HIGH-THROUGHPUT MARLIN VERIFIER

Prize Sponsor

Aleo

Prize Architect

Aleo

Prize Description

Summary

Marlin is a zero-knowledge proof system that is both universal and updateable. It forms the basis for privacy-preserving application platforms such as Aleo. On a public blockchain network, validators must construct blocks out from submitted user transactions in batches over a prescribed interval. Doing this as efficiently as possible is important for scalability in any zk-based L1 or L2.

Optimization Objective

- Verify as many batches of Marlin proofs as possible in a 10-second period as possible
- Minimize total cost

Constraints

Competitors will be required to verify Marlin proofs over multiple rounds. A round consists of a predetermined sequence of proof batches grouped as follows:

- Group 1: 10 batches consisting of 100 proofs / batch
- Group 2: 100 batches consisting of 10 proofs / batch
- Group 3: 20 batches of a variable number of proofs per batch sampled according to a standard distribution with $\mu = 50$ and $\sigma = 25$

Within a round, the different groups of proof batches may be aggregated and verified in parallel. But the rounds themselves must be run serially. The goal is to compute as many **complete** rounds as possible over a ten-second interval.

A solution must finish at least 1 sequence of three verification rounds to be eligible for the prize.

A solution must use the implementation of the Marlin verifier that is provided.

Timeline

- **June 10 -** Competition begins
- **July 25 -** Mid-competition IPR
- **October 15** - Deadline for submissions
- **October 30** - Winners announced

Judging

Competitors for the prize will be selected based on their prior documented experience and academic achievement.   Submissions will be checked for correctness and ranked by performance. 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.

Correctness

We will provide a set of test proofs and public parameters at the start of the competition, as well as a test harness for competitors to verify that they are correctly implementing the verification algorithm. We will also introduce malformed proofs into each round. Verification of those proofs must fail, or the solution will be deemed incorrect.

Performance

The score for this prize will simply be the number of rounds verified in a ten-second period, divided by the cost to replicate your instance.

Hardware & Benchmarks

Each competitor will have a $2,000 budget for use on the Coreweave cloud. Any configuration of hardware may be used.

Prize Allocation

The prize amount will be divided among the top three finishers according to the following proportions: 65% to winning implementation, 25% to second place, and 10% to third place.

A submission will only be considered eligible for a prize if it beats the benchmark by AT LEAST 2x.

In the event that there are only two qualifying submissions, first place will receive 70% of the prize pool and second place 30%. In the event there is only one qualifying submission, they will receive 100% of the prize pool.

Prizes will be given out in good faith and in the sole discretion of the prize committee, which in this case consists solely of representatives designated by Aleo Systems Inc.

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.

Questions

If there are any questions about this prize, please contact *Alex at Aleo*: zprize@aleo.org

References

Marlin paper - https://eprint.iacr.org/2019/1047.pdf