CT Advanced Computing Center (CACC) Security Seminar Series 2024

Speaker: Hadas Zeilberger - Yale University
Date: December 4, 2024
Time: 11:15 12:30pm
Location: ITE 336
Meeting Link : https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m4d36ddf4d36edd727aa04331cdb7d7f6
Meeting number (access code): 2633 368 4613
Meeting password: MqmJMizs533

BaseFold: Efficient Field-Agnostic Polynomial Commitment Schemes from Foldable Codes

This works introduces BaseFold, a new field-agnostic Polynomial Commitment Scheme (PCS) for multilinear polynomials that has O(log2(n)) verifier costs and O(n log n) prover time. An important application of a multilinear PCS is constructing Succinct Non-interactive Arguments (SNARKs) from multilinear polynomial interactive oracle proofs (PIOPs). Furthermore, field-agnosticism is a major boon to SNARK efficiency in applications that require (or benefit from) a certain field choice.

Our inspiration for BaseFold is the Fast Reed-Solomon Interactive-Oracle Proof of Proximity (FRI IOPP), which leverages two properties of Reed-Solomon (RS) codes defined over "FFT-friendly" fields: O(n log n) encoding time, and a second property that we call foldability. We first introduce a generalization of the FRI IOPP that works over any foldable linear code in linear time. Second, we construct a new family of linear codes which we call random foldable codes, that are a special type of punctured Reed-Muller codes, and prove tight bounds on their minimum distance. Unlike RS codes, our new codes are foldable and have O(n log n) encoding time over any sufficiently large field. Finally, we construct a new multilinear PCS by carefully interleaving our IOPP with the classical sumcheck protocol, which also gives a new multilinear PCS from FRI.

BaseFold is 2-3 times faster than prior multilinear PCS constructions from FRI when defined over the same finite field. More significantly, using Hyperplonk (Eurocrypt, 2022) as a multilinear PIOP backend for apples-to-apples comparison, we show that BaseFold results in a SNARK that has better concrete efficiency across a range of field choices than with any prior multilinear PCS in the literature. Hyperplonk withover the web. BaseFold has a proof size that is more than 10 times smaller than Hyperplonk with Brakedown and its verifier is over 30 times faster for circuits with more than 220 gates. Compared to FRI, Hyperplonk with BaseFold retains efficiency over any sufficiently large field. For illustration, with BaseFold we can prove ECDSA signature verification over the secp256k1 curve more than 20 times faster than Hyperplonk with FRI and the verifier is also twice as fast. Proofs of signature verification have many useful applications, including offloading blockchain transactions and enabling anonymous credentials over the web.

CACC UCONN