智能控制、博弈及科学工程计算新进展研讨会日程		
10 月 19 日，周一		
09:00-09:10	开幕式	
时间	报告人	报告主题
09:10-10:10	杨天培	Agent 时代的强化学习
10:10-10:40	茶歇	
11:00-11:40	王坤	高精度先进计算进展
	午餐	
14:30-17:30	青年学者论坛	
17:30-19:00	晚餐	
10 月 20 日，周二		
时间	报告人	报告主题
09:30-10:30	宁建廷	Differential Trust: Dynamic Multi-Authority Anonymous Credentials with Epoch-Weighted Updates
10:30-11:00	茶歇	
11:00-12:00	自由讨论	
	午餐	

14:30-17:30	分组讨论	
17:30-19:00	晚餐	
10 月 21 日，周三		
时间	报告人	报告主题
09:30-10:00	许颖	AI 时代的信任基座：区块链驱动数据要素可信流通新范式
10:00-10:30	雷虹	基于区块链的异构 TEE 可信协作：统一认证与安全互联
10:30-11:00	孙林、姚弛	区块链标准化与测试验证赋能可信链网建设
11:00-11:30	郭庆雷	区块链技术服务能源电力的探索与实践
11:30-12:00	李慧琳	面向区块链 RPC 用户的去匿名方法研究
	午餐	
14:30-17:30	分组讨论	
17:30-19:00	晚餐	
10 月 22 日，周四		
时间	报告人	报告主题
09:30-10:30	高莹	隐私集合计算若干关键问题研究
10:30-11:00	茶歇	
11:00-12:00	贾瑞哲	数据篡改攻击下具有二值量测的多智能体系统多时间尺度趋同控制
	午餐	

14:30-15:30	陈森	量测模型不确定性与控制增益不确定性下的自抗扰控制设计与闭环分析
15:30-16:00	茶歇	
16:00-17:00	分组讨论	
17:30-19:00	晚餐	
10 月 23 日，周五		
时间	报告人	报告主题
09:30-10:30	薛文超	非完备数据不确定系统的估计理论及应用
10:30-11:00	茶歇	
11:00-12:00	陈姚	多智能体强化学习训练系统的架构设计与优化思考
	午餐	
14:30-15:30	孙巍	从改进 DDES 构造到螺旋度 SA 修正：高保真反馈机制与压气机/翼身分离流工程验证
15:30-16:00	茶歇	
16:00-17:00	朱华君	基于粘性子单元限制高阶 CPR 方法的高速流动模拟
17:00-17:10	闭幕式	
17:30-19:00	晚餐	

报告摘要

Agent 时代的强化学习

杨天培

随着大语言模型向自主智能体跨越，强化学习正经历深刻的范式转移。本报告以"Agent 时代下的强化学习演进与挑战"为题，分析了从传统深度强化学习向大模型后训练 RL 的转变：不同于传统 DRL 侧重于在封闭环境下通过海量试错学习基础控制逻辑，Agent 时代的 RL 侧重于在已有知识底座上，通过过程奖赏与强化学习算法提升模型的长程规划、思维链推理及自我纠错能力。在智能体协作维度，探讨了从传统多智能体强化学习向基于自然语言通信的 Agent 集群协作演进，以医疗场景为牵引，展示多智能体会诊系统及覆盖诊前分诊、诊中诊断、诊后管理的医疗智能应用体系。最后，报告围绕记忆与长期适应机制、博弈决策从计算智能向认知智能的跃迁，展望智能体技术的未来方向。

高精度先进计算进展

王坤

本报告中我们将介绍基于组件的高精度直接间断有限元计算框架，并介绍该框架的核心算法。主要介绍在大规模异构并行的进展，包括基于本地矩阵的大规模 MPI 并行算法，基于 CPU/GPU 混合异构的隐式并行计算方法以及量超混合计算方法探索进展以及在可压缩流体计算中的应用。

Differential Trust: Dynamic Multi-Authority Anonymous Credentials with Epoch-Weighted Updates

