UNIVERSIDAD
COMPLUTENSE
MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA
POSGRADO

Zero-knowledge and programmable cryptography for verifiable computation

D. Jordi Baylina

Facultad de Informática
Sala de Grados - martes 17 de octubre de 2023 - 11:00
Entrada libre hasta completar el aforo

Resumen:

In this talk, we will explain the basic concepts of zero knowledge and verifiable computation. In order to illustrate the concepts, we will develop a basic example using circom, a widely used domain-specific language for defining arithmetic circuits that can be used to generate zero-knowledge proofs. An overview of the state of the art of programmable cryptography, where languages like circom play a centric role, will be given.

Sobre Jordi Baylina:

Jordi Baylina is a Co-Founder of Polygon, and the Technical Lead and Co-Founder of Polygon zkEVM. He oversees the development and implementation of Polygon zkEVM, a leading zk-rollup. As one of the most widely recognized Ethereum developers, he has made several high-impact contributions to the Ethereum community, including the languages circom and PIL, free and open-source projects that demonstrate his commitment to Web3 values. He has a long history in the Ethereum community, including co-founding the WhiteHat Group to save funds during The DAO hack early in the network's history. He has spent years as a sought-after auditor, leading the teams that poured over the contracts of MakerDAO and Aragon. Before Hermez, he co-founded a number of projects, including the donation platform Giveth, DAppNode, and Iden3.