Master’s Thesis Engineering Technology 2017-2018

Design of a fully balanced ASIC coprocessor implementing complete addition formulas on Weierstrass elliptic curves

Niels Pirotte

Master of Electronics and ICT Engineering Technology

Design of a fully balanced ASIC coprocessor
implementing complete addition formulas on
Weierstrass elliptic curves

Master of Electronics and ICT Engineering Technology

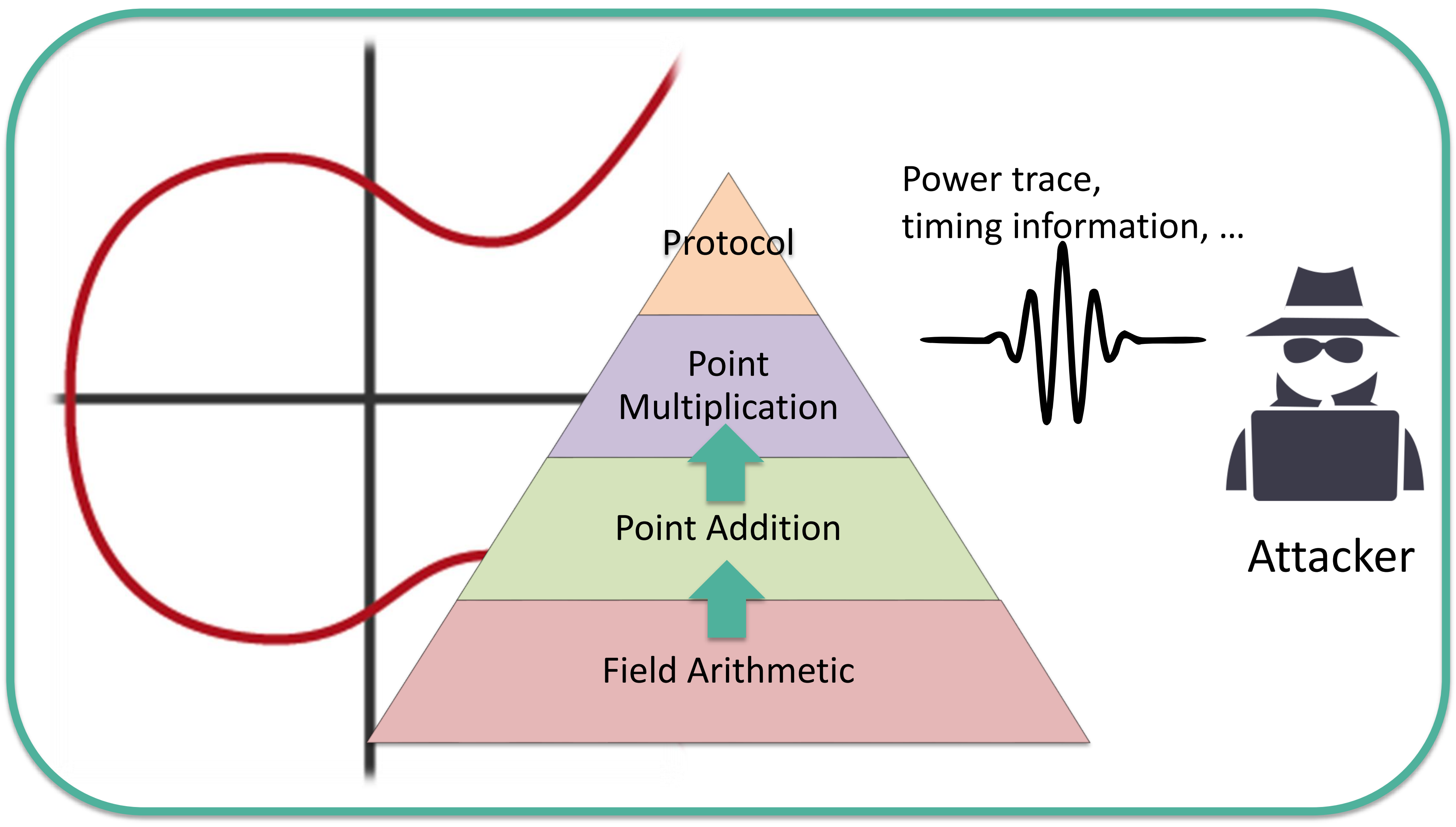
1. Introduction

Elliptic Curve Cryptography (ECC) is better suited for lightweight embedded applications than other Public Key cryptosystems. Traditionally, ECC is based on an addition law which uses two sets of equations. One for a pair of different points (point addition) and another one for a pair of identical points (point doubling).

