

DESIGN OF AN ADVANCED ENCRYPTION STANDARD
CRYPTO-PROCESSOR CORE FOR
FIELD PROGRAMMABLE GATE ARRAY IMPLEMENTATION

MOHD IZUAN BIN ISMAIL

UNIVERSITI TEKNOLOGI MALAYSIA

ABSTRACT

Cryptographic applications becoming increasingly more important in today's world of data exchange. Big volume data needs to be transferred from one location to another through communication path but exposes to attackers. Cryptography services are essential in order to provide the authentication, privacy, non-repudiation and integrity of private data being transmitted. System-on-Chip (SoC) technology enters the mainstream in digital design. The advances in reconfigurable hardware create the possibility of developing a microchip with application-specific processors. The processors perform their respective dedicated algorithm-intensive computations. This thesis presents the architecture for implementation of the new Advanced Encryption Standard (AES) in hardware for operating under SoC environment. The proposed AES Crypto-Processor accelerates the AES algorithm in reconfigurable Field Programmable Gate Arrays (FPGA). The processor design is completely described in hardware description language, VHDL. When designing hardware, the desire is often to achieve the highest performance possible. With implementation on Altera's APEX FPGA, experimental evaluation of the AES Crypto-Processor running at 50 MHz using test vector provided in FIPS (2002) yields an average encryption rate at 188.24 Mb/s and decryption rate at 200 Mb/s which makes the overall performance is at 192.12 Mb/s. The design uses only 3,355 logic elements or 31% of hardware resources. The result of this work is the first step to the ultimate goal of developing a complete cryptographic system processor for security application in embedded system design.

ABSTRAK

Aplikasi Kriptografi menjadi semakin penting dalam penghantaran dan penerimaan data pada zaman kini. Data yang bersaiz besar perlu dihantar dari satu lokasi ke suatu lokasi melalui laluan komunikasi tetapi terdedah kepada bahaya. Kriptografi adalah asas kepada proses ini untuk memberi servis pengesahan, pengrahsiaan, ketelahan dan integriti kepada data peribadi yang dihantar. Dengan kemajuan teknologi Sistem-Atas-Cip (*System-on-Chip, SoC*) telah membolehkan mikro cip pemproses dengan aplikasi yang spesifik dibangunkan. Pemproses tadi hanya melaksanakan proses pengiraan berdasarkan algoritma tertentu yang dikhususkan. Tesis ini membentangkan rekabentuk yang mengimplementasikan algoritma Standard Enkripsi Termaju (*Advanced Encryption Standard, AES*) dalam perkakasan untuk beroperasi dalam persekitaran Sistem-Atas-Cip. Rekabentuk pemproses kriptografi yang menggunakan algoritma AES dibuat atas FPGA. Rekabentuk pemproses ini dibangunkan dan ditulis sepenuhnya menggunakan bahasa deskripsi perkakasan, VHDL. Dalam rekabentuk perkakasan, keutamaan diberikan kepada prestasi yang tinggi. Dengan menggunakan FPGA dari Altera edisi APEX, eksperimen penilaian untuk pemproses kriptografi AES ini pada kelajuan 50 MHz dengan menggunakan vector ujian dari FIPS (2002) memberikan purata bacaan 188.24 Mb/s untuk proses enkripsi dan 200 Mb/s untuk proses dikripsi untuk purata keseluruhan 192.12 Mb/s. Keputusan ini merupakan langkah pertama dalam sasaran untuk membangunkan sistem kriptografi yang lengkap untuk digunakan dalam aplikasi sekuriti pada rekabentuk sistem terbenam.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vi
	LIST OF TABLES	xii
	LIST OF FIGURES	xiii
	LIST OF ABBREVIATIONS	xvi
	LIST OF APPENDICES	xvii
1	INTRODUCTION	1
	1.1 Background and Research Motivation	1
	1.2 Objectives	3
	1.3 Scope of Work	4
	1.4 Significant of Work and Research Contributions	4
	1.5 Research Methodology, Techniques and Tools	5
	1.6 Organization of Thesis	8

