2026 年 10 月 27 日 – 10 月 28 日 · 日报

抗量子无证书协议守卫个人加密钱包

47 篇 · 15 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

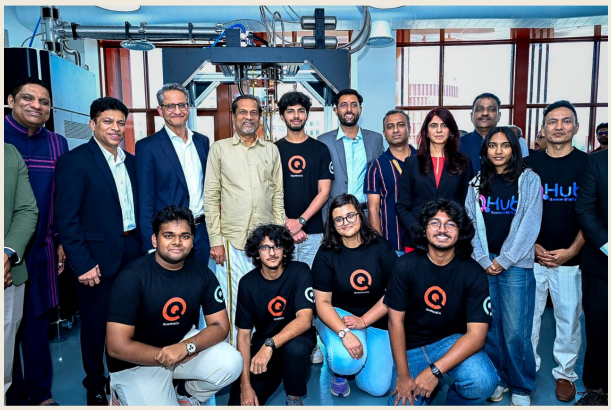
收录报道	47
信息来源	15
阅读时长	约 18 分钟

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 **超导单比特门速刷新至6.8纳秒** 德国于利希研究中心、亚琛工业大学与科隆大学团队在超导比特上实现6.8纳秒门操作，保真度（操作精确度量）超99.98%[6]——压减耗时数倍且跨过纠错阈值，加速高频超导硬件落地。

2 **量子测控软件商获1200万欧元A2轮融资** 欧洲量子测控自动化软件商QuantrolOx完成1200万欧元融资使总融资达2800万欧元[11]——资本向自动化校准层聚集，降低整机厂商调优与运维成本。

3 **量子龙头携手能源巨头攻关高温超导机理** 离子阱龙头Quantinuum与通用电气旗下GE Vernova联手利用量子算力攻坚高温超导机制[23]——破

解材料仿真瓶颈，缩短新型低损耗输电设备研发周期。

02 硬件

硬件前沿



超导路线

德国于利希研究中心、亚琛工业大学与科隆大学联合团队在超导量子比特（超导电路构成的比特）上完成运行耗时仅6.8纳秒（十亿分之一秒）的单比特逻辑门操作，操作保真度（操作精确度量）测得99.98%以上[6]。技术含义上，该速度将超导单比特常规操作耗时（通常在15至30纳秒区间）缩减了一半以上，单比特保真度微幅超越当前云端生产级系统99.95%的基线指标（如IBM Heron r2与Google Willow）；但在完整硬件对标中，该成果尚未覆盖双比特逻辑门，距离超导双比特门主流20至100纳秒时延及两能级系统（TLS，材料微观缺陷能量损耗）波动压制仍有显著工程距离[6]。格局影响上，极短门时为欧洲超导硬件团队探索高时钟频率控制

提供了微波整形范式，将在未来两至三年内推动高频脉冲发生设备的演进[6]。

新型宽间距超导微带单光子探测器在多光子计数测试中实现99.6%的分辨保真度，成功分辨多达8个不同到达时刻的光子，并在第7与第8个光子电信号间测出2.15的峰值分离度[31]。技术含义上，该器件消除了传统单光子探测器仅能区分少量并发光子的饱和失真瓶颈，使时间分辨通道数拓展至8个[31]。格局影响上，高保真多光子探测模块将在未来一年内直接赋能光量子计算纠缠态校验与高通量光纤通信节点[31]。

量子微波脉冲优化算法Q-PRONTO在超导体系测试中实现6.6×10⁻⁴的单比特门误差率（即保真度约99.934%），优化收敛速度呈现二次方收敛特性[32]。技术含义上，相较传统优化工具接近线性的收敛曲线，该方法以更少迭代步数生成控制波形，但单比特误差率相较生产级头部器件99.95%的基线仍略有差距[32]。格局影响上，该方案降低了底层微波标定的计算资源消耗，利好整机厂商缩短多比特芯片开机校准周期[32]。

离子阱路线

德国团队研制出包含31个物理比特（未纠错底层硬件单元）的离子阱（电磁场束缚离子技术）处理器LYNX，在15个物理比特规模上测得量子体积（QV，整机综合性能指标）达到2¹⁵（32768），对应平均双比特门误差率为2.84×10⁻³（保真度约99.716%）[27]。技术含义上，对照离子阱领域公开最优基线，Quantinuum Helios在98比特全连接下

