ZAYD HAMMOUDEH

zayd.hammoudeh@gmail.com | GitHub | Website

EDUCATION

University of Oregon *2018 – 2023*
Doctor of Philosophy in Computer Science – GPA: 4.0
Thesis: *Certified and Forensic Defenses against Poisoning and Backdoor Attacks*
Advisor: Daniel Lowd
Committee Members: Thien Nguyen, Humphrey Shi, and Luca Mazzucato

University of California, Santa Cruz *2017 – 2018*
Postgraduate Research in Computer Science – GPA: 4.0

San José State University *2014 – 2016*
Master of Science in Computer Science – GPA: 4.0
Thesis: *A Fully Automated Solver for Multiple Square Jigsaw Puzzles Using Hierarchical Clustering*
Advisor: Chris Pollett

Drexel University *2002 – 2006*
Bachelor & Master of Science in Computer Engineering (Dual Degree)
Thesis: *ForPowER: A Novel Architecture for Energy Efficient Implementation for Fork-join Parallelism Using System on a Chip*
Advisors: Moshe Kam & Nagarajan Kandasamy

PROFESSIONAL EXPERIENCE

ML Applied Scientist, Qualtrics *Oct. 2023 – Present*
Automated customer journey orchestration, survey question text generation, and user response validation.

Graduate Researcher, Department of Computer Science, University of Oregon *Sep. 2018 – Oct. 2023*
Adversarial machine learning; training data influence analysis; positive-unlabeled learning.

Graduate Researcher, Department of Computer Science, UC Santa Cruz *Sep. 2017 – Sep. 2018*
Exact and probabilistic sampling and counting algorithms for #P problems.

Wireless Power Engineer, Integrated Device Technology *Nov. 2011 – Sep. 2017*
Design of mobile wireless power receivers and transmitters.

Applications Development Engineer, Teradyne *July 2006 – Nov. 2011*
Research and development of high-power semiconductors.

Undergraduate Researcher, Drexel University – Data Fusion Lab *June 2003 – July 2006*
Gene expression statistical analysis; low-power hardware design.

REFEREED JOURNAL PUBLICATIONS

[1] J. Brophy, **Z. Hammoudeh**, and D. Lowd. Adapting and evaluating influence-estimation methods for gradient-boosted decision trees. *Journal of Machine Learning Research*, 24:1–48, 2023.

[2] **Z. Hammoudeh** and D. Lowd. Training data influence analysis and estimation: A survey. *Machine Learning*, 2023.

REFEREED CONFERENCE PUBLICATIONS

[3] **Z. Hammoudeh** and D. Lowd. Provable robustness against a union of ℓ_0 attacks. In *Proceedings of the 38th AAAI Conference on Artificial Intelligence*, AAAI'24, 2024.

[4] **Z. Hammoudeh** and D. Lowd. Reducing certified regression to certified classification for general poisoning attacks. In *Proceedings of the 1st IEEE Conference on Secure and Trustworthy Machine Learning*, SaTML'23, 2023.

[5] W. You, **Z. Hammoudeh**, and D. Lowd. Large language models are better adversaries: Exploring generative clean-label backdoor attacks against text classifiers. In *Findings of the Association for Computational Linguistics*, EMNLP'23, 2023.

[6] **Z. Hammoudeh** and D. Lowd. Identifying a training-set attack's target using renormalized influence estimation. In *Proceedings of the 29th ACM SIGSAC Conference on Computer and Communications Security*, CCS'22, 2022.

[7] **Z. Hammoudeh** and D. Lowd. Learning from positive and unlabeled data with arbitrary positive shift. In *Proceedings of the 34th Conference on Neural Information Processing Systems*, NeurIPS'20, 2020.

[8] S. Jamshidi, **Z. Hammoudeh**, R. Durairajan, D. Lowd, R. Rejaie, and W. Willinger. On the practicality of learning models for network telemetry. In *Proceedings of the 4th Network Traffic Measurement and Analysis Conference*, TMA'20, 2020.