2	BACKGROUND AND LITERATURE REVIEW	9
2.1	What is Cryptography?	9
2.2	Cryptography Services	11
2.3	Type of Ciphers	13
2.3.1	Asymmetric Key or Public Key	13
2.3.2	Symmetric Key or Private Key	14
2.3.2.1	Block Cipher	15
2.3.2.2	Stream Cipher	16
2.4	Block Cipher Algorithms	16
2.4.1	DES	17
2.4.2	MARS	17
2.4.3	RC6	17
2.4.4	AES	18
2.4.5	Serpent	19
2.4.6	Twofish	19
2.5	Advanced Encryption Standard (AES) Cryptography	20
2.6	Previous Related Works	21
2.7	Summary	22
3	ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM AND SPECIFICATION	24
3.1	Introduction	24
3.2	Background Mathematics	25
3.2.1	The Field of $GF(2^8)$	25
3.2.2	Finite Field Addition	26
3.2.3	Finite Field Multiplication	26
3.2.4	Multiplicative Inverse	28
3.2.5	Polynomials with Coefficients in $GF(2^8)$	29
3.3	The Advanced Encryption Standard (AES) Specification	31

3.3.1	State Array and Cipher Key State Array	31
3.3.2	AES Transformation	33
3.3.2.1	AddRoundKey	37
3.3.2.2	SubByte and InvSubByte	38
3.3.2.3	ShiftRow and InvShiftRow	40
3.3.2.4	MixColumn and InvMixColumn	41
3.3.3	AES Key Expander	42
3.3.3.1	Rcon	44
3.3.3.2	Rot	45
3.3.3.3	SubByte	45
3.4	Summary	45
4	DESIGN OF THE AES CRYPTO-PROCESSOR CORE	46
4.1	Design Consideration	46
4.2	Top-Level Design of AES Crypto-Processor	48
4.3	Design of AES Processing Engine	53
4.3.1	AES Transformation	54
4.3.1.1	ShiftSubByte (<i>InvShiftSubByte</i>)	57
4.3.1.1.1	Design of Inverter Circuit	61
4.3.1.1.2	Design of Squarer Circuit	62
4.3.1.1.3	Design of SubByte and InvSubByte Module	62
4.3.1.2	MixColumn (<i>InvMixColumn</i>)	67
4.3.1.2.1	Xtime.	71
4.3.1.2.2	ByteMixColumn	71
4.3.1.2.3	WordMixColumn	72
4.3.1.2.4	MixColumn (<i>InvMixColumn</i>)	73
4.3.1.3	AddRoundKey	74

	4.1.3.4 Data Buffer	75
	4.3.2 AES Key Expander	76
	4.3.2.1 Key Module	79
	4.3.2.2 SBOX (SubByte)	80
	4.3.2.3 Rcon	80
	4.3.2.4 Rot	80
	4.3.2.5 Temp Buffer	81
	4.3.3 Key RAM	81
4.4	Design of Control Unit	83
	4.4.1 Behavioral Flowchart	83
	4.4.2 State Transition and RTL	88
4.5	Summary	89
5	DESIGN VERIFICATION AND PERFORMANCE ANALYSIS	91
	5.1 Design Verification Procedures	91
	5.1.1 Design Synthesis	92
	5.1.2 Functional or Timing Simulation	93
	5.2 Design Synthesis Results	94
	5.3 Timing Simulation Results	95
	5.3.1 ShiftSubByte (<i>InvShiftSubByte</i>)	96
	5.3.2 MixColumn (<i>InvMixColumn</i>)	97
	5.3.3 AES Key Expander	97
	5.3.4 AES Transformation	101
	5.3.5 AES Crypto-Processor Core	104
	5.4 Performance and Comparison	106
	5.5 Summary	107

6	CONCLUSION	108
	6.1 Concluding Remarks	108
	6.2 Future Improvement Works	109
	REFERENCES	111
	APPENDICES A - E	115 - 148

