University of Victoria | Graduate Studies

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

of

BADER HAMMAD ALHAZMI

MSc (Concordia University, 2011)
BSc (King Abdulaziz University, 1999)

"Fast Prime Field Arithmetic Using Novel Large Integer Representation"

Department of Electrical and Computer Engineering

Thursday, July 4, 2019
8:30 A.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. Andrew Rowe, Department of Mechanical Engineering, UVic (Outside Member)

External Examiner:
Dr. Ehab Elmallah, Department of Computing Science, University of Alberta

Chair of Oral Examination:
Dr. Sudhir Nair, School of Business, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

Large integers are used in several key areas such as RSA (Rivest-Shamir-Adleman) public-key cryptographic system and elliptic curve public-key cryptographic system. To achieve higher levels of security requires larger key size and this becomes a limiting factor in prime finite field *GF*(*p*) arithmetic using large integers because operations on large integers suffer from the long carry propagation problem. Large integer representation has direct impact on the efficiency of the calculations and the hardware and software implementations. Attempts to use different representations such as residue number systems suffer from their own problems. In this dissertation, we propose a novel and efficient attribute-based large integer representation scheme capable of efficiently representing the large integers that are commonly used in cryptography such as the five NIST primes and the Pierpont primes used in supersingular isogeny Diffie-Hellman (SIDH) used in post-quantum cryptography. Moreover, we propose algorithms for this new representation to perform arithmetic operations such as conversions from and to binary representation, two's complement, left-shift, numbers comparison, addition/subtraction, modular addition/subtraction, modular reduction, multiplication, and modular multiplication. Extensive numerical simulations and software implementations are done to verify the performance of the new number representation. Results show that the attribute-based large integer arithmetic operations are done faster in our proposed representation when compared with binary and residue number representations. This makes the proposed representation suitable for cryptographic applications on embedded systems and IoT devices with limited resources for better security level.