宁建廷

匿名凭证可让用户在不暴露真实身份的前提下完成属性核验。现有多权威匿名凭证方案普遍假定各签发机构拥有对等权限，难以适配权益证明网络、去中心化自治组织等场景下动态变化的差异化信任关系。本报告提出一种动态多权威匿名凭证方案，其通过引入权重分配与时段更新双重机制，用户仅需单次交互即可申领长期有效凭证，当机构权重发生变动时，由签发方以非交互方式完成凭证同步更新，可为人工智能安全管控、跨主体可信数据交互提供底层隐私认证支撑。

AI 时代的信任基座：区块链驱动数据要素可信流通新范式

许颖

数据要素流通是一个多主体、多流程、跨地域、跨机构的复杂协作过程。区块链凭借不可篡改、可追溯、可验证等特性，已成为数据要素流通中重要的信任基础设施。当前，我国区块链在数据要素领域的应用仍以存证为主，初步解决了多方协作中的证据固化和事后追责问题。但随着数据要素市场从原始数据交易逐步转向数据使用权交易、数据服务交易，单纯依靠存证已经难以满足全过程可信协同的需求。本报告聚焦区块链在数据要素流通中的应用，围绕链上链下协同存储、授权过程约束、隐私计算、信用评价体系和跨链互认五类关键问题展开分析，并提出相应解决思路，为区块链与数据要素的融合应用提供参考。

基于区块链的异构 TEE 可信协作：统一认证与安全互联

雷 虹

面向云边端协同与多方计算，Intel SGX/TDX、ARM TrustZone 等异构可信执行环境（TEE）在认证机制、证据格式和信任模型上存在差异，导致不同平台之间难以统一验证可信状态并建立安全协作关系。本项目围绕异构 TEE 可信协作，提出了基于区块链的统一远程认证和互联互通框架。该框架通过分布式协调器处理不同厂商的认证请求，利用区块链、去中心化标识符（DID）和智能合约实现 TEE 身份及认证状态的可信管理与共享，基于 Noise 协议构建异构 TEE 间的安全通信机制。项目实现了对 Intel SGX、鲲鹏 iTrustee、飞腾 TEE 等异构 TEE 平台的适配，显著提升了跨平台认证效率，为构建安全可靠的异构计算环境提供了重要技术支撑。

区块链标准化与测试验证赋能可信链网建设

孙林、姚弛

本报告聚焦区块链标准化与测试验证赋能可信链网建设。针对区块链标准体系建设，提出构建涵盖基础共性、核心技术、数据治理、安全隐私等标准化研究思考，强化标准供给与协同衔接。测试验证围绕标准符合性、功能性能、安全可靠和互操作能力开展，推动标准落地实施。标准引领与测试验证协同，提升链网可信水平，支撑可信链网规范有序发展。

区块链技术服务能源电力的探索与实践

郭庆雷

本报告系统介绍了区块链技术在能源电力领域的核心应用与技术突破。基于“国网链”主从链架构，实现绿电交易、绿电溯源、小时级绿电交易、电碳协同、能源计量及园区碳排放管理等场景的落地应用。关键技术包括区块链轻量可信计量装置、智能合约驱动的绿电消费凭证自动生成、多链协同数据采集与可信存证，以及基于区块链的碳排放核算与可信溯源方法。同时主导发布多项国际标准，构建起覆盖交易、溯源、碳管理全链条的技术标准体系。

面向区块链 RPC 用户的去匿名方法研究

李慧琳

在当前主流的“钱包—RPC 服务—区块链网络”通信模式下，用户通过 RPC 服务访问区块链网络。然而，这一通信模式在提供便捷访问的同时，也带来了潜在的隐私泄露风险。本报告聚焦区块链 RPC 用户的去匿名化问题，介绍一种基于链上链下时间关联的被动去匿名化方法。该方法通过分析加密 RPC 网络流量，利用链上交易确认时间与链下交易状态查询时间之间的关联关系，结合多轮候选地址交集分析，实现用户 IP 地址与链上伪名的关联。相关研究揭示了 RPC 通信模式下潜在的用户匿名性威胁，为区块链匿名性分析与隐私保护机制设计提供了新的研究视角。

