PRIVACY-PRESERVING SIGNATURES FROM ISOGENIES

Federico Pintore

Università degli Studi di Bari

Privacy-preserving signatures - which have recently found applications in some cryptocurrencies - allow a signer to create a signature on behalf of a group of signers, hiding his/her true identity. In this talk, I will present the first practical privacy-preserving signatures based on isogeny between elliptic curves.