# ZHENG ZHANG

1400 Martin St ⋄ State College, PA 16803
(814) · 323 · 1038 ⋄ zhengzhangedu@gmail.com ⋄ zheng-zhang.com

## EDUCATION

**Doctor of Philosophy in Computer Sciences** *Expected Fall 2026*
*Northwestern University*
Concentrations: Security and Privacy

**Bachelor of Science in Statistics & Data Sciences** *Aug 2016 - Dec 2020*
*The Pennsylvania State University* | 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: Towards Unified, Holistic, and Practical Evaluation of Neural Backdoors**, (Submitted to USENIX Security 2022, currently under review)

## RESEARCH EXPERIENCE

**Research Associate** Feb 2021 - July 2021
*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** May 2019 - Aug 2019
*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.

## PROJECTS

**Trojan-Zoo** May 2020 - June 2021
*Python, PyTorch, Bash* *State College, PA*

- Research project for benchmarking various SToA 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** Sep 2020 - Nov 2020
*Python, PyTorch, Bash* *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** May 2020 - Oct 2020
*Python, PyTorch, Bash* *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** Dec 2018 - May 2019
*R (Personal project)* *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** Oct 2018
*Swift (HackPSU project)* *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** April 2020
*Ranked 3/98* *State College, PA*

**ECoS Summer Undergraduate Research Scholarship** April 2019
*Scholarship for Conducting Research During Summer* *State College, PA*

**DataFest** April 2019
*Finalists & Best Visualization Award* *State College, PA*

**HackPSU** October 2018
*Second Place in AccuWeather Challenge* *State College, PA*

**Penn State Behrend Honors Student** April 2018
*Honors Student Award* *Erie, PA*

## PROFESSIONAL EXPERIENCE

**Teaching Assistant** Aug 2020 - Dec 2020
*CMPSC/DS 410 - Programming Models for Big Data* *State College, PA*

- 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** Jan 2020 - May 2020
*CMPSC 442 - Artificial Intelligence* *State College, PA*

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

**Grader** Aug 2019 - Dec 2019
*CMPSC 410 - Programming Models for Big Data* *State College, PA*

- Assisted Dr. Daniel Kifer in grading 40+ students' homework and lab assignments in CMPSC 410 class.

**Entry Analyst Intern** Jun 2017 - Sep 2017
*Beijing JAYA Technology* *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.

## 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** | Spring 2020 | **IST 597** | Spring 2020 |
| *Machine Learning and AI* | *A* | *Foundations in Data Privacy (Graduate)* | *A-* |

**CMPSC 442** Fall 2019
*Artificial Intelligence* A-

**CMPEN 454** Fall 2019
*Computer Vision* A

**CMPSC 465** Summer 2019
*Data Structures and Algorithms* A

**CMPSC 410** Spring 2019
*Programming Models for Big Data* A

**STAT 440** Spring 2019
*Computational Statistics* A

**STAT 462** Fall 2018
*Applied Regression Analysis* A-