# AN FPGA IMPLEMENTATION OF AN ELLIPTIC CURVE PROCESSOR FOR AN EMBEDDED PUBLIC-KEY CRYPTOSYSTEM

LIM KIE WOON

UNIVERSITI TEKNOLOGI MALAYSIA

# AN FPGA IMPLEMENTATION OF AN ELLIPTIC CURVE PROCESSOR FOR AN EMBEDDED PUBLIC-KEY CRYPTOSYSTEM

LIM KIE WOON

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Engineering (Electrical)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

JANUARY 2005

## ACKNOWLEDGEMENTS

Firstly, I would like to express my gratitude to my supervisor, Prof. Dr. Haji Mohamed Khalil bin Haji Mohd Hani for his invaluable support, patience and unbounded enthusiasm throughout this work. Thanks for helping me to kickstart this research by providing insights and his working experience as reference.

I would also like to express my thankfulness to my friends, J-Wing, Avinash, Eng Kean, Izuan, Arul, Yuan Wen and Kwee Siong. I value the camaraderie we share as well as the time they spent to share with me enriching ideas, as well as their concern. Not excluding my senior, Vincent, who is the author of SHA-1 processor core that provides the softcore and documentations of the hash processor to this work. Many thanks also to our hardworking technicians in ECAD lab, En. Zulkffli bin Che Embong and En. Khomarudden bin Mohd Khair Juhari.

My sincerest thanks to all those who have helped to make this thesis possible. Warmest regards to my parents, siblings and relatives for their seamless caring encouragement and moral support that enable this journey. Without exception, a special thanks to Phaik Yong for her consistent encouragement and concern over time that made the journey enjoyable and meaningful. Without her unwavering support, love and devotion through the years, this thesis could not have been realized.

Finally, an acknowledgement is extended to IRPA for their funding support and Altera Corporation for their equipment grants.

# ABSTRACT

Information security in terms of authentication, confidentiality, data integrity, and non-repudiation is one of the critical aspects in majority of communication and computer networks. The deployment of information security requires the implementation of public-key cryptographic schemes such as encryption, digital signature and key-agreement, as introduced by Diffie and Hellman in 1976. Recently, the elliptic curve cryptography (ECC) is rapidly gaining popularity due to its comparatively high security level and low bandwidth requirements. The main strength of ECC rests on the concept of discrete logarithm problem over the points on an elliptic curve, which provides higher strength-per-bit than any other current public-key cryptosystems. This thesis proposes a design of an elliptic curve processor core (ECP) to accelerate elliptic curve operations. The processor core is designed as a coprocessor to an embedded processor to perform Montgomery point multiplication and point addition. The design is described completely in parameterized VHDL code, such that the core is reconfigurable and reusable. An elliptic curve digital signature cryptosystem is developed as an evaluation platform to validate the proposed processor. The cryptosystem is an integration of a number of processors, which include an Altera Nios embedded processor, a SHA-1 hash processor core and the proposed elliptic curve processor core. The system is implemented on an Altera Nios Development Board (Stratix Professional Edition) and the experimental results show that the prototype can compute elliptic curve point multiplication in 0.14msec in finite field $GF(2^{163})$ with an operating frequency of 95 MHz. This computation speed is the fastest when compared to other existing designs reported in documented literature. Consequently, the result of this work is a reusable IP (Intellectual Property) core targeted for application in high-speed security system.

