**Making zkSNARKs Non-Malleable**

Antonio Faonio

Abstract: Zero-knowledge SNARKs (zkSNARKs) are cryptographic proof systems that allow a prover to convince a verifier that a statement is true, with very small proofs and fast verification, without revealing the underlying witness. The standard security notion for SNARKs is knowledge soundness, which guarantees that any prover who convinces the verifier must "know" a valid witness. A stronger notion is simulation extractability, which ensures that even an adversary who has seen simulated proofs cannot create a new valid proof without actually knowing a witness, and in particular implies non-malleability. This stronger guarantee is especially important in distributed and adversarial settings, where proof malleability can become a real threat.

In this talk, we revisit simulation extractability for universal zkSNARKs in the PIOP-to-SNARK paradigm. We discuss how this property can be achieved and analyzed in systems used in practice, with particular attention to optimizations such as the linearization trick. We also place these results in a broader context, reviewing existing approaches to simulation extractability in the literature and highlighting alternative techniques and trade-offs. The goal is to give a unified and accessible picture of how simulation extractability can be obtained in modern zkSNARK constructions, and what design choices are needed to ensure it in practice.