Challenges in Scalable Zero-Knowledge Proofs

Carla Ràfols*[1]

[1]Universitat Pompeu Fabra [Barcelona] (UPF) – Plaça de la Mercè, 10-12 - 08002 Barcelona, Spain

Abstract

Zero-knowledge proofs have seen significant progress in recent years, driven in large part by applications in blockchain systems. At the same time, these techniques are increasingly being considered in more general settings involving privacy and authentication.

As zero-knowledge systems become more widely deployed, several practical questions become more prominent: how to reduce prover costs, how to support large-scale proof generation, which forms of recursion and aggregation are practical, and how current design choices interact with long-term considerations such as post-quantum security.

This talk will survey some recent directions in scalable zero-knowledge proofs, with a particular focus on proof generation and amortization techniques.

*Speaker