LIST OF TABLES

TABLE NO	TITLE	PAGE
3.1	Rcon values	44
4.1	AES Input and Output Signals	49
4.2	Interface Signals	50
4.3	Coding Names and Related Section	52
4.4	AES Transformation I/O Signals	55
4.5	AES Transformation Control Vector Signals	57
4.6	ShiftSubByte I/O Signals	58
4.7	The Inverse of 4-bit Values	61
4.8	MixColumn I/O Signals	68
4.9	Steps of Obtaining Results of Encryption and Decryption	70
4.10	AddRoundKey I/O Signals	75
4.11	AES Key Expander I/O Signals	78
4.12	AES Key Expander Control Vector Signals	78
4.13	Key RAM I/O Signals	82
4.14	State Transition and RTL Control Sequences	88
5.1	Resources Utilization and Clock Rate	94
5.2	Results of Logic Synthesis of other Components	95
5.3	Simulation Result for AES Key Expander	97
5.4	Simulation Result for AES Transformation	101
5.5	Comparisons with other Implementations	106

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
1.1	Project Workflow	6
1.2	AES Crypto-Processor Research and Design Procedure	7
2.1	Public Key Cryptography	13
2.2	Private Key Cryptography	14
2.3	Block Cipher	15
3.1	(a) Initial input bytes (b) State Array and (c) Key State Array	32
3.2	Example of State Array and Key State Array	33
3.3	AES Algorithm	36
3.4	AddRoundKey Transformation	37
3.5	SubByte and InvSubByte Function	39
3.6	ShiftRow and invShiftRow Transformation	40
3.7	MixColumn and invMixColumn Transformation	41
3.8	Encryption Round Key Expander Algorithm	43
3.9	Decryption Round Key Expander Algorithm	43
3.10	Rot Transformation	45
4.1	Functional Block Diagram of AES Crypto- Processor Processing Engine	47
4.2	Functional Block Diagram of AES Crypto- Processor Core	48
4.3	Handshaking Protocol with Other Control	51

	Processor	
4.4	Hierarchy of the AES Crypto-Processor	52
	Components	
4.5	System Block Diagram of AES Data Processing Engine	53
4.6	AES Transformation Block Diagram	54
4.7	AES Transformation Functional Block Diagram	56
4.8	ShiftSubByte Functional Block Diagram	58
4.9	ShiftRow Design	59
4.10	Schematic Representation of a Hardware-Efficient Calculation of the Inverse in GF (2^8)	60
4.11	Squarer Circuit	62
4.12	Translating Initial Input Signal	63
4.13	Up_input and Low_input	63
4.14	Square of Low_input	63
4.15	Transformation of Up_input to mult	64
4.16	(a) mul2 Transformation (b) part1 Transformation (c) part2 Transformation	64
4.17	(a) invert (b) mult32 (c) mul4	65
4.18	invout Signal	65
4.19	Result for SubByte in Encryption Mode	66
4.20	Result for SubByte in Decryption Mode	66
4.21	Top Level Block Diagram of MixColumn Design	67
4.22	ByteMixColumn Design	71
4.23	WordMixColumn Design	72
4.24	MixColumn Design	73
4.25	AddRoundKey Design	74
4.26	Functional Block Diagram of AddRoundKey Design	74

4.27	Key Expander Module Block Diagram	76
4.28	AES Key Expander Functional Block Diagram	77
4.29	Key Module Design	79
4.30	SBOX Design	80
4.31	Rot Design	81
4.32	Key RAM Design	82
4.33	Behavioral Flowchart for AES Key Expander (Encryption)	84
4.34	Behavioral Flowchart for AES Key Expander (Decryption)	85
4.35	Behavioral Flowchart for AES Transformation (Encryption)	86
4.36	Behavioral Flowchart for AES Transformation (Decryption)	87
5.1	Timing Simulation for ShiftSubByte	96
5.2	Timing Simulation for MixColumn	97
5.3	Timing Simulation for AES Key Expander (Encryption)	99
5.4	Timing Simulation for AES Key Expander (Decryption)	100
5.5	Timing Simulation for AES Transformation (Encryption)	102
5.6	Timing Simulation for AES Transformation (Decryption)	103
5.7	AES Crypto-Processor Core Timing Simulation Result	105

