北京信息科学与技术国家研究中心
Beijing National Research Center for Information Science and Technology

简　报

办公室编印　　2023 年 5 月刊　　2023 年 5 月 31 日

本期导读

焦点要闻

北京信息科学与技术国家研究中心系列交叉论坛（第六十期）举办

5 月 11 日晚，北京信息科学与技术国家研究中心系列交叉论坛（第六十期）通过线上会议和直播的形式举办，本次论坛邀请了国际欧亚科学院院士、IEEE/AAIA Fellow、重庆大学人工智能研究院院长宋永端教授作题为“复杂系统快速高精度控制技术及最

宋永端作报告

新进展”的报告。论坛由清华大学信息学院院长、信息国家研究中心主任戴琼海院士和信息学院副院长任天令教授共同主持。信息国家研究中心扩大会成员、团队负责人以及校内外师生 260 余人通过腾讯会议在线参加论坛，累计约 41 万人次通过上直播、新浪、百度等直播平台在线观看。

报告中，宋永端首先介绍了高精度超指数收敛和预设时间收敛控制理论及设计方法，包括：基于状态变换的鲁棒设计，基于时间变换的自适应设计，多输入多输出系统、多智能体系统的控制器设计等。最后，宋永端讨论了预设时间控制、有限时间控制的联系和几个可能的研究方向，以及潜在的应用领域。

提问交流环节，宋永端同与会人员就在有限的算力开销情况下如何处理对复杂系统的追踪，关于预设时间和预设性是否有相通性，以及控制策略和人工智能如何相互借鉴等问题展开了深入讨论与交流。

北京信息科学与技术国家研究中心系列交叉论坛（第六十一期）举办

马建峰作报告

5 月 25 日晚，北京信息科学与技术国家研究中心系列交叉论坛（第六十一期）通过线上会议和直播的形式举办，本次论坛邀请了西安电子科技大学教授、国务院学位委员会“网络空间安全”学科评议组成员、中国电子学会网络空间安全专家委员会副主任委员马建峰作题为“‘云-网-端’协同安全：无线网络安全的新范式”的报告。论坛由清华大学信息学院院长、信息国家研究中心主任戴琼海院士和信息国家研究中心助理研究员郭雨晨共同主持。信息国家研究中心扩大会成员、团队负责人以及校内外师生 140 余人通过腾讯会议在线参加论坛，累计约 40 万人次通过上直播、新浪、百度等直播平台在线观看。

随着无线通信的物联网化与服务化，无线网络与云计算深度融合，产生“云-网-端”协同的服务架构，围绕“云-网-端”协同架构建立体系化安全防护成为无线网络安全的必然趋势，而“云-网-端”协同安全将成为无线网络安全的新范式。报告中，马建峰从“端-端”协同安全、“端-云”协同安全和端系统安全等三个方面分析了无线网络“云-网-端”协同安全的必然性、可行性与困难性，并介绍了团队在无线网络安全方面的最新进展。

提问交流环节，马建峰同与会人员就位置、身份分离的安全协议是否可以进行形式化安全验证，区块链技术在“云-网-端”协同架构的发展中能够起到的作用，“跨域跨网”的具体含义，以及量子计算的安全保护及技术趋势等问题展开

了深入讨论与交流。

◆ 党政工作

信息国家研究中心“锤炼党性修养，全面从严治党”主题活动第一期举办


报告现场

5 月 12 日下午，由信息国研中心党总支主办，信息国研中心教工第二党支部和第四党支部联合承办的“锤炼党性修养，全面从严治党”主题活动第一期在清华大学信息楼（FIT 楼）1 区 312 会议室举办。本期活动邀请了北京市纪委市监委援青干部张振利作题为“反腐倡廉一刻不能停，永远吹冲锋号”的报告。报告由信息国研中心教工第二党支部书记潘长勇主持，信息国研中心党总支、工物系工物研一一党支部共 60 余人参加。

张振利从腐败的概念切入，围绕中央八项规定、六项纪律展开，详细介绍了十八大以来的反腐败历程、腐败的危害与原因，以及腐败预防的策略，并从当前国家纪检监察政策出发，结合教育行业反腐败形势，通过典型案例进行阐述，教育大家心存戒尺、心存敬畏，树立红线意识、底线思维。此外，张振利还结合自身工作实践，讲解了执纪审查工作的体会，强调高校工作者应将监督置于问题未发之时，加强党员群众的自我监督，远离职务犯罪。

