

TINGHAO XIE

✉ thx@princeton.edu · 🔗 <https://tinghaoxie.com> · 🌐 vtu81

🎓 EDUCATION

Princeton University, Princeton, United States of America 08/2022 – Present

Ph.D. student, Electrical Computer Engineering (ECE)

Zhejiang University, Zhejiang, China 09/2018 – 06/2022

B.E., Computer Science and Technology (CS)

- **GPA**: 3.99/4.00 (92.07/100)
- **Rank**: 1st/186

University of Oxford, Oxford, United Kingdom 10/2021 – 12/2021

Visiting Student, Computer Science

- **GPA**: 4.00/4.00
- **Courses**: *Machine Learning, Computational Learning Theory*

💡 RESEARCH INTERESTS

- Secure, Robust, Reliable and Fair AI Systems; Adversarial Robustness, Certified Robustness
- Explainable and Interpretable AI; Out-Of-Distribution Generalization; Causality

📖 PUBLICATIONS & MANUSCRIPTS

Revisiting the Assumption of Latent Separability for Backdoor Defenses 🔗, 📄, </>

Xiangyu Qi*, **Tinghao Xie***, Yiming Li, Saeed Mahloujifar, Prateek Mittal

Preprint

Fight Poison with Poison: Detecting Backdoor Poison Samples via Decoupling Benign Correlations 🔗, 📄, </>

Xiangyu Qi, **Tinghao Xie**, Saeed Mahloujifar, Prateek Mittal

Preprint

Towards Practical Deployment-Stage Backdoor Attack on Deep Neural Networks 🔗, 📄, </>

Xiangyu Qi*, **Tinghao Xie***, Ruizhe Pan, Jifeng Zhu, Yong Yang and Kai Bu

CVPR 2022 (Oral)

A Handbook for Deep Learning with their Piecemeal Intuitions from Causal Theory 🔗, 📄

Tinghao Xie

Manuscript

Ensemble of Narrow DNN Chains 🔗, 📄, </>

Tinghao Xie

Manuscript

👥 RESEARCH EXPERIENCES

Adaptive Backdoor Attack and Active Backdoor Defense

01/2022 – Present

Advisors: Prof. **Prateek Mittal** (Princeton University), Prof. **Shouling Ji** (Zhejiang University)

Co-worker: Ph.D. Student **Xiangyu Qi** (Princeton University)

- Adaptive backdoor attack circumventing defenses based on latent separability (ICLR 2023, in submission).
- Active backdoor poison sample detector via decoupling benign correlations (to submit to Usenix 2023).

Subnet Replacement Attack (SRA): A Graybox Backdoor Attack

09/2021 – 11/2021

Advisors: Principal Researcher *Jifeng Zhu* (Tencent), Prof. *Kai Bu* (Zhejiang University)

Co-worker: Ph.d. Student *Xiangyu Qi* (Princeton University)

Collaborator with **Zhuque Lab, Tencent, China**

- Deployment-Stage Backdoor Attack on Deep Neural Networks (CVPR 22 Oral).

Backdoor Restoration and Certification

05/2021 – 12/2021

Advisor: Prof. *Ting Wang* (Pennsylvania State University)

Remote Intern at **ALPS Lab, Pennsylvania State University, United States**

- Computing and tightening backdoor certification bounds ([📝blog](#)).
- Faithfully restoring potential backdoor triggers ([📝blog](#)).

Enchecap: An Encrypted Heterogeneous Calculation Protocol

04/2020 – 05/2021

Advisor: Prof. *Jianhai Chen* (Zhejiang University)

Undergraduate Intern at **INCAS Lab, Zhejiang University, China**

- Designed *</>Enchecap*, a protocol securing heterogeneous computation for transmission and host memory.
- Implemented the protocol into a library, with 38% computational overhead and 19% overall overhead.

♥ HONORS AND AWARDS

Outstanding Graduate Thesis	06/2022
Champion of Zhejiang University Bodybuilding Competition (70kg Level)	05/2022
Elite Liu Yongling Scholarship (1/802)	2020 – 2021
Tencent Scholarship (5/802)	2020 – 2021
The 2nd Class Prize in ASC20-21 Student Supercomputer Challenge	01/2021
Narada Scholarship (1/372)	2019 – 2020
Champion of Zhejiang University DFM Hip-hop Crew Battle	2019

⚙ SKILLS

- **Programming:** C/C++, Python, JavaScript, CUDA, Verilog, Shell, MATLAB, ActionScript, HTML.
- **Software:** \LaTeX , Vivado, Adobe {Photoshop, Premiere Pro, After Effects, Audition}.
- **Languages known:** English(fluent), Chinese(native), Cantonese(native).
- **TOEFL iBT:** Total 110/120, Reading 29/30, Listening 30/30, Speaking 26/30, Writing 25/30.
- **GRE General Test:** Verbal 154/170, Quantitative 170/170, Analytical Writing 3.5/6.
- **Hobbies:** Dance(Hip-hop, House, etc.), Power Lifting, Fitness, Swimming, Basketball, Billiards.