Lattice-Based Sigma Protocols

Lisa Kohl, CWI Amsterdam

Abstract:
In this talk, I will introduce the Short Integer Solution (SIS) lattice assumption and explain difficulties that arise when instantiating Sigma Protocols based on SIS, such as the need for rejection sampling, soundness slack, and a smaller challenge space (Lyubashevsky at IACR Asiacrypt 2009 and IACR Eurocrypt 2012). I will further touch on additional issues arising for multi-round protocols, such as compressed Sigma Protocols from lattices, based on joint work with Thomas Attema and Ronald Cramer (IACR CRYPTO 2021).

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.