Polynomial Commitments

Arantxa Zapico, Ethereum Foundation

Abstract:
In this talk, we will define polynomial commitments (Kate, Zaverucha, and Goldberg at IACR Asiacrypt 2010) and their security notions, as well as their relation with vector commitments (Catalano and Fiore at IACR PKC 2013). In particular, we will present and analyze the KZG polynomial commitment and its role in designing a new era of succinct arguments.

Biography:
Arantxa Zapico is a Cryptography Researcher at the Ethereum Foundation. In 2022, she obtained her PhD from Universitat Pompeu Fabra. She is interested in the practical and theoretical aspects of proving systems. Her research focuses on the analysis and design of secure and efficient succinct arguments, such as zkSNARKs and vector and polynomial commitments.