

十四万款手机应用近九成七未防量子破译

64 篇 · 18 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	64
信息来源	18
阅读时长	约 18 分钟

当前 SOTA

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

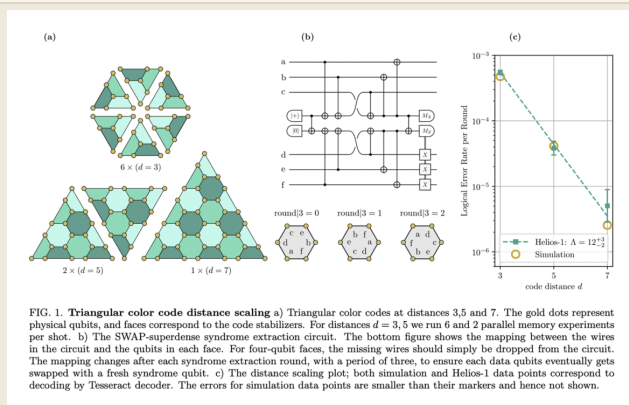


- 1 半导体空穴自旋控制保真度跨过99%门槛** 研发团队在半导体量子点中利用面内电场调控电子空穴自旋量子比特（利用半导体价带空穴角动量编码的单元），单比特门保真度（量子操作精确度）实测突破99%^[23]——攻克各向异性退相干难题，扫清硅基工艺规模化障碍。
- 2 太乙量子成立九个月累计融资超十亿元** 太乙量子完成新一轮融资，自成立九个月内累计吸纳资本超10亿元人民币（约1.496亿美元）并晋升独角兽，加速研制镱原子中性原子整机^[16]——加速中性原子路线工程化。
- 3 德国航空航天中心向IQM采购超导算力** 德国航空航天中心量子计算计划与系统集成商Bechtle

签约，通过云平台采购芬兰IQM超导量子系统以支撑实际科研^[32]——主权机构真金白银买算力，欧洲超导产业获商业造血。

02 硬件

硬件前沿



离子阱

继北京时间2026年10月19日报道逻辑比特（纠错保护的信息单元）内存出错率压至 5×10^{-6} 后，Quantinuum披露Helios离子阱芯片在运行码距（抗错冗余能力指标）为7的色码（二维拓扑容错纠错法）时，单轮纠错耗时接近200毫秒（约20万微秒）^[13]。

在误差压制上，该系统平均每增大一级码距使错误率下降约12倍，压制因子达12，相当于谷歌Willow超导表面码（二维网格排布纠错法）基线

（ $\Lambda \approx 2.1$ ）的5.7倍，双比特门（双粒子纠缠逻辑操作）保真度未披露^[13]；但约0.2秒一轮的纠错周期暴露了离子阱路线的物理瓶颈——受制于离子穿梭输运开销与激光冷却延迟，其实际执行主频仅约5赫

兹，落后超导路线纳秒级门时（20至100纳秒）达六个数量级，在长算法中仍面临环境退相干（量子态衰减退化）累积的物理硬伤^[13]。这一进展确立了离子阱在高精度存储上的优势，但倒逼硬件商攻关低延迟离子路由方案以满足容错计算需求。

英国量子硬件企业Universal Quantum公布新型纠错解码器，实测减少了模块化离子芯片互联时的通信纠错开销与传输误码^[31]。该方案通过自适应校验拓扑降低跨芯片传输离子与光子链路的测量延迟^[31]，为突破单芯片物理囚禁上限、构建千比特分布式离子阱集群扫清通信障碍。

牛津大学科研团队在实验室内将不同元素组成的混合双离子纠缠态相干时间延长至超过10秒^[60]。该技术利用异种离子天然免疫测量光散射串扰的物理特性，相干时间较常规非时钟态离子大幅延长，逼近单种离子时钟态秒级基线^[60]，加速量子中继器与分布式节点抗串扰接口的实用化。

中性原子

太乙量子在成立九个月内完成累计超10亿元人民币（约1.496亿美元）融资并晋升独角兽，专注研发基于镱原子的容错量子计算硬件，并开源了底层编译器与控制工具链LUOSHU^[16]。