最后，张振利分享了《道德经》《泾溪》《论语》中的三句话——“祸莫大于不知足，咎莫大于欲得”“泾溪石险人兢慎，终岁不闻倾覆人。却是平流无石处，时时闻说有沉沦”“乡愿，德之贼也”，希望大家都能以案为戒，在生活、工作中严格要求自己，不断提升理论水平、思想意识、履职能力，真正做到“政治过硬、本领高强”，坚定不移地把全面从严治党、党风廉政建设和反腐败斗争引向深入，锲而不舍营造风清气正的政治生态。

为深入学习贯彻习近平新时代中国特色社会主义思想关于“全面从严治党”的重要论述和精神，信息国家研究中心本年度开展“锤炼党性修养，全面从严治党”系列主题活动，以提升广大师生关于党的自我革命、从严治党的理论水平，深刻领悟我党推进党风廉政建设和反腐败斗争的决心和取得的辉煌成就，锤炼党性修养，筑牢底线意识，提高警戒意识，增长斗争经验，实现强基铸魂的目的。

信息国家研究中心与之江实验室开展“增强使命担当，开拓发展新局”团队共建活动

5 月 15 日，清华大学信息国家研究中心光电智能技术交叉创新群体负责人方璐带领团队到之江实验室光电智能计算研究中心交流，开展“增强使命担当，开拓发展新局”团队共建活动。信息国研中心教工第三党支部书记郑纪元、之江实验室光电智能计算研究中心负责人虞绍良、智能计算研究院联合党支部书记孙世春，以及双方 20 名团队成员参加。

当天上午，双方就科技创新 2030—“新一代人工智能”重大项目中的“片上全光学神经网络计算架构与芯片研究”联合攻关项目，进行了深入细致而富有成效的学术讨论。作为项目首席科学家，方璐带领与会专家总结了项目建设期间取得的主要成果、遇到的问题以及未来解决思路，对重点技术难题进行了透彻分析，制订了有针对性的攻关计划，根据各个课题的执行情况动态灵活地重组科研力量，保障推进项目整体进度，不留短板。通过本次研讨，双方团队组织更加紧密，进一步明确了未来共同合作的思路，优势互补，相得益彰。

当天下午，信息国研中心教工第三党支部与之江实验室智能计算研究院联合党支部就“学习贯彻习近平新时代中国特色社会主义思想”主题开展党支部共建座谈会。会上，双方党支部书记分别介绍了各自支部的基本情况，对学习贯彻习近平新时代中国特色社会主义思想主题教育的重要性进行了深入的探讨。郑纪元表示，习近平新时代中国特色社会主义思想是“两个确立的重要内涵之一”，在二十大开局之年，祖国进入新征程之际，开展主题教育对于凝聚人心，统一思想具有重大意义。孙世春表示，之江实验室非常重视这次主题教育，基层党支部积极开展针对主题教育的践行探索，欢迎信息国家研究中心与之江实验室一同开展学习、交流和研讨。大家纷纷表示，要结合工作实际和职责任务，深入学习习近平总书记关于科技、人才、创新的重要讲话和重要指示批示精神，用习近平新时代中国特色社会主义思想指导实践，努力开拓高质量发展新局面。接着，双方党支部积极围绕有组织科研、人才培养、人才引进、行业发展态势及发展定位等重要问题开展了热烈的讨论，取得了良好的成效。最后，双方对继续保持密切沟通、共建长效合作机制进行了探讨，并达成共识。

信息国研中心教工第二、第四党支部赴河北唐县第三小学开展教育帮扶主题活动

为深入开展学习贯彻习近平新时代中国特色社会主义思想主题教育，积极落实清华大学党委“鼓励支部‘走出去’开展参观实践活动，广泛开展联学共建”的工作要求，5 月 20 日，清华大学信息国研中心教工第二、第四党支部赴革命老区——河北唐县第三小学开展教育帮扶主题活动，与校领导及师生代表进行了深入交流，共同探讨三小的扶贫支教需求、对口帮扶的重点及方式等。

