陈光科

Phone: (+86) 191-2170-2230 Email: chengk@shanghaitech.edu.cn
Website: https://guangkechen.site Date of Birth: 1996-11

教育经历

上海科技大学 2019 年 9 月 - 2024 年 6 月
计算机科学与技术 博士研究生 导师: 宋富

- GPA: 专业 3.91 / 4.0 总 3.8 / 4.0

华南理工大学，广州 2015 年 9 月 - 2019 年 7 月
信息工程 学士；本科

- GPA: 3.77 / 4.0

研究兴趣

可信人工智能：人工智能安全及隐私；人工智能生成内容 (AIGC) 治理

论文

第一作者：

1. Who is Real Bob? Adversarial Attacks on Speaker Recognition Systems
   Guangke Chen, Sen Chen, Lingling Fan, Xiaoning Du, Fu Song, Yang Liu
   In Proc. of the 42nd IEEE Symposium on Security and Privacy (Oakland, S&P), 2021
   CCF-A, EI, Accept rate: 115/952=12%
   Highlight: citation>170; top-4 conference for computer security

2. QFA2SR: Query-Free Adversarial Transfer to Speaker Recognition Systems
   Guanke Chen, Yedi Zhang, Zhe Zhao, Fu Song
   In Proc. of the 32nd USENIX Security Symposium, 2023
   CCF-A
   Highlight: highly effective against commercial APIs and voice assistants; vulnerability disclosure received bounty award; top-4 conference for computer security

3. SLMIA-SR: Speaker-Level Membership Inference Attacks against Speaker Recognition Systems
   Guanke Chen, Yedi Zhang, Fu Song
   To appear in Proc. of the 31st Network and Distributed System Security (NDSS) Symposium, 2024
   CCF-A, Accept rate: 34/483=7% (Fall Cycle; acceptance w/o shepherding or major revisions)
   Highlight: top-4 conference for computer security

4. Towards Understanding and Mitigating Audio Adversarial Examples for Speaker Recognition
   Guangke Chen, Zhe Zhao, Fu Song, Sen Chen, Lingling Fan, Feng Wang, Jiashui Wang
   IEEE Transactions on Dependable and Secure Computing (TDSC)
   CCF-A, JCR-Q1, IF=7.3, EI

5. AS2T: Arbitrary source-to-target adversarial attack on speaker recognition systems
   Guangke Chen, Zhe Zhao, Fu Song, Sen Chen, Lingling Fan, Yang Liu
   IEEE Transactions on Dependable and Secure Computing (TDSC)
   CCF-A, JCR-Q1, IF=7.3, EI

其他：

1. Attack as Defense: Characterizing Adversarial Examples using Robustness
   Zhe Zhao, **Guangke Chen**, Jingyi Wang, Yiwei Yang, Fu Song, Jun Sun

In Proc. of the 30th International Symposium on Software Testing and Analysis (ISSTA), 2021
CCF-A, EI, Accept rate: 51/219=23%

2. Attack as Detection: Using Adversarial Attack Methods to Detect Abnormal Examples
Zhe Zhao, **Guangke Chen**, Tong Liu, Taishan Li, Fu Song, Jingyi Wang, Jun Sun
ACM Transactions on Software Engineering and Methodology (TOSEM)
CCF-A, CAS-JCR-Q1, EI

3. BDD4BNN: A BDD-based Quantitative Analysis Framework for Binarized Neural Networks
Yedi Zhang, Zhe Zhao, **Guangke Chen**, Fu Song, Taolue Chen
In Proc. of the 33rd International Conference on Computer-Aided Verification (CAV), 2021
CCF-A, Accept rate: 79/290=27%

4. QVIP: An ILP-based Formal Verification Approach for Quantized Neural Networks
Yedi Zhang, Zhe Zhao, **Guangke Chen**, Fu Song, Min Zhang, Taulue Chen, Jun Sun
Proc. of 37th IEEE/ACM International Conference on Automated Software Engineering (ASE), 2022.
CCF-A, EI

5. Precise Quantitative Analysis of Binarized Neural Networks: A BDD-based Approach
Yedi Zhang, Zhe Zhao, **Guangke Chen**, Fu Song, Taolue Chen
ACM Transactions on Software Engineering and Methodology (TOSEM)
CCF-A, CAS-JCR-Q1, EI

6. ACROBAT: Accelerating CEGAR-based Neural Network Verification via Adversarial Attacks
Zhe Zhao, Yedi Zhang, **Guangke Chen**, Fu Song, Taolue Chen and Jiaxiang Liu
In Proc. of the 29th Static Analysis Symposium (SAS), 2022
CCF-B

专利

授权：

1. 一种基于深度学习的非常态语音区别方法
奉小慧, **陈光科**, 贺前华, 巫小兰, 李艳雄
发明专利授权，授权号：CN108766419B，授权日期：2020.10.27

