ProtogaLattice: Constant-Round Lattice-based Folding for General Polynomial Relations

Maxime Plançon

Abstract: Folding schemes are gaining traction recently as they unlock practical instantiations of Incrementally Verifiable Computation (IVC) and Proof-Carrying Data (PCD). While the landscape of folding schemes is vast, existing constructions based on lattices for high-degree relations heavily rely on the sum-check protocol. Sumcheck leads to very efficient prover times, but also presents drawbacks: the folded relation must be expressed by products of multilinear polynomials, and the verifier circuits become very large, partially because of the many random oracle calls required. The latter incurs a significant overhead when building IVC or PCD, as the prover must prove the execution of the verifier circuit at every iteration.

We present ProtogaLattice, a new lattice-based folding scheme for general high-degree polynomial relations that drastically reduces the size of the verifier's circuit. We deviate from the sum-check approach and instead take inspiration from Protostar [Bunz & Chen, Asiacrypt '24] and Protogalaxy [Eagen & Gabizon '23], which fold witnesses using algebraic techniques in constant number of rounds. In this talk, we present three contributions: (1) A folding scheme that combines multiple instances of polynomial relations into an accumulator, (2) a bootstrapping protocol to reduce the norm of the accumulator (3) an extension of Lova's [Fenzi et al, Asiacrypt '24] range proof technique to module lattices that fit our construction. Our techniques open new directions towards building lattice-based proofs that support more expressive relations and that present smaller recursion overheads.