全部比特对的双比特门保真度达到99.921%（误差约7.9×10^{-4}），且量子体积达到2^{25}（约3355万）；LYNX的双比特门误差率约为Helios的3.6倍，量子体积落后十个二进制数量级，反映出其多离子协同穿梭控制与串扰抑制仍需跨过高密度光电集成门槛[27]。格局影响上，该芯片为欧洲本土离子阱硬件提供了中等规模自主样机，但进入全球商业算力第一梯队仍需两到三年迭代[27]。

固态自旋与新型能级体系

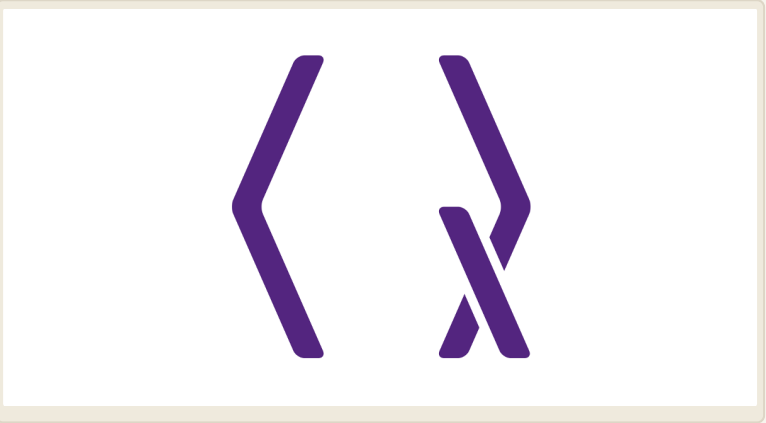
开源测控架构SpinQICK基于射频片上系统实现对全连接量子点（半导体自旋编码单元）的相干控制，仅凭单一振荡参数Nosc=35即可从量子点输运特性中直接反演电压噪声分布[25]。技术含义上，该成果消除了依赖昂贵离散仪器的高成本瓶颈；对比自旋路线在晶圆量产抽测中逾99%的双比特门SOTA水平，低成本测控系统是推动自旋比特突破十比特规模、缓解操作数受限的关键工具[25]。格局影响上，中小科研机构与初创团队研发门槛实质性降低，将加速硅基自旋阵列在未来两年内的实验室验证节奏[25]。

美国罗切斯特大学物理系研究团队推进高维量子比特（Qudit，多能级量子信息单元）实验，通过操控三能级及以上量子态实现信息高密度编码[45]。技术含义上，单节点多能级架构摆脱了传统二进制双能级限制，在相同物理节点下提供更大希尔伯特空间，理论上可将纠错编码所需的物理芯片空间占用减少三分之一以上[45]。格局影响上，高维体系为超导和半导体整机拓宽了拓扑压缩新路径，将在中远期重构特定编译架构的标准规范[45]。

实验人员利用金刚石样品内部的氮-空位色心（固态金刚石缺陷自旋）电子自旋力，成功推动微纳宏观物体移动达1.5微米（百万分之一米）[9]。技术含义上，首次在物理上验证了微观电子自旋量子态对宏观微机械结构的直接机械驱动，跨越了微观自旋相干态与宏观力学位移的耦合分界[9]。格局影响上，为超灵敏量子力学传感器及微机电系统芯片集成提供了全新驱动机制[9]。

03 算法

算法与软件



科研团队提出名为Quantum Cadence的新型抗量子区块链共识协议，取消了传统两百个节点网络依赖汇总广播数字签名的证书体系，改为由各节点直接独立统计接收报文的投票权重[21]。技术含义上，该成果提出无数字签名的抗量子共识机制，有望规避未来量子计算针对椭圆曲线与公钥聚合证书的破译漏洞，同时维持了分布式账本的处理性能[21]。格局影响上，直击当前高度依赖聚合签名的主流公链与金融机构结算底层，为下一代防篡改账本架构提供了免迁移证书的替代路径[21]。

