

项目进展情况：

- (1) RAG模型理解与应用
- (2) 搜索结果优化
- (3) RAG模型性能优化
- (4) 隐私保护与信息安全（输入输出检测）
- (5) 试验评估线上RAG状态

已取得成果：

1. 后台
2. 前端
3. 安全方面：原型系统

下一阶段主要任务与时间安排：

1. 本地知识库，召回，切片（本地大模型、中文）
2. 隐私保护，信息安全（越狱数据集）
3. 搜索结果优化（关键字，拓展：关联搜索、相关搜索）
4. 实验评估
5. graphRAG
6. 论文/专利

存在的问题和困难以及解决思路：

1. 在线知识库与目前最新技术结合
2. 长文本上下文
3. 安全方面