2026 年 11 月 02 日 – 11 月 03 日 · 日报

量子计算机破解银行密码门槛降至两万比特

39 篇 · 12 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

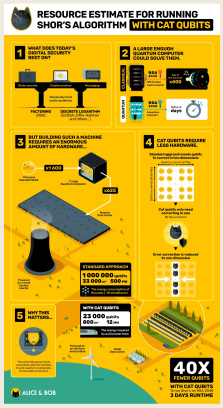
收录报道	39
信息来源	12
阅读时长	约 20 分钟

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 **猫比特芯片翻转寿命破四小时** 法国初创公司爱丽丝与鲍勃（Alice & Bob）在12比特Helium 2芯片上实现闲置比特翻转（量子态0与1误码）寿命超3至4小时，单比特器件达44分钟[8]——首次在多比特验证自主抑制，推动纠错硬件开销缩减。

2 **英国养老金巨头拟投资两家量子企业** 英国苏格兰寡妇基金（Scottish Widows）通过知识产权集团资产组合，首次将职场养老金配置给两家本土量子计算初创公司[34]——长线养老金首次进场量子风投，为研发注入跨周期资本。

3 **香港金管局发布银行抗量子工具包** 香港金融管理局联合香港科技大学于2026年11月2日推出后量

子密码（抗量子密码算法）工具包，指导银行业应对解密威胁[32]——金融监管首发落地工具包，加速商业银行安全架构升级。

02 硬件

硬件前沿



猫量子比特与超导硬件

法国量子计算初创公司爱丽丝与鲍勃（Alice & Bob）在微波超导谐振腔制造的玻色猫量子比特（利用薛定谔猫态编码）处理器上，测得单比特器件平均闲置比特翻转（量子态0与1误码）寿命达到44分钟，其12比特Helium 2处理器的比特翻转寿命达到3至4小时[8]。同日发布的最新资源估算显示，基于猫量子比特构建容错架构，破解主流商用密码体系RSA-2048仅需约23000个物理比特和3天多运算时间[39]。

对照超导路线当前公开最高水平（SOTA）基线（谷歌Willow芯片单比特退相干时间T_1约100微秒，双比特门保真度99.5%至99.9%），常规超导电路（微波超导电路计算）的比特翻转寿命通常在微秒

至毫秒级，Helium 2将闲置比特翻转寿命推升至小时级，在硬件物理层面对比特翻转噪声实现了数百万倍的时间尺度抑制[8]；这使得破解RSA-2048所需的物理比特预算从常规表面码（二维网格量子纠错码）的百万量级直接降至两万余枚[39]。但该路线距离实用化仍存在明显短板：猫量子比特仅在物理硬件上自发压制比特翻转，相位翻转（叠加态相位误码）误差仍随光子数线性增加，仍须依赖一维重复码进行纠错；同时其双比特门保真度当前处于98%至99%区间，较离子阱路线商用全比特对最高纪录99.921%（Quantinuum Helios）低约一个数量级，纠错偏置门操作仍待多比特规模验证[8][39]。这一成果推动行业重估非对称纠错路线的商业化速度，预计将在2至3年内倒逼量子云服务商重估物理比特扩展路线图[8][39]。

中性原子量子计算

研发团队利用里德堡原子（高激发态中性原子）处理器结合样本量子对角化（SQD，采样计算基态能量）算法，成功计算了电子系统费米-哈伯德模型（强关联电子理论模型）的基态能量，在达到56个量子比特规模时依然收敛至接近基态，且在样本量比传统随机采样少10倍的前提下保持了收敛优势[16]。另一组研究人员利用多达107个原子的里德堡阵列开发了问题映射嵌入纠错方案，在传统优化算法无法解出正确结果的测试场景中，实现了不低于8%的最优解恢复率，且未增加额外的控制硬件复杂性[13]。

