中国科学报

CHINA SCIENCE DAILY

中国科学院主管　中国科学报社出版　国内统一连续出版物号 CN 11－0084　代号 1－82

扫二维码 看科学报　扫二维码 看科学网

主办：中国科学院　中国工程院　国家自然科学基金委员会　中国科学技术协会

总第 8569 期　2024 年 8 月 14 日　星期三　今日 4 版

新浪微博 http://weibo.com/kexuebao　科学网 www.sciencenet.cn

做科研“不揉沙子”不留遗憾

——记中国科学院大学密码学院平台团队

■本报记者 刘如楠

在今年的中国科学院大学（以下简称国科大）毕业典礼上，荆继武继续作为导师代表为学生拨穗。

荆继武是国科大密码学院院长、教授，还是密码学院平台团队的带头人。成立密码学院的初衷就是为我国密码研究培养高端人才，如今看着越来越多的年轻人从这里毕业，投身密码事业，他感到很欣慰。

密码学院平台团队不常出现在公众视野里，但他们的研究却常常出现于密码学顶级学术期刊和会议论坛。由于科研工作的特殊性，他们并不被太多人所了解，但其科研成果却和每个人的生活息息相关。

近期，国科大密码学院平台团队获得了第五届中国科学院“科苑名匠”（团队）称号。

当教授的吸引力更大

虽然密码学院 2020 年才成立，但国科大密码学研究已有 40 多年历史。20 世纪 80 年代，著名密码学家曾肯成领衔的研究团队在此开创了我国社会力量密码研究的先河，创办了信息安全国家重点实验室。

1990 年，硕士毕业的荆继武加入这一团队。“当时团队里的人并不多，经费也有限，但我们实验室每 5 年至少能拿一个国家科技进步奖二等奖，做到了国内顶尖。”荆继武回忆说。

后来，在中国科学院的统一部署下，荆继武调入 2011 年新成立的信息工程研究所，任总工程师、副所长，后任中国科学院控股有限公司副总经理。

几年过去，荆继武发现这些工作并不适合自己，面对繁重的行政事务，他总觉得心有余而力不足。2019 年前后，荆继武重新回到国科大，成为一名教授。

随着我国数字化的发展，密码成为我国网络信息安全的重要方向，相关产业发展迅猛，亟须培养一批密码专业人才。

2020 年，国科大密码学院成立，荆继武担任院长，带领团队朝着密码理论与算法设计、密码分析与系统测评、数据安全与隐私保护等七大研究方向进军。

国科大密码学院平台团队，后排左二为荆继武。　受访者供图

将黑名单变为白名单

“没有网络安全就没有国家安全。密码是保障网络与信息安全的核心技术和基础支撑。”给学生讲课或作报告时，荆继武总是这样强调。

如今，密码应用遍及经济社会生活的各个方面，如人们熟知的手机通信、网络交易、身份认证中，都有密码的身影。可以说，在当今数字世界，要想保障安全和保护隐私，就离不开密码。

近年来，骚扰欺诈电话无孔不入，已经成为全球性问题。2020 年，我国电信网络诈骗案件涉及财产损失达 353.7 亿元。

对于通信中的欺骗与假冒，目前有两种解决方法，一种是黑名单，通过标记或拉黑识别出“坏人”；一种是白名单，先把所有人拉黑，确定身份后，只让“好人”的电话接入。

“长期以来，大家都采用黑名单的方式，但随着骚扰欺诈电话的增加，标记识别‘坏人’对运营商和用户来说成了一种负担，我们希望采用白名单的方式，建立一套基于密码令牌的可信通信方案。”荆继武说。

举例来说，如果 A 想和 B 通话，首先 A 需要连接自己的运营商网络，再经过中间网络连接 B 的运营商网络，而后呼叫 B 的手机终端。但 B 仅通过手机上显示的号码，无法判断 A 是否可信，因此 B 就有了上当受骗的风险。

而荆继武带领团队开发的这套可信通信方案，相当于在主叫终端 A 和被叫终端 B 之间直接架起一座桥梁，即通过植入软件密码模块实现令牌消息传送服务。

假设 A 事先通过了身份可信体系的验证，如被身份凭证签发中心认定为教授、公务员、网约车司机等，其身份就会顺着这座桥梁到达 B 的手机上，B 的手机自动通过身份凭证查询系统对其进行验证，整个验证时间只需 100 毫秒。