Optqc理论团队在15.6分贝光场压缩度与两级编码条件下完成连续变量仿真，测算得到单侧量子纠错（QEC，利用冗余消除物理噪声）误差低于10^{-5}阈值，并首次确立了有限级逻辑贝尔误差序[19]。技术含义上，该推演证明在光学连续变量体系下更复杂操作展现出相对更低的逻辑错误率，将理论容错边界推进至前所未有的精度；但硬件落地仍受限于物理光路，当前真实光芯片在15分贝以上高压缩态下的损耗预算仍难达到容错要求[19]。格局影响上，为连续变量光量子初创公司确立了新的架构设计目标，规范了容错模拟的技术基准[19]。

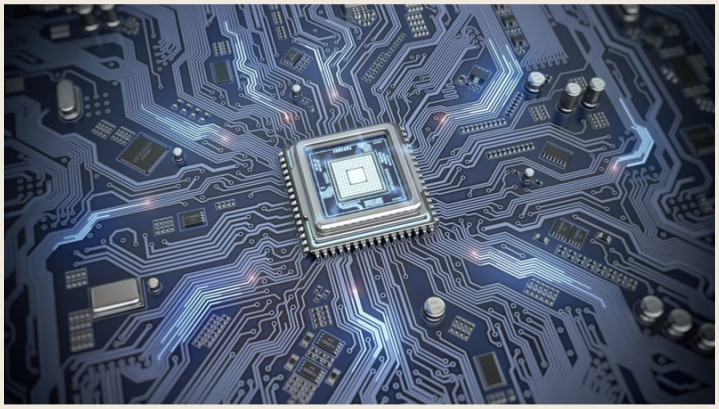
针对五比特量子纠错系统的实验测试中，研究人员采用缺陷排除机制将每轮循环逻辑错误率从1.9%降低至0.x%区间，并实现了93%保真度的逻辑比特纠缠[26]。技术含义上，该方案通过在小尺度拓扑中主动剔除物理坏点，验证了浅层电路无损抑制逻辑翻转的可行性[26]。格局影响上，为当前近近期中等规模容错处理器的表面码（二维拓扑纠错码）布局提供了更具弹性的排障策略[26]。

全经典优化计算协议实现对64量子比特参数化电路损失函数的完整经典训练，突破了传统状态向量在30比特附近的经典模拟上限，并将优化后的模型成功部署至IBM旗下ibm_berlin超导处理器上执行[29]。技术含义上，该算法解决了深层变分量子线路由于维度爆炸引发的经典不可解难题，将经典预训练支持的比特数翻了一倍以上[29]。格局影响上，化工材料与金融组合优化算法在真实量子芯片上的试跑成本显著降低，缩短了混合算力方案的验证周期[29]。

超导量子电路哈密顿量（系统总能量算符）梯度优化通用框架在学术期刊《Quantum》上刊出，为新型量子比特结构发现提供自动化推导工具[16]。技术含义上，该框架通过解析梯度代替传统人工穷举与网格扫描，使定制化非谐振子超导电路的物理参数设计周期从数月压缩至数天[16]。格局影响上，推动半导体电子设计自动化工具向量子专用芯片领域深度延伸，加速设计到流片的工艺闭环[16]。

04 产业

产业与生态



欧洲量子测控自动化软件商QuantrolOx完成1200万欧元（约合1336万美元）A2轮融资，使累计外部股权融资总额增至约2800万欧元[11]。商业含义上，随着百比特规模芯片成为主流，传统人工微调脉冲无法应对数十个控制通道的动态漂移，测控校准软件正从辅助脚本转变为整机制造的必选基础设施，推动测控细分层估值倍数走高[11]。格局影响上，融资将专项用于拓展北美商业交付与运维，对主打自研内部校准工具的整机硬件厂商形成专业化分工冲击[11]。

美国国家标准与技术研究院（NIST）正式敲定后量子密码（抗量子攻击公钥算法）迁移实施路线图，对各级政府机构的高价值资产与关键系统重申了2030年全面替换的法定截止期限[5]。商业含义上，合规要求从政策倡议升级为带有明确时间约束的预算采购指令，加密算法敏捷化改造与数字证书替换进入刚性兑现期[5]。格局影响上，全球金融结算网络、跨国云厂商与跨国安全集成商必须在未来四年内完成核心加密接口重构，催生数十亿美元的存量改造市场[5]。

