量子网络技术

- 事实：Qunnect和Monarch Quantum合作，利用先进制造技术加速纠缠量子网络硬件的商业化、小型化和规模化生产[7]。
- 商业含义：该合作结合了Qunnect的纠缠分发技术和Monarch Quantum的光子系统工程能力，旨在降低量子网络硬件成本。

- 格局影响：量子网络是量子互联网的基础，该合作可能推动量子安全通信网络的早期部署，但大规模商业化仍需多年。

Quantum Optics Jena的ELVIS QKD系统完成ISO/IEC 23837安全评估

- 事实：德国Quantum Optics Jena的ELVIS量子密钥分发（QKD）系统完成了ISO/IEC 23837标准的独立安全评估，由TÜVIT历时三个月测试实施[8]。
- 商业含义：完成国际标准下的独立安全评估是QKD产品进入政府和金融市场的关键门槛之一，ELVIS系统可能因此获得更多商业订单；来源未表述评估的通过或合格结论。
- 格局影响：QKD系统的标准化认证将加速其在关键基础设施中的应用，但QKD的市场规模仍受限于光纤距离和成本。

BTQ与ITRI验证QCIM核心芯片用于NIST后量子标准

- 事实：BTQ Technologies与台湾工研院（ITRI）完成了QCIM芯片的关键里程碑，该芯片采用28纳米工艺，支持NIST后量子密码学标准，测试芯片预计年底前交付客户[38]。
- 商业含义：QCIM芯片旨在保护数字系统免受量子计算机攻击，其硬件实现可能提供比纯软件方案更高的安全性和效率。

— 格局影响：随着NIST后量子标准的推广，硬件安全模块市场可能增长，BTQ与ITRI的合作瞄准了物联网和边缘设备的量子安全需求。

Infosim协调的量子域动态项目启动，FAU RRZE参与

— 事实：德国FAU的区域计算中心Erlangen参与Infosim协调的QDD项目，该项目获BMFTR 326万欧元资助，总预算384万欧元，旨在开发跨域自动化混合QKD和后量子密码学管理，直至2029年[39]。

— 商业含义：该项目探索QKD与后量子密码学的混合部署，为未来网络安全架构提供过渡方案。

— 格局影响：欧洲在量子通信基础设施上的持续投资，将强化其在该领域的领先地位，但项目周期较长，短期商业影响有限。

犹他州州长签署行政令启动全州量子计划

— 事实：犹他州州长Spencer Cox签署行政令，启动犹他量子计划，旨在将犹他州打造成量子研究、制造和商业化的区域中心[9]。

— 商业含义：州级量子计划可能吸引量子初创公司入驻，并带动当地就业和投资。

— 格局影响：美国各州量子竞赛加剧，但犹他州需与科罗拉多、马里兰等已建立量子生态的州竞争。

Quantum Computing Inc. Q2营收激增至560万美元，Fab 2启动

- 事实：Quantum Computing Inc. (QCi)公布2026年Q2财报，营收增至560万美元，并宣布通过收购NHanced启动Fab 2制造设施[11]。
- 商业含义：QCi营收增长加速，来源摘要未披露净利润或盈亏数据。Fab 2的启动可能提升其光子芯片制造能力，但需关注资本支出对现金流的影响。
- 格局影响：QCi作为集成光子量子计算公司，其制造能力的扩张可能加速光子路线的发展，但市场竞争激烈。

05 学术

学术前沿

Quasipolynomial Cryptanalysis of the McEliece Cryptosystem
(or: PIR Meets McEliece)

Ashrujit Ghoshal* Yuval Ishai† Aayush Jain‡ Nuozhou Sun§

August 7, 2026

Abstract

The McEliece code-based cryptosystem, utilizing binary Goppa codes, is the earliest public-key encryption scheme that is still considered post-quantum secure. We present a simple, classical quasipolynomial-time distinguisher for Goppa–McEliece in the asymptotic "Classic McEliece" regime: for code length n, extension degree $m = \Theta(\log n)$, Goppa degree $t = \Theta(n/\log n)$, and public-code dimension $k = \Theta(n)$, the algorithm runs in time $n^{\mathcal{O}(\log n)}$ and distinguishes the McEliece public key from the uniform distribution over $\mathbb{F}_2^{k \times n}$ with advantage $1 - o(1)$. The distinguisher is not merely asymptotic: it applies to all Classic McEliece parameter sets considered in the NIST process and yields improved (though not yet practical) concrete attack estimates.