那么，由谁来签发身份凭证呢？荆继武表示，可由政府部门、学校、正规企业等签发。因此，一个人可能有多个身份信息，在通信时根据需要进行选择。

目前，团队与多家单位联合起草的这项网络安全技术标准已通过国家认定，于今年 4 月发布，并将于 11 月 1 日起正式实施。

从孤军奋战到集体作战

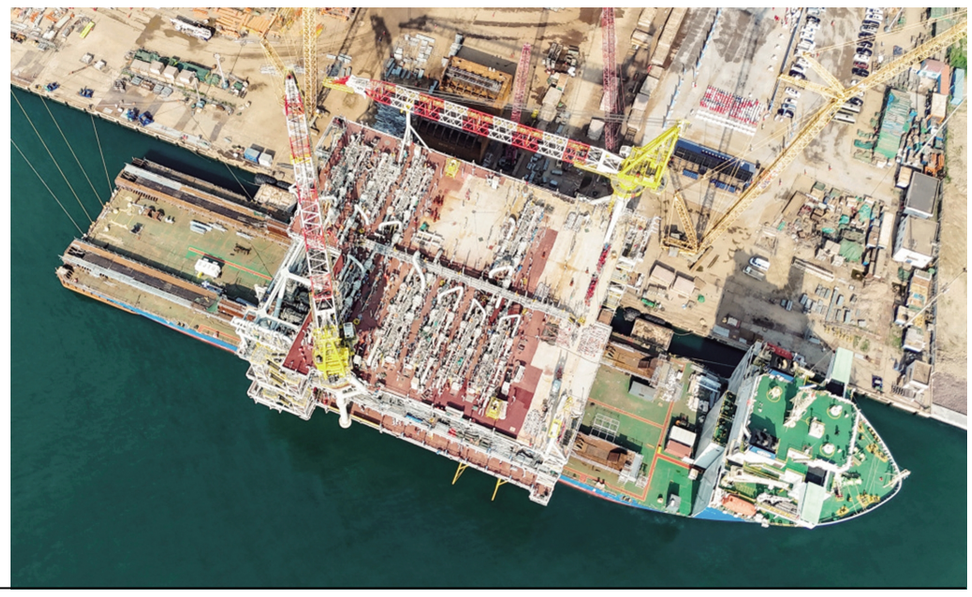
事实上，上述软件密码模块的研发从 2019 年就开始了。那时的荆继武刚刚调回国科大，一边筹建密码学院，一边进行软件密码模块的研发。

“最初的团队就我一个人，真是孤军奋战，但我从没怀疑过密码的重要性。说到底，它是个基础设施，我们开发的软件密码模块，如果只植入 100 人、1000 人的手机是没有效果的，只有推广到所有运营商、让大家都用上才算成功，但这是非常难的。”荆继武说，“我们国家未来的数字经济发展如果缺乏相应的密码保障，就可能是为别人做嫁衣。”

后来，两个人、三个人……团队逐步建立起来。从密码基础理论到密码关键技术研发，这个年轻的团队取得了一系列受国内外认可的成果。

（下转第 2 版）

弘扬科学家精神



8 月 12 日，由中国海油旗下海洋石油工程股份有限公司承建的沙特阿拉伯阿美马赞油气集输平台在山东青岛完工交付，这是我国对外交付的重量最大、集输能力最强的国际海洋油气平台，标志着中国企业国际海洋油气工程建设能力实现新突破。

据悉，此次完工交付的是一座 8 腿海洋油气集输平台，主要负责将开采出的海洋油气汇集并输送到陆地进行处理，每年可以汇集输送原油 2400 万吨，是世界上原油集输能力最强的海洋平台之一。

图片来源：视觉中国

应对气候变化，如何积极稳妥推进“双碳”工作？

■新华社记者 高敬

党的二十届三中全会审议通过的《中共中央关于进一步全面深化改革 推进中国式现代化的决定》提出，协同推进降碳、减污、扩绿、增长，积极应对气候变化。同时，要求构建碳排放统计核算体系、产品碳标识认证制度、产品碳足迹管理体系，健全碳市场交易制度、温室气体自愿减排交易制度，积极稳妥推进碳达峰碳中和。

生态环境部部长黄润秋表示，我国持续实施积极应对气候变化国家战略，将碳达峰碳中和纳入生态文明建设整体布局和经济社会发展全局，协同推进降碳、减污、扩绿、增长，取得显著成效。

全国碳市场是利用市场机制控制温室气体排放、实现碳达峰碳中和目标的重要政策工具，包括强制性的碳排放权交易市场和自愿性的温室气体自愿减排交易市场两个部分。2021 年 7 月，全国碳排放权交易市场启动上线交易，目前纳入发电行业重点排放单位 2257 家，年覆盖二氧化碳排放量约 51 亿吨，成为全球覆盖温室气体排放量最大的碳市场。全国温室气体自愿减排交易市场于 2024 年 1 月正式启动，目前制度框架体系已构建完成，鼓励更广泛的行业企业参与碳减排行动。

