余方超

泰丰大街 168 号 – 安徽淮南，232000 – 中国 ·

chao3236@gmail.com · (+86) 181-588-98402 · chaoge123456.github.io

教育背景

安徽理工大学, 淮南 2018 年 9 月 – 至今

在读硕士研究生 计算机科学与技术, 预计 2021 年 6 月毕业

安徽理工大学, 淮南 2014 年 9 月 – 2018 年 6 月

学士 信息安全

研究兴趣

AI 安全：人工智能系统中常见的安全和数据隐私问题

计算机视觉：设计先进机器学习算法，并应用于计算机视觉领域

工作/研究

绿盟科技, 合肥 2018 年 3 月 – 2018 年 5 月

实习 网络安全工程师

负责维护企业内网安全和漏洞挖掘

方贤进教授课题组, 淮南 2018 年 9 月 – 至今

研究生 网络与信息安全课题组

专注于人工智能安全与隐私保护相关课题研究

论文发表

[1] X. Fang, **F. Yu**, G. Yang, and Y. Qu, "Regression analysis with differential privacy preserving," *IEEE Access*, vol. 7, pp. 129 353–129 361, 2019. (SCI)

[2] **F. Yu**, L. Wang, X. Fang, and Z. Youwen, "The defense of adversarial example with conditional generation adversarial networks," *Security and Communication Networks*, 2020. (CCF C 类, Accepted)

[3] X. Fang, **F. Yu**, G. Yang, and Z. Youwen, "A novel deep learning algorithm with differential privacy preservation," *Chinese Journal of Electronics*, 2020. (Under Review)

[4] **F. Yu**, X. Fang, Z. Youwen, G. Yang, and L. Wang, "Enhanced differential privacy defense mechanism in deep learning," *CCF 8st China Conference on Data Mining (CCDM)*, 2020. (Accepted，并被推荐至《南京大学学报（自然科学版)》)

学术报告

" 人工智能安全与隐私", *第一届安徽省计算机大会 (AHCC)*, 淮南, 中国, 11/2019

参与项目

网络与信息安全课题组项目 2018 年 9 月 – 2019 年 6 月

差分隐私高维数据发布理论与方法研究, 国家自然科学基金 (61572034)

- 差分隐私相关理论研究
- 差分隐私在回归分析中的应用

网络与信息安全课题组项目 2019 年 6 月 – 2020 年 3 月

大数据全生命周期的隐私保护安全关键技术与系统研究，安徽省科技重大专项 (18030901025)

- 人工智能系统中的数据安全风险以及常见的攻击方式
- 差分隐私与深度学习

个人博客项目 2018 年 7 月

Web, Linux 个人项目

GITHUB+HEXO 个人博客（chaoge123456.github.io）

- 博客主题美化
- 添加订阅、提交搜索引擎

CET 自动查分项目 2018 年 8 月

Web, Python 个人项目

忘记准考证号时，可提供自动查分服务（chaoge123456.github.io）

- 利用机器学习模型自动识别验证码、查询 CET 分数
- 添加代理池和多线程机制

实验室内网建设和私有云项目 2018 年 12 月

Linux, Network 个人项目

实验室内网环境建设，搭建 openstack 私有云平台

- 实验室内网建设、服务器环境配置
- openstack 私有云平台部署、hadoop 集群部署

树莓派应用项目 2019 年 3 月

Linux 个人项目

基于树莓派平台构建的各类应用

- 私有云盘（实现文件上传、下载、存储）
- 智能路由（基于 openwrt）
- 智能控制（利用红外线模块实现对智能家居的控制）

IT 技能

- 编程: C，Python，Web，Shell，Markdown，Git，Docker
- 平台: 熟练掌握 Windows 和 Linux 系统的相关操作，具有独立解决问题的能力
- 学术：Office，Latex，Endnote，Matlab，文献阅读和搜索
- 英语：通过 CET6, 正在准备雅思考试
- 机器学习：熟悉机器学习的基础知识以及常用的 python 库（numpy、pandas、sklearn、pytorch 等）