Our distinguishing attack originated from a failed attempt to construct doubly efficient private information retrieval (PIR) protocols from algebraic locally decodable codes, and can be intuitively explained from the PIR perspective. We extend this provable algorithm to a heuristic $n^{\mathcal{O}(\log n)}$-time ciphertext-decryption attack that recovers the message from a noisy codeword.

*IIT Madras. Email: ashrujit@cse.iitm.ac.in
†Technion and AWS. Email: yuval.ishai@gmail.com
‡Carnegie Mellon University. Email: aayushja@andrew.cmu.edu
§Carnegie Mellon University. Email: nuozhous@andrew.cmu.edu

经典McEliece新区分器削弱通用解码优势，但并非破解

- 事实：一项新研究发现了经典McEliece密码系统的新区分器，其攻击成本低于通用解码，影响了所有NIST参数集的安全性论证[6]。
- 技术含义：该区分器并未破解McEliece，但动摇了之前认为结构攻击可忽略的定量论证，意味着McEliece的安全性边界需要重新评估。
- 格局影响：McEliece是NIST后量子密码学标准的候选方案之一，该发现可能影响其标准化进程和部署信心，但短期内不会导致实际攻击。

维也纳大学利用张量网络获得更清晰的光谱间隙界限

- 事实：维也纳大学的研究人员改进了Fannes、Nachtergaele和Werner的方法，利用张量网络获得了量子系统光谱间隙的更清晰界限[18]。
- 技术含义：该理论进展有助于更精确地描述量子多体系统的能隙，对量子相变和拓扑序的研究有重要意义。
- 格局影响：基础研究，短期无直接应用，但可能影响未来量子材料和量子模拟的发展。

耗散可作为纠缠工具

- 事实：据一份机构新闻稿，研究人员展示了如何利用耗散（通常被视为噪声）来产生纠缠[36]。
- 技术含义：该来源为新闻稿，未见期刊或同行评审信息；耗散工程制备纠缠本身已有多年研究积累，该工作在此基础上进一步表明，耗散在特定

条件下可作为量子信息处理的资源，而非仅是有害因素。

- 格局影响：长期来看，可能影响量子纠错和量子计算硬件的设计哲学，但短期内不会改变主流路线。

跟踪控制在理论上给出单氢原子的亚线性光学响应

- 事实：研究人员提出，在氢原子中可通过跟踪控制、由演化中的量子态自洽确定驱动场，从理论上构造出亚线性光学响应，即发射场随驱动场的分数次幂变化[17]。
- 技术含义：该工作超越了传统非线性光学的微扰层次，为极端非线性光学提供了新方法；来源描述为理论与数值方案，未见实验演示。
- 格局影响：纯基础研究，可能对未来量子光源和量子传感有潜在影响。

06 影响

今日影响

1. **Intel投资者**：拟发行的150亿美元普通股将稀释现有股东权益，短期股价可能承压；来源未涉及量子部门，后续投入变化需以公司披露为准[5]。
2. **量子安全产业**：Cloudflare的FedRAMP High认证可能引发连锁反应，推动AWS、Azure等加速量子安全认证，利好后量子密码学软件和硬件厂商[35]。
3. **中性原子量子计算路线**：Pasqal的片上囚禁若成功扩展到门操作，可能降低系统成本，但短期内不会改变QuEra和Atom Computing在逻辑量子比特数量上的领先地位[10]。
4. **国防量子技术投资**：美国立法者推动增加量子国防支出，可能使量子传感和量子通信相关企业优先受益，来源未点名具体公司[37]。
5. **后量子密码学标准化**：McEliece新区分器的发现可能影响其标准化进程与部署信心，但按来源说法并未构成破解[6]。