2. 脉率变异性和睡眠质量融合的心理压力监测方法及装置
邢晓芬, **陈光科**, 江士尧, 林立韬, 陈东华
发明专利授权，授权号：CN107874750B，授权日期：2020.01.10

实审/公开/受理：

1. 基于语音声学特征压缩的语音对抗样本防御方法及应用
宋富，**陈光科**，赵哲
发明专利实质审查，公开号：CN114242083A，公开日期：2022-03-25

2. 一种基于攻击成本的对抗样本检测方法
宋富，赵哲，**陈光科**
发明专利实质审查，公开号：CN112381152A，公开日期：2021.02.19

3. 一种基于样本鲁棒性差异的对抗样本检测方法
宋富，赵哲，**陈光科**
发明专利实质审查，公开号：CN112381150A，公开日期：2021.02.19

项目课题

- 蚂蚁集团学术科研项目 C 类（探索项目）
语音 AI 系统对抗攻防基准平台

经费：30 万人民币
时间：2022.09 - 2023.09
排名：3/12 (学生：1/10); 主要完成人

教学

- 助教：
  - CS240 算法设计与分析, 上海科技大学, 2020-2021 年度春学期
  选课人数: 超过 220 名本科生或研究生
  工作: 设计日常作业题和期末项目题、批改作业和测验、答疑、监考和沟通主讲教师和学生等
- 主讲：
  - 上海科技大学 S3L 课题组周度课程研讨会
  本人主讲涉及课程: Decision Procedure; Interpretable AI; Fuzzing; Computer Systems Security

学术报告

- 学术会议：
  - IEEE S&P, 2021.05, 线上
  Who is Real Bob? Adversarial Attacks on Speaker Recognition Systems
  - USENIX Security, 2023.08, 美国加州阿纳海姆
  QFA2SR: Query-Free Adversarial Transfer to Speaker Recognition Systems
- 论坛:
  - **(Invited)** 可信人工智能研讨会（上海）, 上海, 2023.07
  声纹识别系统语音对抗样本鲁棒性攻击及防御
  - 可信赖人工智能高峰论坛 - 智能软件安全分析，南京, 2021.07
  Who is Real Bob? Adversarial Attacks on Speaker Recognition Systems
- 上海科技大学 S3L 课题组周度论文阅读小组（全英）：
  个人共对 11 篇论文进行汇报

学生指导

- 本科生毕业论文: 2021 年/2023 年, 上海科技大学, 两名本科生均成功通过论文答辩
- 短期科研能力训练项目: 2020-2022 年, 共指导四名上海科技大学本科生
- 项目负责人：国家级大学生创新创业训练项目, 2018 年, 华南理工大学，优秀结题

服务活动

- 国际学术会议程序委员会委员:
  - the 15th International Workshop on Cyberspace Security and Artificial Intelligence (CAI 2023)
  - the 24th International Conference on Information and Communications Security (ICICS 2022)
  - the 23rd International Conference on Information and Communications Security (ICICS 2021)
- 国际学术会议 Artifact Evaluation 程序委员会委员:
  - NDSS 2024
  - USENIX Security 2023
- 学术会议分会主席 (主持人):
  - Session 8 (Attack and Vulnerability Analysis II) of ICICS 2022
- 审稿人:
  - IEEE Transactions on Information Forensics & Security (TIFS)
  - Springer Cybersecurity

- ACM Transactions on Privacy and Security
- the 24th ISCA INTERSPEECH Conference (InterSpeech 2023)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- the 34th IEEE International Symposium on Software Reliability Engineering (ISSRE 2023)
- the 21st International Symposium on Automated Technology for Verification and Analysis (ATVA 2023)
- the 33rd IEEE International Symposium on Software Reliability Engineering (ISSRE 2022)
- IEEE Transactions on Reliability (TR)

- 学校及学院服务:
  - 上海科技大学研究生招生宣讲华南理工大学站驻地高校主要联络人和对接人, 2018
  - 上海科技大学研究生招生夏令营活动研究中心参观组组长, 2023.06/2023.07
  - 上海科技大学本科生新生英语能力测试志愿者, 2022
  - 上海科技大学毕业典礼志愿者, 2023.06
  - 上海科技大学信息科学与技术学院毕业典礼志愿者, 2023.06

荣誉奖项

- 2023 | 博士研究生国家奖学金 (前 2%) | 上海科技大学
- 2023 | 上海科技大学博士生国际培养计划国外访学奖学金 | 上海科技大学
- 2020, 2022, 2023 | 三好学生 | 上海科技大学
- 2020 | 硕士研究生国家奖学金 (前 2%) | 上海科技大学
- 2018 | 校级十大三好学生提名（共 20 名）| 华南理工大学
- 2018 | 本科生国家奖学金 | 华南理工大学
- 2018 | 国家级大学生创新创业训练项目优秀结题（项目负责人）| 华南理工大学
- 2017 | 国家励志奖学金 | 华南理工大学
- 2016 | 企业奖学金 | 华南理工大学
- 2016, 2017, 2018 | 三好学生 | 华南理工大学