YUHAO MAO

D-INFK, ETH Zurich, Switzerland
+41 764428769 | e: myh821746176@outlook.com

EDUCATION

ETH Zurich — Zurich, Switzerland
Doctorate in Computer Science (ongoing) — September 2023 – Now

ETH Zurich — Zurich, Switzerland
Master in Computer Science (GPA: 5.91/6.0) — September 2021 – July 2023

Zhejiang University — Hangzhou, China
Bachelor in Applied Mathematics & Finance (GPA: 3.93/4.0) — September 2017 – July 2021
- Chu Kochen Honors College (top 5% admitted annually)

Massachusetts Institute of Technology — Boston, USA
Machine Learning Summer Program (Score: 96/100) — July 2019

PUBLICATION

- Chenhao Sun*, **Yuhao Mao***, Mark Niklas Müller, Martin Vechev, *Average Certified Radius is a Poor Metric for Randomized Smoothing*, The Forty-Second International Conference on Machine Learning (ICML'25).
- **Yuhao Mao**, Stefan Balauca, Martin Vechev, *CTBENCH: A Library and Benchmark for Certified Training*, The Forty-Second International Conference on Machine Learning (ICML'25).
- Stefan Balauca, Mark Niklas Müller, **Yuhao Mao**, Maximilian Baader, Marc Fischer, Martin Vechev, *Gaussian Loss Smoothing Enables Certified Training with Tight Convex Relaxations*, Transactions on Machine Learning Research 07/2025 (TMLR'25).
- Chenhao Chu, **Yuhao Mao**, Hua Wang, *Transfer Learning Assisted Fast Design Migration Over Technology Nodes: A Study on Transformer Matching Network*, IEEE MTT-S International Microwave Symposium 2024 (IMS'24).
- **Yuhao Mao**, Mark Niklas Müller, Marc Fischer, Martin Vechev, *Understanding Certified Training with Interval Bound Propagation*, The Twelfth International Conference on Learning Representations (ICLR'24).
- Max Baader*, Mark Niklas Müller*, **Yuhao Mao**, Martin Vechev, *Expressivity of ReLU-Networks under Convex Relaxations*, The Twelfth International Conference on Learning Representations (ICLR'24).
- **Yuhao Mao**, Mark Niklas Müller, Marc Fischer, Martin Vechev, *Connecting Certified and Adversarial Training*, The Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS'23).
- Yuyou Gan*, **Yuhao Mao***, Xuhong Zhang, Shouling Ji, Yuwen Pu, Meng Han, Jianwei Yin, Ting Wang, ``*Is your explanation stable?'': A Robustness Evaluation Framework for Feature Attribution*, ACM SIGSAC Conference on Computer and Communications Security 2022 (CCS'22).
- **Yuhao Mao**, Chong Fu, Saizhuo Wang, Shouling Ji, Xuhong Zhang, Zhenguang Liu, Jun Zhou, Alex X. Liu, Raheem Beyah, Ting Wang, *Transfer Attack Revisited: A Large-Scale Empirical Study in Real Computer Vision Settings*, IEEE Symposium on Security & Privacy 2022 (SP'22).

JOB EXPERIENCE

Higgs Asset — Hangzhou, China
Internship in Quant Research — March 2021-July 2021

ADDITIONAL RESEARCH EXPERIENCE

The Helmholtz Center for Information Security — Saarland, Germany
Research Assistant to Dr. Yang Zhang — July 2020 – June 2021
Topic: Injection and Detection of Neural Backdoors

ADDITIONAL INFORMATION

Additional Professional and Extracurricular Experiences
- Oral presentation as one of four specially invited students at the *4th Annual Honors International Faculty Institute Workshop* at Texas Christian University, USA, in June 2019.
- ~200 hours volunteer as an undergraduate.
- Teach math at elementary schools (Olympics) and high schools (Calculus).

Interests
- Individual Quant research and investments.
- Member of the CKC College volleyball team from 2017 to 2020.
- Travel, think, and have fun.

Computer and Language Skills

- Expert: Python, LaTeX, C, R, Markdown, MATLAB
- Experienced: bash, HTML, SQL, Alloy
- Mandarin (native), English (Proficient), Ningbo Dialect of Wu Chinese (native)