当前中性原子路线公开SOTA由Atom Computing保持1,180物理比特规模，QuEra于Nature 2026验证了96个逻辑比特；太乙量子选用镱原子双价电子能级，旨在将两比特门保真度推向哈佛大学创下的99.5%基线，但距离实用化仍受制于该路线1至10赫兹的循环重复率短板与穿梭装载损耗，其实测硬

件指标与后选择率（剔除错误后的有效数据比率）仍有待同行评审公开数据检验^[16]。本轮注资打破了北美对高精度中性原子赛道的资本垄断，预计2027年前将催化国内整机竞性格局形成。

半导体与自旋量子点

科研人员在半导体量子点器件中利用纯面内电场调控电子空穴自旋量子比特，单比特门保真度实测突破99%^[23]。

自旋量子点路线公开SOTA单比特门保真度通常要求 $\geq 99.9\%$ （如Diraq在1开尔文温区实现99.85%），双比特门SOTA最高为澳大利亚SQC创下的99.99%；本次空穴自旋突破99%门槛，成功利用面内场构型规避了价带空穴的各向异性强退相干噪声，但该路线整体仍受限于十比特以内的微小规模（SOTA器件级 ≤ 12 比特）与偏低的门操作寿命比（ 10^2 至 10^3 ）^[23]。该成果证实空穴自旋无需片上微磁体即可实现全电学高速操纵，坚定了芯片制造巨头利用成熟半导体产线代工量子芯片的信心。

超导与新型量子比特

法国量子初创企业爱丽丝与鲍勃在法国国防创新局PROQCIMA项目下完成三款猫量子比特演示芯片测试^[30]。猫量子比特（利用谐振腔非线性光子态内禀抑制位翻转的超导单元）在硬件层面自发抑制位翻转错误，将纠错编码冗余比从传统超导表面码的105:1（谷歌Willow基线）降至数十比一，但其相位翻转率随光子数增加而上升，且两比特门保真度仍落后于超导生产系统99.5%至99.9%的中位基线

^[30]。法国主权资本的深度介入确立了欧洲在紧凑型超导路线上的自主壁垒。

加拿大初创公司Iceberg Quantum完成600万美元种子轮融资，并公布首个全栈容错架构Pinnacle，主打低温芯片互联与低冗余纠错解码^[29]。资金将直接投入首批原型芯片流片测试，加剧北美早期容错硬件方案的技术竞逐。

光量子与网络

研究人员利用人工巨原子（尺度与微波波长相当的超导人工结构）耦合一维波导，在无任何外加控制脉冲的条件下实现保真度超过99%的确定性量子态单向转移^[24]。该方案免去了高频时钟脉冲引入的相位抖动，转移保真度跨过99%门槛，逼近光纤芯片间互连99.72%的SOTA基线，但其实际低温系统损耗预算仍需工程验证^[24]。这一物理机制为模块化超导计算机机柜间互联提供了低功耗无源接口方案。

美国博尔德初创企业EMode Photonix获得100万美元种子轮融资，推进集成化确定性单光子源芯片研发^[20]。资金注入将加速解决光量子计算上游高纯度光源制造痛点，服务光量子干涉网络搭建。

算法与软件



摩根大通、IBM、汇丰银行、美国运通与意大利联合圣保罗银行在IEEE量子周2026公布了金融衍生品定价与资产组合优化的联合实测结论：在当前含噪芯片上运行相关算法未展现出任何加速优势，直接跳过量子硬件采用经典计算集群反倒省下了全部算力支出^[28]。这是四家金融机构与技术硬件服务商IBM联合开展的算法测试，证实因物理门误码率居高不下，耗费海量采样开销进行误差缓解（数学后处理压制噪声的方法）导致等效复杂度远逊于经典GPU张量网络优化^[28]。此举打破了金融行业短期实现量子商业优越性的非理性预期，迫使华尔街机构将研发重心从昂贵的云端硬件租用转向长周期容错算法设计。