黄润秋说，全国碳排放权交易市场已顺利完成两个履约周期建设运行，有效推动企业碳减排责任落实与行业技术进步。

近期发布的《全国碳市场发展报告（2024）》显示，“排碳有成本、减碳有收益”的低碳意识正在形成。碳市场控制温室气体排放、促进能源结构调整的导向作用日益显现。2023 年全国火电碳排放强度（单位火力发电量的二氧化碳排放量）相比 2018 年下降 2.38%，电力碳排放强度（单位发电量的二氧化碳排放量）相比 2018 年下降 8.78%。

生态环境部新闻发言人裴晓菲介绍，下一步，将坚持全国碳市场作为控制温室气体排放政策工具的基本定位，持续完善相关配套政策，扩大行业覆盖范围，丰富交易主体和产品，探索推行免费和有偿相结合的配额分配方式，深化碳市场国际交流与合作，着力建设更加有效、更有活力、更具国际影响力的碳市场，助力实现碳达峰碳中和目标。

记者注意到，碳市场之外，当前一系列改革举措也正在持续发力——

国务院办公厅近期印发了《加快构建碳排放双控制度体系工作方案》，有利于科学精准开展评价考核，树立鼓励可再生能源发展、重点控制化石能源消费的鲜明导向，也有利于促进绿色低碳先进技术的研发应用。

从一些具体领域看，《电解铝行业节能降碳专项行动计划》出台，部署大力推进节能降碳改造、实施非化石能源替代、推动产业链协同绿色发展等重点任务；《数据中心绿色低碳发展专项行动计划》印发，聚焦加快数据中心节能降碳改造和用能设备更新；《关于建立碳足迹管理体系的实施方案》紧扣碳达峰碳中和目标任务，分阶段明确碳足迹管理体系的建设目标……

在习近平生态文明思想研究中心副主任俞海看来，积极应对气候变化，推进绿色低碳发展，对于地方和企业而言，在绿色转型中推动发展实现质的有效提升和量的合理增长，将带来巨大的发展新机遇、新空间，不断用生态“含绿量”提升发展“含金量”。

学习贯彻党的二十届三中全会精神

科学家首次实现无漏洞 Hardy 佯谬检验

本报讯（记者王敏）中国科学技术大学教授潘建伟、张强、陈凯等组成的研究团队与南开大学教授陈景灵等合作，通过发展高效率和高保真度的光学量子纠缠态制备与测量系统，成功实现了关闭探测效率漏洞与局域性漏洞的 Hardy 非定域性演示。该研究为量子力学非定域性提供了新证据，并为相关的量子信息应用奠定了基础。近日，相关研究成果以“编辑推荐”的形式发表于《物理评论快报》。

量子力学预言的非定域与经典物理学观念中的定域实在论存在深刻的矛盾，揭示了量子力学与经典物理学的本质不同，因此，对量子力学非定域性的检验一直是物理学的重要研究内容。

在这项研究中，研究团队在理论上进一步发展了 Hardy 约束的 Eberhard 不等式，该不等式允许在探测效率漏洞被关闭且存在噪声的情况下，进行 Hardy 佯谬检验。实验上，研究团队通过优化空间光路参数，产生了可预报探测效率为 82%、保真度为 99.1%的纠缠光子对，成功关闭了探测效率漏洞。此外，研究团队通过精心设计的时空配置，确保了纠缠光子对的产生和观测者的测量选择，测量事件和观测者的测量选择均处于类空间隔，从而关闭了局域性漏洞，首次实现了无漏洞的 Hardy 佯谬检验。

该研究不仅对量子物理基础研究具有重要意义，而且对量子密钥分发、量子随机数认证等量子信息技术的发展具有重要影响。审稿人高度评价了这项工作，认为“实验结果以及检验局域实在性的量化证据令人印象深刻”。

相关论文信息：

https://doi.org/10.1103/PhysRevLett.133.060201

新研究将推动超快闪存技术产业化应用

本报讯（见习记者江庆龄）复旦大学微电子学院教授周鹏和芯片与系统前沿技术研究院研究员刘春森团队合作，在国际上首次实现最大规模 1Kb 纳秒超快闪存阵列集成验证，证明了其超快特性可延伸至亚 10 纳米，将推动超快颠覆性闪存技术的产业化应用。8 月 12 日，相关研究成果发表于《自然－电子学》。

随着人工智能的飞速发展，用户对高速非易失存储技术的需求日益迫切。然而，主流非易失闪存的编程速度普遍在百微秒级，无法支撑人工智能的应用需求。研究团队前期发现，二维半导体结构能够将闪存的编程速度提升 1000 倍以上，实现纳秒级超快存储闪存。然而，如何实现规模集成并走向实际应用仍极具挑战性。

在此基础上，研究团队开发了超界面工程技术，在规模化二维闪存中实现了具备原子级平整度的异质界面，结合高精度的表征技术，显示集成工艺显著优于国际水平。测试结果表明，二维新机制闪存在 1Kb 存储规模中，纳秒级非易失编程速度下的良率高达 98%，高于国际半导体技术路线图对闪存制造 89.5%的良率要求。

