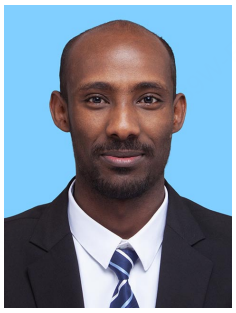
马济

Jifar Wakuma Ayana
地址：北京科技大学
邮箱：wakexayanajifar01@gmail.com
电话：186-1880715782
LinkedIn：https://www.linkedin.com/in/jifar-ayana-a9ab561aa/



研究领域

- **隐私保护、密码学**、安全计算
- 机器学习隐私、大语言模型隐私、人工智能隐私
- 联邦学习、区块链
- **AI Agent**、云安全、Web 安全、网络安全

研究与项目经历

2022 年至今

- **基于 Transformer 模型的快速安全推理研究**（硕士学位论文，2022 年至今）
- **辅助私有域的智能无人机决策过程解释与可追溯性**（导师项目，2023 年至今）
- **基础模型推理的高性能多方安全计算：聚焦非线性激活函数**（导师项目，2024 年至今）
- **EthioLLM-Oromo**：为扩展埃塞俄比亚 AI 访问而微调的 LLAMA 7B 模型（中国埃塞俄比亚学者项目，2024 年至今）
- **基于 AI Agent 的自主网络安全防御系统**：开发用于实时威胁检测和响应的 AI 驱动代理（导师项目，2024 年至今）
- **云安全隐私保护框架**：设计基于同态加密的云端数据处理解决方案（北京科技大学项目，2023-2024 年）
- **Web 安全漏洞检测工具**：利用机器学习检测 Web 应用程序中的 SQL 注入和 XSS 攻击（个人项目，2023 年）
- **网络安全流量分析**：使用深度学习模型分析网络流量以识别潜在的 DDoS 攻击（导师项目，2022-2023 年）
- **使用生成对抗网络进行图像超分辨率重建**（本科毕业论文，2018-2022 年）
- **开发 Android 应用程序**，在电子科技大学利用 Java 进行 UI 开发的研讨会（2020-2021 年）
- **构建英汉词典**（Python 与人工智能项目）

教育背景

- **北京科技大学，2022 年至今**
  - 信息与通信工程硕士学位
  - GPA：3.5/4.0，平均分：84.7

- **电子科技大学，2018-2022 年**
  - 计算机科学与技术学士学位
  - GPA：3.69/4.0，平均分：84.97

技能

编程语言	Python, C/C++, Java, Matlab, Go, Solidity
框架	Pytorch, Tensorflow, Secretflow-Secure MPC 框架, Tensor Flow Federated, SEAL Library, PySyft, Truffle Suite
语言	英语（专业熟练），汉语（工作熟练），阿姆哈拉语（母语），奥罗莫语（母语）

待出版论文

1. **PrivLLMSwarm**：首个将大型语言模型与无人机群安全集成的方案（已提交至 IEEE 物联网期刊）
2. **GuardLLM**：安全且准确的 Transformer 推理

荣誉与奖项

- 重庆市政府市长奖学金丝绸之路高级研讨会，重庆邮电大学，2022 年
- 北京科技大学校长奖学金，2022 年至今（全额奖学金）
- 电子科技大学学术成就奖，2018-2020 年（二等奖）
- 埃塞俄比亚教育部 Betre-科学奖学金，2018 年

课外活动与证书

- 清华大学创新与创业项目结业证书，2022 年
- 重庆邮电大学高级 ICT 技能研讨会结业证书，2022 年
- 电子科技大学冬季运动会男子排球一等奖，2021 年