

# 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:** 1/186<sup>1</sup>

**University of Oxford**, Oxford, United Kingdom

10/2021 – 06/2022 (expected)

Visiting Student, Computer Science

- **Courses taking:** Computational Learning Theory, Machine Learning

## 💡 RESEARCH INTERESTS

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

## 📖 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 a co-first author to CVPR'22.

**Backdoor Restoration and Certification**

05/2021 – Present

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

*Remote Intern* in **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* in **Intelligent Computing and System Lab, Zhejiang University, China**

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


<sup>1</sup>Official rank for exam-free postgraduate entrance, while another official rank by overall 5-point GPA is 2/186. 186 is the number of students majoring in Computer Science and Technology, not counting in students from Chu Kochen Mixed Class.

## SELECTED PROJECTS

---


- </> **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
- </> **RCC: A Remarkable/Retarded C-like Compiler** 05/2021 – 06/2021
- Defined a simplified C EBNF and built up the frontend with FLEX and BISON
  - Built up an abstract syntax tree for code generation in C++
  - Implemented Intermediate Code generation (*type binding, structure and array*) with LLVM as the backend
- </> **Tron: A 3D Graphic Engine Based on WebGL & a Flying Game Demo** 12/2020 – 01/2021
- Completed voxel, material and texture expression modules
  - Wrote GLSL shader codes involving fogs and the animated sky
  - Implemented cross-platform interaction and front-end web pages

## **Other Course Projects** 2020 – 2021

- **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
- **Garbage Classification:** a ResNet model for garbage images classification, achieving 91.5% accuracy
- **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
-  **Research on the Texture Packing Problem**
- **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 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 Danqing Dance Competition 2019 and New Year's Eve Showcase 2020
  - Won the championship in a battle of DFM Hiphop crew
- 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:**  $\text{\LaTeX}$ , 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(Hiphop, House, Breaking, Choreography), Swimming, Basketball, Fitness, Billiards