座谈会上，唐县第三小学副校长赵克红简要回顾了自 2017 年 10 月以来开展的对接帮扶活动情况。唐县第三小学校长田晓丽就学校 2015 年建校以来取得的成绩及学校当前教育教学情况作了介绍，并立足第三小学的问题导向、需求导向，提出了下一步帮扶的重点需求。田晓丽表示，希望通过教育帮扶为三小的基础教育注入清华精神和灵魂，推动三小教育向更高质量的方向发展。信息国研中心党总支委员冯建玲、第二党支部书记潘长勇和副书记董炜对三小提出的教育研究支持、教师跟岗培训、学生德育教育、科技素养培养和假期清华研学等需求进行了详细分析和深入交流，双方达成了长期的教育帮扶意向。

座谈会现场

本次活动还举行了图书捐赠仪式，将由信息国研中心党总支发起倡议、教工第二和第四党支部党员积极捐赠的二百多册图书赠予三小学生，为学生们学习科学文化知识提供精神食粮。

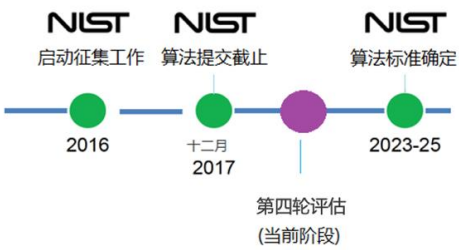
当天途中，党员们还参观了狼牙山五勇士陈列馆和白求恩柯棣华纪念馆。在狼牙山五勇士雕塑前，党员们重温入党誓词，接受了一次生动的党史教育和革命理想信念教育，铮铮誓言，字字铿锵，再次坚定了每一位共产党员积极接受党性熏陶，矢志不渝听党话、跟党走的决心。

清华大学信息国家研究中心秉持“教育服务社会”的理念，对接唐县第三小学开展支教工作多年来，在设备及图书资源、教学内容和教师资源等方面给予了唐县三小大力支持，在机器人编程、科学课教学、教育教学研究等方面积极开展了丰富多彩、富有成效的支教工作，得到了唐县三小师生及校领导的热烈欢迎和高度认可。

◆ 科学研究

王小云团队对 NIST 抗量子密码标准候选算法安全性分析研究

近日，清华大学高等研究院、信息国家研究中心王小云教授团队对美国国家标准与技术研究院（NIST）抗量子密码标准候选算法 BIKE 的安全性进行深入分析，取得了重要进展。研究团队发现了一种新的“聚集性质”，并用它构造出一类弱密钥，不仅使解密失败概率的下界大幅提高，还利用解密失败的先验信



NIST 抗量子密码标准算法征集过程

息设计了一种高效的密钥恢复算法，其攻击复杂度远低于传统攻击方法，也低于128 位的安全参数要求。

BIKE 算法是 NIST 抗量子密码标准化征集中的有力竞争者，其基于编码计算困难问题构造，具有抵抗量子计算攻击、密钥体积小、加解密速度快等优点。但BIKE 算法也有一个缺陷：即使对合法的密文，持有私钥的解密者也有非零的解密失败概率。

之前有学者指出这种解密失败可能泄露私钥信息，BIKE 对此采取了应对措施：通过实验数据外推的方法控制平均解密失败概率，使其为一个极小的可忽略值(<1/2^128)，从而使获取解密失败的复杂度不低于直接攻击的复杂度。然而，这种方法缺乏可靠的理论依据，小规模参数下的规律在大规模参数下可能失效。

研究团队针对这一潜在漏洞展开研究，通过构造弱密钥证明了外推结果的误差，并据此设计相应攻击算法。具体来说，研究团队发现了一种“聚集性质”：当私钥的非零元比较集中时，其对应的解密失败概率显著高于平均值。这一规律在解码算法中有理论模型支持，并且在不同参数下得到了实验验证。

利用具有聚集性质的弱密钥，研究团队设计了多目标密钥恢复攻击：首先对每个目标进行多次解密，若产生解密失败，则认为该目标的私钥为弱密钥，再利用聚集性质的先验信息进行信息集译码恢复私钥。该算法根据是否使用多目标保护（是否允许重用密文）分为两个版本。对于当前未使用多目标保护的 BIKE 算法，攻击复杂度约为 98.77 比特；即使使用了多目标保护，复杂度也只增至 116.61比特，仍低于其安全参数 128 比特。

