ACCELERATING OPERATIONS WITH PLONKUP

Prize Sponsor

anoma

Prize Architect

anoma

POLYCHAIN

AZTEC

Prize Description

Summary

Plonkup is a zero-knowledge proof system harmonizing Plonk and Plookup. By leveraging lookup gates in Plonkup the number of constraints in a circuit can be reduced by a significant amount—shrinking prover time and making zero-knowledge proof creation achievable on a wider range of devices.

Cryptographic primitives such as BLS signatures, elliptic curve operations and hash functions, such as Blake2s and Reinforced Concrete, are used widely across the zero-knowledge space.

Efficient circuits written for these primitives are often pivotal. For this competition category, participants who can complete the challenges listed below will be eligible to receive the associated prize.

This prize will consist of three sub-prizes, described below.

Sub-Prize 1: Implement Plumo using PLONK ($300k)

Optimization Objective

Implement Plumo protocol in ZK-Garage/plonk using the fewest constraints possible.

Constraints

- The circuit must use a circuit arity of 4: three input witness wires and one output witness wire.
- The circuit must use BLS12-377 with BW6-761 as its 2-chain of elliptic curves.
- The submission must use the KZG polynomial commitment scheme.
- Submissions must include documentation, in English, to understand the optimization approach.
- The number of validators and epochs used within a circuit, as described in the Plumo protocol, will be fixed. The validator number is set to 143 and the epoch number is set to 120
- This implementation must be able to use the BW6-761 set up ceremony that Celo ran for the trusted set up.
- The implementation of Plumo must be another module like plonk-hashing and plonk-core, as seen in ZK-Garage

Benchmarks

The baseline is the proving time in the Plumo circuit as implemented by Celo. Submissions must beat this baseline by at least 30% in order to be eligible for a prize. Concrete targets to be given in the Github Issue, and released when the issue competition commences.

Sub-Prize 2: Implement Reinforced Concrete in PLONK ($70k)

Optimization Objective

Implement Reinforced Concrete hash function in ZK-Garage/plonk using as few constraints as possible. The constraint count is the number of arity-4 gates required to perform a hash of a single scalar inside a snark circuit.

Constraints

- The circuit must use a circuit arity of 4: three input witness wires and one output witness wire
- The circuit must use BLS12-381 and perform hashing over the BLS12-381 scalar field
- Competitors do need to derive their own constants and the field parameters. Constants for the BLS family are presented in the paper, and should be used.

Benchmarks

The threshold is 300 constraints. Only below this amount will competitors become eligible to receive a prize.

Sub-Prize 3: Design a Low-Complexity IOP for Lookups ($40k)

Optimization Objective

Design a Polynomial IOP for lookups with the lowest complexity. See more details here.

Constraints

- The number of polynomials sent by the prover must be constant, i.e. not depending on the degrees of the input polynomial, the preprocessed polynomial, or the size of the scalar field.

Benchmarks

Complexity is measured by the sum of the degrees of the polynomials sent by the prover.

The baseline is Plookup, which has a complexity of $O(n + d)$. Any submission with less complexity than this baseline is eligible for a prize.

Logistics

Competitors will be provided with access to a Coreweave-provided virtual workstation: consisting of an NVIDIA Quadro RTX 4000 with 8GB of GDDR6 RAM and 5 vCPU cores with 30 GB of CPU RAM.

Timeline

- **June 10 -** Competition begins
- **July 25 -** Mid-competition submission due
- **September 10 -** Final submission due

Judging

Submissions will be checked for both correctness and ranked by performance as described in each sub-prize section.

In addition, all submissions will be manually reviewed by the prize committee consisting of representatives from:

- Anoma
- Polychain Capital
- Aztec

Prizes will be given out in good faith and in the sole discretion of the prize committee. In addition, documentation (in English) must be provided along with the implementation. The documentation can be written in-line or as a separate document. It should be thorough and explanatory enough to provide an understanding of the techniques used in the submitted implementation without requiring an associated verbal explanation.

Prize Allocation

For the Main Prize, and Bonus Prize 1, the prize amounts will each be divided among the top three finishers according to the following proportions: 75% to winning implementation, 15% to second place, and 10% to third place. In the event that there are only two qualifying submissions, first place will receive 80% of the prize pool and second place 20%. In the event there is only one qualifying submission, they will receive 100% of the prize pool.

For Bonus Prize 2, the first winning submission will receive 100% of the prize amount.

Prizes will be given out in good faith and in the sole discretion of the prize committee.

Notes

All submission code must be open-sourced at the time of submission. Code and documentation must be dual-licensed under both the MIT and Apache-2.0 licenses.

All will be defined as detailed issues in the Github before competition start date. This will include extra details, tips and pointers to all existing resources pertinent to each category.

Link where it will be described: https://github.com/ZK-Garage/plonk/issues

Questions

If there are any questions about this prize 1 or 2, please contact *Josh or Luke* (joshua@heliax.dev luke@polychain.capital).

Regarding prize 3, please contact either of the above emails or *Ariel* (ariel@aztecprotocol.com)