ELLIPTIC-CURVE CRYPTOGRAPHIC ARCHITECTURES FOR SYSTEM-ON-CHIP BASED ON FIELD PROGRAMMABLE GATE ARRAYS

ARIF IRWANSYAH

UNIVERSITI TEKNOLOGI MALAYSIA

ABSTRACT

Elliptic curve cryptography (ECC) is an alternative mechanism for implementing public-key cryptographic system. The main reason for the attractiveness of ECC in data security systems is the fact that significantly smaller parameters are needed as compared to other competitive systems, but with equivalent levels of security. This thesis presents the design exploration of elliptic-curve cryptographic architectures for Field Programmable Gate Arrays (FPGA)-based System-on-Chip (SoC). The architectures explored include tightly-coupled custom logic and loosely-coupled coprocessor. The ECC hardware is designed and parameterized for key sizes of 163, 193, and 233 bits. The designs are described in Verilog and VHDL. A demonstration application prototype is developed in which an Elliptic Curve Digital Signature Algorithm (ECDSA) system is combined with a hybrid encryption cryptosystem in one SoC implementation. This application prototype is used in the verification of the designs. Experimental results show that, while utilizing less logic, tightly-coupled architecture improves the execution time of point multiplication operation by about 50% as compared to the loosely-coupled coprocessor. For point addition operation execution time, the tightly-coupled architecture offers 56% improvement as compared to the loosely-coupled coprocessor. The benchmarking of the design with other existing ECC tightly coupled hardwares shows that the design is about fourteen times faster in terms of clock cycles.

ABSTRAK

Kriptografi lengkung bujur (ECC) merupakan alternatif untuk melaksanakan mekanisma sistem kriptografi kunci-awam. Tarikan utama ECC untuk sistem keselamatan data ialah parameter yang diperlukan lebih kecil jika dibandingkan dengan sistem yang lain, untuk tahap keselamatan yang setara. Tesis ini mempersembah penjelajahan reka bentuk ECC untuk seni bina Sistem-atas-Cip (SoC) berasaskan tata susunan get boleh diatur cara medan (FPGA). Seni bina yang dikaji termasuk gandingan ketat logik langganan dan gandingan longgar kompemproses. Perkakasan ECC ini direkabentuk dan diparameterkan untuk kunci bersaiz 163,193 dan 233 bit. Reka bentuk ini diperihalkan dalam bahasa Verilog dan VHDL. Satu aplikasi prototaip telah dibina di mana algoritma tandatangan digital lengkung bujur (ECDSA) digabungkan dengan kriptosistem enkripsi hibrid dalam satu SoC. Prototaip aplikasi ini telah digunakan dalam penentusahan reka bentuk. Hasil kajian menunjukkan bahawa penggunaan get logik yang sedikit, seni bina gandingan ketat memperbaiki waktu pelaksanaan operasi pendaraban titik sebanyak 50% jika dibandingkan dengan gandingan longgar. Bagi operasi pertambahan titik pula, waktu perlaksanaan untuk seni bina gandingan ketat diperbaiki sebanyak 56%. Penanda aras reka bentuk ini jika dibandingkan dengan perkakasan gandingan ketat ECC yang lain menunjukkan bahawa reka bentuk ini 14 kali ganda lebih pantas dari segi kitar jam.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

This thesis presents the design exploration of alternative elliptic-curve cryptographic architectures for FPGA-based System-on-chip (SoC). This chapter covers the background, problem statement, research objectives, scope of work, overview of research methodology, the significance and contribution of the research, and finally the thesis organization.

1.1 Background and Motivation

The need for secure communications has led to a high demand for cryptographic service such as encrypted communications between unfamiliar hosts over insecure channels (such as the Internet). With the rapid deployment of applications like online banking, stock trading and corporate remote access, recent years have seen an explosive growth in the amount of sensitive data exchanged over the Internet. These days, an increasing number of Internet hosts are battery-powered, wireless, handheld devices with restricted memory, CPU, latency and bandwidth. For these constrained environments, besides security, it is very important to consider about the speed performance and logic cost.

Elliptic Curve Cryptography (ECC) is a public key mechanism, independently proposed by Miller (1986) and Kobiltz (1987). ECC offers secure and efficient solutions for the new communication technologies. It requires fewer bits than the well known RSA (Rivest, Shamir, Adleman) for similar level of security.

For example, a 163-bit ECC key provides a level of security equivalent to a 1024-bit RSA key (Certicom, 2000). As a result of using smaller key sizes, it is possible to achieve higher speeds, and at the same time use less power, bandwidth and storage (Juliato *et al.*, 2007). Nowadays, this technology is well accepted in the industry and the academic communities and has been the subject of several standards such as ANSI X9.62 and IEEE P1363.

