University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Doctor of Philosophy

of

IBRAHIM HAZMI

MSc (RMIT University, 2009)
BSc (King Saud University, 2001)

"Systolic Design Space Exploration of EEA-Based Inversion Over Binary and Ternary Fields"

Department of Electrical and Computer Engineering

Friday, August 24, 2018
1:00 P.M.
Engineering/Computer Science Building
Room 468

Supervisory Committee:
Dr. Fayez Gebali, Department of Electrical and Computer Engineering, University of Victoria (Co-Supervisor)
Dr. Atef Ibrahim, Department of Electrical and Computer Engineering, UVic (Co-Supervisor)
Dr. Phalguni Mukhopadhyaya, Department of Civil Engineering, UVic (Outside Member)

External Examiner:
Dr. Huapeng Wu, Department of Electrical and Computer Engineering, University of Windsor

Chair of Oral Examination:
Dr. Michelle Wiebe, Department of Curriculum and Instruction, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

Public-key cryptographic protocols are implemented in hardware to ensure low-area, high speed and reduced power consumption especially for mobile devices. Elliptic Curve Cryptography (ECC) is the most commonly used encryption technique and its performance depends heavily on efficient finite field arithmetic hardware. Finding the multiplicative inverse (inversion) is the most expensive finite field operation in ECC. The two predominant algorithms for computing finite field inversion are Fermat's Little Theorem (FLT) and Extended Euclidean Algorithm (EEA). EEA is reported to be the most efficient inversion algorithm in terms of performance and power consumption.

This dissertation presents a new reformulation of EEA algorithm, which allows for speedup and optimization techniques such as concurrency and resource sharing. Modular arithmetic operations over GF(p) are introduced for small values of p, observing interesting figures, particularly for modular division. Whereas, polynomial arithmetic operations over GF(p^m) are discussed adequately in order to examine the potential for processes concurrency. In particular, polynomial division and multiplication are revisited in order to derive their iterative equations, which are suitable for systolic array implementation. Consequently, several designs are proposed for each individual process and their complexities are analyzed and compared. Subsequently, a concurrent divider/multiplier-accumulator is developed, while the resulting systolic architecture is utilized to build the EEA-based inverter.

The processing elements of our systolic architectures are created accordingly, and enhanced to accommodate data management throughout our reformulated EEA algorithm. Meanwhile, accurate models for the complexity analysis of the proposed inverters are developed. Finally, a novel, fast, and compact inverter over binary fields is proposed and implemented on FPGA. The proposed design outperforms the reported inverters in terms of area and speed. Correspondingly, an EEA-based inverter over ternary fields is built, showing the lowest area-time complexity among the reported inverters.