对照中性原子路线当前公开最高水平基线（QuEra在2026年实现448物理比特、96个逻辑比特纠错操

作，Atom Computing实现1180个物理比特阵列），本次56比特费米-哈伯德模拟在分子能级对角化精度上追平了小规模精确数值解，证明中性原子在多体物理基态搜索上具备实用采样优势[16]；107比特嵌入纠错则首次将原子几何排列的映射冗余开销直接转化为纠错增益[13]。但中性原子路线距离通用容错计算仍面临底层硬约束：其循环重复率受限于原子激光冷却与重载过程，典型值仅在1至10赫兹区间，较微波超导电路慢4至5个数量级；同时其中路读出（计算过程中测量部分比特）的保真度与串扰控制尚未达到表面码容错阈值[13][16]。该进展为凝聚态物理模拟提供了即时可用的准容错方案，预计在1至2年内推动材料模拟企业从纯数值模拟向中性原子混合计算迁移[13][16]。

光量子与通信器件

研究人员研制出一种高非简并纠缠光子对光源，能够同时发射波长为548纳米的可见光光子与波长为1550纳米的通信波段红外光子，具备降低基于量子纠缠的QKD（量子密钥分发）系统探测器成本的潜力[23]。

在传统纠缠型量子密钥分发系统中，双端均需配备成本高昂的1550纳米超导单光子探测器，而该方案仅需在远距离通信光纤单端保留通信波段探测器，本地端可采用价格低廉的高效率硅基雪崩光电探测器，直接减少了一个昂贵红外探测器的硬件开支[23]。对照光量子当前公开最高水平基线（PsiQuantum在300毫米晶圆上实现的99.22%双比特融合保真度与探测效率≥95%），该光源有效降低了QKD终端部署的边际硬件成本，但全系统的

端到端损耗预算与多用户网络接口复用率仍有待进一步测试验证[23]。此方案将削减城域量子安全专网与数据中心机房节点的部署成本，预计在2年内加速金融与政务干线量子密钥分发终端的普及速度[23]。

量子传感与精密测量

实验团队采用精细化动力学解耦（用微波脉冲抑制噪声）脉冲序列，将量子传感器在强噪声环境下的量子信息相干存储时间从毫秒级延长至数十毫秒，实现了整整10倍的时间跨度提升[12]。另一项纳米尺度测量实验证实，微观结构中先前被忽略的纳米级机械耗散效应对全球灵敏度最高的部分纳米弦传感器产生了结构性干扰[27]。

脉冲序列技术在不改变探针物理化学结构的前提下，消除了由控制漂移和微波畸变引起的系统误差，将信噪比门槛降低了一个数量级[12]；而纳米级耗散效应的发现则为极低信噪比弱力测量划定了物理边界[27]。该技术直接赋能生物微磁场测量与地下重力梯度导航，预计在1至2年内转化为高端地质勘探与医疗成像硬件的升级方案[12][27]。

超导工程化与拓扑硬件

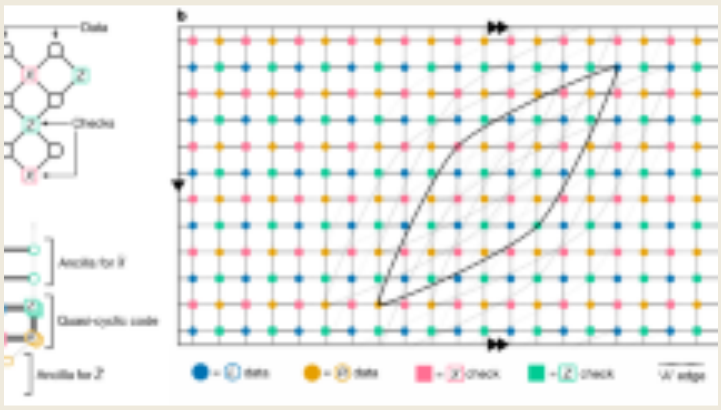
由德国尤利希研究中心（Forschungszentrum Jülich）牵头、历时近五年的德国量子计算重大专项QSolid联盟正式结项，成功交付了贯通超导芯片硬件与底层软件栈的完整演示原型机[18]。苏格兰超导硬件制造商Quantcore向苏格兰创新与高等教育大臣展示了其超导量子硬件研发工作与制造雄心[36]。爱尔兰初创公司Equal1宣布任命拥有二十余年

半导体制造经验的安德鲁·弗林（Andrew Flynn）为首席运营官，主导其机架式量子计算机RacQ的商业化交付[37]。研究团队则在实验上为拓扑量子计算（用任意子编织抵抗噪声）的理论基础提供了最新抗局部扰动实验支撑[4]。

