Master Thesis Contract

Rasmus Kirk Jakobsen - 201907084 Abdul Haliq Abdul Latiff - 202303466

Thesis Title

Incrementally Verifiable Computation (IVC) Over Signatures Using Halo2

Objective

The primary focus of this thesis is to investigate Incrementally Verifiable Computation (IVC) using Halo2, a recursive proof system designed. Our implementation will build upon existing work from previous projects covering PLONK and accumulation schemes.

Scope

1. **Full Working and Succinct Plonk**
   - Develop a fully functional implementation of the Plonk protocol using Rust and Arkworks.
   - A succinct verifier that can be used for IVC.
2. **Implement Gadgets**
   - Construct utility sub-circuits using our Plonk implementation.
3. **Generalize Plonk and PCDL**
   - Allow our Plonk and discrete logarithm polynomial commitment scheme to be general over pasta curves.
4. **Benchmark performance over circuit size**
   - Benchmark the performance of our implementation and estimate its average complexity.
   - Compare benchmark data with theoretical expected performance required for IVC.
5. **Create Circuit Components required for IVC**
   - This involves:
     - Using poseidon hashes for Fiat-Shamir.
     - Finding an efficient way to do Scalar Multiplication in circuits.
     - Encoding our verifiers into circuits.
6. **Extend Plonk to TurboPlonk:**
   - In order to acheive efficient circuits we aim to implement TurboPlonk[1]:
     - TurboPLONK: PLONK arithmetization + custom gates + larger fan-in/fan-out
     - PlonkUp: PLONK arithmetization + lookup tables using plookup.
     - UltraPLONK: PLONK arithmetization + custom gates + larger fan-in/fan-out + lookup tables using plookup.
7. **Investigate Chain of Signatures**
   - Explore the feasibility of IVC over a chain of signatures to be used in committee based blockchain consensus protocols.
   - Ideally, we would want a reference implementation to show this idea.

Expected Outcomes

- A complete and functional Halo2-based implementation; Plonk with lookups, accumulation schemes and potentially gadgets.
- A performance analysis comparing the feasibility of using IVC in blockchains.
- An exploration of potential use cases, particularly in the domain of blockchain scalability.
- An implementation showing off the concept of Chain of Signatures IVC

[1] Link: https://zkjargon.github.io/definitions/plonkish_arithmetization.html

Methodology

- **Programming Languages & Tools**: Rust and Arkworks.
- **Research & Development**: Iterative design, testing, and validation of cryptographic primitives.
- **Evaluation Metrics**: Performance benchmarks, security proofs, and benchmarking.

Conclusion

The thesis aims to deepen our practical understanding of IVC through our Halo2 implementation. We will explore the feasibility of applying IVC over cryptographic signatures. By benchmarking this approach, we aim to assess its viability for blockchain companies seeking to develop more secure and efficient light clients.