# ABSTRAK

Keselamatan maklumat dalan konteks pengesahan, kerahsiaan, kewibawaan data dan tidak penolakan merupakan salah satu aspek kritikal dalam kebanyakan rangkaian komunikasi dan komputer. Penyediaan keselamatan maklumat memerlukan pelaksaan skim kriptografi kunci-awam seperti enkripsi, tandatangan digital, perjanjian kunci, seperti yang diperkenalkan oleh Diffie dan Hellman pada 1976. Sejak kebelakangan ini, kriptografi lengkung eliptik mendapat populariti dengan cepat disebabkan oleh tahap sekuriti yang tinggi dan keperluan lebar jalur yang rendah secara bandingan. Kekuatan utama kriptografi lengkung eliptik terletak pada masalah logaritma diskret dalam titik lengkung eliptik, dimana ia memberikan kekuatan bit tertinggi jika dibandingkan dengan sistem kriptografi kunci-awam yang lain. Tesis ini mancadangkan rekabentuk satu teras pemproses lengkung eliptik untuk mempercepatkan operasi lengkung eliptik. Teras pemproses ini direkabentuk sebagai satu kopemproses kepada satu pemproses terbenam untuk menjalankan pendaraban titik Montgomery dan penambahan titik. Rekabentuk ini dibina dengan menggunakan kod VHDL berparameter, supaya teras ini boleh diaturcara dan digunakan semula. Satu sistem kriptografi tandatangan digital lengkung eliptik dibina sebagai pelantar penilaian untuk mengesahkan pemproses yang dicadangkan. Sistem kriptografi ini merupakan integrasi beberapa pemproses iaitu satu pemproses terbenam Nios oleh Altera, satu teras pemproses *hash* SHA-1 dan teras perproses lengkung eliptik yang dicadangkan. Sistem ini dilaksanakan pada papan pembangunan Nios (Edisi Stratix Profesional) oleh Altera dan keputusan eksperimen menunjukkan bahawa prototaip ini berupaya mengira pendaraban titik lengkung eliptik dalam tempoh 0.14 milisaat untuk medan terhingga $GF(2^{163})$ pada 95 megahertz sebagai frekuensi operasinya. Kelajuan pengiraan ini merupakan yang terpantas dibandingkan rekabentuk yang sebelumnya pada karya yang didokumentasikan. Justeru itu, hasil kerja ini merupakan teras *IP* yang boleh diguna semula dan disasarkan untuk aplikasi sistem sekuriti yang pantas.

# TABLE OF CONTENTS

## LIST OF TABLES

# LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| AES | - | Advanced Encryption Standard |
| ASIC | - | Application Specific Integrated Circuit |
| ASM | - | Algorithmic State Machine |
| BDF | - | Block Diagram File |
| CAD | - | Computer Aided Design |
| CPU | - | Central Processing Unit |
| DLP | - | Discrete Logarithm Problem |
| DSA | - | Digital Signature Algorithm |
| DSP | - | Digital Signal Processing |
| EAB | - | Embedded Array Block |
| ECC | - | Elliptic Curve Cryptography |
| ECDLP | - | Elliptic Curve Discrete Logarithm Problem |
| ECDSA | - | Elliptic Curve Digital Signature Algorithm |
| ECDSC | - | Elliptic Curve Digital Signature Cryptosystem |
| ECP | - | Elliptic Curve Processor Core |
| EDA | - | Electronic Design Automation |
| EEA | - | Extended Euclidean Algorithm |
| FPGA | - | Field Programmable Gate Array |
| GUI | - | Graphic User Interface |
| I/O | - | Input/Output |
| IC | - | Integrated Circuit |
| IFP | - | Integer Factorization Problem |
| IEEE | - | Institute of Electrical and Electronics Engineers |
| IP | - | Intellectual Property |
| JTAG | - | Joint Action Test Group |
| LC | - | Logic Cell |
| LE | - | Logic Element |

| | | |
|---|---|---|
| LED | - | Light Emitting Diode |
| LSD | - | Least Significant Digit |
| LUT | - | Lookup Table |
| MSD | - | Most Significant Digit |
| MUX | - | Multiplexer |
| PDA | - | Personal Digital Assistant |
| PIN | - | Personal Identification Number |
| PIO | - | Parallel Input/Out |
| PKI | - | Public-Key Infrastructure |
| RAM | - | Random Access Memory |
| RSA | - | Rivest, Shamir, Adleman |
| RTL | - | Register-Transfer-Level |
| SDK | - | Software Development Kit |
| SHA-1 | - | Secure Hash Algorithm |
| SoC | - | System-on-Chip |
| SOPC | - | System-on-a-Programmable-Chip |
| UART | - | Universal Asynchronous Receiver/Transmitter |
| UTM | - | Universiti Teknologi Malaysia |
| VHDL | - | Very High Speed Integrated Circuit Hardware Description Language |

# LIST OF APPENDICES

# CHAPTER 1

# INTRODUCTION

This research work proposes an FPGA implementation of a dedicated processor core to accelerate elliptic curve computations as required by high-speed cryptosystem applications. This chapter covers the motivation, research objectives, scope of the work, research contribution and thesis organization.

## 1.1 Motivation

Security plays an important role in the majority of communication and computer networks nowadays. The development of digital communication media such as Internet, which requires high-end security over a transparent medium that becomes more and more accessible to public, means that security measures will have to be strengthened. These data exchanges must be protected from fraudulent access by third parties. The basic technology, which can warrant this kind of protection, is known as public-key cryptography.