QSolid与Quantcore的进展标志着欧洲超导量子路线从分散的科研探索向工业化代工制造标准的系统收敛[18][36]；Equal1则推动硅基CMOS（互补金属氧化物半导体）量子比特向标准服务器机柜物理形态收容[37]。这将增强欧洲在量子硬件制造供应链上的本土自给能力，预计将把企业客户采购机架式量子算力的部署周期从按年定制压缩至按季交付[18][36][37]。

03 算法

算法与软件



量子纠错与动力学噪声抑制

发表在《npj量子信息》上的最新研究提出了一种针对相干噪声环境的恒定激发稳定子码容错量子纠错方案，证实即使在存在相干误差累积的复杂干扰

下，逻辑比特仍能保持纠错保护边界[3]。另一支理论团队提出了一种利用碰撞动力学过程检测并抑制量子退相干（量子态受干扰失效）的通用协议，无需事先精确掌握环境噪声谱即可保护任意数量的量子比特[14]。

传统量子纠错多假设噪声为独立无相干的随机微扰，该研究突破了相干噪声破坏纠错阈值的理论瓶颈，首次在恒定激发子空间构建了数学自洽的容错电路设计[3]；无须噪声先验知识的动力学协议则放宽了硬件控制校准的门槛[14]。这两项成果为超导和半导体自旋路线的底层测控软件库提供了固件层纠错方案，预计在1年内被各大主流量子云平台的底层编译器采纳[3][14]。

量子搜索与核物理基态求解

科研人员开发出名为QDMin的新型量子算法，将格罗弗算法（量子无序数据库搜索）应用于寻找复杂原子核的真实能量最低基态；在单次量子计算迭代后，定位真实基态能量极小值的成功概率从传统方法的25%跃升至92%[11]。

相较于在指数级参数空间中逐点枚举的传统数值算法，QDMin实现了超二次加速的极小值定位，但在向更大核子系统拓展时暴露了态制备保真度受限的工程瓶颈[11]。该算法为极端条件核物理反应堆材料模拟与天体物理计算提供了全新求解工具，预计将在3年内缩短高能物理大型模拟任务的高性能计算耗时[11]。

自适应量子态层析理论

理论与实验研究证实，在多比特量子态表征任务中，自适应测量方法所需纠缠态样本复本数量随比特数增长仅呈对数级增加，而所有静态测量备选方案均需指数级增长的样本量[22]。

这是全球首个在不依赖量子相干性或受限协议前提下，利用测量动态反馈实现指数级加速的量子学习范式，消除了多比特态层析必然面临维度灾难的理论限制[22]。该方法降低了多比特量子芯片在出厂校准与逻辑门保真度基准测试中的时间开销，预计将在2年内成为半导体与超导量子芯片自动化测试的标准软件模块[22]。

医学数据中的量子模式挖掘

佛罗里达大西洋大学（FAU）工程与计算机科学学院团队开展了一项量子计算应用测试，评估量子分类算法在极小样本量肺癌症状与危险因素数据集上的特征模式挖掘能力[30]。

针对生物医学领域高维度、小样本数据的过拟合难题，研究探索了量子态高维希尔伯特空间在受限医学特征映射中的表达能力[30]。该工作为早期肿瘤筛查中小规模专病队列的数据分析开辟了量子算法探索方向，但在临床转化前仍需更大规模的多中心对照验证[30]。

产业与生态



机构投资与资本动向

管理着数百亿英镑资产的英国大型养老金提供商苏格兰寡妇基金（Scottish Widows）正式宣布将职场养老储蓄配置于英国风险成长型科技企业，首期资产组合由知识产权集团（IP Group）运营，预计初始投资中包含两家英国量子计算企业[34]。与此同时，美国田纳西州查塔努加的CO.LAB量子孵化器公布了首批入选商业化加速计划的四家初创企业名单，其中包括转化橡树岭国家实验室（ORNL）加密技术的Ridge Quantum、软件开发商Superquantum和Esoteriq，以及量子传感企业Kottackal[38]。