量子计算软件商Haiqu与QMill发布针对深层量子线路（量子逻辑门序列）压缩的对比评测，Haiqu利用近似逼近算法实现了更激进的门深度削减，使复杂算法得以在当前含噪芯片上跑出正确解，而QMill则坚持精确等价转换^[5]。该对比揭示了容差编译与严格编译在含噪时代的工程取舍，通过引入可控的微小酉算子（保持总概率守恒的变换）误差大幅缩减两比特门深度，有效规避了硬件物理退相干^[5]。

这为现阶段含噪量子化学分子模拟与组合优化应用开辟了实用化生存空间。

量子软件公司Classiq副总裁克里斯·里德公开指出，美国联邦机构在量子科技领域的资金投放过度偏向底层硬件，而在算法综合工具与跨学科人才培养上的投入明显不足^[6]。底层硬件若无高阶编译器支撑将沦为算力孤岛，呼吁资金向算法生态平衡倾斜^[6]。

量子网络开发商Welinq利用英伟达CUDA-Q混合架构对分布式量子纠错网络中的探测器错误模型进行高速抽样计算，缩短了网络纠错协议基准测试周期^[26]。该工具加速了量子中继器解码算法在经典高算力硬件上的并行验证^[26]。

Postquant Labs在Aglais测试网正式上线Quip虚拟机，并部署了首批量子智能合约，为去中心化网络调用经典与量子混合算力提供了统一执行环境^[50]。该平台降低了跨平台调用分布式量子接口的工程开发门槛^[50]。

04 产业

产业与生态



移动安全评测机构NowSecure对苹果App Store与谷歌Play商店中的136,711款手机应用展开代码扫描，实测发现高达97%的应用中完全不存在任何后量子密码（抵御量子攻击算法）代码，即使在下载量最大的主流应用中具备防护能力的也低于十分之一^[55]。这揭示了移动端软件生态在抗量子迁移上的严重滞后，尽管美国国家标准与技术研究院

（NIST）已颁布正式标准，但第三方软件面临编译库体积庞大与握手延迟上升的阻力，缺乏主动改造动力^[55]。数亿用户的个人通信与网银支付暴露在“先窃取后解密”威胁之下，将倒逼手机操作系统巨头在2027年前将后量子密码列入强制上架要求，开启百亿美元级软件改造市场。

德国航空航天中心量子计算计划正式与IT解决方案服务商Bechtle签约，通过云端采购芬兰IQM的超导量子计算机服务，直接用于真实科研^[32]。该模式由政府主权机构出资直购商用算力，验证了“云端硬件商+传统IT集成商”的B2B销售模式，推动欧洲超导硬件从依赖科研补贴转向获得稳定的经常性商业收入^[32]。

后量子安全机构Project Eleven与百慕大Relm保险公司达成合作，将其机构级资产防护产品Strongpoint纳入数字资产保险核保流程，制定抗量子技术风控标准^[52]。双方合作旨在探索如何在数字资产保险核保中评估机构的后量子安全控制机制，目前尚未量化为商业承保硬指标^[52]。

越南IT服务商FPT与法国光量子企业Quandela签署为期两年的合作备忘录，在越南联合推进光量子计算技术工程化落地与云端算力服务^[21]。配合越南科

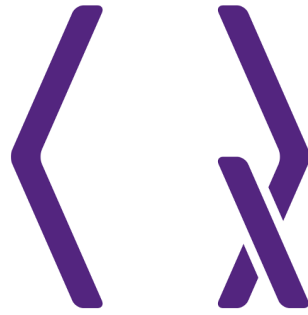
研学者呼吁深化与欧盟量子合作的倡议^[51]，欧洲光量子产业链正加速向东南亚软件外包高地渗透^[21]。

日本量子战略产业革命联盟与芬兰国家技术研究中心签署合作备忘录，强化两国在量子软硬件生态与产业化层面的协同协作^[4]^[60]。该协议深化了七国集团与北欧国家在量子材料及控制系统供应链上的互认互信。

