

# Elisa Tsai (Wentao Cai)

---

Department of Computer Science, 2260 Hayward Street, Ann Arbor, MI, 48105, USA  
Email: [eltsai@umich.edu](mailto:eltsai@umich.edu) Homepage: [eltsai.github.io](https://eltsai.github.io)

## INTERESTS

Web security; machine learning for security; machine learning efficiency.

My research focuses on building pragmatic, GenAI-powered systems for web security. I also design algorithms for efficient, high-quality training data selection for vision and large language models.

## EDUCATION

**University of Michigan, Ann Arbor**  
Ph.D. Candidate, Computer Science  
Advisor: Prof. Atul Prakash

**Shanghai Jiao Tong University (SJTU)** 2020  
B.S., Computer Science and Technology

## WORK EXPERIENCE

**Google Summer of Code - HoneyNet RiotPot** June. 2023 - Aug. 2023  
Software Engineer  
I contributed to Riotpot, an IoT honeypot, with more protocol emulation to increase the honeypot's relevance to real-world attacks.

## PUBLICATIONS

- [ELFS: Enhancing Label-Free Coreset Selection via Clustering-based Pseudo-Labeling](#)  
Haizhong Zheng (co-lead), Elisa Tsai (co-lead), Yifu Lu, Jiachen Sun, Brian R. Bartoldson, Bhavya Kailkhura, Atul Prakash  
*In Submission*
- [Modeling and Detecting Internet Censorship Events](#)  
Elisa Tsai, Ram Sundara Raman, Atul Prakash, Roya Ensafi  
**NDSS (Network and Distributed System Security Symposium) 2024**
- [CERTainty: Detecting DNS Manipulation at Scale using TLS Certificates](#)  
Elisa Tsai, Deepak Kumar, Ram Sundara Raman, Gavin Li, Yael Eiger, Roya Ensafi  
**PETS (Privacy Enhancing Technologies Symposium) 2023**
- [DOLMA: Securing Speculation with the Principle of Transient Non-Observability](#)  
Kevin Loughlin, Ian Neal, Jiacheng Ma, Elisa Tsai, Ofir Weisse, Satish Narayanasamy, Baris Kasikci  
**USENIX Security 2021**
- [Terms of Deception: Exposing Obscured Financial Obligations in Online Agreements with Deep Learning](#)  
Elisa Tsai, Anoop Singhal, Atul Prakash  
**DLSP (Deep Learning Security and Privacy Workshop) 2024**
- [Detecting Social Engineering Scams While Preserving User Privacy in the Digital Era \(Proposal Position Paper\)](#)  
Atul Prakash, Shivani Kumar, Elisa Tsai  
**ConPro (Workshop on Technology and Consumer Protection) 2024**

**GRANT  
PROPOSALS**

I actively contributed to the proposal design, proposal writing, and presentation for the following grants:

**Data Efficiency of LLMs Fine-tuning with RLHF**  
\$150K *per year*

Cisco, 2023  
PI: Atul Prakash

**Intelligent Assistants for Detecting Social Engineering Scams**  
\$100K

OpenAI, 2023  
PI: Atul Prakash

**TEACHING**

**Graduate Student Instructor**  
Computer & Network Security

*Winter 2024*  
UMich [EECS 588](#)

**Graduate Student Instructor**  
Data Structures and Algorithms

*Fall 2023*  
UMich EECS 281

**Graduate Student Instructor**  
Secure and Trustworthy Machine Learning

*Winter 2023*  
UMich [EECS 598](#)

**Teaching Assistant**  
Operating Systems

*Winter 2019*  
USTC

**SERVICE**

- [SECURIT](#) (SECurity Reading Is Terrific) Reading Group Host
- CSEG (CSE Graduate Students) Outreach Chair
- CSEG (CSE Graduate Students) Social Co-Chair

2021 – 2024  
2022 – 2023  
2022 – 2023