Nicolas Liochon, Théodore Chapuis-Chkaiban, Alexandre Belling, Olivier Bégassat

Many thanks to Thomas Piellard

, Blazej Kolad

and Gautam Botrel

for their constructive feedback.

Hi all, here is a proposal for an efficient zk-EVM arithmetization which we are starting to implement. Our objective was to satisfy the 3 following design goals:

1. support for all EVM opcodes including internal smart contract calls, error management and gas management,
2. ability to execute bytecode as is,
3. minimal prover time.

We strive to provide an arithmetization that respects the EVM specification as defined in the Ethereum yellow paper. We provide a comprehensive approach which is technically realizable using existing zero-knowledge proving schemes. We would greatly appreciate any feedback you may have!

ZK_EVM.pdf (2.1 MB)