

谷歌估计最少1200个逻辑比特可攻破比特币

23 篇 · 7 个来源 | [PDF](#) | 本期汇总免费阅读

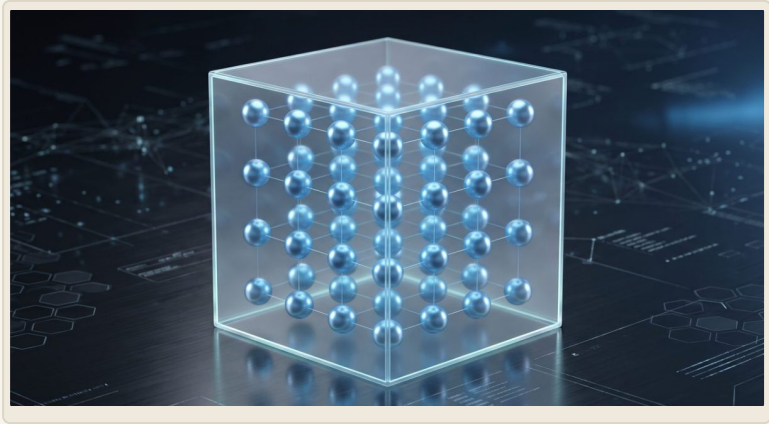
本期目录

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	23
信息来源	7
阅读时长	约 10 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



- 量子纠错编译提速42倍** ONEX框架将量子纠错时钟速率最高提升至现有方法的42.1倍，在超过2000比特模拟中验证^[13]——纠错编译任务被重构为一维问题，并在实用时间尺度内求解。
- SEALSQ量子安全商业史** SEALSQ Corp（纳斯达克：LAES）是少数完全围绕量子计算机威胁构建业务的上市公司^[19]——可作为观察量子安全市场早期形态的样本。
- 芝加哥大学整数规划拓扑解码器** 基于整数线性规划的解码器在多个拓扑码模型中超越多种现有方法^[17]——量子纠错解码从启发式走向全局最优。

硬件前沿



离子阱量子模拟

研究者从临界点出发进行量子淬火，在离子阱量子模拟器中验证了理论预言^[1]。该论文包含临界点淬火的理论与离子阱量子模拟器上的实验验证，来源仅给出标题与DOI，更多细节未披露。离子阱路线在量子模拟领域保持高保真优势，但距通用容错计算仍需解决比特数扩展瓶颈。

玻色量子态制备

利用宇称测量制备压缩态、猫态和GKP态的新方案^[2]。该方案以宇称测量这一工具制备上述三类玻色量子态，来源未披露更多技术细节，为连续变量量子纠错提供可能路径。光子与超导路线均可受益，但方案对测量保真度要求极高，离实用化尚有距离。

自由空间量子网络

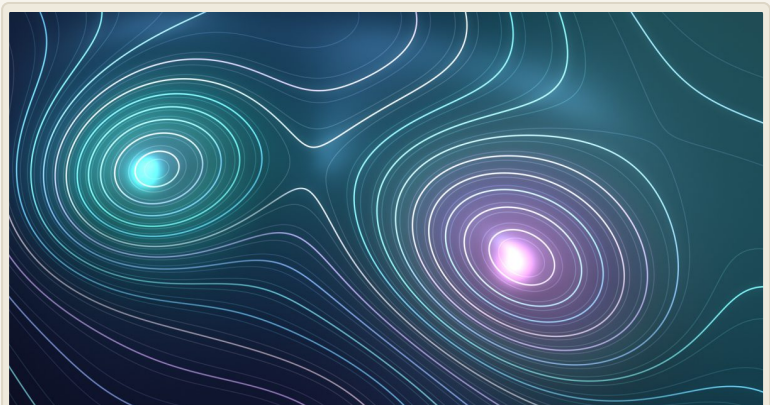
布鲁克海文国家实验室与石溪大学演示美国首个永久性自由空间光量子链路，跨度13英里^[4]。来源称布鲁克海文、石溪与耶鲁三家机构的设施共同构成该自由空间光链路，具体链路拓扑与13英里跨度的对应关系未披露。自由空间量子网络可绕过光纤损耗限制，但大气湍流与天气影响是长期挑战。

光声相互作用增强

冻结光纤液芯使光与声相互作用强度提升超过1000倍，并用于制造光声存储器^[20]。该结果比普通光纤中光声耦合强三个数量级，为低能耗光子计算和量子接口提供新平台。技术尚处实验室阶段，集成度与稳定性待验证。

03 算法

算法与软件



量子纠错编译提速

ONEX框架将量子纠错编译任务重构为一维问题，时钟速率最高提升至现有方法的42.1倍，并在超过

2000比特系统上模拟验证^[13]。该框架将复杂编译任务化简为可在实用时间尺度内求解的一维问题，来源指向qLDPC码与中性原子平台，直接缓解该路线在扩展中的软件瓶颈。若经独立验证，将加速大规模量子纠错部署。

