Samuel Yeom

www.samuelyeom.com samuel-yeom

Education

2016–present **Candidate for Ph.D. in Computer Science**
Carnegie Mellon University
Advisor: Matt Fredrikson

2016–2018 **M.S. in Computer Science – Research**
Carnegie Mellon University
Advisor: Matt Fredrikson

2012–2016 **B.S. in Mathematics with Computer Science**
Massachusetts Institute of Technology
GPA: 5.0/5.0

Experience

Summer 2018 **Research Intern**
International Computer Science Institute
Analyzed various notions of fairness for machine learning models

Summer 2016 **Graduate Technical Intern**
Intel Corporation
Automated a port scan of existing Intel assets on external cloud and created a prioritized list of recommendations for improving their security

Summer 2015 **Technical Assistant**
MIT Lincoln Laboratory
Applied multi-party computation and threshold encryption to design a provably secure, auditable log

2014–2015 **Undergraduate Researcher**
MIT Computer Science and Artificial Intelligence Laboratory
Proved the subexponential-time security of a lattice-based cryptographic assumption under the Exponential Time Hypothesis

Awards

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

Publications

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

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

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

[4] **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

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

[6] **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

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)

*Equal contribution