LIST OF ABBREVIATIONS

AES	-	Advanced Encryption Standard
ASIC	-	Application Specific Integrated Circuit
CAD	-	Computer Aided Design
CPU	-	Central Processing Unit
FIPS	-	Federal Information Processing Standard, USA
FPGA	-	Field Programmable Gate Array
I/O	-	Input / Output
NIST	-	National Institute of Science and Technology, USA
PC	-	Personal Computer
RAM	-	Random Access Memory
SoC	-	System-on-Chip
ROM	-	Read Only Memory
UTM	-	Universiti Teknologi Malaysia
VHDL	-	VHSIC Hardware Description Language

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Block Diagrams and VHDL Codes for the AES Crypto-Processor Design	115
B	SubByte and InvSubByte Transformation Results in Hexadecimal	141
C	Test Vector	143
D	UTM-VHDLMG	145
E	Altera Quartus-II	147

CHAPTER 1

INTRODUCTION

This thesis proposes an Application Specific Integrated Circuit (ASIC) design of Advanced Encryption Standard (AES) processor core on Field Programmable Gate Array (FPGA). The design is to accelerate fast computation of digital data encryption and decryption using AES algorithm. In this chapter, the challenges of cryptography are discussed, providing a framework for the objectives of this project. This chapter covers the background, research motivation, research objectives, significant of the work, scope of work, research methodology and finally the thesis organization.

1.1 Background and Research Motivation

As we move into twenty-first century, almost all information processing and telecommunication are in digital formats. Most data, for example photos, music and private information can be transmitted through copper, optical or wireless network to a recipient anywhere in the world. In order to protect the data and keep privacy, the

information system should be equipped with cryptography and robustness techniques (M. H. Jing *et al.*, 2001).

Cryptographic services are required across variety of platforms in a wide range of applications such as secure access to private networks, electronic commerce and health care. Cryptography means hidden writing, the practice of using encryption to conceal text. The security of conventional encryptions depends on several factors. First, the encryption algorithm must be powerful enough that is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of the algorithm. That is, it is assumed that is also impractical to decrypt a message on the basis of the cipher text plus knowledge of the encryption or decryption algorithm.

Generally, most of cryptography algorithms are implemented in software, but software implementation cannot offer the physical security for the key (Joon *et al.*, 2002). Software is operating system (OS) dependent and also exposed to viruses and hackers attacks that may interrupt the OS running on the general computer, for example on Microsoft Windows based computer or Apple Macintosh machine. Execution on general-purpose processor (CPU) of the algorithm will use most CPU's resources to calculate and execute all processes in the algorithm because CPU lacks of instructions for modular arithmetic with operations on very large operands. Thus, word sizes mismatch, less parallel computations and algorithm/architecture are the main problems faced by software implementation of cryptosystem (Janssens *et al.*, 2001).

Different applications of the data encryption algorithm may require different speed/area trade-offs. Some applications, such as smart card and cellular phone, require a small area. Other applications, such as World Wide Web (WWW) servers and Asynchronous Transfer Mode (ATM) networks are speed critical. Some other applications, such as digital video recorders, require an optimization of speed/area ratio (Xinmiao *et al.*, 2003).

In general, hardware based solution are the embodiment of choice for military and serious commercial applications (Schneier, 1996). As an encryption algorithm running on a generalized computer has no physical protection, hardware cryptographic devices can be securely encapsulated to prevent any modification of the implemented algorithm and also can be embedded the hardware as co-processor in any devices that require data security processing.

In this research, the AES Crypto-Processor design is implemented on hardware (FPGA) with key RAM, which can make not only a forward key scheduling for encryption but also a reversed key scheduling for decryption. Therefore, compared to software implementation, hardware implementation enhances the physical security as well as higher speed and outside attackers cannot easily attack, interrupt or modify its operation.

