Compressed Sigma Protocols

Lisa Kohl, CWI Amsterdam

Abstract:
Sigma Protocols provide a well-understood basis for zero-knowledge proofs, allowing a prover to prove knowledge of a witness x such that C(x)=0 for an arithmetic circuit C without revealing anything beyond the truth of the statement. A downside of traditional Sigma protocols is the large amount of communication required between the prover and verifier, which scales linearly in the circuit size |C|. To overcome this, Attema and Cramer (IACR CRYPTO 2020) introduced the notion of compressed Sigma Protocols, which allow for reducing the communication complexity from linear to logarithmic or even constant, building on the Bulletproof compression mechanism (Bootle et al. at IACR Eurocrypt 2016, Bunz et al. at IEEE S&P 2018).

In this talk, I will present the compression mechanism and explain how it can be used to construct zero-knowledge proofs for proving knowledge of a witness x such that C(x)=0 for arbitrary arithmetic circuits with logarithmic (or less) communication complexity.

Biography:
Lisa Kohl is a tenured researcher in the CWI Cryptology group. A special focus of her work lies in exploring new directions in secure computation with the goal of developing practical post-quantum secure protocols. Before coming to CWI, she worked as a postdoctoral researcher with Yuval Ishai at Technion. In 2019, she completed her PhD at Karlsruhe Institute of Technology under the supervision of Dennis Hofheinz. During her PhD, she spent eight months in the FACT center at IDC Herzliya (now Reichman University) for a research visit with Elette Boyle.