英国上市公司Arqit宣布完成对国防网络通信服务商Sirius Computer的战略投资，旨在将量子安全加密方案嵌入国防与关键基础设施的专有硬件系统^[54]。此举推动后量子软件公司通过股权绑定加速向高毛利军工供应链下沉。

老牌量子算法开发商Zapata宣布聘请1994年提出质因数分解算法的麻省理工学院数学家彼得·肖尔等四位科学家出任科学咨询委员会委员^[58]。这强化了企业在后量子密码破译评估与容错算法知识产权层面的学术权威壁垒。

韩国三星电子与印度科学理工学院在班加罗尔联合成立量子技术联合实验室，支持数百名科研人员开展前沿器件研发^[22]。全球电子制造龙头以此深度锁定南亚高性价比研发人才与量子芯片制造试验节点。



科研人员在学术期刊《Quantum》发表论文，系统分析了振幅阻尼（光子损失）噪声通道下多模玻色 Fock 态（光子数本征态）的纠错极限，首次证明当系统总激发数无界增长且光子损失率有限时，存在渐近良好的玻色码（连续变量谐振腔纠错法）^[17]。该结论打破了学界对连续变量谐振腔纠错码在光子损耗下难以保持有限码率的悲观预期，证明连续变量纠错可以实现与离散量子比特码相当的渐近容错性能^[17]。这为超导微波腔与连续变量光量子路线奠定了坚实的理论基石，指引下一代低硬件冗余纠错架构设计。

理论计算机学者在《Quantum》提出针对内存受限与弱数据访问条件下的交互式证明系统，用于严格核验量子学习与性质测试的正确性^[18]。该研究首次构造出经典验证者可在多项式时间内严格核验量子态性质学习真伪的数学协议，解决了黑盒量子态生成过程不可查验的理论难题^[18]。这为未来分布式量子云计算客户在不拥有完整量子硬件的前提下验证云端计算结果真实性提供了数学工具。

密码学研究团队在《Quantum》提出基于半正定松弛算法的数值框架，可直接依据观测到的测量统计关联严格估算条件冯·诺依曼熵（量子态不确定性度量）^[19]。该方法大幅提升了设备无关量子随机数发生器与设备无关保密通信的熵提取界限计算效率，在无需对物理器件内部机制做任何信任假设的条件下给出了安全底线^[19]。该成果推动极端安全等级的无条件保密通信协议向实用化参数边界快速推进。

香港城市大学物理学系奥斯卡·达尔斯滕领衔的团队通过严谨数学推导与数值模拟，发现在微观涨落环境中利用量子相干性可实现零熵增的定向能量转移^{[11][60]}。该发现突破了传统热力学在非平衡微观环境下必然伴随耗散损失的经典边界，提出了从量子热涨落中高效提取可用功的新范式^[11]。这为解决纳米芯片在极小尺度下的热耗散瓶颈以及开发自驱动量子测量控制器提供了全新物理路径。

实验物理学家在《物理评论快报》发文，利用光镊悬浮的二氧化硅微球光学谐振系统，在实验室内首次高信噪比探测到单个气体分子与介观质点碰撞产生的反冲信号^[9]。该工作推动介观量子态探测灵敏度跨入单粒子撞击极限，为微弱力学传感与基本物理常数精密测量开辟了新途径^[9]。

理论物理学者在最新论文中系统论证指出，近百年来试图从更基础数学公理直接导出玻恩定则（量子测量概率判定法则）的各种尝试，均在推导链条中隐蔽引入了关于概率的先验假设，证实其具有不可简化的基本公理地位^[10]。该结论澄清了量子力学诠释长期以来的数学争议，明确了测量公理的认知边界^[10]。

