Introduction 2

Michele Ciampi, University of Edinburgh

Abstract:
In this lecture, we will define and provide a few examples of a class of interactive proof systems protocols called Sigma Protocols. We will see a few examples of efficient instantiation of Sigma Protocols and show how to instantiate constant-round zero-knowledge protocols. We will then argue what security zero-knowledge protocols retain when executed in sequence, parallel, and concurrency.

Biography:
Michele Ciampi is a Chancellor's Fellow (equivalent to Assistant Professor) at the School of Informatics at the University of Edinburgh. He obtained his PhD in Computer Science from the University of Salerno, and after that, he became a research associate at the University of Edinburgh. His work focuses on theoretical aspects of cryptography, including multi-party computation protocols, zero-knowledge proofs, and blockchain.