

GUANGKE CHEN

Phone: (+86) 191-2170-2230

Email: chengk@shanghaitech.edu.cn

Website: guangkechen.site

Education Experiences

ShanghaiTech University, Shanghai, China

Sept. 2019 - June 2024 (expected)

Computer Science Ph.D student Supervisor: Fu Song

– GPA: major 3.91 / 4.0 total 3.8 / 4.0

– Selected Courses: Convex Optimization (A+) Deep Learning (A) Cryptography (A) Algorithm Design and Analysis (A) Theory of Computation (A+)

South China University of Technology (SCUT), Guangzhou, China

Sept. 2015 - June 2019

Information Engineering Bachelor

– GPA: 3.77 / 4.0

– Thesis: Adversarial Attack against Speaker Recognition System

Honors and Awards

- 2022 | Merit Student | ShanghaiTech University
- 2020 | National Scholarship for Graduate | ShanghaiTech University
- 2020 | Merit Student | ShanghaiTech University
- 2018 | Nomination of the top ten merit students (20 students in total) | SCUT
- 2018 | National Scholarship | SCUT
- 2018 | Outstanding conclusion of national College Students' Innovation and Entrepreneurship Training Program (project leader) | SCUT
- 2017 | National Encouragement scholarship | SCUT
- 2016 | Enterprise Scholarship | SCUT
- 2016, 2017, 2018 | Merit Student | SCUT

Research Interests

trustworthy artificial intelligence (e.g., voiceprint recognition and speech recognition)

Security and privacy of multimedia (e.g., speech)

Publications

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>145; 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, CAS-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, CAS-JCR-Q1, IF=7.3, EI
6. 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%
7. 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
Under minor revision of ACM Transactions on Software Engineering and Methodology (TOSEM)
CCF-A, CAS-JCR-Q1, EI
8. 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%
9. QVIP: An ILP-based Formal Verification Approach for Quantized Neural Networks
Yedi Zhang, Zhe Zhao, **Guangke Chen**, Fu Song, Min Zhang, Taolue Chen, Jun Sun
Proc. of 37th IEEE/ACM International Conference on Automated Software Engineering (ASE), 2022.
CCF-A, EI
10. 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
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 Proc. of the 29th Static Analysis Symposium (SAS), 2022
CCF-B

Patents

1. A deep learning-based approach for distinguishing abnormal speech
Xiaohui Feng, **Guangke Chen**, Qianhua He, Xiaolan Wu, Yanxiong Li | CN108766419B
Granted
2. Method and apparatus for monitoring psychological stress with integration of pulse rate variability and

sleep quality

Xiaofen Xing, **Guangke Chen**, Shiyao Jiang, Litao Lin, Donghua Chen | CN107874750B
Granted

3. Audio adversarial example defense based on speech acoustic feature compression
Fu Song, **Guangke Chen**, Zhe Zhao | CN114242083A
Pending
4. Adversarial example detection method based on robustness differences
Fu Song, Zhe Zhao, **Guangke Chen** | CN112381150A
Pending
5. Adversarial example detection method based on attack cost
Fu Song, Zhe Zhao, **Guangke Chen** | CN112381152A
Pending

Services

- Program Committee Member:
 - 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)
- Artifact Evaluation Committee Member:
 - NDSS' 24
 - USENIX Security 2023
- Session Chair:
 - Session 8 (Attack and Vulnerability Analysis II) of ICICS 2022
- Reviewer:
 - 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)
- Sub-reviewer:
 - IEEE Transactions on Reliability (TR)
- Teaching Assistant:
 - CS240 Algorithm Design and Analysis, ShanghaiTech University, 2020-2021, Spring Semester

Skills and Qualifications

- Languages: native in Chinese, proficient in English (CET-6: 520)
- Programming: Python, Matlab, Java, C/C++, \LaTeX
- Techniques:
 - Machine learning (NumPy, Scipy, Scikit-learn)
 - Deep learning (PyTorch, TensorFlow)
 - Speech processing (Kaldi, torchaudio, SpeechBrain)