Constructing and deConstructing Trust in ML: A new Role for Cryptography Today

Shafi Goldwasser*[1,2]

[1]Massachusetts Institute of Technology – États-Unis
[2]Weizmann Institute of Science – Israël

Résumé

For decades now cryptographic tools and models have at their essence transformed technology platforms controlled by worst case adversaries to trustworthy platforms. In this talk I will describe how to use cryptographic tools and cryptographic modeling 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 robustness in presence of adversaries. If time permits, we will show how cryptographic tools can be brought to build trust in the legal domain.

*Intervenant