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

FPGA Acceleration for MSM

Master Thesis

Jens Ernstberger, April 24, 2023

Title: "FPGA Acceleration for MSM"
Supervisor: Jens Ernstberger
Period: 24 weeks

Context

Multi-Scalar Multiplication (MSM) on elliptic curves is a critical primitive and bottleneck in many zero-knowledge proof systems. Enhancing the performance of MSM can lead to faster proof generation, ultimately making zero-knowledge-based applications more practical. Recent advancements in the field, particularly those focused on hardware acceleration, have the potential to improve efficiency even further. Of particular interest are folding schemes, which primarily face the challenge of computing a single MSM per step [1, 3, 2].
The goal of this thesis is to design and develop a hardware acceleration toolkit for Multi-Scalar Multiplication using Field-Programmable Gate Arrays (FPGAs). Although previous efforts [5, 4, 6] have explored preliminary solutions, none have reached production status at the time of writing. The proposed solution should target the gnark-crypto library, building on existing work to optimize performance and usability.

Requirements

- High: Independent work ethic and mathematical background.
- High: Knowledge of FPGA implementation and Golang.

Tasks

1. Familiarization with SNARKs and solutions for FPGA acceleration
2. Definition of resources required
3. Proposing a detailed methodology for implementation
4. Implementation of the proposed methodology
5. Experiments: Measure performance of the proposed methodology

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/2022/999.pdf

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