There are likely to be two groups of devices which will participate in public key cryptography application, such as secure mobile and wireless environments: servers and end devices (Weimerskirch *et al.*, 2003). The server platform are bring less likely to problems due to the availability of high-speed processors and extensive memory space. However, end devices are often lever restricted regarding computing power, memory for software code, RAM size and energy supply. The implementation of public key cryptography on end devices or embedded systems, for example smart card and mobile phone, requires fast computation, small memory and high energy efficiency.

Typically, application running on an embedded system platform can be executed either as a firmware running on embedded processor or a specialized hardware unit that purposes as a coprocessor. The implementation of public key cryptography in embedded systems performs slowly in software. However, this approach is economical in logic cost and is flexible to change in algorithm. Software implementations of cryptographic algorithms often spend the majority of their execution time in a few performance-critical code sections (Hankerson *et al.*, 2004). Typical examples of such code sections are the inner loops of long integer arithmetic operations needed in public-key cryptography. The hardware-based accelerators are often the solution reaching an acceptable performance-cost ratio (Meurice *et al*., 2007).

Two key factors influence the performance of embedded system with hardware accelerator (Batina *et al*., 2006) are the communication interface between processor and co-processor; and the boundary between hardware and software in terms of hardware/software partitioning.

A conventional technique to enhance the performance cryptographic operations in an embedded system is to off-load the computational heavy sections of an algorithm into a dedicated hardware accelerator. An alternative architecture is to extend the functionality of an embedded processor by applying a tightly-coupled custom logic, and utilizing it to define new custom instructions set (Tillich and Großsch¨adl, 2006). This thesis explores the potential use of tightly-coupled custom logic in elliptic curve cryptographic operations.

1.2 Research Objectives

The objectives of this thesis are as follows:

1. To propose alternative architectures for ECC hardware accelerator that enhances the embedded processor by using tightly-coupled custom logic and extending the instruction set.

2. To improve ECC hardware accelerator performance by eliminating communication bottleneck between processor and hardware accelerator.

1.3 Scope of Work

1. The architectures explored include a tightly-coupled custom logic (TC-H) and a loosely-coupled coprocessor (LC-H). The architectures are designed in Verilog HDL and VHDL code in 163-bit, 193-bit and 233-bit field size, with the digit size (or degree of parallelism) of 32-bit.

2. Polynomial basis representations have been chosen as the basis of binary field arithmetic of ECC. In this work, we utilize the recommended elliptic curve domain parameters from Certicom (2000).

3. The implementation of the ECC hardware accelerator must fit into Altera Stratix EP1S40F780C5 FPGA development board and the running frequency is 50 MHz. The embedded processor is Altera Nios II CPU soft core.

4. The evaluation of the explored architecture design is limited to speed performance and resource utilization.

1.4 Overview of Research Methodology

As illustrated in Figure 1.1, this research work is divided into two phases. The first phase is the literature review and design specification. Then the work continues with design of ECC hardware accelerator, both in TC-H and LC-H architectures. This involves the hardware/software partitioning in ECC finite field arithmetic level and ECC point arithmetic level. Hardware test verification and performance comparison between tightly-coupled hardware and loosely-coupled coprocessor architectures is also evaluated here. Constraints of speed and hardware resource are taken into considerations.

The second phase is to develop an elliptic curve cryptosystem to validate the design correctness and functionality of the proposed ECC TC- hardware. This ECC embedded systems utilize Nios II soft-core embedded processor core (Altera, 2007), 233-bit Modular Arithmetic Processor (MAP), SHA-1 (Secure Hash Algorithm) cryptographic hash processor core, 256-bit AES encryption processor core and the proposed ECC TC-hardware. Elliptic Curve – AES (EC-AES) Hybrid Encryption and Elliptic Curve Digital Signature Algorithm (ECDSA) (Certicom, 2000a) demonstration application prototype was implemented in this work.

For the development of our cryptosystem, we choose the Altera FPGA hardware system based on Nios II 32-bit RISC embedded processor as the prototyping platform. This development system contains a powerful and flexible IDE, the Quartus II SOPC Builder that facilitates the tasks of extending Nios II instruction set to include custom instructions, and also the creation of a tightly-coupled custom logic.

