

ZHENG ZHANG

1400 Martin St ◇ State College, PA 16803

(814) · 323 · 1038 ◇ zhengzhangedu@gmail.com ◇ zheng-zhang.com

EDUCATION

The Pennsylvania State University

Aug 2016 - Dec 2020

B.S. in Statistics & Data Sciences | 3.73/4.00

Concentrations: Computational Statistics, Statistical Modeling Data Sciences

Minors in Computer Science & Mathematics

Member of Mu Sigma Rho - National Honorary Society for Statistics

PUBLICATIONS

- Conference: Xinyang Zhang, Zhang, Zheng, and Ting Wang. **Trojaning Language Models for Fun and Profit**. 2020, <https://arxiv.org/abs/2008.00312>, Euro S&P 2021
- Preprint: Xinyang Zhang, Zheng Zhang, and Ting Wang. **Composite Adversarial Training for Multiple Adversarial Perturbations and Beyond**
- Preprint: Ren Pang, Zheng Zhang, Xiangshan Gao, Zhaohan Xi, Shouling Ji, Peng Cheng, and Ting Wang. **TROJANZOO: Everything you ever wanted to know about neural backdoors (but were afraid to ask)**, (Submitted to IEEE S&P 2021, currently under review)

RESEARCH EXPERIENCE

Research Associate

Feb 2021 - Present

ALPS Lab, Department of Information Science & Technology

State College, PA

- Advised by: Dr. Ting Wang
- Ongoing independent research on the project of deep learning privacy/security.

Research Assistant

Mar 2020 - Dec 2020

ALPS Lab, Department of Information Science & Technology

State College, PA

- Advised by: Dr. Ting Wang
- Conducted deep learning security research in attacking and defending the general natural language models.
- Conducted adversarial machine learning research in defending multiple adversarial perturbations for image classification models.
- Implemented and evaluated deep learning attack and defense methods using PyTorch.
- Presented and discussed the research progress weekly.
- Co-authored and submitted three conference proceedings to the major machine learning / security and privacy conferences.

Research Assistant

Aug 2019 - Jan 2020

The Mahony Lab, Center for Eukaryotic Gene Regulation

State College, PA

- Advised by: Dr. Shaun Mahony
- Developed algorithms and models for predicting the signal of biochemical activities in human genome.
- Utilized Spark and HDFS to provide solutions for handling over 4 TBs massive datasets.
- Created parallel applications for data pre-processing and post-processing.

- Link to Research: <https://secantzhang.github.io/project/encode-imputation>

Bioinformatics Programmer

The Mahony Lab, Center for Eukaryotic Gene Regulation

May 2019 - Aug 2019

State College, PA

- Advised by: Dr. Shaun Mahony
- Participated in the "Encode Imputation" challenge hosted by Stanford University.
- Developed high-performance parallel algorithms and the data processing pipeline to model the massive datasets.

PROJECTS

Trojan-Zoo

Python, PyTorch, Bash

May 2020 - Present

State College, PA

- On-going research project involving the benchmarking of various STOA attacks and defenses for deep learning systems in adversarial machine learning.
- Implemented and integrated the method in paper **An Embarrassingly Simple Approach for Trojan Attack in Deep Neural Networks** Link: <https://arxiv.org/abs/2006.08131>
- Implemented and integrated the method in paper **Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning** Link: <https://arxiv.org/abs/1712.05526>
- Evaluated various metrics in the Trojan-Zoo system such as attack accuracy and defense successful rate.

Composite Perturbations

Python, PyTorch, Bash

Sep 2020 - Nov 2020

State College, PA

- Research project for defending multiple adversarial perturbations for deep neural networks.
- Co-authored the conference proceeding "Anonymous" and submitted to ICLR 2021, currently under blind review.

NLP Security

Python, PyTorch, Bash

May 2020 - Oct 2020

State College, PA

- Research project for backdoor-attacking and defending general language models.
- Co-authored the conference proceeding "Trojaning Language Models for Fun and Profit" and submitted to Euro S&P 2021.

rmodel2tex

R (Personal project)

Dec 2018 - May 2019

State College, PA

- R package for easily converting various existing r model to latex code.
- Supported various statistical models such as linear regression and logistic regression.
- Took into consideration of the differences between population model and fitted model, and supported different representation of interaction and categorical terms.
- Link to Project: <https://secantzhang.github.io/project/rmodel2tex>

A-weather

Swift (HackPSU project)

Oct 2018

State College, PA

- Developed an AR iOS application using AccuWeather API on HackPSU Fall 2018.
- Integrated Augmented Reality within the mobile application to visually sense the weather condition at home.
- Link to Project: <https://secantzhang.github.io/project/a-weather>

HONORS AND AWARDS

CMPSC 448 Deep Learning Classification Challenge <i>Ranked 3/98</i>	April 2020 State College, PA
ECoS Summer Undergraduate Research Scholarship <i>Scholarship for Conducting Research During Summer</i>	April 2019 State College, PA
DataFest <i>Finalists & Best Visualization Award</i>	April 2019 State College, PA
HackPSU <i>Second Place in AccuWeather Challenge</i>	October 2018 State College, PA
Penn State Behrend Honors Student <i>Honors Student Award</i>	April 2018 Erie, PA

PROFESSIONAL EXPERIENCE

Teaching Assistant <i>CMPSC/DS 410 - Programming Models for Big Data</i>	Aug 2020 - Present State College, PA
<ul style="list-style-type: none">· Developed guided tutorials and solutions to interact students from diverse linguistic and culture backgrounds on their labs and homework.· Individualized learning with 70+ students through one-on-one tutorials in office hours.	
Grader <i>CMPSC 442 - Artificial Intelligence</i>	Jan 2020 - May 2020 State College, PA
<ul style="list-style-type: none">· Assisted Dr. Kelvin Kamali in grading 100+ student's homework in CMPSC 442 class.	
Grader <i>CMPSC 410 - Programming Models for Big Data</i>	Aug 2019 - Dec 2019 State College, PA
<ul style="list-style-type: none">· Assisted Dr. Daniel Kifer in grading 40+ students' homework and lab assignments in CMPSC 410 class.	
Entry Analyst Intern <i>Beijing JAYA Technology</i>	Jun 2017 - Sep 2017 Beijing, China
<ul style="list-style-type: none">· Crawled and collected public-available financial data published in 5 companies' annual report.· Visualized and analyzed the data extensively using R and Python.	

TECHNICAL STRENGTHS

Computer Languages	Python, R, Scala, Swift, C++, JAVA, SAS, Shell Script
Data Analysis & Processing	Spark, Hadoop, HDFS, Scikit-Learn, Pandas
Deep Learning	PyTorch, TensorFlow

COURSEWORK

CMPSC 448 <i>Machine Learning and AI</i>	Spring 2020 A	CMPSC 442 <i>Artificial Intelligence</i>	Fall 2019 A-
IST 597 <i>Foundations in Data Privacy (Graduate)</i>	Spring 2020 A-	CMPEN 454 <i>Computer Vision</i>	Fall 2019 A

CMPSC 465	Summer 2019	STAT 440	Spring 2019
<i>Data Structures and Algorithms</i>	<i>A</i>	<i>Computational Statistics</i>	<i>A</i>
CMPSC 410	Spring 2019	STAT 462	Fall 2018
<i>Programming Models for Big Data</i>	<i>A</i>	<i>Applied Regression Analysis</i>	<i>A-</i>