综上所述，研究团队首次发现了具有聚集性质的弱密钥，并据此重新估计了BIKE 算法的解密失败概率和相应的攻击算法，发现目前 BIKE 密码方案存在安全隐患。

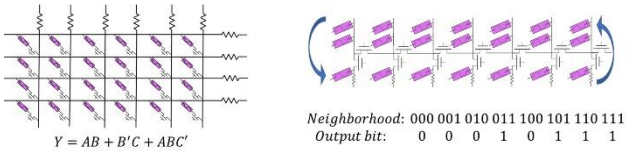
相关研究以“探究 BIKE 的解密失败概率：新的弱密钥和密钥恢复攻击”（Exploring Decryption Failures of BIKE: New Class of Weak Keys and Key Recovery Attacks）为题于 5 月被密码学顶会 2023 年美密会（CRYPTO）接收。

清华大学网络研究院 2022 级博士生王天睿为本文第一作者，清华大学高等研究院副研究员王安宇为本文通讯作者。该研究得到科技部、国家金融业密码应用研究中心、北京信息科学与技术国家研究中心等的支持。

任天令团队提出元胞自动机算法集成至二维晶体管和忆阻器混合电路方案

清华大学集成电路学院、信息国家研究中心任天令教授团队提出将元胞自动机算法集成至二维晶体管和忆阻器混合电路，并基于此架构提出了基于该电路的储备池计算功能。

元胞自动机是一种用于研究复杂系统动力学的有效手段，是作为冯·诺依曼提出的一种普遍存在且大规模并行的计算模型。元胞自动机硬件实现的主要方法包括超大规模集成电路（VLSI）和现场可编程门阵列（FPGA）。VLSI 的电路配置固定，限制了转换不同元胞自动机转换规则的灵活性，而 FPGA 则允许电路重配置，但它导致了更高的硬件成本。因此，元胞自动机的硬件实现需要新设计以确保低成本和高灵活性。近年来，忆阻器电路以其低成本且高性能的特性，成为实现内存计算的理想解决方案。忆阻器阵列的基本操作主要是矩阵乘累加计算或逻辑运算，而元胞自动机的转换规则可以转化为相应的布尔函数，这为忆阻器电路实现元胞自动机转换规则提供了良好平台。



传统存内计算的交叉方案与本研究的循环逻辑运算方案对比

本研究将忆阻器和二维材料晶体管相结合完成电路设计，提出了一种循环逻辑运算方案，从而硬件实现了元胞自动机算法。方案里结合了忆阻器的存储和计算功能，在忆阻器内部循环传输，最大限度地降低了硬件代价。研究中完成了基础元胞自动机 110 号的功能演示。通过把元胞自动机的传递规则分解到忆阻器的存内运算的方式，进行迭代更新。

研究团队同时在循环逻辑运算方案中验证了元胞自动机的多数分类算法和边缘检测算法。尤其对于边缘检测算法而言，基于元胞自动机的循环逻辑运算方案与 FPGA 实现相比，硬件成本可最高降低 79 倍。另外，该研究还提出了基于循环逻辑运算方案的存储库计算方法，能够优化数据搬运过程，进一步结合多层忆阻器阵列，可以最大限度降低储备池计算中的数据搬运消耗。该研究为忆阻器的后续应用探索了新的可能性，指出了可以通过忆阻器阵列低硬件代价的实现元胞自动机算法，在边缘检测计算等领域有潜在的应用价值。

相关成果以“基于元胞自动机的嵌入式忆阻器再循环逻辑内存计算”（Cellular automata imbedded memristor-based recirculated logic in-memory computing）为题，于 5 月 10 日在线发表在国际顶级学术期刊《自然·通讯》（Nature Communications）上。

论文通讯作者为清华大学集成电路学院任天令教授和田禾副教授，清华大学集成电路学院 2021 级博士生刘晏铭、田禾副教授、2018 级博士生吴凡为共同第一作者，其他参加研究的作者包括清华大学集成电路学院 2022 级博士生刘安晗、2020 级未央书院本科生李奕好、2019 级集成电路学院本科生孙昊和阿卜杜拉国王科技大学（KAUST）物理科学与工程系马里奥·兰扎（Mario Lanza）教授。研究得到国家自然科学基金委、科技部重点研发计划、北京市自然基金委、北京信