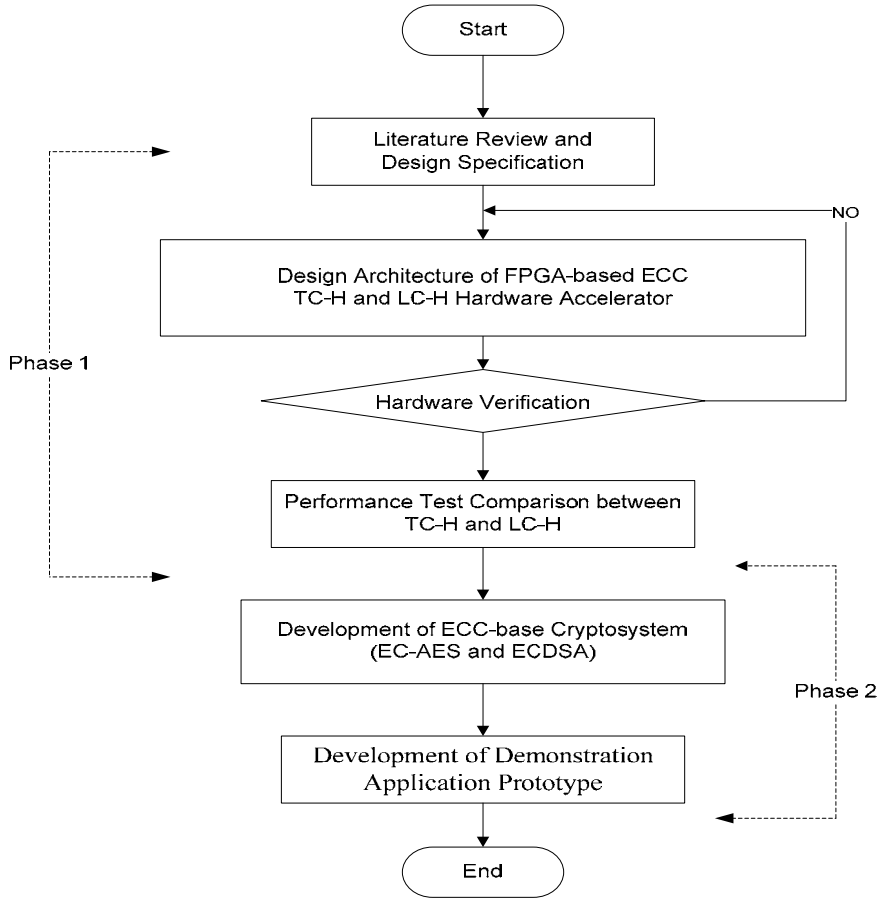

Figure 1.1 System Design Flow

1.5 Research Contribution

The contributions of this thesis are as follows:

1. Introduce design exploration and performance comparison between tightly-coupled custom logic and loosely coupled coprocessor for ECC field arithmetic and point arithmetic.

2. Implement elliptic curve cryptography in FPGA-based embedded system modules which are applied in EC-AES Hybrid Encryption and ECDSA schemes.

3. Develop an application demonstration prototype that implements an e-cheque application as secure document through insecure network. This is used to validate the ECC architectures.

1.6 Thesis Organization

The thesis is organized into seven chapters. The first chapter introduces the research motivation, research objectives, research scope, overview of research methodology, research contribution, and the thesis organization.

Chapter 2 reviews the background of the research. Related works are presented. Summary of the literature review is given to clarify the research rationale.

Chapter 3 presents the brief introduction of the mathematical concepts of finite fields and elliptic curves. Various design styles of hardware accelerator to implement elliptic curve arithmetic are described. The ECDH, EC-AES Hybrid Encryption, and ECDSA scheme are discussed in this chapter.

REFERENCES

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

Altera Corporation. (2007). *Nios II Processor Reference Handsbook: User Guide*. Altera Corporation.

Altera Corporation. (2008). *Nios II Custom Instruction: User Guide*. Altera Corporation.

ANSI, ANSI X9.62 *The elliptic curve digital signature algorithm (ECDSA)*. Available from: http://www.ansi.org

Batina L., Hodjat A., Hwang D., Sakiyama K. and Verbauwhede I. (2006). Reconfigurable Architectures for Curve-based Cryptography on Embedded Micro-controllers, In *16th International Conference on Field Programmable Logic and Applications (FPL 2006.* Madrid: IEEE, 1-4.

Certicom Corporation. (1999). *GEC2: Test Vector for SEC1*. Certicom Research. Available from: http://www.secg.org

Certicom Corporation. (2000a). *SEC1: Elliptic Curve Cryptography*. Certicom Research. Available from: http://www.secg.org

Certicom Corporation. (2000b). *SEC2: Recommend Elliptic Curve Domain Parameters*. Certicom Research. Available from: http://www.secg.org

Certicom Corporation. (2000c). *The Elliptic Curve Cryptosystem: Current Public-Key Cryptographic Systems.* Certicom Research. Available from: http://www.secg.org

Cheung, R.C.C. Telle, N.J. Luk, W. and Cheung, P.Y.K. (2005). Customizable Elliptic Curve Cryptosystems, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems.* 13(9), 1048-1059.