传统养老金作为风险偏好极度稳健的长期机构资金，进场配置未上市量子初创股权，标志着量子技术在英国已从早期的政府前沿拨款阶段跨入养老金等长线资产负债表认可的商业成长期[34]；区域级产业孵化器则加速了国家实验室防务级技术的民间商业转化[38]。这拓宽了硬件企业在后续融资中的资金来源，预计将带动欧美其他主流主权与企业养老基金在未来1至2年内跟进试水量子赛道[34][38]。

国家超算融合与防务布局

韩国科学技术信息通信部宣布其第六代国家超级计算机“汉江”系统已正式全面投入商业运行，系统设计目标为位列全球算力前十强；韩国政府明确宣布计划于2027年上半年将汉江超算与一台物理量子计算机进行互联集成，组成经典-量子混合系统[33]。在美国防务方向，量子技术集成商Qtonic Quantum任命前北约盟军陆军司令部司令、退役陆军中将罗杰·L·克鲁蒂埃（Roger L. Cloutier Jr.）担任公司首席运营官，主导防务量子技术的战术部署[29]。

这标志着超算与量子计算机的混合部署从学术演示进入国家骨干算力基础设施阶段，预计日韩与欧洲国家将在2027年前掀起一轮国家超算中心的量子算力外挂加装潮[33]；防务高级指挥官执掌运营则表明量子加密与传感技术在北约军事指挥体系中的战术落地进程正在提速[29]。

金融抗量子改造与公有云支持

北京时间2026年11月2日，香港金融管理局（HKMA）联合香港科技大学正式发布面向银行业的后量子密码（PQC）工具包，为商业银行提供了系统排查、迁移路径评估及密码敏捷性升级的标准化框架[32]。在东南亚，网络安全服务商ExeQuantum与泰国上市公司Bluebik旗下的蓝比克泰坦签署战略合作协议，针对泰国国家网络安全局主导的“Quantum-Ready 2030”国家战略，面向银行、金融服务、保险、能源及政府机构提供抗量子密码迁移落地服务[20]。同日，亚马逊云科技

（AWS）密钥管理服务（KMS）宣布正式支持美国国家标准与技术研究院（NIST）定稿的后量子密钥封装标准ML-KEM[39]。

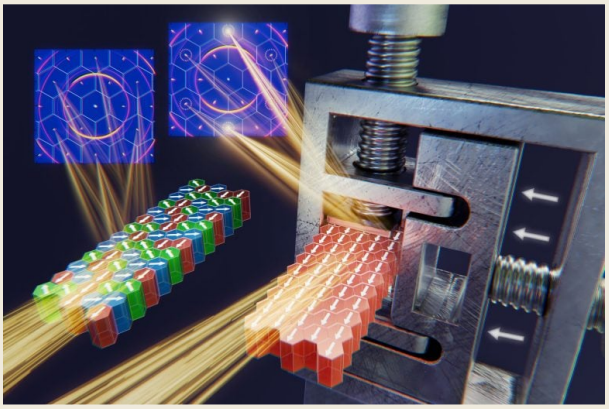
金融监管机构发布实操工具包与公有云基础设施开箱即用支持，标志着抗量子密码彻底越过算法选型阶段，进入系统合规改造与商业落地阶段[32][39]。跨国银行与关键信息基础设施企业的IT系统面临确定性改造预算支出，相关抗量子安全咨询与系统集成商在未来3至5年内将迎来明确的合同放量期[20][32][39]。

人才智库与学术生态

量子初创公司Iceberg Quantum在继悉尼和旧金山之后正式设立柏林办公室，并宣布聘请柏林自由大学量子计算学者延斯·艾泽特（Jens Eisert）教授担任公司科学顾问，吸纳多名来自其课题组的核心研发人才[19]。前谷歌量子硬件团队领头人、加州大学圣塔芭芭拉分校约翰·马蒂尼斯（John Martinis）教授受邀将于下月在西澳大学（UWA）发表量子计算四十年技术演进公开演讲[35]。

