Tinghao Xie

vtu@zju.edu.cn · https://tinghaoxie.com · vtu81

Education

Zhejiang University (ZJU), Zhejiang, China 09/2018 – 06/2022 (expected)

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

- **GPA**: 3.99/4.00 (92.13/100)
- **Rank**: 1st/186[1]

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

Visiting Student, Computer Science

- **Courses and Grades**: *Machine Learning* (A+), *Computational Learning Theory* (A)

Research Interests

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

Publications or Pre-prints

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

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

arXiv e-print, under review at CVPR 2022

Research Experience

</> Subnet Replacement Attack (SRA): A Graybox Backdoor Attack 09/2021 – 11/2021

Advisor: 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**

- Implemented, tuned and evaluated SRA on various models and datasets to show its universal compatibility.
- Extended SRA to different trigger types (patch, blend, perturb, Instagram filters, etc.).
- Made SRA more practical for realizing physical triggers under complex real-world environments.
- Finished and submitted the paper *Towards Practical Deployment-Stage Backdoor Attack on Deep Neural Networks* as the co-first author to CVPR'22.

Backdoor Restoration and Certification 05/2021 – Present

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

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

</> **Backdoor Certification** (ongoing)

- Implemented tools for certifying the (non-)existence of perturbation backdoors based on LiRPA.
- Formed an optimizable method to tighten the backdoor certification bounds.

</> **Faithful Backdoor Restoration**

- Proposed an effective way for faithful trigger restoration.

</> Enchecap: An Encrypted Heterogeneous Calculation Protocol 04/2020 – 05/2021

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

Undergraduate Intern at **Intelligent Computing and System Lab, Zhejiang University, China**

- Designed *Enchecap*, a protocol securing heteorogeneous computaion for transmission and host memory.
- Implemented the protocol into a library, with 38% computational overhead and 19% overall overhead.

[1] Official rank for exam-free postgraduate entrance considering both overall and major GPA, while another official rank by overall 5.0-scale GPA is 2nd/186. 186 is the number of students majoring in Computer Science and Technology, not counting in students (about 90) from Chu Kochen Mixed Class.

Selected Projects

A Handbook for Deep Learning with their Piecemeal Intuitions from Causal Theory 12/2021

- Studied causal theory and its connections with machine learning.
- Surveyed recent works including causality as an intuition for improving deep learning.
- Classified them by: OOD Generalization; Generation; Robustness, interpretability, and fairness.

ENDC: Ensemble of Narrow DNN Chains 12/2021

- Proposed ENDC, a lightweight ensemble framework for classification with narrow DNNs as base classifiers.
- Compared ENDC with traditional ML models and showed its supiriority in smaller size and higher accuracy.

</> NaiveVQA: A Visual Question Answering model 07/2021

- Reimplemented *Show, Ask, Attend, and Answer: A Strong Baseline for Visual Question Answering*.
- Translated the PyTorch implemented model into a MindSpore (a new AI framework) implementation.
- Trained and achieved 40.6% overall accuracy on a small VQA 2.0 sub-dataset provided by the course.

Other Course Projects 2020 – 2021

- </> **RCC**: A Remarkable/Retarded C-like Compiler
- </> **Tron**: A 3D Graphic Engine Based on WebGL & a Flying Game Demo
- **AI for Reversi**: An AI for the game Reversi based on the MCTS method.
- **Facial Recognition**: A PCA model for recognizing and restoring human faces.
- **Robot in Maze**: A maze-walking AI (implemented with DFS, reinforcement Q-Learning, Deep Q-Learning).
- </> **MiniSQL**: A Single-user Database Management System (SQL Engine).
- </> **HWMS**: A Homework Management System.
- **Approximate Algorithms for the Texture Packing Problem**: A course research project.
- **A MIPS CPU on FPGA**: A SoC on Xilinx FPGA and a pixel game in MIPS assembly.

Campus Activities

Member, **SuperComputing Team (ZJUSCT)** 09/2019 – 02/2021

- Obtained the certificate of competency of Nvidia Accelerated Computing Basics – CUDA C/C++.
- Won the 2nd class prize in ASC 2020-2021, where I optimized QuEST on GPU by 4.7%.

Member, **DFM Street Dance Crew** 03/2019 –- 09/2019

- Attended the 2019 Danqing Dance Competition and 2020 New Year's Eve Showcase.
- Won the final battle of the DFM Hip-hop crew as the champion.

Member, **Summer Social Practice Group** 06/2019 –- 09/2019

- Recorded the social practice in Guangzhou and produced a short documentary.

Volunteer, **Zhejiang University** 09/2018 – 11/2018

- Helped sorting and recycling garbage in the dormitory buildings.

Honors and Awards

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

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, Breaking, and Choreography), Swimming, Basketball, Fitness, Billiards.

Latest update date: 01/15/2022