Ye Yuan

School of Cyber Science and Engineering, Huazhong University of Science and Technology (CS Department, HUST)
+86-138-1068-2605 maxwell_yuan@hust.edu.cn maxwell.yuanyeh@gmail.com YEthYuan.github.io

Education

University of California, Santa Barbara **Sep. 2022 – Jun. 2023 (expected)**
Huazhong University of Science and Technology **Sep. 2019 – Jul. 2023 (expected)**
Bachelor of Engineering in Cyberspace Security *GPA: 3.96/4.0 (Rank 7/253)*

- TOEFL: 103 (R28+L27+S23+W25)
- GRE: 323 (V156+Q167)+AW4.0

Relevant Coursework and Grades

- Calculus: 99/100
- Linear Algebra: 96/100
- Prob Thry&Stat: 97/100
- Discrete Math: 97/100
- AI: 90/100
- Cryptography: 99/100
- Programming(C): 94/100
- Comp Arch: 97/100

Publications

Zeyuan Yin, ***Ye Yuan****, Panfeng Guo, Pan Zhou*, "Backdoor Attacks on Federated Learning with Lottery Ticket Hypothesis." ArXiv abs/2109.10512 (2021) [PDF] [Code]

- Read papers about DNNs' robustness and several types of data poisoning methods, reproduce the code to implement BadNet & Complex Trigger attack toward the LotteryFL system.
- Led the exploration of the essence of backdoor embedding as well as the intrinsic mechanism of backdoor learning, write codes with pytorch to demonstrate our ideas.
- Conducted extensive experiments to validate our ideas, used Pandas lib. to collect and organize experimental data, used Matplotlib & Seaborn libs. to visualize data.
- Helped to design the algorithm of Backdoor Defense on LotteryFL.
- Wrote the paper with partners by LaTeX through the Overleaf platform.

Research Experience

Research Intern, advised by Prof. Yingyan Lin **Feb. 2022 – At present**
Efficient and Intelligent Computing (EIC) Lab, ECE Department, Rice University *Houston, TX*

- Learned the principle and categories of the Transfer Learning, mastered the principle and application of the feature-representation transfer under the Inductive Transfer Learning domain, and reproduced the code
- Investigated the state-of-the-art research on the model robustness, including the Robust Scratch Tickets and the Adversarial Contrastive Learning, and play with their codes
- Proposed the idea and project motivation to study the efficient & robust transfer learning, and planned the detailed experimental arrangement and the time schedule under the guidance of Prof. Lin and Dr. Yonggan Fu
- Implemented the tickets transfer and the downstream finetune by programming with pytorch based on the Robust Scratch Tickets code, and conducted the relevant experiments

Research Assistant, supervised by Prof. Pan Zhou **Nov. 2020 – Oct. 2021**
Big Data Intelligence and Information Security Lab, National Laboratory for Optoelectronics, HUST *Wuhan, PRC*

- Learned the principle and method of the adversarial machine learning, analyzed the lack of robustness in DNNs, and studied the codes to enhance the robustness of the model by using adversarial training
- Studied the methods of model compression, including pruning, quantization and knowledge distillation, focused on the Lottery Ticket Hypothesis, which was at the forefront of pruning techniques, and reproduced the code with pytorch
- Investigated the Early Bird Ticket, one of the SOTA researches on the Lottery Ticket Hypothesis, and researched on its security issues, including the robustness toward adversarial attacks and backdoor attacks
- Researched on the principle and application of the backdoor attack toward DNNs, wrote the code with pytorch to implement the data poisoning, and conducted attack experiments on the Early Bird Ticket algorithm
- Participated in conducting the backdoor attack on LotteryFL, and designing the algorithm to improve the robustness toward backdoor attacks of the Federated Learning system

Research Intern, advised by Prof. Zhangyang Wang **Oct. 2021 – Jan. 2022**
Visual Informatics Group (VITA Laboratory), ECE Department, University of Texas at Austin *Austin, TX*

- Researched the SOTA algorithm of protecting the intellectual property of pre-trained models
- Designed an algorithm based on the Lottery Ticket Hypothesis to protect the differential privacy of sensitive models
- Implemented the differentially private lottery tickets based on the opacus library, and conducted relevant experiments

Intern Experience

Lenovo, Intelligent Data Department **Jan. 2022 – At present**

Algorithm Engineer Intern, Supervised by Xuguang Gu *Remote*

- Created a benchmark, tested the performance gap of different NLP model architectures on different types of GPU.
- Developed the semantic recognition system for hardware fault determination and produced structured training data.

Course Projects

Subway ride navigation system [Code] **Feb. 2021**

- Provided optimal route recommendations for a complex subway system with dozens of lines and hundreds of stations using efficient graph algorithms such as the A-star algorithm, implementation in Cpp and its STLs
- Efficiently organized the graph with a large number of nodes and edges in memory using adjacency list
- Designed and implemented the graphical UI for the system and released the software

Student information database management tool [Code] **Oct. 2021**

- Created and maintained a multi-table database using MySQL, which contains students' personal information and course information, and build indexes and create primary keys in the tables
- Wrote an user-oriented database management program in python and the pymysql library, connected to the MySQL student database for its efficient management
- Designed and implemented an user-friendly interactive interface, and wrote documentation to assist users in using the program

MIPS CPU Simulation (Cornell CS3410 Lab) [Code] **Jul. 2021**

- Designed combinational logic circuits from basic gate circuits, step-by-step designed the half-adder, full-adder and ALU
- Replicated MIPS RAM and registers, and implement different cache mapping algorithms through circuit design, including fully associative cache, n-way set associative cache and direct mapping cache, etc.
- Designed single-cycle and multi-cycle MIPS CPUs with the previously completed medium-scale logic circuits, and was able to read in programs & data and run several sorting algorithms

Skills

Programming Skills:

- C, C++, Python, Qt, Assembly (x86 arch), Matlab, LaTeX, Linux
- **py libs: ML:** pytorch, numpy, opacus (for differential privacy); **Experimental Data & Visualization:** matplotlib, pandas, seaborn

Math background/Machine Learning Theories:

- Deep Learning, Calculus, Linear algebra, Probability theory and mathematical statistics
- Discrete Mathematics, Numerical Analysis, Cryptography, Information Security Mathematics (Arithmatic)

Problem-Solving and Entrepreneurial Skills:

- Think creatively; strongly desired and skilled to test out and iterate new ideas rapidly;
- Adept at identifying goals, establishing a reasonable timeline and anticipate possible challenges.

Honors & Awards

National Scholarship 21' (Top 4 of 253 students) **Dec. 2021**

National Scholarship 20' (Top 4 of 253 students) **Dec. 2020**

Outstanding Undergraduates in Term of Academic Performance (Top 2 of 253 students) **Sept. 2020**

Merit Student 21' (Top 5% of 253 students) **Oct. 2021**

Merit Student 20' (Top 5% of 253 students) **Oct. 2020**

Academic Excellence Scholarship (Top 10% of 253 students) **Jun. 2020**

Others

President of Student Union **Dec. 2020 – Oct. 2021**

Enhance the abilities of communication, cooperation and coordination

- **Hobbies:** Badminton, Skiing, Photography, Electronic Music