Group/pairing zk-SNARKs

Carla Ràfols, Universitat Pompeu Fabra

Abstract:
This talk will start with a general introduction to assumptions in DLOG groups (with or without an efficiently computable bilinear map) and show how to build different commitments with these assumptions. It will then give a general overview of the state-of-the-art SNARKs in DLOG groups, focusing on different properties such as transparent/trusted setup, linear/constant verifier, and constant/logarithmic proof size.

The remainder of the talk will be divided into two blocks. In the first one, I will introduce the main techniques available in the DLOG setting in groups without a pairing, such as Bulletproofs (Bootle et al. at IACR Eurocrypt 2016, Bunz et al. at IEEE S&P 2018), and techniques to amortize the cost of the verifier (Halo, Bowe et al. at IACR ePrint 2019/1021). The second block will focus on pairing groups and will explain how to prove linear relations in a pairing group and the design principles underlying the SNARK with a shorter proof size, i.e., Groth16 (Groth at IACR Eurocypt 2016).

Biography:
Carla Ràfols is an associate professor in the Engineering Department at Universitat Pompeu Fabra. After obtaining her PhD from the Polytechnical University of Catalonia, Carla was a postdoctoral researcher in the Unesco Chair in Data Privacy (Universitat Rovira i Virgili, Tarragona) and in the Foundations of Cryptography Group at the Ruhr University Bochum. Carla is interested in theoretical and practical aspects of public key cryptographic protocols, and in recent years, she has focused on improving group-based zero-knowledge proofs.