Information security is also one of the main aspects of e-commerce and e-government. In this fast growing area, new services will only find acceptance when they provide a sufficient level of security in terms of authentication, confidentiality, data integrity and non-repudiation. The necessity of security has fueled research in the area of cryptographic protocols and encryption algorithms.

Elliptic curve cryptography (ECC) is a public-key cryptosystem that is rapidly evolving as an alternative to other schemes such as Rivest-Shamir-Adleman (RSA) scheme and Digitals Signature Algorithm (DSA) scheme by offering smallest key size and higher strength per bit (Certicom, 2000c). It is believed that the underlying mathematical hard problem, which ECC is based on, is harder to break than other traditional public-key cryptosystem. The ability to offer security with smaller keys and computationally more efficient algorithms in elliptic curve cryptosystems compared to the traditional asymmetric cryptographic algorithms are the two main reasons why elliptic curve cryptography has become popular (Johnson *et al*., 2001).

General-purpose microprocessors are not optimized for fast execution of cryptographic algorithm such as RSA and ECC mainly because they lack instructions for modular arithmetic with operations on very large operands. Thus, word size mismatches, insufficient parallelism in computations and algorithm/architecture mismatches are the main problems faced by software implementation of cryptosystem (Janssens *et al*., 2001). As a result, such systems have low performance/cost ratios. As the popularity of ECC increases, so will the need for efficient hardware solution that accelerates the computation of elliptic curve point multiplication.

For hardware implementation of elliptic curve applications, reconfigurable devices such as field programmable gate arrays (FPGAs) are of particular interest due to its high degree of flexibility compare to traditional application specific integrated circuits (ASICs). The reconfigurability of FPGA logic allows implementations to realize different security level in the same hardware. The ability to instantiate different architectures in FPGA logics provides benefit of architecture efficiency where the complexity of the arithmetic unit of the cryptosystem depends greatly on whether it support for specific finite field representation or arbitrary finite field representations (Orlando, 2002). Scalable architecture of the elliptic curve arithmetic unit in FPGA also allows implementers to explore different performance-cost trade-off.

## 1.2 Research Objectives

The objectives of this work are:

1. To design an elliptic curve processor core (ECP) for high-speed cryptographic applications, where the core is reconfigurable and parameterizable to promote reusability in future developments.

2. To implement the proposed ECP in the form of a VHDL-coded IP (Intellectual Property) softcore, serving as a coprocessor to an embedded processor.

3. To develop an elliptic curve digital signature cryptosystem as an evaluation platform to validate the proposed ECP, by integrating a control processor, a cryptographic hash processor core and the proposed ECP into a System-on-Chip (SoC) system.

## 1.3 Scope of Work

This research work is divided into two phases. The first phase is to design the ECP with parameterized VHDL code as design entry. This involves the hardware mapping of the chosen finite field arithmetic and elliptic curve algorithms into a hardware core. Constraints of speed, hardware resources and portability are taken into considerations.

The second phase is to develop an elliptic curve cryptosystem to validate the design correctness of the proposed ECP. The SoC-based cryptosystem employs Altera soft-core embedded processor core, a SHA-1 (Secure Hash Algorithm) cryptographic hash processor core and the proposed ECP, as shown in Figure 1.1. The ECP and hash processor core functions as a coprocessor to the soft-core processor, which is the main control processor to carry out the elliptic curve digital

signature scheme. Test cases of elliptic curve digital signature algorithm (ECDSA) are applied to validate the correctness of the ECP and evaluate the performance of the hardware.

