Zero-Knowledge Proofs from Multiparty Computation: Recent Advances

Matthieu Rivain*[1]

[1]CryptoExperts – N – France

Résumé

In this talk, we will present the so-called MPC-in-the-Head paradigm which compiles a secure multiparty computation (MPC) protocol into a zero-knowledge proof (or argument) of knowledge. This paradigm is instrumental in the construction of several modern post-quantum signature schemes. We will explain the principle of the MPC-in-the-Head transformation and review some recent advances in this field.

*Intervenant