今日影响



- 1 **移动智能终端与金融支付开发者：**全球主流移动操作系统生态中的应用软件开发者、加密钱包厂商及手机银行安全团队受直接影响^[55]。近14万款手机App的抽检证实97%的应用完全没有构筑后量子密码防线，终端通信与资产凭据面临“先窃取后解密”的长期潜伏危机^[55]。下一步需紧盯苹果与谷歌是否会在2027年前将后量子密码纳入应用商店强制上架审核标准，以及第三方轻量级加密库的移动端适配速度^{[3] [55]}。
- 1 **华尔街金融机构与量子算法团队：**寄望于用短期含噪量子芯片实现投资加速的对冲基金、跨国银行与量子软件初创企业受直接影响^[28]。摩根大通、汇丰等五大机构的联合实测明确证实，现阶段跳过量子芯片直接使用经典计算反而更省成本，行业非理性泡沫被无情刺破^[28]。下一步需紧盯金融巨头的预算流向——从昂贵的含噪云算

力租用转向抗量子保险风控^[52]以及面向长远容错硬件的高阶算法储备。

1 **量子硬件创业阵营与产业资本**：主攻中性原子、离子阱及自旋量子点等路线的硬件初创团队与硬科技风险投资机构受直接影响^{[13][16][23]}。太乙量子以超10亿元融资晋升独角兽创下国内硬件融资纪录^[16]，叠加Quantinuum在0.2秒时延纠错上的持续突破^[13]与空穴自旋门保真度越过99%门槛^[23]，资本与人才正加速向工程指标清晰的容错梯队集聚，缺乏物理自治性的概念团队融资通道迅速关闭。下一步需紧盯太乙量子LUOSHU工具链在整机上的实测门保真度公布^[16]，以及牛津大学等机构在长寿命原子纠缠技术上的工程转化进度^[60]。

1 **数字资产托管与合规承保机构**：加密基金合规托管人、代币化现实资产发行机构与专业技术保险公司受直接影响^{[52][57]}。Relm保险与Project Eleven首次将后量子技术控制嵌入数字资产承保评估流程，抗量子合规直接从“技术演练”晋级为“保险定价与牌照准入”的硬门槛^[52]。下一步需紧盯七国集团金融监管机构是否会参照商业保险标准，出台针对数字资产私钥抗量子迁移的强制性监管时间表^{[3][52]}。

07 编辑

编辑点评

量子科技行业正在经历一场深刻的理性重构。一方面，物理底层的技术推进呈现出极高的工程密度：

离子阱在微秒与毫秒尺度上向物理极限持续挤压交错时延，中性原子与硅基空穴自旋不断刷新保真度与集成度门槛，巨额主权与民间资本以高度聚焦的形态向头部梯队汇流。但另一方面，来自终端市场的真实反馈正在给全行业浇上一盆清醒的冷水：国际金融巨头对含噪芯片算力性价比的断然证伪，移动软件生态面对后量子密码迁移高达九成以上的惊人真空，无不清晰暴露出底层技术供给与实际产业承接力之间的巨大鸿沟。

这种断层标志着量子产业正在彻底走出概念狂欢期，进入以绝对工程指标与严苛商业逻辑为检验标准的去泡沫深水区。对于技术研发者而言，任何回避全芯片误码压制、后选择率口径与时钟主频短板的纸面突破都已难以获得同行认可；对于产业投资与金融从业者而言，看清哪些是依靠经典计算即可轻松碾压的虚假需求，哪些是事关国家安全、数字资产存续与主权算力重构的真正时代刚需，才是穿越当前认知周期、精准锚定下一代信息基础设施价值的关键分水岭。

参考资料

[1] Securing the Robotics Supply Chain: New White Paper Lays Out Research Priorities and Federal Investment Opportunities for a U.S. Robotics Ecosystem	[3] Preparing for PQC Migration at Federal Agencies
[2] UK halfway milestone in mission to unlock neutrino secrets	[4] Q-STAR and VTT strengthen quantum technology collaboration between Japan and Finland
	[5] QMill Exactness vs Haiqu Approximation