离子阱整机制造商IonQ获得美国空军研究实验室（AFRL）下拨的750万美元第二阶段资金支持，用于扩建纽约州罗马市的量子网络试验场[13]。商业含义上，该阶段核心攻坚光纤与自由空间开空链路的混合组网，通过引入频率转换（将离子发光波长转至通信波段）解决跨节点波长不匹配与长距光损难题[13]。格局影响上，巩固了IonQ在美国国防分布式算力网络中的承建方地位，推动量子通信从单一实验室光纤环路走向多环境实战互通[13]。

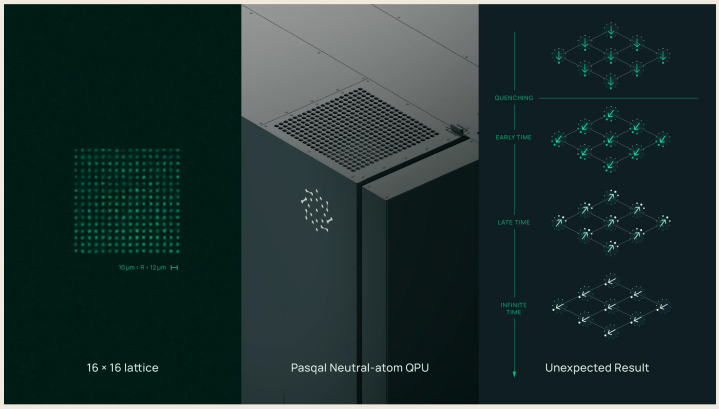
继近日报道IDEMIA与韩国电信（KT）参与国家级后量子试点后，双方正式将兼容NIST国际标准与韩国本土KpqC算法的双标准抗量子SIM卡部署至韩国军用通信网络[14]。商业含义上，标志着移动终端硬件芯片层面的抗量子改造完成实网打通，验证了多算法在轻量级安全载体上的热切换能力[14]。格局影响上，成为全球首个将双轨后量子算法部署于军工移动网络的成熟案例，预计将对亚太及北约防务通信终端规范产生示范效应[14]。

量子计算全栈厂商Quantinuum与通用电气旗下能源技术公司GE Vernova先进研究中心达成商业合作，联手运用离子阱算力解析高温超导微观机理[23]。商业含义上，双方合作绕过经典超算模拟强关联电子体系的指数级阻碍，直接瞄准发电机减重、海上风电传输及零电阻电网材料的微观机理[23]。格局影响上，验证了高保真度量子计算在万亿级重工业与能源电力核心材料研发中的切入价值，预计三至五年内产出新型超导合金设计指标[23]。

全球量子情报机构（GQI）发布2026年第三季度产业监测，显示量子领域一级市场资本加速向具备全栈交付能力的头部主体集中，硬件路线向具备容错能力的第二代架构加速换轨，同时后量子合规要求倒逼政企迁移周期大幅压缩[12]。商业含义上，单纯依赖无纠错物理比特数估值的商业逻辑被挤出，腰部纯硬件初创企业的融资窗口加速关闭[12]。格局影响上，缺乏清晰逻辑纠错路线图的团队面临并购整合或清算，全栈龙头通过标准锁定进一步抬高行业竞争壁垒[12]。

安全芯片与模块方案商SEALSQ宣布计划收购12颗WISeSat.Space低轨卫星的卫星信道容量及配套地面测控服务，用于推进量子空间轨道安全云（QSOC）建设[22]。商业含义上，将端到端防篡改硬件根拓展至近地轨道资产，实现天基节点至地面终端的安全链接[22]。格局影响上，加速低轨天基专网抗量子加密协议的商业化，直接竞争传统地面物理专线安全市场[22]。

学术前沿



物理学家在混合硬件架构上完成费米子（构成物质的基本粒子）共振散射动力学模拟，测得的粒子衰变率与理论预测偏差压减至数个百分点之内[20]。技术含义上，实验将费米子物质编码于离散量子比特、标量场物理量编码于连续变量模态（Qumode），首次在真实物理体系上演示了强相互作用实时散射过程，避开了经典数值计算在符号问题上的维度崩溃[20]。格局影响上，为高能核物理与粒子对撞实验提供了非微扰实时演化模拟工具，开辟了基础物理计算新分支[20]。

研究团队利用一台256量子比特处理器观测二维量子磁体非平衡态弛豫动态，测得的自旋关联演化行为超出了经典张量网络（经典多体模拟算法）的有效算力边界[30]。技术含义上，在无纠错的物理比特阵列上，借助长程相互作用高精度操控直接测出经典算法无法收敛的宏观纠缠扩散数据，构成针对特定多体物理演化问题的确定性算力优越性证据[30]。格局影响上，确立了百比特级模拟机在强关联凝聚态物理中的不可替代性，为新型磁性材料研发提供了实验算力支撑[30]。

