Bocconi

25 OCTOBER 2023
04:00 PM

Bocconi University
Room 3-E4-SR03
Via Röntgen 1, Milano (3° floor)

Constructing and deConstructing Trust: A Cryptographers perspective

Speaker

Shafi Goldwasser
Director of Simons Institute for Theory of Computing
University of Berkeley

Abstract

For decades now cryptographic tools and models have enabled the use of technology platforms controlled by worst case computationally bounded adversaries. In this talk I will describe how to use cryptographic modeling and tools to build trust in various phases of the machine learning pipelines. We will touch on privacy in the training and inference stage, verification protocols for the quality of machine learning models and data sources, robustness in presence of adversaries, and if time permits, will show how cryptographic tools can be brought to build trust in various legal verification dilemmas.

Università Bocconi
DEPARTMENT OF COMPUTING SCIENCES