Zero-Knowledge Proofs for Verifiable Computation on Encrypted data

Dario Fiore, IMDEA Software Institute

Abstract:
In this talk, I will present the problem of verifying computation on data encrypted under fully homomorphic encryption and how succinct zero-knowledge proofs can be used in this application to guarantee the integrity of the computation and privacy of the data. The talk will give an overview of the state of the art and cover a set of techniques for designing efficient protocols specialized for this task.

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.