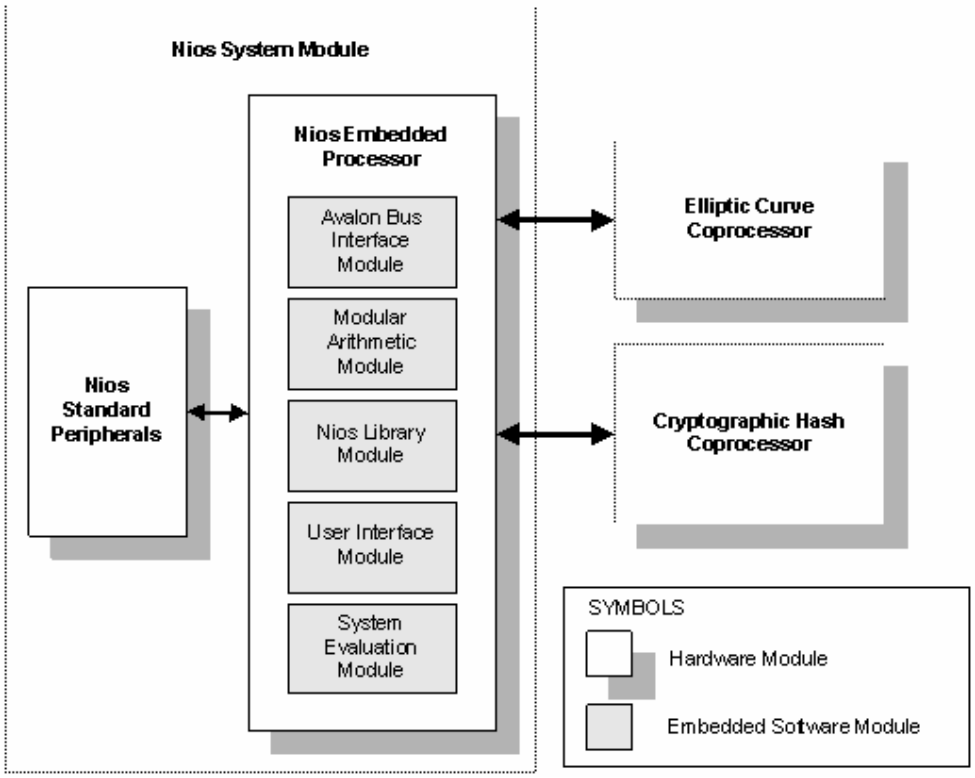


**Figure 1.1: SoC-based Elliptic Curve Cryptosystem**

## 1.4 Research Contribution

1. A simplified documented summary of the theory and algorithms of finite fields and elliptic curves for fast and efficient hardware implementation of elliptic curve cryptography.

2. A parameterizable ECP as the elliptic curve accelerator to perform elliptic curve point multiplication and point addition with competitive performance compared to existing implementations reported in documented literature.

3. An SoC-based elliptic curve digital signature cryptosystem, which consists of an Altera Nios embedded processor, a SHA-1 hash processor core and the proposed ECP.

4. A set of embedded software modules to program the embedded processor that controls the proposed elliptic curve and SHA-1 coprocessor, where an application-level programmer can use it to access all the resources on the coprocessors and to perform elliptic curve operations and cryptographic hashing.

## 1.5 Thesis Organization

The thesis is organized into eight chapters. The first chapter introduces the motivation, research objectives, research scope, research contribution and together with thesis organization.

Chapter two reviews the background of the research. Related works similar to this field are presented. Summary of the literature review is given to clarify the research rationale.

Chapter three describes the methodology, system design environment and procedures that been used in this research.

Chapter four presents the brief introduction of the mathematical concepts of finite fields and elliptic curves. Algorithms and design rules needed to realize the arithmetic operations are discussed. The cryptographic scheme implemented in this research together with the functional block diagram is shown.

Chapter five presents the hardware design of the proposed ECP. It begins with the design of sub-modules in the datapath arithmetic unit, followed by the control unit. It is elaborated in a bottom-up manner according to arithmetic hierarchy

discussed in the Chapter four. Design of data interface to facilitate data transaction between buses with different sizes is also presented in this chapter.

Details on the development of elliptic curve digital signature cryptosystem (ECDSC) as the hardware evaluation system to validate the proposed ECP are presented in Chapter six. Integration of an Altera embedded processor, a cryptographic hashing processor and the proposed ECP is discussed. The ECP functions as a coprocessor to accelerate elliptic curve computations.

Chapter seven reports on the design verification and test result of the ECP and ECDSC. The results are analyzed to give the performance of the cryptosystem prototype with different digit size. Comparison between the proposed ECP and previous implementations is made.

In the final chapter, the research work is summarized and the potential future works are given.

## REFERENCES


Agnew, G. B., Mullin, R. C., and Vanstone, S. A. (1993). An Implementation of Elliptic Curve Cryptosystem over $F_2155$. *IEEE Journal on Selected Area in Communications*. 11(5): 804-813.

Altera Corporation. (2003a). *Avalon Bus Specification: Reference Manual*. Altera Corporation.

Altera Corporation. (2003b). *Introduction to Quartus II*. Altera Corporation.

Altera Corporation. (2003c). *Nios 3.0 CPU Data Sheet*. Altera Corporation.

Altera Corporation (2003d). *Nios Development Board: Reference Manual, Stratic Professional Edition*. Altera Corporation.