1.2 Objectives

From the discussion from previous section, this thesis sets out two main objectives for the research:

1. To design a cryptography processor core using the new symmetric key data encryption standard, Advanced Encryption Standard (AES) which supports 128 bits of data block and 128 bits of key size.
2. To implement the AES cryptography processor core to Altera APEX20KE200 FPGA device and perform simulation for design verification.

1.3 Scopes of Work

Based on available hardware and software resources, limited time frame and expertise, this research project is narrowed down to the following scope of work:

1. The research is only to design fixed 128-bit of data block size and 128-bit of key size based on an AES algorithm.
2. The design is targeted to FPGA technology. The FPGA device used is APEX20KE200 from Altera.
3. The research is limited to design, to synthesis, to simulate and to verify the design correctness in Altera Quartus II software.
4. The test vector used to verify the design is based on FIPS 197, NIST (2002).

1.4 Significant of Work and Research Contributions

1. A FPGA prototype of an Advanced Encryption Standard to perform 128 bits data encryption and decryption computation.
2. A new Intellectual Property (IP) for embedded applications in data encryption and cryptography is produced.

1.5 Research Methodology, Techniques and Tools

In order to make this research successful and complete within a limited time frame, a proper planning is essential and all working procedures should be identified clearly. This research involves mostly efforts on hardware design and the remaining is software development to support the hardware environment for validation and testing purposes. The project workflow is shown in Figure 1.1 beside.

The work begins with the literature review on cryptography and its application. Then, problem formulation and scope identification are done after sufficient knowledge on the targeted application in cryptography, which is the mapping one of symmetric key cryptography algorithm to digital hardware design in Altera's FPGA is obtained. Targeted applications are in smart card and other security devices. The most important part before designing the hardware is to understand deeply on AES algorithm and specification as well as other essential mathematical concepts such as finite field theory, modular arithmetic, number theory, and etc. Doing arithmetic in finite field is the key part to the implementation of the communication and coding systems including the newly developed AES (M. H. Jing *et al.*, 2001). From the flow of AES algorithm, most of the research works are concentrated on architectural design of the AES Crypto-Processor with all resources needed are counted in.

All of AES Crypto-Processor architecture designs are coded in VHDL (*Very-High-Speed Hardware Design Language*) using UTM-VHDLMG. UTM-VHDLMG then used to generate synthesizable VHDL files. The files compilation, synthesis and simulation are performed using Altera Quartus II design software. Any design errors or bugs are fixed before a limited and experimental prototype is developed. Timing and waveform simulation are then performed using test vector pattern for design verification and validation. Both UTM-VHDLMG and Altera Quartus II roles is illustrated in Figure 1.2.