拓扑解码器整数规划

芝加哥大学团队开发基于整数线性规划的拓扑码解码器，在多个测试模型上超越多种现有方法^[17]。该解码器利用任意子编码的全局约束，但需将纠错表述为含大量约束与变量的整数规划问题，可扩展性可能受限。需注意此处的任意子与拓扑码指纠错码中的激发，与拓扑量子比特硬件路线并非同一概念。

噪声诱导均衡提升学习精度

研究显示噪声诱导均衡可提高量子学习模型精度，涉及巴塞尔大学与帕维亚大学团队^[6]。该工作考察了噪声在量子学习中的正面效应，为NISQ时代算法设计提供新视角。短期可提升变分量子算法表现，长期需与纠错结合。

量子动力学增强图学习

QDAger Transformer网络利用时间分辨量子信号注入注意力机制，在多个图学习任务上优于传统方法^[10]。该模型利用量子演化模拟数据，相比现有方法展现更强的归纳偏置，消融实验证实改进源于动力学信息而非单纯算力增加。为量子机器学习与经典图神经网络的结合开辟新路径。

实时数据模拟虚时演化

Dakota团队提出的新方法从实时演化的标准测量数据推导虚时演化，无需额外量子比特^[11]。该方案建立了实时与虚时动力学之间的通路，简化了量子态制备流程。对量子化学与优化问题有实用价值，但测量开销与精度需进一步验证。

仿真误差转化为资源

策略训练的量子模拟可泛化到全新初始条件，并扩展到训练时十倍大的系统^[12]。该工作首次将仿真近似误差作为可纠正资源，而非不可消除缺陷。为长时间量子模拟提供新思路，但泛化边界与误差模型仍需理论支撑。

块编码降低T门数

新方法通过块编码减少么正操作的T门数，但要求误差容限随系统规模增大而提高^[14]。该技术首次在特定条件下实现T门数压缩，但适用性受限于误差要求，复杂计算场景下可能失效。对容错量子计算资源优化有参考价值。

监测电路模拟二维量子态

科学家利用监测电路模拟二维量子态，与DMRG方法在J1-J2模型上定性一致^[16]。该工作目前属概念验证，受有限键维制约，定量精度仍不足。为量子计算机模拟强关联材料提供替代路径。

WHO'S NEWS Strategic Appointments in Quantum Tech

人事变动

D-Wave任命Kevan P. Krysler为董事会及审计委员会成员，Krysler现任Carbon Robotics首席财务官^[3]。此人拥有超过二十年财务领导经验，曾担任Everpure首席财务官等职。D-Wave强化财务治理，或为后续商业化与资本运作铺路。

比特币量子攻击时间线

谷歌量子AI团队新估计显示，量子计算机最少1200个逻辑比特即可攻破比特币密码学^[7]。该数字显著低于此前估计，将量子威胁时间线大幅提前。比特币及加密货币生态面临安全升级压力，后量子密码迁移需求紧迫。

量子安全纯标的

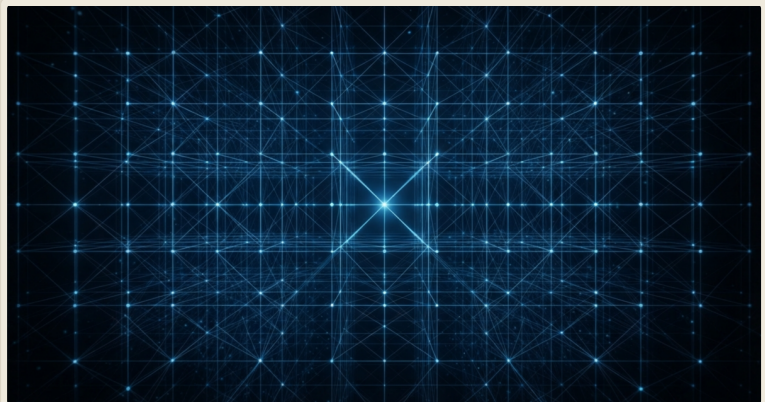
SEALSQ Corp（纳斯达克：LAES）是少数完全围绕量子计算机威胁构建业务的上市公司^[19]。其商业历史揭示量子安全市场的早期形态与演进逻辑。投资者可将其作为量子安全板块的观察样本。

量子意识倡导

EDHEC量子研究所Lionel Martellini提出，商业领袖需要量子意识而非量子洗白^[23]。该观点强调区分真实量子能力与营销话术，对产业健康发展有警示意义。企业量子战略制定需建立技术评估框架。

05 学术

学术前沿



量子淬火理论验证

npj Quantum Information发表论文，从临界点出发的量子淬火理论与离子阱实验验证^[1]。来源仅提供论文标题与DOI，实验的定量结论未披露，为量子多体物理提供可参照的研究方向。