Altera Corporation. (2003e). *Nios Embedded Processor: Software Development Reference Manual*. Altera Corporation.

Altera Corporation. (2003f). *Nios Hardware Development Tutorial*. Altera Corporation.

Altera Corporation. (2003g). *Nios Timer Data Sheet*. Altera Corporation.

Altera Corporation. (2003h). *SOPC Builder Data Sheet*. Altera Corporation.

Altera Corporation. (2003i). *Stratix Device Handbook: Volume 1*. Altera Corporation.

Beauregard, D. (1996). *Efficient Algorithms for Implementing Elliptic Curve Public-Key Scheme*. Worcester Polytechnic Institute: M.Sc. Thesis.

Carpinelli, J. D. (2001). *Computer Systems, Organization & Architecture*. U.S.: Addison Wesley.

Certicom Corporation. (1999). *GEC2: Test Vector for SEC1*.. Certicom Research.

Certicom Corporation. (2000a). *SEC1: Elliptic Curve Cryptography*. Certicom Research.

Certicom Corporation. (2000b). *SEC2: Recommend Elliptic Curve Domain Parameters*. Certicom Research.

Certicom Corporation. (2000c). *The Elliptic Curve Cryptosystem: Current Public-Key Cryptographic Systems*. Certicom Research.

Chong, W. S. (2001). *Design of a Hash Processor Chip and the Implementation of a Digital Signature Subsystem for Data Security*. Universiti Teknologi Malaysia: M. Sc. Thesis.

Choi, Y. J., Kim, H. W. and Kim, M. H. (2002). Implementation of elliptic curve cryptographic coprocessor over GF(2^163) for ECC protocols. *Proceedings of International Technical Conference on Circuits/Systems, Computers and Communications*. July 16-19, Phuket, Thailand: Sirindhorn International Institute of Technology, Thammasat University, 674-677.

Gaubatz, G. (2002). *Versatile Montgomery Multiplier Architectures*. Worcester Polytechnic Institute: M. Sc. Thesis.

Gura, N., Shantz, S. C., Eberle, H., Gupta, S., Gupta, V., Finchelstein, D., Goupy, E. and Stebila, D. (2002) An End-to-End Systems Approach to Elliptic Curve Cryptogarphy. *Proceedings of the Fourth International Workshop on Cryptographic Hardware and Embedded Systems*. August 13-15. Heidelberg: Springer Verlag, 349 – 365.

Hankerson, D., Hernandez, J. L. and Menezes, A.(2000). Software Implementation of Elliptic Curve Cryptography over Binary Fields. *Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems*. August 17-18. Heidelberg: Springer Verlag, 1 – 24.

Hasegawa, T., Nakajima, J. and Matsui, M. (1999). A Small & Fast Implementation of Elliptic Curve Cryptosystems over *GF*(*p*) on a 16-Bit Microcomputer. *ICICE Transaction on Communications, Electronics, Information and Systems*. E82-A(1): 98-106.

Institute of Electrical and Electronics Engineers (2000). *IEEE Standard Specifications for Public-Key Cryptography*. New York, Std 1363-2000

Itoh, T. and Tsuji, S. (1988). A Fast Algorithm for Computing Multiplicative Inverses in *GF*($2^m$) Using Normal Bases. *Information and Computation*. 78(3): 171-177.

Janssens, S., Thomas , J., Borremans, W., Gijsels, P., Verbauwhede, I., Vercauteren, F., Preneel, B. and Vandewalle, J. (2001). Hardware/Software Co-Design of an Elliptic Curve Public-Key Cryptosystem. *Proceedings of the 2001 IEEE Workshop on Signal Processing Systems*. September 26-28. Antwerp, Belgium: IEEE, 209- 216.

Johnson, D., Menezes, A. and Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1): 36-63.

Khalil, M. and Koay, K.H. (1999). VHDL Module Generator: A Rapid-Prototying Design Entry Tool for Digital ASICs. *Jurnal Teknologi*, 31(D): 45-61.

Leung, K. H., Ma, K. W., Wong, W. K. and Leong, P. H. W. (2000). FPGA Implementation of a Microcoded Elliptic Curve Cryptographic Processor. *Proceedings of IEEE Symposium on Field-Programmable Custom Computing Machines*. April 17-19. Napa Valley, CA USA: IEEE, 68-76.