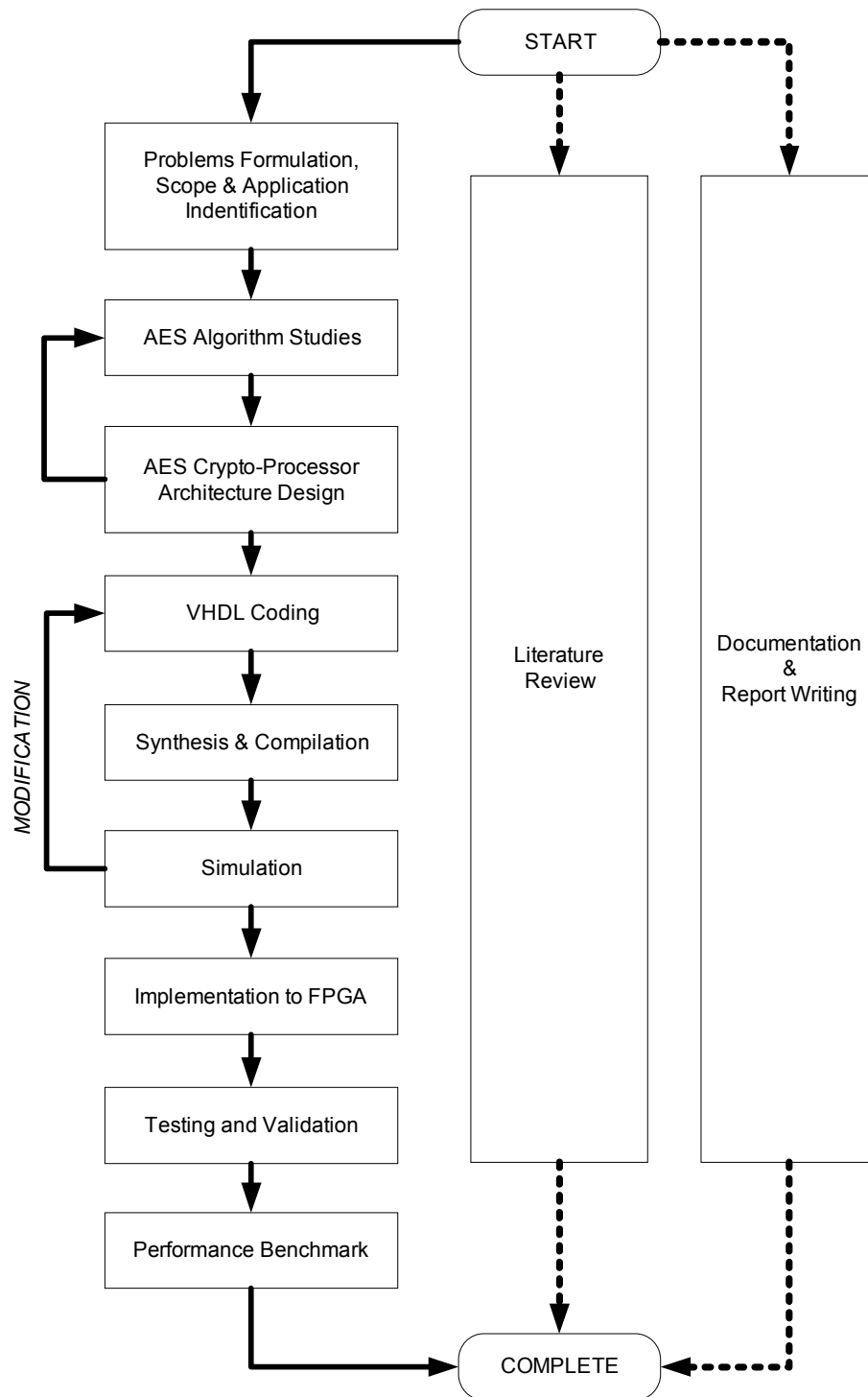


Figure 1.1: Project Workflow

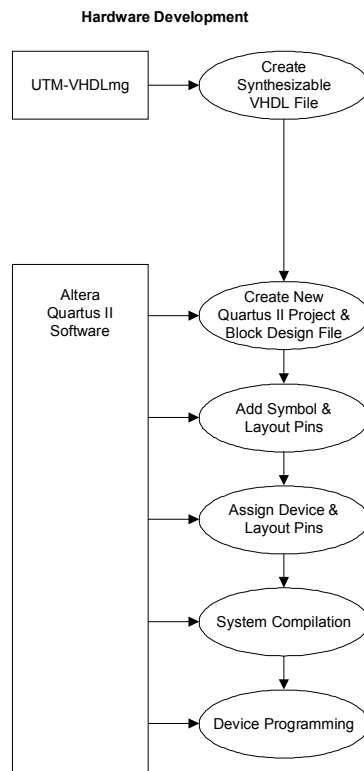


Figure 1.2: AES Crypto-Processor Research and Design Procedure

From the starting to ending of this research, literature review is a continuous process in order to get the latest update related to the research. At the same time, every research progress and status are documented and reported. Any problems and issues faced can be solved effectively by supervision and discussion.

1.6 Organization of Thesis

This thesis is organized into six chapters. The first chapter is the introduction chapter which covers the background, problem statement, objectives, scopes, the significant and contributions of the project. End of the chapter deals with the methodology, tools and techniques employed in this project. It discusses on design environment and also the ways on how the hardware mapping of Advanced Encryption Standard algorithm is possible in this project using state-of-the-art design tools.

