Post-Quantum Signatures from Secure Multiparty Computation

Thibauld Feneuil*[1,2]

[1]Institut de Mathématiques de Jussieu - Paris Rive Gauche – Sorbonne Universite, Centre National de la Recherche Scientifique, Université Paris Cité – France
[2]CryptoExperts – Sans laboratoire – France

Résumé

Zero-knowledge proofs of knowledge are useful tools for designing signature schemes. Among the existing techniques, the MPC-in-Head (MPCitH) paradigm provides a generic framework to build quantum-resilient proofs using techniques from secure multiparty computation. This paradigm has recently been improved in a series of works which makes it an effective and versatile tool.

In the last few years, several post-quantum signature schemes following the MPC-in-the-Head framework have been proposed. These schemes outperform the former schemes based on the Fiat-Shamir transformation. In this talk, I will present them, describe their characteristics, and highlight their differences. I will also present the achieved performances and compare them with the current state of the art.

*Intervenant