Zero-Knowledge Proofs for Secure and Private Machine Learning

Dario Fiore, IMDEA Software Institute

Abstract:
In this talk, I will present the application of zero-knowledge proofs to enhance the security and privacy of outsourced machine learning, focusing on neural networks and decision trees. In particular, the talk will present an information-theoretic framework to build efficient interactive proofs based on the sum check protocol in a modular way and how to use this framework to construct an efficient protocol for convolutional neural networks. This is based on the joint work with David Balbás, Maria Isabel Gonzalez Vasco, Damien Robissout, and Claudio Soriente (ACM CCS 2023).

Biography:
Dario Fiore is an Associate Research Professor at the IMDEA Software Institute in Madrid. Prior to joining IMDEA in 2013, he obtained a PhD in computer science from the University of Catania and then was a postdoc at ENS Paris, NYU, and the Max Planck Institute for Software Systems. His research interests are theoretical and practical aspects of cryptography and its applications to security and privacy. His current research revolves around succinct proof systems (including functional and vector commitments, homomorphic authentication, verifiable computation, and zero-knowledge proofs) and computation on encrypted data.