An RNS-Enabled Microprocessor for Public Key Cryptography

Zhining Lim

B.E.(Comp. Sys.)(Hons.)

A THESIS SUBMITTED IN FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

SCHOOL OF ELECTRICAL AND ELECTRONIC ENGINEERING
THE UNIVERSITY OF ADELAIDE · AUSTRALIA

February 2010

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ALGORITHMS

ABSTRACT

Mobile computing platforms must be secure, fast, small, and power efficient. While public key cryptography methods provide the framework for secure communications, their algorithms tend to be computationally complex and hence need some form of hardware acceleration. This thesis investigates an alternative implementation of public key cryptology algorithms on a microprocessor that has been augmented with hardware support for the residue number system (RNS).

The RNS promises efficient arithmetic by replacing the long integers used in public key cryptology with sets of smaller independent numbers. Doing so allows flexibility in instruction scheduling and reduces carry propagation delays. Past RNS public key cryptosystem implementations used a parallel architecture. Although well-suited to the RNS, a parallel architecture is not necessarily power efficient nor small since it requires several copies of the RNS hardware. The microprocessor implementation in this thesis has a novel sequential architecture that has modest area and power consumption because it uses just one set of the RNS hardware.

The RNS-enhanced microprocessor, the $\mathbb{Z}$-Core, is based on the small, low-power Xtensa LX2.1 core from Tensilica, Inc. It was augmented with RNS hardware specified using the Tensilica Instruction Extension language. Unlike other cryptographic accelerators, these RNS enhancements are useful for a variety of cryptosystems. The $\mathbb{Z}$-Core was used for implementations of RSA and the elliptic curve digital signature algorithm. The RNS implementations on the $\mathbb{Z}$-Core outperformed equivalent implementations that use the normal multiprecision methods. The area and power consumption of the $\mathbb{Z}$-Core were within the GSM 11.18 1.8-V SIM specifications for smart cards when running the two algorithms, hence it satisfied the requirements of mobile computing.

DECLARATION OF ORIGINALITY

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 to Zhining Lim 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 the thesis, when deposited in the University Library, being available for loan, photocopying, and dissemination through the library digital thesis collection, subject to the provisions of the Copyright Act 1968.

I also give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library catalogue, the Australasian Digital Thesis Program (ADTP) and also through web search engines, unless permission has been granted by the University to restrict access for a period of time.

Zhining Lim
8 February 2010

ACKNOWLEDGEMENTS

My deepest gratitude goes to my supervisor, Dr Braden Phillips. I would like to thank him for his continued support, encouragement, and helpful ideas along the way. I would also like to thank my co-supervisor, Associate Professor Michael Liebelt, for his guidance in the project.

This project would not have been possible without the generosity of Tensilica, Inc. in Santa Clara, California, USA. Under their University Program, I was given extensive access to their Xtensa LX2.1 microprocessor core. Their RTL licence provided the capabilities to run area and power measurements using Synopsys tools. I would not have been able to explore the RNS architectural enhancements nor collect the results as easily and painlessly without the Tensilica tools.

This project has been supported by the Australian Research Council's Discovery Projects funding scheme (project number DP0557582). My research candidature was supported by an Australian Postgraduate Award and by the Frank Perry Supplementary Scholarship from the University of Adelaide. In addition, I gratefully acknowledge the IEEE South Australian Section for covering some of my travel expenses through their Travel Award.

Finally, but in no means the least, I would like to thank my family for their support and love.

Zhining Lim
8 February 2010

PUBLICATIONS

LIM, Z., PHILLIPS, B. J., AND LIEBELT, M. 2009. Elliptic Curve Digital Signature Algorithm over $GF(p)$ on a Residue Number System Enabled Microprocessor. In *IEEE Region 10 Conference TENCON 2009*. Singapore.

LIM, Z., AND PHILLIPS, B. J. 2007. An RNS-Enhanced Microprocessor Implementation of Public Key Cryptography. In *41st Asilomar Conference on Signals, Systems, and Computers*. Pacific Grove, California, USA, 1430–1434.

LIM, Z., AND PHILLIPS, B. J. 2007. An RNS-Enabled Architecture on the Tensilica Xtensa LX Processor. Tech. Rep. CHIPTEC-07-01. Centre for High Performance Integrated Technologies and Systems, The University of Adelaide, Adelaide, Australia.

LIST OF ABBREVIATIONS

ANSI	American National Standards Institute
CIOS	Coarsely Integrated Operand Scanning
CISC	Complex Instruction Set Computer
CRT	Chinese Remainder Theorem
DPA	Differential Power Analysis
ECC	Elliptic Curve Cryptography or Cryptosystem
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
GSM	Global System for Mobile communications
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
MRS	Mixed Radix System
NIST	National Institute of Standards and Technology
RISC	Reduced Instruction Set Computer
RNS	Residue Number System
RTL	Register Transfer Level
RSA	Rivest-Shamir-Adleman Public Key Cryptosystem
SECG	Standards for Efficient Cryptography Group
SPA	Simple Power Analysis
SRAM	Static RAM
TIE	Tensilica Instruction Extension language

TSMC Taiwan Semiconductor Manufacturing Company

LIST OF PRINCIPAL SYMBOLS

$\vee$	Bit-wise OR
$\wedge$	Bit-wise AND
$\Longleftarrow$	Base extension
$\mathcal{O}$	ECC point at infinity
a	32-bit Xtensa address register, or its contents
A	64-bit user-defined register, or its contents
$\mathtt{A}_L$	Lower 32-bits of 64-bit A
$\mathtt{A}_U$	Upper 32-bits of 64-bit A
$\mathcal{B}_A$	RNS base A
$\mathcal{B}_{A \cup B}$	RNS base containing channel moduli of base A and base B
(C, S)	Product of two numbers separated into two words, S and C
G_i	Channel i of RNS form of G
G mmod p	Montgomery modular reduction of G modulo p
$\langle G \rangle_p$	RNS value G reduced modulo p
$\langle G \rangle_{\mathcal{B}_A}$	RNS value G reduced modulo all moduli in RNS base A
$\widetilde{G}$	RNS value G with corrective Montgomery factor
k_i	ith bit or word of k, depending on the context
m_i	Modulus of RNS channel i
m_{A_i}	Modulus of RNS channel i of $\mathcal{B}_A$
M	Dynamic range of an RNS base
M_A	Dynamic range of $\mathcal{B}_A$
M_{A_i}	Dynamic range of $\mathcal{B}_A$ divided by modulus of channel i in $\mathcal{B}_A$

`MEM32[a]`	32-bit memory access at memory address `a`
`MEM64[a]`	64-bit memory access at memory address `a`
$R[i]$	ith element of array R
x_{dec}	A number x in decimal form or base 10
x_{hex}	A number x in hexadecimal form or base 16
x_G	x-coordinate of ECC point G in affine form
X_G	x-coordinate of ECC point G in a projective form
$\langle x \rangle_p$	Modular reduction of x modulo p
$\langle x^{-1} \rangle_p$	Multiplicative inverse of x modulo p