Modular Multiplication in the Residue Number System

A DISSERTATION SUBMITTED TO
THE SCHOOL OF ELECTRICAL AND ELECTRONIC ENGINEERING
OF THE UNIVERSITY OF ADELAIDE
BY

Yinan KONG

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY

July 2009

Declaration of Originality

Name: Yinan KONG Program: Ph.D.

This work contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

I give consent to this copy of my thesis, when deposited in the University Library, being made available for loan and photocopying, subject to the provisions of the Copyright Act 1968.

The author acknowledges that copyright of published works contained within this thesis (as listed below) resides with the copyright holder/s of those works.

Signature: Date:

Acknowledgments

My supervisor, Dr Braden Jace Phillips, is an extremely hard working and dedicated man. So, first and foremost, I would like to say "thank you" to him, for his critical guidance, constant sustainment and role modelling as a supervisor. It is my true luck that I have been able to work with him for these years. This has been a precious experience which deserves my cherishing throughout my whole life.

I am also grateful to Associate Professor Cheng-Chew Lim and Dr Alison Wolff for their guidance through important learning phases of this complex technology. Throughout the course of my study I have received considerable help from my colleagues Daniel Kelly and Zhining Lim, who have been, and will remain, my great friends.

Acknowledgement is given to the Australian Research Council (ARC) as this work has been supported by the ARC Discovery Project scheme.

Thanks to the support from my family and friends. I have been relying on you throughout my candidature. Thanks are due to Mum, Dad, Ranran, Zhaozhao and Jingdong JU, who flew over 5000 miles to take care of me. I would definitely not have been able to get to this point without your encouragement. You are the real pearls lying on the bottom of my mind.

Mother, thank you for giving birth to me as well as cultivating me through those tough years. This thesis has your sweat in it.

My love, BEN YA, you are my greatest inspiration. Thank you for all you have done for me.

Yinan KONG
November 2008

Abstract

Public-key cryptography is a mechanism for secret communication between parties who have never before exchanged a secret message. This thesis contributes arithmetic algorithms and hardware architectures for the modular multiplication $Z = A \times B \mod M$. This operation is the basis of many public-key cryptosystems including RSA and Elliptic Curve Cryptography. The *Residue Number System* (RNS) is used to speed up long word length modular multiplication because this number system performs certain long word length operations, such as multiplication and addition, much more efficiently than positional systems.

A survey of current modular multiplication algorithms shows that most work in a positional number system, e.g. binary. A new classification is developed which classes these algorithms as Classical, Sum of Residues, Montgomery or Barrett. Each class of algorithm is analyzed in detail, new developments are described, and the improved algorithms are implemented and compared using FPGA hardware.

Few modular multiplication algorithms for use in the RNS have been published. Most are concerned with short word lengths and are not applicable to public-key cryptosystems that require long word length operations. This thesis sets out the hypothesis that each of the four classes of modular multiplication algorithms possible in positional number systems can also be used for long word length modular multiplication in the RNS; moreover using the RNS in this way will lead to faster implementations than those which restrict themselves to positional number systems. This hypothesis is addressed by developing new Classical, Sum of Residues and Barrett algorithms for modular multiplication in the RNS. Existing Montgomery RNS algorithms are also discussed.

The new Sum of Residues RNS algorithm results in a hardware im-

plementation that is novel in many aspects: a highly parallel structure using short arithmetic operations within the RNS; fully scalable hardware; and the fastest ever FPGA implementation of the 1024-bit RSA cryptosystem at 0.4 ms per decryption.

Publications

1. Yinan Kong and Braden Phillips, "Fast Scaling in the Residue Number System", accepted by IEEE Transactions on VLSI Systems in December 2007.

2. Yinan Kong and Braden Phillips, "Simulations of modular multipliers on FPGAs", Proceedings of the IASTED Asian Conference on Modelling and Simulation, Beijing, China, Oct. 2007, pp. 11281131.

3. Yinan Kong and Braden Phillips, "Comparison of Montgomery and Barrett modular multipliers on FPGAs", 40th Asilomar Conference on Signals, Systems and Computers. Pacific Grove, CA, USA: IEEE, Piscataway, NJ, USA, Oct. 2006, pp. 16871691.

4. Yinan Kong and Braden Phillips, "Residue number system scaling schemes", in Smart Structures, Devices, and Systems II, ser. Proc. SPIE, S. F. Al-Sarawi, Ed., vol. 5649, Feb. 2005, pp. 525536.

5. Yinan Kong and Braden Phillips, "A classical modular multiplier for RNS channel operations", The University of Adelaide, CHiPTec Tech. Rep. CHIPTEC-05-02, November 2005.

6. Yinan Kong and Braden Phillips, "A Montgomery modular multiplier for RNS channel operations", The University of Adelaide, CHiPTec Tech. Rep. CHIPTEC-05-02, November 2005.

Publications in Submission

1. Yinan Kong and Braden Phillips, "Modular Reduction and Scaling in the Residue Number System Using Multiplication by the Inverse", submitted to IEEE Transactions on VLSI Systems in November 2008.

2. Yinan Kong and Braden Phillips, "Low latency modular multiplication for public-key cryptosystems using a scalable array of parallel processing elements", submitted to 19th IEEE Computer Arithmetic in October 2008.

3. Braden Phillips and Yinan Kong, "Highly Parallel Modular Multiplication in the Residue Number System using Sum of Residues Reduction", submitted to Journal of Applicable Algebra in Engineering, Communication and Computing in June 2008.

4. Yinan Kong and Braden Phillips, "Revisiting Sum of Residues Modular Multiplication", submitted to International Journal of Computer Systems Science and Engineering in May 2008.

Nomenclature

$\langle X \rangle_M$	The operation X mod M.
D	The dynamic range of a RNS.
M	The modulus of a modular multiplication, typically n bits.
m_i	The ith RNS channel modulus.
N	The number of RNS channels.
n	The wordlength of M.
w	The RNS channel width.
$\lceil X \rceil$	The ceiling of X. The smallest integer greater than or equal to X.
$\lfloor X \rfloor$	The floor of X. The largest integer smaller than or equal to X.
BE	Base Extension.
CRT	Chinese Remainder Theorem.
DSP	Digital Signal Processing.
ECC	Elliptic Curve Cryptography.
LUC	Look-Up Cycle.
LUT	Look-Up Table.
LUT	Look-Up Table

MRS Mixed Radix Number System.

QDS Quotient Digit Selection.

RNS Residue Number System.

RSA RSA Cryptography.

Contents

List of Figures

List of Tables