初创企业正在沿着全球顶尖学术高地设立研发分支，争夺稀缺的量子纠错与硬件架构高阶人才，顶尖团队的“学术顾问+衍生创业”正成为产业扩张的标准范式[19][35]。

学术前沿



凝聚态物理与非平衡态系统

德国蒂宾根大学研究团队证明，当粒子间长程相互作用按照距离代数衰减率(1+|x-y|)^(-π)且满足π>2d（d为系统空间维度）时，费米子多体能谱中的“体能隙（激发粒子所需的最小能量跃迁门槛）”即使在弱相互作用扰动下也能保持稳定，系统能够平滑演化至新的基态[15]。另一项关于非厄米时间晶体（非平衡态周期性微观结构）的研究指出，即便存在微弱的环境噪声干扰，理论上预期能够无限期振荡的时间晶体宏观周期性行为也会被破坏，其寿命存在严格物理上限[17]。此外，材料科学家通过中子衍射实验证实，能够在不改变材料化学组分的前提下，通过微观晶格畸变实现材料磁性的受控调制[28]。

蒂宾根团队为量子模拟器在长程库仑或偶极相互作用下的稳定性提供了数学严谨的保证界限[15]；非厄米时间晶体的噪声脆弱性则修正了此前对开放量子多体相干态长期存续的乐观预期[17]。这规范了拓扑绝缘体与高温超导材料量子模拟的算力边界，为自

旋传感器与拓扑存储器件的寿命估算修正了理论模型[15][17][28]。

全息对偶与量子模拟复杂度

理论物理学家胡安·马尔达西那（Juan Maldacena）在科普播客《The Quantum Kid》中对全息原理进行了通俗讲解，探讨了利用量子计算模拟宇宙的设想[31]。

该研究将高能理论物理中的反德西特/共形场论对应转化为可计算的量子线路深度评估，为强引力奇点物理的量子实验室检验划定了算力蓝图[31]。这拓展了量子计算在理论物理终极问题上的学术远景，推动多国国家级量子基础科学基金向交叉学科方向倾斜配置[31]。

单分子量子网络接口

实验物理学者论证了利用单一分子作为量子网络基本构建单元的物理可行性，证实单个有机分子能作为高相干性的单光子接口，实现长距离分布式量子计算节点之间的量子信息光学传输互联[5]。

相比目前主流的冷原子或固体色心方案，单分子体系具备化学可修饰性与波长可调谐性，为量子中继器提供了极低材料缺陷诱导损耗的新型载体[5]。该成果为未来跨数据中心的分布式量子计算机互联提供了低成本材料路径，将在5至10年维度上影响量子互联网物理层器件选型[5]。

今日影响



1. **全球银行业与云安全系统**：受影响主体为商业银行、跨国金融机构及公有云用户。香港金融管理局发布银行落地工具包[32]，亚马逊云科技密钥管理服务集成ML-KEM后量子算法[39]，标志着抗量子安全防御从前沿探索全面切换至生产系统强制合规实操。下一步紧盯欧美与亚太主要金融监管机构是否出台针对传统公钥密码体系迁移退役的硬性合规时间表[20][32][39]。

2. **容错量子计算硬件路线格局**：受影响主体为超导微波芯片开发商与纠错算法团队。爱丽丝与鲍勃将12比特芯片闲置比特翻转寿命延长至3至4小时，配合两万物理比特破解RSA的资源估算模型，打破了超导必须依赖百万级物理比特表面码的传统预期。下一步紧盯该团队在Helium 2芯片上能否在压制翻转的同时，将双比特门保真度推过容错门槛[8][39]。

3. **机构长线资本与创投资产配置**：受影响主体为全球养老金基金、主权财富管理机构与早期量子硬件企业。英国苏格兰寡妇基金首次将职场养老金配置给本土量子计算创业公司[34]，打破了养老资金对前沿深科技风险投资的流动性壁垒。下一

步紧盯未来两个季度内是否有北美或欧洲大型养老基金跟进设立专项量子成长基金[34]。

4 **国家级高性能算力中心**：受影响主体为国家超算中心。韩国汉江超算全面投用并锁定2027年上半年与量子计算机联合组网，结合56比特中性原子在费米-哈伯德基态对角化上的收敛优势，推动经典高性能计算与量子协同从仿真演练转入生产运行。下一步紧盯2027年上半年韩国首个经典-量子异构混合集群的端到端调度延迟与实际加速表现[16][33]。

