New and Improved Constructions for Partially Equivocable Public Key Encryption

Mahshid Riahinia

ENS de Lyon, Laboratoire LIP, France

Non-committing encryption (NCE) is an advanced form of public-key encryption which guarantees the security of a Multi-Party Computation (MPC) protocol in the presence of an adaptive adversary. Brakerski et al. (TCC 2020) recently proposed an intermediate notion, termed Packed Encryption with Partial Equivocality (PEPE), which implies NCE and preserves ciphertext-rate (up to a constant factor). In this work, we propose four new constructions of rate-1 PEPE based on standard assumptions. In particular, we obtain the first constant ciphertext-rate NCE construction from the LWE assumption with polynomial modulus, from DCR, and from the Subgroup Decision assumption. We also propose an alternative DDH-based construction with guaranteed polynomial running-time. We also introduce a new abstraction called mixed hidden bits generator (mHBG) that can be used to construct PEPE, and therefore NCE.

This is a joint work with Benoît Libert and Alain Passelègue, and the talk will be given by Mahshid Riahinia, PhD student.