空间工程与量子计算交叉团队将高斯玻色采样（光量子专用采样算法）与进化算法结合，成功在多达25个空间轨道碎片的目标池中完成主动清除路径的协同规划[33]。技术含义上，该方案将高维非凸NP难组合优化问题拆解为两阶段混合管线，展示了光量子专用采样硬件在航天调度上的加速潜力[33]。格局影响上，打破了光子采样硬件仅限于分子振动谱计算的应用局限，向大型商业航天运营体系渗透[33]。

理论学者在《Quantum》期刊发表严格数学证明，正式确立了高斯玻色采样中的隐藏猜想[17]。技术含义上，该证明补齐了光量子采样复杂度下界推导中的核心链条，确立了经典算法无法在多项式时间内有效模拟该采样过程的数学完备性[17]。格局影响上，终结了学术界关于经典张量网络能否有效击穿光量子优越性的争论，强化了光量子专用计算的技术可信度[17]。

科研人员在《Quantum》期刊提出首个系统性推导制备-变换-测量场景下上下文性（量子非经典关联的本质特征）见证者的方法，运用线性量词消去法精确解析出经典局域多胞体边界[15]。技术含义上，该方法摆脱了对特定对称测量与纯态制备的理论假设，为检验微观系统的真实量子性提供了普适代数判定判据[15]。格局影响上，为无设备依赖的保密通信自检验协议提供了更严密的测试标准[15]。

06 影响

今日影响



1. **公链验证节点与加密钱包生态**[21]：传统基于数字签名的链上共识面临潜在破解风险，Quantum Cadence展示了无需聚合签名的无证书抗量子投票架构。链上治理与共识协议的攻击面发生质变，下一步紧盯该类无签名协议在以太坊等主流开源测试网中的吞吐压测与拜占庭容错验证。

2. **企业级网络安全与国防通信采购方 [5, 14]**：NIST将联邦系统后量子替换的最终法定截止期限焊死在2030年，而韩国军方已率先生态化落地双算法抗量子SIM卡实体硬件。密码迁移从战略评估期全面转入预算执行期，下一步紧盯全球系统集成商在身份凭证与核心交换机芯片层面的兼容改造订单。

3. **超导整机硬件与测控软硬件厂商 [6, 11, 32]**：于利希将单比特门时压缩至6.8纳秒，结合QuantrolOx的1200万欧元融资，表明超导路线正从单纯比拼物理比特总数转向单周期高时钟频率与测控自动化的工程效率战。系统装配调试门槛与微波延迟成为核心分水岭，下一步紧盯数十

比特阵列中超快单双门协同并行下的串扰抑制表现。

4 **重工业与清洁能源研发机构**[23]：GE Vernova与Quantinuum结盟攻关高温超导，标志着量子硬件算力正式向强关联材料微观机理的万亿级工业场景发起冲击。传统依靠经验试错的材料工程面临模拟范式转变，下一步紧盯离子阱全连接处理器在铜氧化物超导晶格哈密顿量基态求解上的实验数据披露。

07 编辑

编辑点评

当前量子计算产业正经历两股力量的深度交汇：一端是物理层工程精度的极限突进与测控工业化，另一端则是来自密码合规死线的外部强力倒逼。从微观门控耗时被压入个位数纳秒，到测控自动化工具链斩获千万欧元级资本注入，无一不在表明硬件路线竞争已经跨越了单纯堆砌物理比特数量的展示期，迈入了考验时钟频率、纠错解码吞吐与工业级调优效率的系统工程期。资本向具备第二代架构与自动化能力的头部标的聚拢，印证了市场对单纯概念炒作的脱敏与对商业闭环路径的苛求。

与此同时，随着标准化机构将全球敏感通信与关键设施的后量子迁移锚定在2030年，抗量子安全防御正在从理论方案演进为军政网络与金融终端中的实体芯片和协议革新。对于身处这一周期的从业者与资本方而言，衡量整机价值的标尺已彻底转向双比