宇称测量制备玻色态

npj Quantum Information发表利用宇称测量制备压缩态、猫态和GKP态的方案^[2]。该理论方案以宇称测量制备三类玻色量子态，为连续变量量子计算提供新工具。

量子学习噪声效应

Quantum Science and Technology发表噪声诱导均衡研究，涉及巴塞尔大学与帕维亚大学团队^[6]。该论文考察噪声诱导均衡对量子学习模型精度的影响，为算法设计提供新视角。

量子理论普适性

牛津团队证实量子理论的普适性质，基于动力学演化的一致性约束^[9]。该工作延续海森堡电磁场量子化思路，从代数一致性角度排除经典与量子混合描述。对量子基础研究有理论意义。

高纠缠GHZ态模拟

西北大学等机构利用Bethe-Heitler过程模拟超过900个高度纠缠的GHZ态^[15]。该工作首次在模拟中展示简单相互作用产生复杂纠缠的潜力，为量子信息编码提供新思路。

今日影响



- 1 比特币安全时间线收紧：**谷歌新估计将量子攻击所需逻辑比特降至最少1200个，加密货币社区需加速后量子密码迁移，相关标准与硬件部署可能提前^[7]。
- 2 量子纠错软件栈成熟：**ONEX框架最高42.1倍提速使千比特级纠错编译进入实用时间尺度，qLDPC码与中性原子平台的大规模纠错实验将受益，可能加速逻辑比特演示^[13]。
- 3 拓扑解码器新路径：**整数规划解码器在多个模型上超越多种现有方法，若在真实硬件上验证，将提升拓扑纠错码的解码效率，对相关纠错方案有直接意义^[17]。
- 4 自由空间量子网络落地：**美国首个永久性自由空间量子链路建立，为跨城市量子通信提供新选项，但需解决天气与稳定性问题^[4]。
- 5 量子安全投资标的清晰化：**SEALSQ等纯量子安全公司的商业历史为观察该市场早期形态提供样本，来源未涉及估值或投资价值判断，量子安全市场教育加速^[19]。

编辑点评

本期最值得关注的是谷歌对量子攻击比特币所需逻辑比特数的新估计：最少1200个逻辑比特。来源称这意味着量子攻击比此前认为的更近，量子威胁不再是遥远未来。然而，必须清醒：来源并未给出当前量子计算机的逻辑比特规模与错误率对照，1200这一门槛距现有演示还有多远，仍需公开数据支撑。数量增长之外，错误率的下降同样是前提。市场可能高估短期风险，但低估长期确定性。

另一个趋势是量子纠错软件栈的快速成熟。ONEX框架42倍提速、整数规划解码器、噪声诱导均衡等进展，表明软件优化正在成为硬件之外的第二条扩展路径。在物理比特保真度提升趋缓的背景下，编译与解码效率的提升可能带来数量级的实际收益。投资者应关注那些能同时优化硬件与软件的公司。

参考资料

[1] Quantum quenches from the critical point: theory and experimental validation in a trapped-ion quantum simulator	[3] Who's News: Strategic Appointments at D-Wave, BTQ Technologies, Symmetrics, and Rigetti Computing
[2] Preparing squeezed, cat and GKP states with parity measurements	[4] Brookhaven Lab and Stony Brook Demonstrate First US Free-Space Quantum Network Link Across 13 Miles
	[5] Six channels of data with quantum OAM comb set new record

- [6] Noise-induced equalization improves quantum learning accuracy
- [7] New estimates From Google Quantum AI show quantum attack on Bitcoin is closer than thought
- [8] Eth Zürich Team Detects Atom Impacts with 96% Certainty
- [9] Oxford Team Confirms Quantum Theory's Universal Nature
- [10] Researchers Boost Graph Learning with Quantum Dynamics
- [11] Dakota Team Simulates Imaginary Time Using Real-Time Data
- [12] Researchers Harness Simulation Errors for Improved Accuracy
- [13] Researchers Speed Quantum Error Correction by up to 42 Times
- [14] Researchers Cut T-Count for Unitaries Using Block Encoding
- [15] Researchers Simulate over 900 Highly Entangled GHz States
- [16] Researchers Simulate 2D Quantum States Using Monitored Circuits
- [17] Chicago Team Builds Integer Programming Topological Decoder
- [18] Technical Munich Team Enables 86% More Quantum Benchmarks on Small Chips
- [19] SEALSQ Corp (LAES): A Complete Commercial History
- [20] This frozen fiber makes light and sound interact 1,000x more strongly
- [21] Why trauma changes how our memory engages with our conscious experience
- [22] Anthropic's LLM watermarking
- [23] Lionel Martellini (EDHEC Quantum Institute): Why business leaders need quantum awareness, not quantum washing

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。