

YUHAO MAO

+41 764428769 | myh821746176@outlook.com | algebraloveme.github.io/about

EDUCATION

ETH Zurich

Doctorate in Computer Science (ongoing)

Zurich, Switzerland

September 2023 – Now

ETH Zurich

Master in Computer Science (GPA: 5.91/6.0)

Major: Machine Intelligence; Minor: Theoretical Computer Science

Zurich, Switzerland

September 2021 – July 2023

Zhejiang University

Bachelor in Applied Mathematics & Bachelor in Finance (GPA: 3.93/4.0)

Chu Kochen Honors College (top 5%)

Hangzhou, China

September 2017 – July 2021

PUBLICATION

TRUSTWORTHY AI

- **Yuhao Mao***, Yani Zhang*, Martin Vechev, *On the Expressiveness of Multi-Neuron Convex Relaxations*, The Fourteenth International Conference on Learning Representations (ICLR'26).
- Chenhao Sun, **Yuhao Mao**, Martin Vechev, *Dual Randomized Smoothing: Beyond Global Noise Variance*, The Fourteenth International Conference on Learning Representations (ICLR'26).
- 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 Balaucă, Martin Vechev, *CTBENCH: A Library and Benchmark for Certified Training*, The Forty-Second International Conference on Machine Learning (ICML'25).
- Stefan Balaucă, 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 (TMLR'25).
- **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).

AI FOR SCIENCE

- 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).

EDGE AI

- Shengpu Wang, **Yuhao Mao**, Yani Zhang, Martin Vechev, *Learning Compact Boolean Networks*, preprint.

JOB EXPERIENCE

Higgs Asset

Quantitative Researcher Intern

Hangzhou, China

March 2021-July 2021

ADDITIONAL INFORMATION

Experiences

- ~200 hours volunteer as an undergraduate.
- Teach math at elementary schools (Olympics) and high schools (Calculus).

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)
- Actively building PIRA (<https://github.com/AlgebraLoveme/PIRA>), a research-specialized agent.