Introduction 3

Michele Ciampi, University of Edinburgh

Abstract:
In this lecture, we will show how Sigma Protocols can be used to construct efficient non-interactive arguments in the Random Oracle Model (ROM). Part of the lecture will be dedicated to discussing the different types of setups needed to design non-interactive zero-knowledge protocols. In the final part of the lecture, we will discuss non-malleability for zero-knowledge proofs.

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.