ZK Proofs: How fast can we go?

Anca Nitulescu, Input Output

Abstract:

In this talk, I will discuss the recent advancements in the ZK proof area, with the same blockchain applications in mind: more expressive statements to prove, memory savings, prover cost improvements, transparent setup, and more advanced folding techniques. Then, I will mention what is left to explore and improve based on the properties and shortcomings observed in these schemes. I will go over some early ideas on using new tools for SNARKs, like graphs and cycles of elliptic curves, error-correcting codes, or "elastic" instantiations for memory-time tradeoffs.

Biography:

Anca Nitulescu is an Applied Cryptography Researcher at Input Output Global (IOG) working on SNARK-focused projects. Prior to joining IOG, Anca was a Cryptography Researcher at Protocol Labs with contributions to the design and analysis of secure decentralized storage protocols. Anca was a postdoc at Aarhus University in 2018. Before that, Anca completed a PhD at ENS Paris under the supervision of David Pointcheval and Dario Fiore and worked on topics such as post-quantum secure SNARKs based on lattices, verifiable computation over encrypted data and authentication primitives, as well as on writing outreach material about Zero-Knowledge SNARKs. Anca's current main areas of interest are zk-SNARK protocols, focusing on scalability improvements through aggregation or folding. Anca also works on protocols for distributed settings, formalizations, and security studies of blockchain protocols.