特门保真度能否跨过容错门槛、逻辑比特纠错能否带来净增益，以及应用侧能否真正切入高温超导或高密度密码迁移等经典算力完全束手无策的真实场景。凡不能在时钟周期与纠错效率上形成正反馈的架构，将在接下来的标准化与工业化洗牌中迅速失去生存空间。

参考资料

[1] New Brief: How Industry Can Build More Trustworthy Software with AI

[2] Momentum builds for world-leading neutrino experiment hosted by Fermilab

[3] IQT The Quantum Dragon Podcast Episode 91 – Let’s Drink Coffee

[4] IonQ | Leading with Proof: IonQ’s Blueprint for Quantum-Safe Enterprise Security

[5] NIST Finalizes Post-Quantum Road Map as Agencies Face 2030 Deadlines

[6] Quantum gates set speed record at 6.8 nanoseconds with over 99.98% accuracy

[7] Quantum sensor loop design could improve magnetic measurements for medicine and communications

[8] New converter could bridge light wavelength gap in quantum communications

[9] Electron spin force moves a macroscopic object

[10] PhD Position in Theoretical Physics – Dipolar Quantum Gases

[11] QuantrolOx Raises €12 Million ($13.36 Million USD) Series A2 to Scale Automated Quantum Control Software and U.S. Operations

[12] GQI Q3 2026 State of Play: Investment Consolidation, Accelerating Q-Day Horizons, and the Shift to Second-Generation Architectures

[13] IonQ Secures $7.5 Million Phase 2 AFRL Allocation to Expand Rome, NY Quantum Network with Free-Space Optics and Frequency Conversion

[14] IDEMIA and KT Deploy Quantum-Resistant SIMs Supporting Dual NIST and KpqC Algorithms for South Korean Military Networks

[15] Noncontextuality inequalities for prepare-transform-measure scenarios

[16] A General Framework for Gradient-Based Optimization of Superconducting Quantum Circuits using Qubit Discovery as a Case Study

[17] Proof of hiding conjecture in Gaussian boson sampling

[18] Quantum X Labs Launches Quantum Error Correction Program

[19] Optqc Team Bounds Quantum Errors below One in Ten Thousand

[20] Quantum Computing Resolves Fermion Collisions with Few Percent Precision

[21] Researchers Bypass Blockchain Certificates in Post-Quantum Protocol

[22] SEALSQ to Buy Satellite Capacity for Quantum Security Cloud

[23] Quantinuum and GE Vernova Collaborate to Advance High-Temperature Superconductivity Research

[24] Researchers Map Complex Material States Using AI Agent

[25] Researchers Control Fully Connected Quantum Dot with RFSoC System

[26] Researchers Entangle Logical Qubits with 93% Fidelity

[27] Gmbh Team Builds Trapped-Ion Chip with 31 Qubits

[28] Researchers Find Photon Pairs Boost Loss Measurement Precision

[29] Researchers Train 64-Qubit Circuits Entirely with Classical Tools

[30] A 256-qubit QPU shows a quantum magnet relaxing in unexpected ways

[31] Researchers Achieve 99.6% Fidelity in Photon Counting with New Detectors

[32] Optimized Gates Achieve Low Error Rate: One in Fifteen Hundred Per Gate

[33] Researchers Speed Debris Removal Planning Using Quantum Computing

[34] The Vera C. Rubin Observatory may have just discovered our solar system’s sixth dwarf planet

[35] OpenAI just scooped human researchers on a million-dollar quantum math problem

[36] How a 16th century pirate accidentally spawned a centuries-old math problem

[37] CDC deputy director Jennifer Shuford resigns after just four months in the role

[38] Dueling proofs from OpenAI and Anthropic astound scientists

[39] Sleep and depression may be more intertwined than we thought

[40] Underwater data centers may be coming to the U.S.—smack in the middle of endangered whale habitat

[41] Why we’ ll never have another Black Death

[42] A New Chemistry Breakthrough Could Change How Scientists Build Quantum Computers

[43] From 54% to 100%: Scientists Reveal a Potential Breakthrough in Quantum Technology

[44] Guest Post: The Next Threat to Encryption May Not Need a Quantum Computer

[45] Beyond Binary Quantum Computing: Exploring Higher-Dimensional Qudits

[46] OpenAI Computing Claim Faces Review, Raising Questions About Quantum Advantage

[47] The Qubit Report: October 27, 2026

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。