编辑点评

今日量子产业动态凸显了资本节奏与技术突破之间的张力。Intel的150亿美元拟增发对外给出的理由是承接AI算力需求与新兴领域投入，而非财务紧缩；但它提醒我们，大型科技公司的资本配置一旦重排，量子这类长线投入的优先级同样会被外界重新审视。与此同时，Pasqal的片上中性原子囚禁展示了量子硬件的工程化进步，但未触及保真度这一核心指标，产业界需警惕“演示通胀”——即用新颖性替代性能。在量子安全领域，Cloudflare的FedRAMP认证标志着后量子密码学从标准制定走向实际部署，政府市场的开启可能比预期更快。投资者应区分短期商业机会（如量子安全加密）与长期技术赌注（如容错量子计算），并密切关注国防资金流向，因地缘政治正成为量子技术加速的关键推手。

参考资料

[1] The A.I. Magic Show Is Ending - What Now?

[2] Infleqtion Selected by Eaton to Support Research Advancing Quantum Computing for U.S. Grid Resilience

[3] IQT Sunday Edition

[4] Intel Gamer Days 2026 Kicking Off with AAA Gaming Bundle & Partnerships

[5] Intel Announces Proposed $15 Billion Common Stock Offering

[6] A New Classic McEliece Distinguisher Undercuts Generic Decoding. It Is Not a Break.

[7] Qunnect and Monarch Quantum Partner for Commercializing and Deploying Quantum Networking Technologies Using Advanced Manufacturing

[8] Quantum Optics Jena’s ELVIS System Completes First ISO/

IEC 23837 Hardware Security Evaluation

[9] Utah Governor Spencer Cox Signs Executive Order Launching Statewide Quantum Initiative

[10] Pasqal Achieves First On-Chip Neutral-Atom Qubit Trapping via Photonic Integrated Circuits

[11] Quantum Computing Inc. Reports Q2 2026 Financial Results: Revenue Surges to $5.6M and Fab 2 Launch via NHanced Acquisition

[12] Interacting collaborators reveal noninteracting fermions

[13] York team tested quantum keys on the SPOQC mission

[14] Lithuania Quantum Computing Companies, The Complete Vendor Guide

[15] Q-CTRL runs 100-qubit quantum algorithm on IBM hardware

[16] Szegedy Walk's Transition Matrix Perturbation Has Spectral Norm 1/N

[17] Tracking Control Enables Sublinear Optics in Single Hydrogen Atom

[18] University of Vienna Achieves Clearer Gap Bounds via Tensor Networks

[19] Spain Quantum Computing Companies, The Complete Vendor Guide

[20] How Lower, Upper Bounds Define CSM Discrimination Simulation Costs

[21] Classiq Shows Quantum Circuit Width Grows Logarithmically for Spatial Search

[22] Quantum Resource Comparison for Two Leading Surface Code Lattice Surgery Approaches

[23] Scientists are using AI to design new viruses. Should they be?

[24] Trump issues executive order aimed at rewriting childhood vaccine schedule

[25] Colombia rocked by 7.4 magnitude earthquake—its largest in the past decade

[26] Can dogs read your facial expressions? It depends on your mood

[27] Cyclosporiasis-linked Taylor Farms recalls jalapeños tied to Salmonella outbreak

[28] World ocean temperatures hit extreme new record for July

[29] How the 'happy ending problem' launched a new branch of math—and a romance

[30] Sperm with DNA damage might be the true cause of repeated miscarriages

[31] Can 'magic mushrooms' help treat cocaine dependence?

[32] SpaceX rocket crashes into the moon as cyberattacks hit U.S. water systems

[33] Sizhen Chip Demonstrates Multi-Qubit Photonic Quantum States on Silicon Chip

[34] The Quantum Kid: Peter Shor, Steven Chu & John Preskill Explain Quantum – So You Can Finally Understand It

[35] Cloudflare Expands Quantum-Safe Government Security Platform With FedRAMP High Authorization

[36] Dissipation Can Be a Tool For Entanglement

[37] U.S. Lawmakers Reportedly Pushing Higher Defense Spending on Quantum as China Race Intensifies

[38] BTQ and ITRI Validate QCIM Core for NIST Standards

[39] FAU RRZE and Partners Launch Quantum Domain Dynamics Project for Cross-Domain Quantum Encryption