隐私集合计算若干关键问题研究

高 莹

隐私集合运算是安全多方计算领域理论成熟、应用需求突出的基础协议，能够保护各方原始集合隐私并完成集合协同计算，可规避跨域协作的明文泄露风险，在联合风控、联合营销、联合监管等场景具备广阔前景。该技术在大规模落地中存在明显局限：多方隐私集合求并依赖公钥运算，可扩展性不足；多方隐私集合求交依托通用混淆电路，开销随参与方数量快速增长；模糊隐私集合求交协议复杂度高，依赖高维下难以满足的假设，难以处理大规模高维数据集。针对上述瓶颈，本报告介绍团队三项成果：基于对称密码原语构造可扩展多方集合求并协议，摆脱公钥依赖，保障多方场景性能稳定；提出双中心零秘密分享机制，将多方求交规约至两方求交，避开通用混淆电路开销，实现四倍以上效率提升；提出模糊映射 Fmap 原语，搭建通用模糊匹配框架，构造严格线性复杂度的汉明距离与 Lp 距离 FPSI 实例。系列构造突破同期已有方案的性能瓶颈，相关思路推动后续相关研究，为跨域大规模安全数据协同提供可行路径。

数据篡改攻击下具有二值量测的多智能体系统多时间尺度趋同控制

贾瑞哲

无人机集群系统的协同运行，依赖于节点之间的信息交换。当通信受到约束、数据呈现低精度特性，甚至还可能遭到数据篡改攻击时，节点如何获得邻居的状态，又如何实现系统的全局状态趋同？本报告围绕这一问题，从量化通信与数据篡改攻击的特点出发，介绍多智能体系统趋同控制研究的背景与思路，重点讨论如何通过噪声和二值量测特性，在有限时间内实现对邻居状态的准确估计，以及如何借助双时间尺度算法设计篡改攻击下的系统状态趋同控制算法。

量测模型不确定性与控制增益不确定性下的自抗扰控制设计与闭环分析

陈 森

非线性不确定性普遍存在于实际系统中，非线性不确定系统的控制设计与分析问题是控制科学与工程中的关键性问题。近年来，自抗扰控制已成功应用于一大类具有非线性不确定性的积分器串联型工业对象，其理论基础也逐步建立。针对具有更复杂非线性的对象，基于自抗扰控制等技术，进一步发展一套高效、高精度的控制方法并给出其理论分析结果，具有重要的意义。本报告考虑了几类常见的非积分串联型非线性不确定系统，例如含有非线性未建模部分的量测模型、控制输入增益系数大范围未知的情况。本报告介绍几种改进的自抗扰控制设计方案，理论分析其能包容的非线性不确定性范围，并分析闭环系统全时域的跟踪效果。

非完备数据不确定系统的估计理论及应用

薛文超

报告针对高速高机动飞行器及集群面临的挑战性控制技术难题凝练基础的科学问题。介绍补偿系统动态、传感量测及执行机构等中多重不确定性的飞行控制方法及理论，并建立了所提出方法实现预期动态性能的理论基础；进一步介绍针对目标搜捕场景的集群协同分布式估计与决策方法，并给出所提出方法的稳定性与最优性理论等；最后，汇报典型飞行器及集群系统的应用研究。

多智能体强化学习训练系统的架构设计与优化思考

陈 姚

多智能体强化学习（MARL）在游戏 AI、自动驾驶、机器人协作等场景中展现出巨大潜力。与传统 RL 不同，MARL 面临智能体间强耦合、环境高度动态、策略非平稳等特性，给计算机系统带来了全新的挑战。本报告从计算机系统视角出发，围绕环境仿真、经验数据管理、分布式通信、异构计算（CPU/GPU）以及资源调度等关键环节，系统分析 MARL 在大规模训练中的性能瓶颈与架构难题，并探讨当前主流框架与硬件趋势下的优化方向，为构建高效可扩展的 MARL 训练系统提供参考。

从改进 DDES 构造到螺旋度 SA 修正：高保真反馈机制与压气机/翼身分离流工程验证

孙 巍

基于粘性子单元限制高阶 CPR 方法的高速流动模拟

朱华君