ACCELERATING MULTI-ASSET SHIELDED POOLS IN WASM

Prize Sponsor

anoma

Prize Architect

anoma

Prize Description

Summary

This prize will be awarded to the fastest WebAssembly prover implementation for the Groth16 proof system and Anoma's Multi-Asset Shielded Pool circuits over the BLS12-381 curve.

Anoma's Multi-Asset Shielded Pool (MASP) is an extension of Zcash's Sapling protocol that allows for multiple assets to be exchanged privately. Like Sapling, the MASP uses a UTXO model for transactions and queries Merkle trees of notes and nullifiers.

The MASP consists of three circuits: Spend, Output, and Convert. All of these circuits are written using R1CS for the Groth16 proving system. (Spend and Output are borrowed from Zcash's Sapling protocol.)

To facilitate proving in the browser, Anoma would like a fast implementation of a prover for the MASP circuits in WebAssembly.

Optimization Objective

Achieve the lowest weighted proving time for the MASP Spend, Output, and Convert circuits in WASM runtimes.

Constraints

- Runtime must be in WASM
- Single-threaded only
- Circuit must use the BLS12-381 curve
- The implementation can be constructed in a high-level language (Rust, C, C++, Javascript, etc.) or manually written in WebAssembly.
- All submissions must include documentation (in English) sufficient to understand the approach being taken.

Timeline

- **June 17** - Competition begins
- **July 25** - Mid-competition IPR
- **September 17** - Deadline for submissions
- **October 1** - Winners announced

Judging

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

The submission will be checked against MASP test vectors provided to the participants as well as randomly selected test vectors that are not disclosed to any competitors.

Performance

The degree of performance improvement will be measured against an up-to-date version of the MASP at https://github.com/anoma/masp on the day of judging. The proving time for the three circuits will be weighted as: *2×Spend* proving time, *2×Output* proving time, and *1×Convert* proving time.

Hardware & Benchmarks

Implementations will be compiled to WASM and benchmarked on a consumer-laptop with at least 8 cores in Google Chrome.

Prize Allocation

The top three performing submissions are eligible for prizes. Fifty-percent of the prize amount will be distributed ordinally, and the remaining fifty-percent will be distributed proportionally according to the degree of performance improvement.

Ordinal Allocation

Fifty-percent of the prize amount will be divided among the top three finishers according to the following proportions: 30% to the winning implementation, 15% to second place, and 5% to third place.

In the event that there are less than three qualifying submissions the remaining prize money will be divided proportionally among the finishers

Proportional Improvement Bonus

Fifty-percent of the prize is distributed among the top three submissions proportionally by their improvement ratios.

As an example, if the top three submissions give improvement ratios of 0.80, 0.85, and 0.90 respectively, the top finisher will receive a bonus of 23% of the total prize money.

(0.50) x (1/0.80 - 1) / ((1/0.80 - 1) x (1/0.85 - 1) x (1/0.90 - 1)) ≈ 23%

This means any participant in the top three places can increase their share of the prize by improving their own submission, even if it does not change their finishing rank.

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 Anoma.

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 *Joshua Fitzgerald* at joshua@heliax.dev or *Chris Goes* at cwgoes@heliax.dev.

References