Samuel Yeom

www.samuelyeom.com samuel-yeom

Education

08/2016–06/2021	**Ph.D. in Computer Science** Carnegie Mellon University Advised by Matt Fredrikson Thesis Title: Black-Box Approaches to Fair Machine Learning
08/2016–12/2018	**M.S. in Computer Science – Research** Carnegie Mellon University Advised by Matt Fredrikson
09/2012–06/2016	**B.S. in Mathematics with Computer Science** Massachusetts Institute of Technology

Awards

2018	Distinguished Paper Award at IEEE Computer Security Foundations Symposium
2016	Phi Beta Kappa inductee
2014	Putnam Mathematical Competition top-200 contestant

Leadership and Service

2020–2021	**Student Organization Officer** Puzzle Hunt CMU Co-led the creation and oversight of multi-day puzzle events every semester with over 1000 participants each
Spring 2019	**Admissions Committee Member** Carnegie Mellon University Computer Science Department Evaluated hundreds of PhD applications and helped analyze the results of the admissions process for possible biases

Teaching

Spring 2020	**Teaching Assistant** Probability and Computing (15-259, CMU)
Spring 2017	**Teaching Assistant** Software Foundations of Security and Privacy (15-316, CMU)
Spring 2015	**Grader** Introduction to Algorithms (6.006, MIT)

Publications

[1] **Avoiding Disparity Amplification under Different Worldviews**
Samuel Yeom and Michael Carl Tschantz
ACM Conference on Fairness, Accountability, and Transparency, 2021

[2] **Individual Fairness Revisited: Transferring Techniques from Adversarial Robustness**
Samuel Yeom and Matt Fredrikson
International Joint Conference on Artificial Intelligence, 2020

[3] **Learning Fair Representations for Kernel Models**
Zilong Tan, Samuel Yeom, Matt Fredrikson, and Ameet Talwalkar
Conference on Artificial Intelligence and Statistics, 2020

[4] **FlipTest: Fairness Testing via Optimal Transport**
Emily Black*, Samuel Yeom*, and Matt Fredrikson
ACM Conference on Fairness, Accountability, and Transparency, 2020

[5] **Overfitting, Robustness, and Malicious Algorithms: A Study of Potential Causes of Privacy Risk in Machine Learning**
Samuel Yeom, Irene Giacomelli, Alan Menaged, Matt Fredrikson, and Somesh Jha
Journal of Computer Security, 2020

[6] **Hunting for Discriminatory Proxies in Linear Regression Models**
Samuel Yeom, Anupam Datta, and Matt Fredrikson
Advances in Neural Information Processing Systems, 2018

[7] **Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting**
Samuel Yeom, Irene Giacomelli, Matt Fredrikson, and Somesh Jha
Distinguished Paper at the *IEEE Computer Security Foundations Symposium*, 2018

*Equal contribution