- [6] Classiq's Chris Reid: Quantum Software Deserves More Attention
- [7] A hidden rivalry between two quantum states at the heart of superconductors
- [8] Steering electrons with extreme ultraviolet light—team achieves quantum coherent control
- [9] Individual atomic collisions can now be detected in the lab, potentially opening up pathways to new physics
- [10] Quantum probability can't be derived without assuming it first
- [11] A quantum pathway to entropy-free energy transfer
- [12] From space to folk music: quantum hackathon explores diverse use cases
- [13] Quantinuum Reports Record Error Suppression on Helios, at About a Fifth of a Second per Correction Round
- [14] Single-Molecule Sensors and NanoSystems International Conference
- [15] Quminex Raises \$1.5M CAD (\$1.06M USD) Pre-Seed Round Led by Quantacet and QAI Ventures to Advance Mineral Discovery Platform
- [16] Taiyi Quantum Surpasses ¥1 Billion RMB (\$149.6M+ USD) in Cumulative Funding for Ytterbium Neutral-Atom Systems
- [17] Asymptotically good bosonic Fock state codes
- [18] Interactive proofs for verifying (quantum) learning and testing
- [19] Reliable Entropy Estimation from Observed Statistics for Device-Independent Quantum Cryptography
- [20] Five errors in a million, Helios sets a new quantum record
- [21] EMode Photonix gets \$1 million to speed up quantum light design
- [22] FPT and Quandela sign a two-year quantum agreement
- [23] NVIDIA's Record simulation of a 104-qubit fault-tolerant quantum computer
- [24] Samsung and IISc open a new lab for quantum research in India
- [25] Hole spin qubits gain ground with in-plane control
- [26] Giant atoms boost quantum state transfer to over 99%
- [27] WISeSat tests quantum-resistant security on new satellite in orbit
- [28] Error model sampling with NVIDIA cuts time for quantum network tests

- [29] Trains, floods and wedding guests tested quantum computing for logistics at QCE26
- [30] In quantum finance at QCE26 the only money saved came from skipping the chip
- [31] \$6 million Seed round fuels Iceberg Quantum' s fault-tolerance work
- [32] Three cat-qubit chips tested by Alice & Bob in France
- [33] Universal Quantum decoder cuts errors in linked qubits
- [34] German Aerospace Center buys IQM quantum systems for real-world work From DLR
- [35] Scientists reach the ultimate quantum limit on a surface
- [36] Christina Applegate says she was misdiagnosed with MS—how could that happen?
- [37] The mathematical impossibility of making a perfect world map
- [38] Scientists left in the dark by National Science Foundation grant application delays
- [39] Green stars do exist—and others shine pink or purple, too
- [40] The Selfish Gene at 50
- [41] Math Puzzle: Baby bottle mix-up
- [42] The provocative new theory that could explain aging and disease
- [43] Inside the bold, quixotic quest to store planet-warming carbon in the ocean
- [44] We' re addicted to social media. How do we get sober?
- [45] Why we probably live in a quantum multiverse
- [46] Our love-hate relationship with social media
- [47] How a fusion start-up could help maintain the U.S. nuclear arsenal
- [48] Why data centers are reviving solid-state transformers
- [49] How your brain learns to cope with uncertainty
- [50] November 2026: Science history from 50, 100 and 150 years ago
- [51] 40 Years of Superconductor Science Just Got Turned Upside Down by a Stunning Discovery
- [52] Postquant Labs Launches Quip Virtual Machine for Quantum and Classical Computing
- [53] Vietnam Quantum Expert Urges Closer EU Ties to Build National Capabilities
- [54] Project Eleven and Relm Explore Post-Quantum Risk in Digital Asset Insurance
- [55] Monarch Quantum Supplies Photonics Hardware for NASA Gravity Sensor Mission

[56] Arqit Invests in Sirius to Develop Quantum-Safe Defence Communications

[57] NowSecure Finds No Detectable PQC Code in 97% of Mobile Apps

[58] BIRD Foundation Approves \$7.4 Million for Seven U.S.-Israel R&D Projects

[59] Guest Post: Why Tokenised Assets Need Quantum-Ready Security

[60] Zapata Quantum Adds Peter Shor and Three Scientists to Advisory Board

[61] Xanadu Receives Provisional Approval for Up to \$10M in DARPA Funding

[62] Quantinuum Breaks Error Correction World Record Is This Just Chest-Puffing or a Substantive Milestone?

[63] The Qubit Report: October 19, 2026

[64] The Qubit Report: October 20, 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。