A Story of ZK Proofs: How Efficient ZK-Proofs Enable Signatures and New Applications

Emmanuela Orsini*[1]

[1]Bocconi University [Milan, Italy] – Italie

Résumé

Zero-Knowledge (ZK) proofs have evolved from theoretical constructs into powerful tools that drive practical innovations in cryptography and security.
In this talk, we explore the remarkable development of ZK proofs, focusing on prover-efficient schemes based on VOLE (Vector Oblivious Linear Evaluation),

which drastically improve proof efficiency and scalability for large statements.

We illustrate how these efficient ZK proofs enable advanced cryptographic primitives, particularly post-quantum signatures.

Beyond signatures, we also highlight novel applications emerging in privacy-preserving authentication,
secure computation and machine learning.

*Intervenant