陈光科 男 | 26岁 | 博士

联系电话：19121702230

邮箱：chengk@shanghaitech.edu.cn

学科领域：计算机科学与技术

所在城市：上海

研究方向：网络空间安全

教育背景

上海科技大学 | 博士 | 计算机科学与技术 2019-09-2024-07

华南理工大学 | 本科 | 信息工程 2015-09-2019-07

论文情况

- **概述：目前博士在读共发表论文11篇，SCI收录4篇 （均为JCR Q1分区及中科院1区），CCF推荐A类10篇，B类1篇；第一作者论文5篇，包含3篇计算机安全四大顶级会议（其中一篇引用大于145）及2篇计算机安全旗舰期刊**

[1] Who is Real Bob? Adversarial Attacks on Speaker Recognition Systems. Guangke Chen, Sen Chen, Lingling Fan, Xiaoning Du, Fu Song, Yang Liu. In Proceedings of the 42nd IEEE Symposium on Security and Privacy (IEEE S&P 2021, Oakland 2021). 第一作者；计算机安全四大顶级会议之一；CCF推荐A类会议；EI收录；会议录用率：12%；论文引用：大于145

[2] QFA2SR: Query-Free Adversarial Transfer to Speaker Recognition Systems. Guanke Chen, Yedi Zhang, Zhe Zhao, Fu Song. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 2023). 第一作者；计算机安全四大顶级会议之一；CCF推荐A类会议；系统安全漏洞汇报获得厂商致谢以及现金奖励。

[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. 第一作者；计算机安全四大顶级会议之一；CCF推荐A类会议。

[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 (IEEE TDSC). 第一作者；计算机安全旗舰期刊；SCI收录，JCR分区Q1，中科院1区，影响因子：7.3；CCF推荐A类期刊；EI收录

[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 (IEEE TDSC). 第一作者；计算机安全旗舰期刊；SCI收录，JCR分区Q1，中科院1区，影响因子：7.3；CCF推荐A类期刊；EI收录

[6] 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 (ACM TOSEM; under minor revision). 第二作者；软件工程旗舰期刊；SCI收录，JCR分区Q1，中科院1区；CCF推荐A类期刊；EI收录

[7] Attack as Defense: Characterizing Adversarial Examples using Robustness. Zhe Zhao, Guangke Chen, Jingyi Wang, Yiwei Yang, Fu Song, Jun Sun. In Proceedings of the 30th International Symposium on Software Testing and Analysis (ISSTA 2021). 第二作者；软件工程顶级会议之一；CCF推荐A类会议；EI收录。

[8] 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 (ACM TOSEM). 第三作者；软件工程旗舰期刊；SCI收录，JCR分区Q1，中科院1区；CCF推荐A类期刊；EI收录

[9] QVIP: An ILP-based Formal Verification Approach for Quantized Neural Networks. Yedi Zhang, Zhe Zhao, Guan

gke Chen, Fu Song, Min Zhang, Taulue Chen, Jun Sun. In Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering (ASE 2022). 第三作者；软件工程顶级会议之一；CCF推荐A类会议；EI收录。
[10] BDD4BNN: A BDD-based Quantitative Analysis Framework for Binarized Neural Networks. Yedi Zhang, Zhe Zhao, Guangke Chen, Fu Song, Taolue Chen. In Proceedings of the 33rd International Conference on Computer-Aided Verification (CAV 2021). 第三作者；形式化验证顶级会议；CCF推荐A类会议。
[11] ACROBAT: Accelerating CEGAR-based Neural Network Verification via Adversarial Attacks. Zhe Zhao, Yedi Zhang, Guangke Chen, Fu Song, Taolue Chen and Jiaxiang Liu. In Proceeding of the 29th Static Analysis Symposium (SAS 2022). 第三作者；形式化验证顶级会议；CCF推荐B类会议。

工作经历

- **上海科技大学** | **助教** 2021-03-2021-07

  上海科技大学信息科学与技术学院CS240算法设计与分析课程助教

项目情况

- **概述：参与蚂蚁集团学术科研项目C类（探索项目）一项**

1. 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，30万，2022.9-2023.9，唯一学生参与人，在研

专利专著

- **概述：授权发明专利2项，发明专利实质审查3项**

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

实质审查：
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

获奖情况

- 2023 | 上海科技大学博士生国际培养计划国外访学奖学金
- 2022 | 上海科技大学三好学生
- 2020 | 硕士研究生国家奖学金
- 2020 | 上海科技大学三好学生
- 2018 | 国家级大学生创新创业训练项目优秀结题（项目负责人）
- 2018 | 华南理工大学十大三好学生标兵提名奖（全校共10人）

- 2018 | 本科生国家奖学金
- 2018 | 华南理工大学三好学生
- 2017 | 国家励志奖学金
- 2017 | 华南理工大学三好学生
- 2016 | 华南理工大学三好学生
- 2016 | 澳门校友奖学金

其他说明

学术服务情况：

【1】国际学术会议程序委员会委员：the 23rd International Conference on Information and Communications Security (ICICS 2021), the 24th International Conference on Information and Communications Security (ICICS 2022)，the 15th International Workshop on Cyberspace Security and Artificial Intelligence (CAI 2023)

【2】国际学术会议Artifacts Evaluation委员会委员：the 32nd USENIX Security Symposium 2023 (USENIX Security 2023)， the 32nd Network and Distributed System Security Symposium (NDSS 2024)

【3】国际学术会议审稿人：InterSpeech 2023, ISSRE 2022/2023, AVTA 2023

【4】国际期刊审稿人：IEEE TDSC， IEEE TIFS, IEEE TR, ACM TOPS, Springer Cybersecurity

【5】国际学术会议Session chair: ICICS 2022