Tianshuo Cong | CV

Room 401, Science Builiding, Tsinghua Universiry – Beijing – China

congtianshuo@gmail.com • tianshuocong.github.io

(Last update: December 12, 2023)

Research Interests

My main research interests are in the field of Information security, which includes privacy and security in deep learning (DL) and cryptography. Concretely, my research concentrates on the copyright protection of DL models, poisoning attacks against DL systems, and privacy disclosure risks in large language models (LLMs). Meanwhile, I am also interested in the design and cryptanalysis of lightweight block ciphers, and secure multi-party computation (MPC).

Current Position

Institute for Advanced Study, Tsinghua University — **Beijing, China**
Shuimu Post-Doctoral Researcher, hosted by Prof. Xiaoyun Wang — *07/2023 - Present*
Field of Research: Privacy and security in large language models

Education

Institute for Advanced Study, Tsinghua University — **Beijing, China**
Ph.D. in Mathematics, advised by Prof. Xiaoyun Wang — *08/2017 - 06/2023*
Ph.D. thesis: Research on Privacy and Security Issues in Deep Learning

CISPA Helmholtz Center for Information Security — **Saarbrücken, Germany**
Visiting Ph.D. Student, advised by Prof. Yang Zhang — *08/2021 - 01/2023*
Field of Research: Trustworthy Machine Learning (Safety, Privacy, and Security)

Department of Electronic Engineering, Tsinghua University — **Beijing, China**
B.Eng. in Electronic Engineering, advised by Prof. Yong Ren — *08/2013 - 06/2017*
Field of Research: Data Mining

Honors & Awards

- CACR Outstanding Doctoral Dissertation Award — *11/2023*
- Tsinghua Shuimu Scholar — *07/2023*

Service

- **PC Member:**
  - ACM CCS 2023 Artifact Evaluation Committee
- **Reviewer:**
  - Conference:
    - ACM CSCW 2024
    - IEEE/CVF CVPR 2024
    - NeurIPS 2023 workshop on New In ML
  - Journal:
    - IEEE Transactions on Dependable and Secure Computing (TDSC)

- ACM Transactions on Knowledge Discovery from Data (TKDD)
- PeerJ Computer Science

Publication

Conference

i. Tianshuo Cong and Xinlei He and Yun Shen and Yang Zhang. **Test-time Poisoning Attacks Against Test-time Adaptation Models.** In *IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2024.

ii. Tianshuo Cong and Xinlei He and Yang Zhang. **SSLGuard: A Watermarking Scheme for Self-supervised Learning Pre-trained Encoders.** In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2022.

Journal

i. Keting Jia and Xiaoyang Dong and Congming Wei and Zheng Li and Haibo Zhou and Tianshuo Cong. **On the Design of Block Cipher FESH.** *Journal of Cryptologic Research*, 2019.

ii. Tianshuo Cong and Jingjing Wang and Sanghai Guan and Yifei Mu and Tong Bai and Yong Ren. **Big Data Driven Oriented Graph Theory Aided tagSNPs Selection for Genetic Precision Therapy.** *IEEE Access*, 2019.

Preprint

i. Yichen Gong and Delong Ran and Jinyuan Liu and Conglei Wang and Tianshuo Cong and Anyu Wang and Sisi Duan and Xiaoyun Wang. **FigStep: Jailbreaking Large Vision-language Models via Typographic Visual Prompts.** *arXiv:2311.05608*, 2023.

ii. Yugeng Liu and Tianshuo Cong and Zhengyu Zhao and Michael Backes and Yun Shen and Yang Zhang. **Robustness Over Time: Understanding Adversarial Examples' Effectiveness on Longitudinal Versions of Large Language Models.** *arXiv:2308.07847*, 2023.

Teaching

Teaching Assistant — **Advanced Numerical Analysis**
Fall 2019, Tsinghua University

Teaching Assistant — **Introduction to Information Science and Technology**
Spring 2018, Tsinghua University

Student

Delong Ran *(co-supervised with Prof. Xiaoyun Wang)* *06/2023 -Now*
Ph.D. student at the Institute for Network Sciences and Cyberspace, Tsinghua University

Jinyuan Liu *(co-supervised with Prof. Xiaoyun Wang)* *06/2023-Now*
Undergraduate at the School of Cyber Science and Technology, Shandong University

Yichen Gong *(co-supervised with Prof. Hongbo Yu)* *10/2023-Now*
Ph.D. student at the Department of Computer Science and Technology, Tsinghua University

Conglei Wang *(remote internship)* *11/2023-Now*
Master student at Carnegie Mellon University

Talk

Attack AI Models: From ResNet to GPT-4V *12/2023*
Xi'an Jiaotong University