

Zheng Zhang

(814) · 323 · 1038 ◇ Mudd Hall, Room 3120, Northwestern University

zheng.zhang@northwestern.edu ◇ <https://secantzhang.github.io/>

EDUCATION

Doctor of Philosophy in Computer Science

Sep 2021 - Present

Northwestern University

Concentrations: System Security and Privacy

Bachelor of Science in Statistics & Data Sciences

Aug 2016 - Dec 2020

The Pennsylvania State University

Concentrations: Computational Statistics, Statistical Modeling Data Sciences

Minors in Computer Science & Mathematics

Member of Mu Sigma Rho - National Honorary Society for Statistics

RESEARCH INTERESTS

I have a broad interest in the area of system security and privacy. More concretely, I've been working on improving the security and privacy guarantees of database management systems by applying differential-privacy mechanisms and cryptography protocols. I'm also interested in adversarial and backdoor attacks of deep learning models/systems.

PUBLICATIONS

- IEEE EuroS&P 22': 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)**, <https://arxiv.org/abs/2012.09302>
- IEEE EuroS&P 21': Xinyang Zhang, Zhang, Zheng, and Ting Wang. **Trojaning Language Models for Fun and Profit**, <https://arxiv.org/abs/2008.00312>

WORK & RESEARCH EXPERIENCES

Research Associate

Mar 2020 - July 2021

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.

Bioinformatics Programmer

May 2019 - Jan 2020

The Mahony Lab, Center for Eukaryotic Gene Regulation

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.

- 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>

Business Analyst, Internship

Beijing JAYA Technology

Jun 2017 - Sep 2017

Beijing, China

- Crawled and collected public-available financial data published in 5 companies' annual report.
- Visualized and analyzed the data extensively using R and Python.

TEACHING EXPERIENCES

Teaching Assistant

CMPSC/DS 410 - Programming Models for Big Data

Fall 2019, Fall 2020

State College, PA

- Developed guided tutorials and solutions to interact students on their labs and homework.
- Individualized learning with 70+ students through one-on-one tutorials in office hours.

Grader

CMPSC 442 - Artificial Intelligence

Spring 2020

State College, PA

- Assisted Dr. Kelvin Kamali in grading 100+ student's homework in CMPSC 442 class.

PROJECTS

Trojan-Zoo

Python, PyTorch, Bash

May 2020 - June 2021

State College, PA

- Research project for benchmarking various SoTA attacks and defenses of 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 paper "Composite Adversarial Training for Multiple Adversarial Perturbations and Beyond", in preparation.

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", accepted by 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

Ranked 3/98

April 2020

State College, PA

ECoS Summer Undergraduate Research Scholarship

Scholarship for Conducting Research During Summer

April 2019

State College, PA

DataFest

Finalists & Best Visualization Award

April 2019

State College, PA

HackPSU

Second Place in AccuWeather Challenge

October 2018

State College, PA

Penn State Behrend Honors Student

Honors Student Award

April 2018

Erie, PA

TECHNICAL STRENGTHS

Programming Languages

Python, R, C++, Shell Script

Data Analysis & Processing

Spark, Hadoop, HDFS, Scikit-Learn, Pandas

Deep Learning

PyTorch, TensorFlow

COURSEWORKS

Artificial Intelligence

Machine Learning, Artificial Intelligence, Computer Vision

Statistics & Data Sciences

Applied Regression Analysis, Computational Statistics,
Programming Models for Big Data

Security & Privacy

Data Privacy, Introduction to Cryptography,
Advanced Cryptography

Core Computer Sciences

Data Structures and Algorithms, Database Management Systems
Concurrent Scientific Programming