The unavoidable conditional branching in implementations, as a consequence of the traditional formulas, makes designs susceptible to Side-Channel Attacks (SCA)**.**

The complete addition formulas by Renes et al. for Weierstrass elliptic curves should provide a balanced operation, resistant against Simple Power Analysis (SPA) attacks.

The goal of this Master’s thesis is to provide the first ASIC implementation of these complete formulas optimized for implementation area.



3. Results

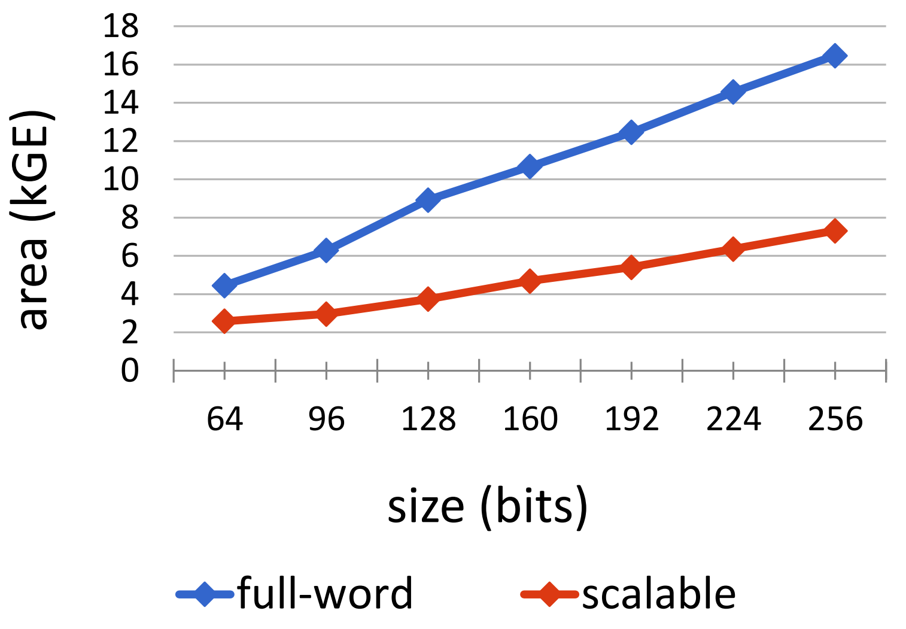
- Design was realized with VHDL and results were generated using Design Compiler 2016 with the NanGate 45nm library
- Scalable MMALU was 55% smaller than full-word MMALU, however 35 times slower
- Future work includes SCA to check resistance of the design

# bits	Area (kGE)	Area w/ reg. file (kGE)	max. Freq. (MHz)	Point mult. (ms)
64	17.77	10.03	333.33	-
96	26.30	14.77	250.00	-
128	34.12	18.64	166.67	-
160	42.48	23.22	166.67	5.52 (secp160k1)
192	51.02	27.96	142.86	-
224	59.12	32.45	111.11	-
256	66.51	36.06	100.00	23.06 (secp256k1)

Without randomization of operations

# bits	Area (kGE)	Area w/ reg. file (kGE)
64	21.58	13.84
96	31.91	20.38
128	41.51	26.03
160	51.08	31.81
192	61.35	38.29
224	71.59	44.92
256	81.89	51.45

