Tianhang Zheng

📱 +16476716884 • ✉ th.zheng@mail.utoronto.ca

Google Scholar: https://scholar.google.com/citations?user=DDP03z4AAAAJ&hl=en
Github: https://github.com/tianzheng4

Education

○ **University of Toronto (UofT) Ph.D.** **Toronto, ON, Canada**
Electrical and Computer Engineering GPA: 4.0/4.0 *2019.9-present*

○ **State University of New York at Buffalo (UB) M.Sc.** **Buffalo, NY, U.S.A.**
Computer Science and Engineering GPA: 3.89/4.0 *2017.1 - 2019.6*

○ **Peking University (PKU) B. Eng.** **Beijing, China**
Engineering Structure Analysis (Mechanics) *2012.9 - 2016.6*

Selected Awards & Honors

○ NeurIPS 2021 Outstanding Reviewer Award	2021
○ Best MS Research Award, Department of Computer Science and Engineering, UB	2019
○ Award for Academic Excellence, PKU	2015
○ First Award in National Undergraduate Physics Competition	2013

Publications

Conferences & Journals

1. Mengnan Zhao, Bo Wang, Wei Wang, Yuqiu Kong, **Tianhang Zheng**, Kui Ren “Guided Erasable Adversarial Attack (GEAA) towards Shared Data Protection” To Appear in IEEE Transactions on Information Forensics & Security (TIFS).
2. **Tianhang Zheng**, Baochun Li “InfoCensor: An Information-Theoretic Framework against Sensitive Attribute Inference and Demographic Disparity” In ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2022).
3. Mengdi Huai, **Tianhang Zheng**, Chenglin Miao, Liuyi Yao, Aidong Zhang “On the Robustness of Metric Learning: An Adversarial Perspective” In ACM Transactions on Knowledge Discovery from Data (TKDD).
4. **Tianhang Zheng**, Baochun Li “Poisoning Attacks on Deep Learning based Wireless Traffic Prediction" In IEEE INFOCOM 2022-IEEE Conference on Computer Communication (INFOCOM22)
5. Yi Zhu, Chenglin Miao, **Tianhang Zheng**, Foad Hajiaghajani, Lu Su, Chunming Qiao “Can We Use Arbitrary Objects to Attack LiDAR Perception in Autonomous Driving?” In ACM Conference on Computer and Communications Security, 2021 (CCS21)
6. Hengtong Zhang, **Tianhang Zheng** Jing Gao, Yaliang Li, Lu Su and Bo Li “Profanity-Avoiding Training Framework for Seq2seq Models with Certified Robustness” In Empirical Methods in Natural Language Processing, 2021 (EMNLP21)
7. **Tianhang Zheng**, Baochun Li “First-Order Efficient General-Purpose Clean-Label Data Poisoning” In IEEE INFOCOM 2021-IEEE Conference on Computer Communication (INFOCOM21)
8. Zhongjie Ba*, **Tianhang Zheng***, Xinyu Zhang, Zhan Qin, Baochun Li, Xue Liu, Kui Ren “Learning-based Practical Smartphone Eavesdropping with Built-in Accelerometer” In Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2020) (*equal contribution)
9. Kui Ren, **Tianhang Zheng**, Zhan Qin, and Xue Liu. “Adversarial attacks and defenses in deep learning”

Engineering (2020).

10. **Tianhang Zheng**, Changyou Chen, Junsong Yuan, Bo Li, and Kui Ren. "PointCloud Saliency Maps" In Proceedings of the IEEE International Conference on Computer Vision, pp. 1598-1606. 2019 (ICCV19)
11. **Tianhang Zheng**, Changyou Chen, and Kui Ren. "Distributionally adversarial attack" In Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 2253-2260. 2019 (AAAI19)
12. Hengtong Zhang, **Tianhang Zheng**, Jing Gao, Chenglin Miao, Lu Su, Yaliang Li, and Kui Ren. "Data poisoning attack against knowledge graph embedding" In Proceedings of the 28th International Joint Conference on Artificial Intelligence, AAAI Press, 2019 (IJCAI19)
13. Qi Wei, Kai Fan, Wenlin Wang, **Tianhang Zheng**, Chakraborty Amit, Katherine Heller, Changyou Chen, and Kui Ren "InverseNet: Solving Inverse Problems of Multimedia Data with Splitting Networks" In 2019 IEEE International Conference on Multimedia and Expo, pp. 1324-1329. IEEE, 2019 (ICME19)
14. **Tianhang Zheng**, Zhi Sun, and Kui Ren. "FID: Function Modeling-based Data-Independent and Channel-Robust Physical-Layer Identification" In IEEE INFOCOM 2019-IEEE Conference on Computer Communications (INFOCOM19)

Academic History at University of Toronto

- ECE1784H Trustworthy Machine Learning (A+)
- ECE1502H Information Theory (A)
- ECE1771H Quality of Service (A+)
- ECE1504H Statistical Learning (A+)
- ECE1505H Convex Optimization (A+)

Professional Activities

- Program Committee of AAAI Conference on Artificial Intelligence (AAAI)
- Reviewer of IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI) and The Conference on Neural Information Processing Systems (NeurIPS)
- Subreviewer of International Conference on Distributed Computing Systems (ICDCS), ACM Multimedia (MM), ACM Conference on Computer and Communications Security (CCS)

Professional Skills

- **Programming:** Python (tensorflow & pytorch), C++, CUDA
- **Language Proficiency:** English (proficient), Chinese (native)
- **Other Skills**: Strong background in Mathematics, Physics, Machine Learning, Computer Vision, Computer Security, and Differential Privacy

Teaching Experience

- Teaching Assistant in ECE1505 (UofT): Convex Optimization 2021
- Teaching Assistant in ESC180 (UofT): Introduction to Computer Programming 2020
- Teaching Assistant in CSE191 (UB): Discrete Structures 2018
- Teaching Assistant in CSE574 (UB): Introduction to Machine Learning 2017
- Teaching Assistant in CSE111 (UB): Great Ideas in Computer Science 2017