University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Master of Applied Science

of

KAREEM MOEEN

BSc (Kuwait University, 2009)

"Progressive Product Reduction for Polynomial Basis Multiplication over GF(3^m)"

Department of Electrical and Computer Engineering

Friday, December 2, 2016
11:00 A.M.
Engineering and Computer Science Building
Room 467

Supervisory Committee:
Dr. Fayez Gebali, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Kin Li, Department of Electrical and Computer Engineering, UVic (Member)

External Examiner:
Dr. Alex Thomo, Department of Computer Science, UVic

Chair of Oral Examination:
Dr. Colin Bradley, Department of Mechanical Engineering, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

Galois fields are essential blocks of building many of cryptographic schemes. The main advantage of applying Galois fields over cryptographic applications are to reduce cost and increase the sufficiency of the performance. In past, they were interested in implement Galois field of characteristic 2 in most of the crypto-system application, but in the meantime, the researcher started to work on Galois field of odd characteristics which it has applications in many areas like Elliptic Curve Cryptography, Identity-based Encryption, Short Signature Schemes and etc.

In this thesis, an odd characteristic Galois field was implemented. In particular, this thesis focuses on implementation of multiplication and reduction on GF(3m). Overview about the thesis idea was presented in the beginning. Finite field arithmetic was discussed where it shows some of the Galois fields important definitions and properties. In addition, irreducible polynomials over GF(p) where p is prime and the basic additional and multiplication over GF(pm) was discussed as well. Introduction to the proposed implementation started with the arithmetic of the Galois field characteristics 3 GF(3). The problem formulation introduced by its mathematical representation and the Progressive Product Reduction (PPR) technique which is the technique used in this thesis. Implement three different semi-systolic arrays architecture with different projection functions. This stage followed by modeling assumption for complexity analysis for both area and delay where it used to compare proposed designs with other published designs. Proposed design gets verified by Matlab code implementation at the end of this thesis.