[9] D. Achlioptas, **Z. Hammoudeh**, and P. Theodoropoulos. Fast sampling of perfectly uniform satisfying assignments. In *Proceedings of the 21st International Conference on Theory and Applications of Satisfiability Testing*, SAT'18, 2018. **Best Student Paper Award**. Authors alphabetical.

[10] **Z. Hammoudeh** and C. Pollett. Clustering-based, fully automated mixed-bag jigsaw puzzle solving. In *Proceedings of 17th International Conference on Computer Analysis of Images and Patterns*, CAIP'17, 2017.

REFEREED WORKSHOP PUBLICATIONS

[11] **Z. Hammoudeh** and D. Lowd. Feature partition aggregation: A fast certified defense against a union of ℓ_0 attacks. In *Proceedings of the 2nd ICML Workshop on New Frontiers in Adversarial Machine Learning*, AdvML-Frontiers'23, 2023.

[12] W. You, **Z. Hammoudeh**, and D. Lowd. Large language models are better adversaries: Exploring generative clean-label backdoor attacks against text classifiers. In *Proceedings of the 2nd ICML Workshop on New Frontiers in Adversarial Machine Learning*, AdvML-Frontiers'23, 2023.

[13] **Z. Hammoudeh** and D. Lowd. Simple, attack-agnostic defense against targeted training set attacks using cosine similarity. In *Proceedings of the 3rd ICML Workshop on Uncertainty and Robustness in Deep Learning*, UDL'21, 2021.

[14] Z. Xie, J. Brophy, A. Noack, W. You, K. Asthana, C. Perkins, S. Reis, **Z. Hammoudeh**, D. Lowd, and S. Singh. What models know about their attackers: Deriving attacker information from latent representations. In *Proceedings of the 4th BlackboxNLP Workshop on Analyzing and Interpreting Neural Networks for NLP*, 2021. (Oral).

[15] **Z. Hammoudeh** and D. Lowd. Positive-unlabeled learning with arbitrarily non-representative labeled data. In *Proceedings of the 37th International Conference on Machine Learning's Workshop on Uncertainty & Robustness in Deep Learning*, UDL'20, 2020.

SCHOLARSHIPS, HONORS, & AWARDS

Highlighted Reviewer, ICLR	*2022*
Gurdeep Pall Graduate Student Fellowship, University of Oregon	*2022*
J. Donald Hubbard Family Scholarship, University of Oregon	*2021*

Travel Award, IJCAI	*2019*
Best Student Paper Award, SAT Conference	*2018*
Travel Award, Federated Logic Conference (FLoC)	*2018*
Travel Award, SAT Association	*2018*
Chancellor's Fellowship, University of California, Santa Cruz	*2017*
Arnold H. Kaplan Academic Excellence Scholarship, Drexel University	*2005*
Undergraduate Student Research Award, Drexel University	*2005*
Teaching Assistant Excellence Award, Drexel University	*2004*

TEACHING EXPERIENCE

CIS315 Intermediate Algorithms *Spring 2021 & 2022*
Teaching Assistant, University of Oregon

CIS472/572 Probabilistic Methods in Artificial Intelligence *Winter 2021*
Teaching Assistant, University of Oregon

CIS212 Computer Science III – C++ & Unix *Fall 2018*
Teaching Assistant, University of Oregon

TDEC221 & TDEC222 Fundamentals of Systems and Differential Equations I & II *2003 – 2006*
Teaching Assistant, Drexel University

TDEC231 & TDEC232 Evaluation of Experimental Data and Engineering Ethics I & II *2004 – 2006*
Teaching Assistant, Drexel University

PROFESSIONAL SERVICE

Journal Reviewer	Artificial Intelligence Journal (AIJ)
Conference Reviewer	NeurIPS (2020, 2022, 2023), ICLR (2022, 2023, 2024), ICML (2023)