Diffie, W. and Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Trans. Inf. Theory*. IT-22(6), 644–654.

Fei, S., Srivaths, R., Anand, R. and Niraj, K.J. (2006). Hybrid Custom Instruction and Co-processor Synthesis Methodology for Extensible Processors. *Proceedings of the 19th International Conference on VLSI Design.* 3-7 January. 473 – 476.

Großchädl, J. and Savas, E. (2004). Instruction Set Extensions for Fast Arithmetic in Finite Fields GF(p) and GF(2*m*). *Workshop on Cryptographic Hardware and Embedded Systems - CHES 2004.* August 11-13. Cambridge, MA, USA, 3156, 133-147.

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.

Hamid, N., Farhad, M., Kazuaki, M., Koji, I. and Morteza, S. (2008), An Architecture Framework for an Adaptive Extensible Processor. *The Journal of Supercomputing*. 45(3), 313-340.

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. Worcester, MA, USA, 1-24.

Hankerson D.R., Menezes A.J. and Vanstone S.A. (2004), *Guide to Elliptic Curve Cryptography*. Heidelberg: Springer Verlag.

Hodjat A. and Verbauwhede, I. (2004), Interfacing a High Speed Crypto Accelerator to an Embedded CPU. *Proceedings of the 38th Asilomar Conference on Signals, Systems, and Computers*. New York : IEEE, 1, 488–492.

Hodjat,A. and Verbauwhede, I. (2004). High-throughput programmable cryptocoprocessor. *IEEE Micro.* 24(3), 34-45.

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.

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

Juliato M., Araujo G., Lopez J. and Dahab R. (2007). A Custom Instruction Approach for Hardware and Software Implementations of Finite Field Arithmetic over F2163 using Gaussian Normal Bases. *Journal of VLSI Signal Processing.* 47, 59–76.

Khalil, M., and Hau, Y.W. (2005). *An Embedded Cryptosystem Implementing Symmetric Cipher and Publick Key-Crypto Algorithms in Hardware.* M.Sc. Thesis, Universiti Teknologi Malaysia, Skudai.

Khalil, M., and Lim K.W. (2005). *An FPGA Implementation of an Elliptic Curve Processor for an Embedded Public-Key Cryptosystem.* M.Sc. Thesis, Universiti Teknologi Malaysia, Skudai.

Khalil, M., and Irwansyah, A. (2008). *veCAD-NIOS-TUT-TR2007011 Nios II Tutorial: Custom Instruction.* VLSI ECAD Research Laboratory, Universiti Teknologi Malaysia, Skudai.

Krasner, J. (2004). *Using Elliptic Curve Cryptography (ECC) for Enhanced Embedded Security : Financial Advantages of ECC over RSA or Diffie-Hellman (DH).*

Embedded Market Forecasters, American Technology International, Inc. White Paper.

Koblitz N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation.* (48), 203–209.

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.

Meurice G., and Quisquater J.J. (2007), High-Speed Hardware Implementations of Elliptic Curve Cryptography: A survey, *Journal of Systems Architecture*. 53(2-3), 72-84.

Miller V. S. (1986). Use of Elliptic Curves in Cryptograph. Advance in Cryptology-CRYPTO'85. In Williams H. C. (Ed.) *Lecturer Notes in Computer Science,* 128, (pp. 417–426). Berlin: Springer-Verlag.

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.

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*. M. Sc. Thesis, Worcester Polytechnic Institute.

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

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.

Schaumont, P., Ching and Verbauwhede, I. (2006). An interactive codesign environment for domain-specific coprocessors, *ACM Transactions on Design Automation of Electronic Systems.* 11(1), 70-87.

Schaumont, P., Sakiyama, K., Hodjat, A. and Verbauwhede, I. (2004). Embedded Software Integration for Coarse-grain Reconfigurable Architectures. *18th IEEE International Parallel and Distributed Processing Symposium (IPDPS 2004).* IEEE, 137-142.

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.

Tillich, S., and Großsch¨adl, J. (2004). A Simple Architectural Enhancement for Fast and Flexible Elliptic Curve Cryptography over Binary Finite Fields GF(2^m). In Advances in Computer Systems Architecture — ACSAC 2004 *Lecture Notes in Computer Science*, 3189, (pp. 282–295). Springer Verlag.

Weimerskirch, A., Stebila, D., and Chang, S. (2003). Generic GF(2^m) arithmetic in software and its application to ECC. In Information Security and Privacy — ACISP 2003 *Lecture Notes in Computer Science*, 2727, (pp. 79–92). Springer Verlag.

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