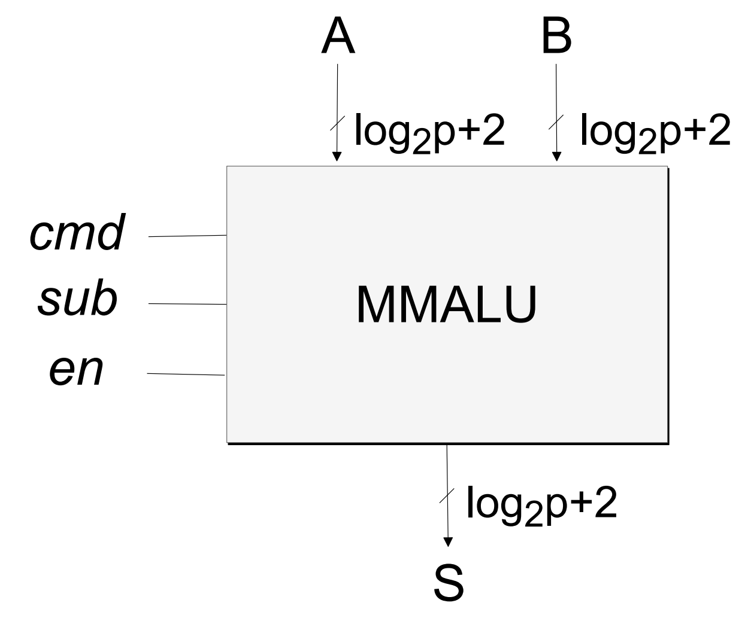
With randomization of operations



2. Bottom-up design

Field Arithmetic

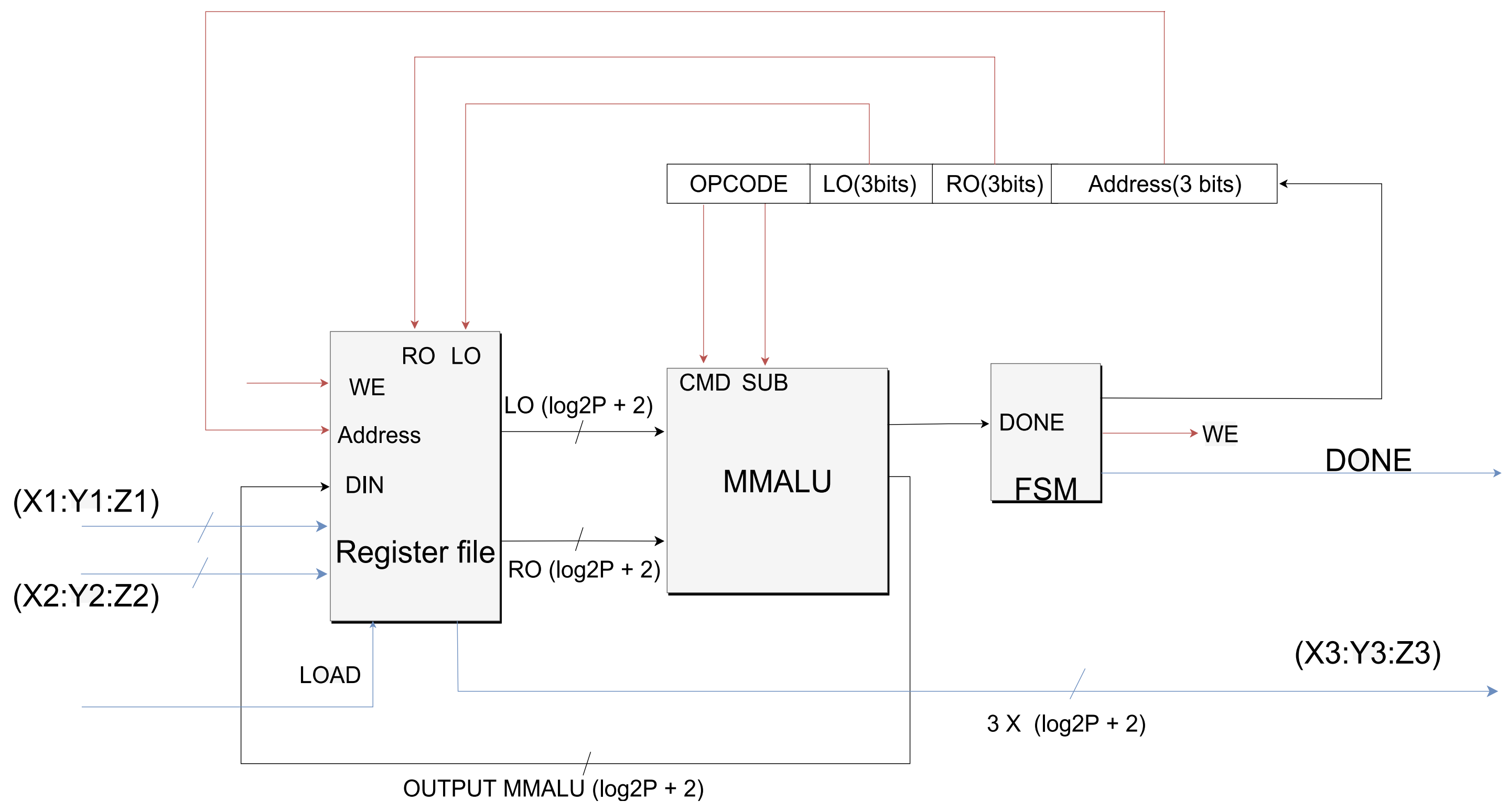
- Exploration of the Montgomery algorithm design parameters
- Both full-word and scalable datapath were designed and compared



Functionality	CMD	SUB
multiply	0	0
add	1	0
subtract	1	1
scale	0	1

Point Addition

- Minimization of operation count and register file size
- Addition law formulas are implemented in a Finite State Machine (FSM)



Point Multiplication

- Implemented using the Montgomery ladder algorithm
- The complete formulas enable modification of the Montgomery ladder in order to double the size of the key space
- Alternative version of the design implements randomization of the point operations as a countermeasure against Differential Power Analysis (DPA) attacks

Supervisors / Cosupervisors: Dr. Ing. Jo Vliegen, Prof. Dr. Ir. Nele Mentens, Prof. Dr. Lejla Batina