Mathematical aspects of SPDZ-like protocols

Emmanuela Orsini
KU Leuven, imec-COSIC

Secure multi-party computation (MPC) is a general toolbox of cryptographic techniques which allows a set of parties to compute a public function on their private inputs while preserving a number of security properties such as privacy and correctness. The past decade has seen a huge amount of progress in making MPC more efficient. A major pillar of this advance has been in the case of a dishonest majority, where the main breakthrough came with the SPDZ protocol by Damgård et al. (CRYPTO 2010) and its improvements (Damgård et al. ESORICS 2013).

In this talk I will present the main aspects of SPDZ-like protocols over finite field and describe some mathematical constructions used to make these protocols more efficient and secure.