



中共党员 | 2024 级博士（本科直博）| 大模型多智能体

zhiyao@mail.nwpu.edu.cn/sxswz@foxmail.com | 18640744749

教育背景

本科	2020.09-2024.06	西北工业大学	网络空间安全学院	信息安全专业	GPA: 3.817/4.1 (2/94)
	工科数学分析（上）100	线性代数 90	概率论与数理统计 98	网络安全 94	
	工科数学分析（下）99	数据结构 94	信息安全数学基础 97	密码学 96	
	程序设计基础 100	离散数学 94	计算机组成与系统结构 91	计算机系统基础 91	
博士	2024.09 至今	西北工业大学	网络空间安全学院	网络空间安全专业	
	导师：王震 教授		研究方向：大模型多智能体系统		

获奖情况

- 2024 年 06 月 西北工业大学“优秀毕业生”“百篇优秀本科毕业设计（论文）提名奖”
- 2023 年 10 月 西北工业大学“优秀大学生”“学业先进个人”
- 2023 年 08 月 全国大学生信息安全竞赛作品赛国家级三等奖
- 2022 年 10 月 国家奖学金
- 2022 年 10 月 校一等奖学金
- 2022 年 10 月 西北工业大学“优秀大学生”“学业先进个人”“创新创业先进个人”
- 2022 年 08 月 全国大学生信息安全竞赛创新实践能力赛国家级三等奖（pwn 方向）
- 2022 年 08 月 第六届“强网杯”全国网络安全挑战赛 强网先锋
- 2022 年 05 月 西北工业大学“十佳团支书”
- 2022 年 05 月 西北工业大学数学建模竞赛二等奖、西北工业大学数学竞赛二等奖
- 2022 年 03 月 西北工业大学网络空间安全挑战赛三等奖、“工大抗疫”杯 CTF 竞赛三等奖
- 2022 年 03 月 西北工业大学第二十届“三航杯”科技竞赛三等奖
- 2021 年 10 月 校一等奖学金
- 2021 年 10 月 西北工业大学“优秀大学生”“崇德先进个人”“学业先进个人”“体育先进个人”
- 2021 年 05 月 西北工业大学 C 语言程序设计实验技能竞赛一等奖

科研成果

- S. Ren, **Z. Cui**, R. Song, Z. Wang, S. Hu, Emergence of Social Norms in Generative Agent Societies: Principles and Architecture, Proceedings of the 33rd International Joint Conference on Artificial Intelligence (IJCAI), 2024. (CCF-A, 共同一作)
- M. Qi, **Z. Cui** and G. Liang, TBVPAKE: An efficient and provably secure verifier-based PAKE protocol for IoT applications, Journal of Systems Architecture (2023), DOI: 10.1016/j.sysarc.2023.102874. (JCR Q1, 导师一作本人二作)
- H. Zhang, **Z. Cui**, Q. Zhang, S. Hu, Multi-LLM-Agents Debate-Performance, Efficiency, and Scaling Challenges. The Fourth Blogpost Track at ICLR 2025. (第二作者, 本文为部分结果, 完整结果见 <https://arxiv.org/abs/2502.08788>)

实习经历

- 2024 年 08 月 20 日-2025 年 02 月 14 日 上海人工智能实验室 大模型实习生 大模型多智能体系统研究
- 2022 年 07 月 01 日-2022 年 08 月 31 日 华为西安研究所 软件开发实习生 物联网设备底层软件开发

项目经历

1.大模型多智能体辩论框架统一评测与性能提升研究2024 年 9 月至 2025 年 1 月

部分成果发表于 ICLR 2025 blogpost Track（第二作者）

完整成果见 <https://arxiv.org/abs/2502.08788>

本文对多种代表性的 MAD 方法进行了系统评估，发现即使在推理过程中消耗了额外计算资源，MAD 方法无法稳定地优于简单的单智能体基线方法（如 CoT 和 Self-Consistency）。进一步分析表明，模型的异质性可以显著提升 MAD 框架的性能，因此本文提出 Heter-MAD 方法，使单个 LLM 智能体能够访问来自不同基础模型的输出，从而增强现有 MAD 框架的表现。

2.基于大语言模型的社会规范涌现研究2023 年 9 月至 2024 年 5 月

相关成果发表于 IJCAI 2024（共同一作）

代码：<https://github.com/sxswz213/CRSEC>

本文提出了一套基于 LLM 的具有理解和遵守社会规范功能的生成式智能体架构 CRSEC，使生成式智能体一定程度上具有自主识别、学习、适应、服从或反对以及传播社会规范的能力，从而解决多智能体社会中的各类社会冲突，提升生成式智能体行为的类人性与可靠性。本文在 Park 等人设计的 Smallville 沙盒环境（斯坦福虚拟小镇环境）中验证了架构性能。

3.基于国密 SM2 数字签名算法的双因子身份认证系统2022 年 4 月至 2023 年 8 月

相关成果发表于 JCR Q1 期刊（导师一作本人二作）

全国大学生信息安全竞赛作品赛国家级三等奖（负责人）

国家级大学生创新创业训练计划项目良好结题（项目负责人）

本项目利用智能手机作为令牌，基于国密 SM2 数字签名算法实现了一套双因子身份认证系统。系统在用户的本地终端生成 SM2 公私钥对，并在本地实现双因子认证保护，利用数字签名算法实现 Challenge-Response 机制对用户进行身份认证。为实现安全传输，针对物联网应用设计了一种安全、高效、轻量级的 PAKE 协议 TBVPAKE，能够抵御离线字典攻击和服务器泄露攻击，并支持前向保密。在常用的椭圆曲线群上实例化此协议，结果表明 TBVPAKE 具有更好的计算效率。

专业及英语技能

编程能力：能够使用 Python（主要）、C/C++、go、HTML 等在 Windows 和 Linux 系统平台进行开发。

英语能力：IELTS：6.0，CET-6：459，CET-4:567，能进行英文文献阅读与翻译，具备基本英文写作能力。

学生工作

2025 年 2 月至今	西北工业大学网络空间安全学院研究生第一团支部书记
2022 年 9 月-2023 年 8 月	西北工业大学学生信息安全协会团支部书记 并协管西北工业大学网络空间安全大学生创新实践基地
2021 年 9 月-2024 年 6 月	西北工业大学网络空间安全学院 SC012001 班团支部书记
2021 年 9 月-2022 年 8 月	西北工业大学学生武术协会团支部书记
2020 年 9 月-2021 年 8 月	西北工业大学网络空间安全学院 DL062048 班团支部书记

其他

爱好与特长：跆拳道黑带、电子琴十级