Associate Professorship of Embedded Systems and Internet of Things
Department of Electrical and Computer Engineering
Technical University of Munich

Folding in gnark

Master Thesis

Jens Ernstberger, April 24, 2023

Title: “Folding in gnark”
Supervisor: Jens Ernstberger
Period: 24 weeks

Context

Recursive SNARK computation ensures the feasibility of many state-of-the-art solutions for blockchain scalability and on-chain identity verification. IVC (Incrementally Verifiable Computation) enables the prover to recursively prove the correct execution of incremental computations at n steps. A well-known approach to construct IVC is to use succinct non-interactive arguments of knowledge (SNARKs) for NP: at each incremental step n, the prover produces a SNARK proving that it has applied F correctly to the output of step n-1 and that the SNARK verifier represented as a circuit has accepted the SNARK from step n-1.

The goal of this thesis is to implement a folding scheme, such as Nova [1, 5, 3, 2], in the gnark library [8]. gnark already provides the SNARK primitive in a usable interface, such that the main task lies in implementation of the folding scheme itself. So far, there only exists a folding scheme implementation in circom with Groth16 [10] and a Nova implementation that makes use of the Spartan proof system based on the hardness of the discrete logarithm problem [9]. Ideally, the folding scheme to be implemented enables usage of arbitrary predicates at each step [5], and relies on plonkish arithmetization [3].

Requirements

- High: Independent work ethic and strong mathematical background.
- High: Knowledge of Golang and number theory.

Tasks

1. Familiarization with SNARKs and folding schemes
2. Familiarization with gnark and gnark-crypto
3. Proposing a detailed methodology for implementation
4. Implementation of the proposed methodology
5. Experiments: Measure performance of the proposed methodology as compared to existing implementations

Preliminary Schedule

Task / Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Familiarization	■	■	■	■																				
Definition of resources			■	■	■																			
Proposal of a Methodology						■	■	■	■	■														
Implementation											■	■	■	■	■	■								
Experiments																	■	■	■	■				
Report																					■	■	■	■

References

[1] https://eprint.iacr.org/2021/370.pdf

[2] https://eprint.iacr.org/2023/573.pdf

[3] https://github.com/geometryresearch/technical_notes/blob/main/sangria_folding_plonk.pdf

[4] https://www.ingonyama.com/blogs/sparkworks-native-hardware-acceleration-in-arkworks

[5] https://eprint.iacr.org/2022/1758.pdf

[6] https://eprint.iacr.org/2022/999.pdf

[7] https://eprint.iacr.org/2022/1396.pdf

[8] https://github.com/ConsenSys/gnark

[9] https://github.com/microsoft/Nova

[10] https://github.com/nalinbhardwaj/Nova-Scotia