

梁正涛

AI 研究 · LLM / RAG · 开源工程

17684269881

1392452425a@gmail.com

2003.05 · 共青团员

github.com/Serennity007

个人主页

教育背景

北京理工大学（985/211/双一流）

2026.09 - 2029.06（预计）

人工智能学院 · 智能科学与技术 · 学术硕士

- 研究方向：智能体协作研究、智能体安全、多模态大模型安全研究

贵州大学（211 & 双一流）

2022.09 - 2026.06

计算机科学与技术学院 · 人工智能专业 · 学士

- 加权平均成绩排名：1/69 · 综合测评排名：1/69 · GPA：4.14/5
- 雅思：6.5 · 英语六级：572 · 具备扎实的学术英文阅读、写作及沟通能力

科研经历

科研成果：KSEM（CCF-C）会议论文已中稿。

面向司法判决的认知智能构建：大语言模型导向的知识-经验双轨融合与推理机制（负责人）

2025.03 - 至今 · 法律 AI · 知识与先例检索

- 主导知识与先例双轨检索架构，结合案件事实、法律条文与相似判决进行预测
- 使用 7B LLM 提取犯罪构成要素，驱动 Milvus 先例检索与法律条文匹配
- 将多源检索结果组织为模型上下文，调用 30B LLM 生成综合判决预测

多模态大语言模型的安全对齐方法研究

2026 至今 · 硕士阶段研究课题

- 硕士阶段研究课题，围绕多模态大模型的安全对齐方法展开

政务服务智能问答系统（负责人）

2024.03 - 至今

- 设计后端与大模型集成方案，使用 LangChain 编排 LLM API 与核心问答逻辑
- 基于 FastAPI 搭建原型后端，并通过 Web 界面验证问答流程

代表开源项目

AI 选股与量化投研工具链 · 41 Stars

GitHub 41 Stars · 8 Forks（截至 2026-10-24）

- 原创实现：开发 30 个 Agent Skills、32 个 Python 脚本，实现 23 套投资方法参考框架，覆盖筛选、评分、共识与含成本回溯。
- 工程细节：对齐年报期与 TTM 估值字段，标记缺失数据；记录调仓成本、逐期持仓与输入哈希。
- 可复核验证：40 项本地测试通过（2026-10-25）；2026-10-24 使用 AKShare 1.19.3 完成 600519 的 2021-2025 年报取数与筛选，提供离线复现入口。

Python · AKShare · pandas · Agent Skills · [项目案例](#) · [运行演示](#) · [验证记录](#) · [真实取数记录](#)

GhostTrack · 网络信息查询与域名检查

在原有 GhostTrack 查询工具上扩展域名批量检查，新增 DNS、证书有效期和 HTTP 状态检查、快照对比及结果导出。实现任务队列的暂停、取消与失败重试。

Python · Tkinter · Android · Web · [GhostTrack](#)

XSS Audit Desktop · 源码静态扫描工具

在 xss-audit 审计方法基础上新增源码静态扫描引擎，实现 JS/TS/Python 的规则匹配、AST 流向分析和源码行定位。支持本地目录及公开 GitHub 仓库扫描、人工复核与 HTML/SARIF 导出。
Python · Tree-sitter · Tkinter · SARIF · [xss-audit-desktop](#)

AI Agent 会话分析 CLI

解析多种编码 Agent 的本地会话日志，汇总 token 用量、成本估算与工具调用；提供终端报告与 JSON 输出。
Node.js · JavaScript · CLI · [agent-trace](#)

财经 RSS 阅读器与摘要工具

基于 Qiaomu AI RSS 改造 Obsidian 财经阅读器，内置 45 个源，支持文章转 Markdown、日记摘录与 OPML；另开发飞书摘要工具，支持消息去重、分组卡片和分批发送。
TypeScript · Obsidian API · Node.js · [飞书摘要工具](#)

实习经历

学而思（好未来旗下）

贵阳
教育科技有限公司 · 教育产品开发

- 参与教育产品开发，运用 AI 技术改善教学体验

彩虹集团

成都
科技企业 · 软件开发

- 参与企业级项目开发，熟悉工业界软件工程规范与实践

国际交流

新加坡国立大学 (NUS)

2023.07 - 2023.08

- 入选贵州省"千人海外留学计划"并获专项资助（计算机学院重点推荐）
- 深度研修前沿人工智能理论与计算金融建模核心课程
- 独立完成"手写数字识别"项目，核心成员全程英语协作完成金融工程项目
- 两项课程均以优异表现结业

荣誉奖项

华为 ICT 大赛 · 国家一等奖
国家奖学金
贵州省三好学生

技术栈

编程语言

Python TypeScript JavaScript Go Rust LaTeX

AI / ML

PyTorch Transformers LangChain OpenAI API RAG MCP

前端

React Next.js Vue Tailwind CSS

后端 & DevOps

FastAPI Node.js PostgreSQL Docker GitHub Actions