Chapter II reports some related literature review and similar previous works done by other researchers through out the world. Several topics related to this research are reviewed to give an overall picture of the background knowledge and the design environment. Chapter III elaborates the specification of AES algorithm. It covers all the functions and transformation in AES in details. Chapter IV discusses the design and development of the AES Crypto-Processor. It includes on how the original AES algorithm can be rearranged and restructured in such a way to make it easy and possible to design in hardware. All signals including the needed control signals to drive the AES Crypto-Processor are clearly identified and defined.

Chapter V deals with the validation and performance analysis of the AES Crypto-Processor. It presents the results obtained from running the performance analysis with artificially generated data. Timing simulation used to proof the design correctness. In the final Chapter VI, the research work is summarized and potential improvements, extensions and suggestions of the project are given.

REFERENCES

- Alam, M., Badawy, W., and Jullien, G. (2002). A Novel Pipelined Threads Architecture for AES Encryption Algorithm. *IEEE International Conference on Application-Specific System, Architectures, and Processors (ASAP'02)*: IEEE, 1063-6862/02.
- Ali, N. B. Z., and Noras, J. M. (2001). Optimal Data Path Design for a Cryptographic Processor. The Blowfish Algorithm. *Malaysian Journal of Computer Science*, Vol. 14 No. 1: 1063-6862/02.
- Bertoni, G., Breveglieri, L., Koren, I., Maistri, P., and Piuri, V. (2002). On the Propagation of Faults and Their Detection in a Hardware Implementation of the Advanced Encryption Standard. *IEEE International Conference on Application-Specific System, Architectures, and Processors (ASAP'02)*: IEEE, 1063-6862/02.
- Brown, S. (2000). *Fundamentals of Digital Logic With VHDL Design*. New York: McGraw-Hill.
- Brown, S., Manjikian, N., Vranesic, Z., Caranic, S., Grbic, A., Grindley, R., Gusat, M., Loveless, K., Zilic, Z., and Srblic, S. (1994). *Experience in Design a Large-scale Multiprocessor using Field-Programmable Devices and Advanced CAD Tools*. San Jose: Logic Modeling Corp. merged with Synopsys.
- Daemen, J., and Rijmen, V. (1999). *AES Proposal: Rijndael*. Brussels.

Daemen, J., Rijmen, V. (1999). The Rijndael Block Cipher. Document Version 2.

Dandalis, A., and Prasanna, V. K. (2000). *An Adaptive Cryptographic for IPsec Architectures*. Los Angeles: Department of Electrical Engineering-Systems University of Southern California.

Duc, D. A., Triet, T. M., and Co, L. H. (2002). The Extended Rijndael-like Block Ciphers. *International Conference on Information Technology: Coding and Computing (ITCC'02)*: IEEE, 0-7695-1506-1/02.

Ernst, M., Klupsch, S., Hauck, O., and Huss, S. A.. (2001). Rapid Prototyping for Hardware Accelerated Elliptic Curve Public-Key Cryptosystems. *12 th IEEE workshop on Rapid System Prototyping*. Monterey, Canada: IEEE.

Fenn, S. T. J., Bennaissa, M., and Taylor, D. (1996). *Finite Field Inversion Over the Dual Basis*. IEEE.

Ferguson, N. and Schneier, B. (2003). *Practical Cryptography*. New York: Wiley

Gladman, B. (2002). *A Specification for the AES Algorithm*. Berkeley.

Jing, M.H., Chen, C.H., Chang, Y.T., and Hsu, C.H. (2001). *The Design of A Fast Inverse Module in AES*. IEEE, 0-7803-7010-4//01.

Joon, H. S., Dae, W. K., Young, K. K., Taek, W. K., and Jun, R. C. (2002). *A Rijndael Cryptoprocessor Using Shared On-the-fly Key Scheduler*. Seoul: Kyungpook National University, School of Electrical Engineering.

