Secure Machine Learning

Shafi Goldwasser [1]

[1] MIT & Simons Institute for the Theory of Computing

This talk will focus on cryptography-inspired models of adversaries in the machine learning landscape and results to address three challenges. These challenges include verification of machine learning models given limited access to good data, training at scale on private training data, and robustness against adversarial examples controlled by worst-case adversaries.