同时，研究团队研发了不依赖先进光刻设备的自对准工艺，并结合原始创新的超快存储叠层电场设计理论，实现了沟道长度为 8 纳米的超快闪存器件。这是当前国际最短沟道闪存器件，突破了硅基闪存物理尺寸极限（约 15 纳米）。在原子级薄层沟道支持下，这一超小尺寸器件具备 20 纳秒超快编程、10 年非易失、10 万次循环寿命和多态存储性能。

相关论文信息：

https://doi.org/10.1038/s41928-024-01229-6

人工孵化“抢救”最濒危的海洋鱼类

寰球眼

本报讯 几个月前，研究人员采取了激进的干预措施，以保护一种仅在澳大利亚某个栖息地存活的鱼类。现在，这种世界上最濒危的海洋鱼类之一——莫吉安鳐鱼有望免于灭绝。

莫吉安鳐鱼只生活在澳大利亚塔斯马尼亚岛西南海岸极其偏远的麦考瑞港。该地区天然的低氧环境使鱼类难以生存，而人类的影响，特别是鲑鱼养殖和水电站大坝导致的河流流量变化，使情况变得更加糟糕。

澳大利亚塔斯马尼亚大学的 Jayson Semmens 表示，虽然没有人知道这些鳐鱼的确切数量，但在 2014 年至 2021 年间，其数量应该减少了一半，现在可能只剩下 1000 多个个体。更令人担忧的是，其中大部分还是未发育成熟的个体。

去年，当这片海域发生海洋热浪时，Semmens 和同事决定采取激进的干预措施，以保护这些鳐鱼。

2023 年 12 月，研究小组收集了 50 个鱼卵，其中一半以上在人工环境中成功孵化。他们还收集了 4 条成年鳐鱼，其中两条在两周内死亡，剩下的两条被分开饲养。

当幸存的雌鱼产卵时，研究小组非常惊喜。Semmens 说，这是因为这种鱼能够储存精子，以便以后使卵子受精。“它平均每 4 天产一次卵，每次产两个。现在我们已经获得了 100 多个卵，而且绝大多数看起来很有生命力。”

为了使人工饲养幼体的遗传多样性最大化，研究小组正在考虑收集其他已经受精的雌鱼以获取鱼卵，然后再将雌鱼放归野外。

然而，同样来自塔斯马尼亚大学的团队成员 David Moreno 表示，人工繁殖只是解决方案的一部分。因此，研究人员还在努力解决麦考瑞港的环境问题，包括开展向水中泵入氧气的试验。

壮大莫吉安鳐鱼队伍的努力无法立竿见影，即使人工繁殖的个体能够立即被放归，也需要 4 到 5 年才能成熟并对种群繁衍作出贡献。

如果人工孵化的努力失败，那么这种濒危鱼类很可能灭绝，“成为现代历史上第一种灭绝的鳐鱼物种”。“因此，人工孵化是非常重要的保障。”Moreno 说。　（文乐乐）

“多物理谱仪关键技术与应用”成果通过专家鉴定

本报讯（记者朱汉斌 通讯员张玮）8 月 12 日，中国散裂中子源“多物理谱仪关键技术与应用”项目科技成果鉴定会在广东东莞举行。由 9 位专家组成的鉴定委员会认为，多物理谱仪填补了国内中子全散射谱仪的空白，综合性能达到同类型谱仪国际先进水平，关键指标国际领先，取得了一批国际一流研究成果。

多物理谱仪是散裂中子源科学中心、东莞理工学院和香港城市大学共同建设的国内首台中子全散射谱仪，也是在国家重大科技基础设施中国散裂中子源上建成的第一台合作谱仪。

据中国科学院高能物理研究所研究员、多物理谱仪负责人殷雯介绍，运行 3 年来，多物理谱仪完成 300 多项用户实验，研究领域包含电池与能源、化学与环境、合金材料、稀土与磁性材料等，为材料科学、物理学、化学、环境等领域提供了结构研究平台，在服务国家重大需求、产业需求与基础研究领域取得了一批重要成果。利用多物理谱仪，科研人员在《自然》等学术期刊上已发表 100 余篇高水平论文。多物理谱仪关键技术指标——样品处单位功率中子通量处于国际同类型谱仪的领先水平，谱仪衍射分辨率和实空间分辨率达到国际同类型谱仪的最好水平。

多物理谱仪在研制过程中，也实现了一系列关键技术突破：首次成功研制国产位置灵敏型氦三管探测器并实现工程应用，性能达到国际先进水平，为后续谱仪探测器自主化研制奠定了坚实基础；自主开发了首个用于中子衍射与对分布函数数据规约的国产软件，构建全散射数据采集与分析技术全链条，实现中子全散射数据规约软件的国产化。