Karri, R., Wu, K., Mishra, P., and Kim, Y. (2001). *Fault Based Side-Channel Cryptanalysis Tolerant Rijndael Symmetric Block Cipher*. IEEE.

Lin, T. F., Huang, C. T., and Wu, C. W. (2002). *A High-Throughput Low-Cost AES Cipher Chip*. Taiwan: Laboratory for Reliable Computing Department of Electrical Engineering National Tsing Hua University Hsinchu.

- Lu, C. C. and Tseng, S. Y. (2002). Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter. *IEEE International Conference on Application-Specific System, Architectures, and Processors (ASAP'02)*: IEEE, 1063-6862/02.
- Mangard, S., Aigner, M., and Dominikus, S. (2003). *A Highly Regular and Scalable AES Hardware Architecture*. IEEE Transactions On Computers.
- Mao, W. (2003). *Modern Cryptography: Theory and Practice*. New Jersey: Prentice Hall PTR.
- McLoone, M. and McCanny, J.V. (2001). *High Performance Single-Chip FPGA Rijndael Algorithm Implementations*. Berlin Heidelberg: Springer-Verlag.
- McLoone, M. and McCanny, J.V. (2001). *Rijndael FPGA Implementation Utilizing Look-Up Tables*. IEEE 0-7803-7145-3/01.
- McLoone, M. and McCanny, J.V. (2001). *Single-Chip FPGA Implementation of the Advanced Encryption Standard Algorithm*. Berlin Heidelberg: Springer- Verlag.
- McMillan, S and Petterson, C. (2001). *JBits™ Implementations of the Advanced Encryption Standard (Rijndael)*. San Jose.
- Morioka, S., and Satoh, A. (2002). A 10 Gpbs Lull-AES Crypto Design with a Twisted-BDD S-Box Architecture. *IEEE International Conference on Computer Design: VLSI in Computers and Processor, (ICCD,02)*: IEEE, 1063-6404/02.
- Panato, A., Barcelos, M., and Reis, R. (2002). An IP of an Advanced Encryption Standard for Altera™ Devices. *15 th Symposium on Integrated Circuit and System Design (SBCCI'02)*: IEEE, 0-7695-1807-9/02.
- Pfleeger, C. P. (1997). *Security In Computing, Second Edition.*, Upper Saddle River, New Jersey: Prentice Hall

- Phan, R.C.W. (2002). *Classes of Impossible Differentials of Advanced Encryption Standard*. Electronics Letters.
- Phan, R.C.W., and Siddiqi, M.U. (2001). *Generalised impossible differentials of advanced encryption standard*. Electronics Letters.
- Rudra, A., Dubey, P. K., Jutla, C. S., Kumar, V., Rao, J. R. and Rohatgi, P. (2001). *Efficient Rijndael Encryption Implementation with Composite Field Arithmetic*. Berlin Heidelberg: Springer-Verlag.
- Satoh, A., Morioka, S., Takano, K., and Munetoh, R. (2001). *A Compact Rijndael Hardware Architecture with S-Box Optimization*. Berlin Heidelberg: Springer-Verlag.
- Satoh, A. and Morioka, S.(2003). *Unified Hardware Architecture for 128-Bit Block Ciphers AES and Camellia*. Berlin Heidelberg: Springer-Verlag.
- Sanchez, C., Avila, K. and Reillo, S. (2001). *The Rijndael Block Cipher (AES Proposal): A Comparison with DES*. IEEE: 0-7803-6636-0/01.
- Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition*. New York: Wiley.
- Stallings, W. (1999). *Cryptography and Network Security*. International, Upper Saddle River, New Jersey: Prentice Hall.
- Stinson, D. R. (2002). *Cryptography: Theory and Practice, Second Edition*. New Heavens: Chapman & Hall.
- Weaver, N. and Wawrzynek, J. (2002). *High Performance, Compact AES Implementation in Xilinx FPGAs*. Berkeley: U.C. Berkeley Brass group.
- Wu, L., Weaver, C., and Austin, T. (2001). *Crypto Maniac: A Fast Flexible Architecture for Secure Communication*. IEEE.