息科学与技术国家研究中心等的支持。

◆ 交流合作

信息国家研究中心与凌云光、咪咕“大视频 MIGU 融合创新链”合作交流会召开

5 月 22 日下午，清华大学北京信息科学与技术国家研究中心与凌云光技术股份有限公司、咪咕文化科技有限公司在清华大学信息楼（FIT）1 区 415 会议室召开了“大视频 MIGU 融合创新链”项目合作交流会。信息国家研究中心主任戴琼海院士、副主任丁贵广教授、信息国家研究中心灵境智能技术交叉创新群体核心成员陶建华教授，凌云光公司总裁姚毅、高级副总裁杨艺、CTO 赵严，咪咕公司副总经理况铁梅、副总经理向阳、技术服务事业群 VP 周冰等以及信息国家研究中心灵境智能技术交叉创新群体相关人员 20 余人参加了会议。

会议现场

丁贵广致辞，介绍了信息国家研究中心和清华大学信息学院的整体情况，以及灵境智能技术交叉创新群体的成立背景和建设目标。丁贵广表示，信息国家研究中心面向国家重大需求和产业发展需求，组织多学科优势科研力量集中攻关，重视移动信息现代化产业发展，与咪咕和凌云光公司具有很好的前期交流与合作基础，会全力支持大视频 MIGU 融合创新链相关项目的有序推进和发展。

杨艺介绍了大视频 MIGU 融合创新链项目合作背景，表示希望凌云光与信息国家研究中心、咪咕公司共同推进 6G+元宇宙大视频技术变革，构建大科学装置，打造科研创新平台。

况铁梅介绍了咪咕公司的总体情况，元宇宙 MIGU 演进路线图，以及咪咕全力推进的冬奥冰雪元宇宙、鼓浪屿元宇宙、数智竞技等全场景沉浸体验项目，表示内容+科技的融合创新和打造用户全新内容极致体验是未来科技产业合作发展的方向。

会上，戴琼海、陶建华等与两家公司代表深入探讨了合作模式、项目实施方案等议题，初步确定了由科学家引领的元宇宙大科学装置的三方合作机制和基本内容。

“大视频 MIGU 融合创新链”是中国移动打造的“移动信息现代产业链”的重要组成部分，由中国移动咪咕公司担任秘书处单位，旨在通过科学家引领构建 6G+元宇宙大视频科学装置，打造产学研用一体化平台，为实现数字经济创新融

合发展新生态贡献力量。

◆ 重点成果介绍

任天令团队提出基于柔性传感器的可穿戴步态系统

基于柔性传感器的可穿戴步态系统

慢性外侧踝关节不稳（CLAI）通常继发于先前的外侧踝关节韧带损伤，伴随的潜在韧带联合损伤会延长恢复时间并增加严重创伤性关节炎的风险。然而，在 CLAI 病例的诊断中，很难通过常规的身体和放射学检查来区分胫腓联合损伤和孤立的外侧踝关节韧带损伤。为了提高胫腓联合损伤诊断的准确性，信息国家研究中心任天令教授团队提出了一种集成石墨烯柔性传感器的可穿戴步态系统（SISS）。该系统通过测量步行期间的足底压力和香菇智能算法，来自动判断检测是否存在胫腓联合损伤。

该研究包括 27 名踝关节扭伤并接受检查的参与者。测量了双肢八个感兴趣区域的足底压力，并使用关节镜检查检查了韧带联合损伤。测量韧带联合的宽度以评估其严重程度。比较正常和受伤韧带联合患者的足底压力特征。结果表明，logistic 回归预测值大于 0.51 的足底峰值压力比可以较为准确的区分步行过程中伴发的胫腓联合损伤，具有较高灵敏度（80%）和特异性（75%）。测试后发生胫腓联合损伤的概率为 80%。这些发现基本证明了低成本低可穿戴传感器系统在诊断 CLAI 病例中伴发的胫腓联合损伤方面具有较高的有效性，未来有可能应用于临床的相关疾病诊断。

报：清华大学党政领导、信息国家研究中心建设运行管理委员会成员、信息国家研究中心学术委员会成员、信息学院党政联席会成员、信息国家研究中心党政联席会成员
送：相关院系、部处负责人
发：信息国家研究中心各部门负责人

编辑：李琳 审核：丁贵广
联系电话：62792099 E-mail：bnrist@tsinghua.edu.cn