07 编辑

编辑点评

量子计算的工程化叙事正在经历一场深层次的校准。在过去数年里，行业往往执着于物理比特总数的线性堆砌，以此作为衡量技术进展的直观标尺；然而，本期所展现的硬件动态清晰地表明，针对底层物理噪声特性的非对称工程与架构效率，其战略价值已超越了纯粹的比特数字。以猫量子比特为代表的硬件自发噪声抑制方案，通过微观量子态的几何设计将比特翻转消除在萌芽阶段，使得破译经典加密算法所需的物理比特规模出现了数量级的收敛。这种从依赖大规模物理比特蛮力纠错向物理原生抗噪与高效纠错协同的转变，预示着量子计算的实用化进程并不一定需要等待数百万物理比特晶圆的成熟，通往容错计算的门槛正在以超出预期的速度被重新定义。

与此相对，全球网络防御的反应齿轮正被迫以相同的加速度高速啮合。从公有云巨头在云端密钥服务中对后量子标准的实质性支持，到区域金融监管机构直接面向商业银行下发落地工具包，安全防线的重塑已经脱离了务虚探讨，进入了与金融机构资产负债表挂钩的工程实操期。当硬件侧的算法推演已经将破解标准加密的时间压至数日以内，针对全球数字基础设施的后量子密码迁移便不再是一场未雨绸缪的演习，而是一场容不得半点迟疑的工程竞速。

参考资料

[1] An A.I. Bubble Or A Data Center Bubble?

[2] Powering up for a pivotal moment

[3] Fault-tolerant quantum error correction for constant-excitation stabilizer codes under coherent noise

[4] Experiment supports theoretical foundation for potentially more error-resistant quantum computing

[5] Single molecules could provide the building blocks for future quantum networks

[6] Ultrathin kagome material opens a route to study unusual quantum states

[7] PhD position in quantum control and nonequilibrium dynamics, Bar-Ilan University, Israel

[8] Alice & Bob Demonstrates Multi-Hour Physical Bit-Flip Suppression on Single-Cat and Helium 2 Processors

[9] Quantum Zeitgeist Weekly Digest

[10] IQST backs events for the next quantum innovators

[11] Researchers Find Nuclear Solution with Quantum Grover Algorithm

[12] Researchers Boost Quantum Sensor Coherence by Tenfold

[13] Researchers Correct Errors Using Rydberg Atom Embeddings

[14] Protocols Robustly Preserve Qubits Against General Environmental Noise Processes

[15] Tübingen Team Preserves Fermion Gap with Weak Interactions

[16] Rydberg atom processors beat random sampling for quantum diagonalization

[17] How noise limits the lifetime of quantum time crystals

[18] QSolid consortium ends five years of quantum hardware and software work

[19] Iceberg Quantum gains Jens Eisert as quantum advisor

[20] ExeQuantum, Bluebik Titans partner on Thailand's quantum security

[21] Quantum Biology Lab's math camp sparks STEM interest in young students

[22] Researchers Find Adaptive Measurements Outperform Static Ones Exponentially

[23] Photon Source May Lower Telecom Detector Costs for QKD

[24] This bull and donkey show interspecies homosexual bonds can run deep

[25] How to tell if a voice recording is AI-generated

[26] Ebola update, AI math scoop and permanent daylight saving time

[27] A Hidden Nanoscopic Effect Is Disrupting Some of the World's Most Sensitive Sensors

[28] Researchers Discover a New Way To Control Magnetism Without Changing a Material's Chemistry

[29] Qtonic Quantum Appoints Former NATO Commander as Head of Operations

[30] FAU Researchers Test Quantum Machine Learning for Lung Cancer Prediction

[31] How Many Qubits Would it Take to Simulate a Holographic Universe?

[32] HKUST and HKMA Launch PQC Toolkit for Banks

[33] South Korea Launches Hangang Supercomputer, Plans Quantum Integration

[34] Scottish Widows Targets Quantum Computing With UK Venture Growth Investments

[35] Nobel Laureate John Martinis to Deliver Quantum Computing Lecture at UWA

[36] Quantcore Welcomes Innovation Minister to Showcase Manufacturing Ambitions

[37] Equal1 Appoints Andrew Flynn as Chief Operating Officer

[38] Chattanooga Accelerator Selects Four Quantum Startups For Commercialization Program

[39] The Qubit Report: November 2, 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。