Lopez, J., and Dahab, R. (1999). Fast Multiplication on Elliptic Curves over *GF*($2^m$) without Precomputation. *Proceedings of the First International Workshop on Cryptographic Hardware and Embedded* Systems. August 12-13. Heidelberg: Springer Verlag, 316 – 327.

Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A. (2001). “Handbook of Applied Cryptography.” CRC Press.

Morioka, S. and Katayama, Y. (2000). $O(\log_2 m)$ Iterative Algorithm for Multiplicative Inversion in $GF(2^m)$. *Proceedings of IEEE International Symposium on Information Theory*. June 25-30. Sorrento, Italy: IEEE, 449.

National Institute of Standards and Technology (2000). *Digital Signature Standards (DSS)*. Gaithersburg, FIPS 186-2.

National Institute of Standards and Technology (2001). *Introduction to Public Key Technology and the Federal PKI Infrastructure*. Computer Security Research Center.

Okada, S., Torii, N., Itoh, K. and Takenaka, M. (2000). Implementation of Elliptic Curve Cryptographic Coprocessor over $GF(2^m)$ on an FPGA. *Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems.* August 17-18. Heidelberg: Springer Verlag, 25-40.

Orlando, G. and Paar, C. (1999). A Super-Serial Galois Fields Multiplier for FGPAs and Its Application to Public-Key Algorithms. *Proceedings of the Seventh Annual IEEE Symposium on Field-Programmable Custom Computing Machines*. April 21-23. Napa Valley, CA USA: IEEE, 232-239.

Orlando, G. and Paar, C. (2000). A High-Performance Reconfigurable Elliptic Curve Processor for $GF(2^m)$. *Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems*. August 17-18. Heidelberg: Springer Verlag, 41 – 56.

Orlando, G. (2002). *Efficient Eliptic Curve Processor Architecture for Field Programmable Logic*. Worcester Polytechnic Institute: M. Sc. Thesis.

Pelzl, J. (2002). *Hyperelliptic Cryptosystem on Embedded Microprocessors*. Ruhr-University Bochum: M. Sc. Thesis.

Riedel, I. (2003). *Security in Ad-hoc Networks: Protocols and Elliptic Curve Cryptography on an Embedded Platform*. Ruhr-University Bochum: Dip. Thesis.

Rintakoski, T. (2002). *IP-centric SOPC Implementation of a WCDMA Baseband Modem*. Tampere University of Technology: M.Sc. Thesis.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A Method for Obtaining Digital Signature and Public-Key Cryptosystems. *Communications of the ACM*. 21(2):120-126.

Rosing, M. (1999). *Implementing Elliptic Curve Cryptography*. Greenwich C.T.: Manning Publications.

RSA Security Inc. (2000). *RSA Laboratories: Frequently Asked Questions about Today's Cryptography.* RSA Laboratories.

Saeki, M. (1997). *Elliptic Curve Cryptosystems.* McGill University: M.Sc. Thesis.

Sramka, M. (2002). *Public-Key Cryptosystems based on Elliptic Curves and XTR*. Slovak University of Technology: M. Sc. Thesis.

Scott, P. A., Tavares, S. E. and Peppard, L. E. (1986). A Fast VLSI Multiplier for $GF(2^m)$. *IEEE Journal on Selected Areas in Communications*. 4(1): 62-66.

Song, L. and Parhi, K. K. (1996). Efficient Finite Field Serial/Parallel Multiplication. *Proceedings of International Conference on Application Specific Systems, Architectures and Processors*. November 3-5. Chicago, IL USA: IEEE, 72-82.

Song, L. and Parhi, K. K. (1998). Low-Energy Digit-Serial/Parallel Finite Field Multipliers. *Journal of VLSI Signal Processing*. 19(2): 149-166.

Stalling, W. (1999). *Cryptography and Network Security: Principles and Practice*.2nd Ed. Upper Saddle River, New Jersey: Prentice Hall.

Yeh, C. S., Reed, I. S. and Truong, T. K. (1984). Systolic Multipliers for Finite Fields $GF(2^m)$. *IEEE Transaction on Computers*. 33(4): 357-360.

Wolkerstorfer, J. and Wolfgang, B. (2002). A PCI-card for accelerating Elliptic Curve Cryptography. *Proceedings of Austrochip.* October 4. Graz, Austria: Institute for Applied Information Processing and Communication (IAIK), 1-8.

Wu, H. (2002). Bit-Parallel Finite Field Multiplier and Squarer Using Polynomial Basis. *IEEE Transaction on Computers*. 51(7): 750-758.