VERILOG DESIGN OF A 256-BIT AES CRYPTO PROCESSOR CORE

LAI YIT PIN

UNIVERSITI TEKNOLOGI MALAYSIA

To my beloved mother and father, sister and brothers, and fiancée.

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my thesis supervisor, Professor Dr. Mohamed Khalil bin Hj. Mohd Hani, for encouragement, guidance, critics and friendship. Without his continued support and interest, this thesis would not have been the same as presented here.

I am also indebted to Intel Microelectronics (M) Sdn. Bhd for funding my part-time Master study. My manager, Intel-University staffs, UTM School of Postgraduate Study and Faculty of Electrical Engineering staffs also deserve special thanks for their assistance in providing stable and comfortable environment for me to focus on my research.

My fellow postgraduate coursemates should also be recognized for their support. Special appreciation to Mohd. Izuan Ismail and Norashikin M. Thamrin for their support in ramping me up on previous UTM research made on this topic.

I am truly grateful to all my family members, who motivated me the most throughout this research. Without their support, I would not have gone so far.

ABSTRACT

The 21st Century is the Century of Digital, almost all of the information processing and telecommunication are in digital formats, therefore it is a must to ensure the digital data storage and transmission are secured, thus to ensure privacy. Cryptography is the practice to protect one's information through encryption. As of today, the most widely used and studied algorithm is the Advanced Encryption Standard (AES) published 2001. AES algorithm is fast and easy to be implemented in both software and hardware; however software implementation is vulnerable due to loopholes in operating system and generally is less efficient than hardware implementation. This thesis proposes a design of 256-bit AES crypto-processor core in Verilog RTL, by extending from previous UTM student's research, targeted at FPGA implementation in System-on-Chip (SoC) designs. This soft core is designed in compact form and generalized to comply with multiple AES specifications, which will be a valuable asset in UTM soft core IP bank that helps in future SoC researches.

ABSTRAK

Abad ke-21 adalah Abad Digital, hampir kesemua activity pemprosesan maklumat dan telekommunikasi adalah dijalankan dalam format digital, oleh itu adalah kemestian supaya penyimpanan and pertukaran data digital adalah selamat dan dipertahankan daripada penceroboh maklumat, supaya kesulitan maklumat adalah terjamin. Kriptografi adalah suatu bidang mempertahankan maklumat digital melalui *encryption*. Pada masa kini, algorithm yang paling banyak digunakan and dipelajari adalah *Advanced Encryption Standard* (AES) yang diterbitkan pada tahun 2001. Algorithm AES adalah pantas dan senang dilaksanakan melalui perisian ataupun perkakasan. Walaubagaimanapun, kriptografi melalui perisian adalah kurang selamat kerana perisian selalu dipengaruhi oleh masalah system operasi, dan biasanya kekecapan perisian adalah kurang berbanding dengan perkakasan. Thesis ini melanjutkan penyelidikan pelajar UTM yang lalu, mencadangkan satu rekabentuk prosessor kriptografi menggunakan 256-bit AES algorithm dengan *Verilog RTL*, menujukan penggunaan FPGA dalam rekabentuk *System-on-Chip* (SoC). Rekabentuk ini adalah padat dan boleh melaksanakan beberapa spesifikasi AES, menjadikannya salah satu asset yang penting kepada UTM dalam penyelidikan SoC pada masa akan datang.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	– Advanced Encryption Standard
AES128	– AES specification in 128-bit architecture
AES192	– AES specification in 192-bit architecture
AES256	– AES specification in 256-bit architecture
FIPS PUBS	– Federal Information Processing Standards Publications
FIPS-197	– Federal Information Processing Standards Publication 197 a.k.a. ADVANCED ENCRYPTION STANDARD (AES)
NIST	– National Institute of Standards and Technology, USA
RCON	– Round Constant
SBOX	– SubByte Transformation

LIST OF SYMBOLS

Nb	– Number of columns (32-bit words) comprising the State array.
Nk	– Number of 32-bit words comprising the Cipher Key.
Nr	– Number of rounds, which is a function of Nk and Nb (which is fixed).
Rcon[]	– The round constant word array
K	– Cipher Key
M	– Plain Text (in encryption) or Cipher Text (in decryption)
S	– State array
W	– Key State array
$\oplus$	– Exclusive OR
$\bullet$	– Finite field multiplication

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

This thesis proposes system level modeling of an encryption core in Verilog Hardware Description Language (HDL) for Field-Programmable Gate Array (FPGA) implementation. The design is to accelerate fast computation of digital data encryption and decryption using the Advanced Encryption Standard (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 UTM-Crypto256 Processor Core 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 report set out two main objectives for the research:

1. To design a 256-bit architecture AES encryption processor core in Verilog HDL based on previous UTM-Crypto128 IP.

2. To explore the implementation of pipeline architecture to the design.

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 UTM-Crypto128 processor core was designed in VHDL using AES128 architecture, it will be migrated to Verilog HDL modeling and be upgraded to

256-bit architecture (128-bit data block and 256-bit key length), with backward compatibility to AES128 specification.

2. The design is to be modeled at system level, and be translated to RTL abstraction by hand.

3. The design is targeting implementation with Altera APEX20KE FPGA, using EP20K200EFC484-1 device specifically.

4. Logic design and functional validation is performed using the Mentor Graphics Modelsim simulator, it also acts as primary debugger tool due to its rich debug capabilities.

5. Synthesis and timing simulation for verify the design correctness in FPGA implementation is performed with the Altera Quartus II Web-Edition software.

6. Test vectors used to verify the design is based on the "Advanced Encryption Standard" published by National Institute of Standards and Technology, USA (Federal Information Processing Standards Publication 197), hereafter referred as FIPS-197.

1.4 Significant of Work and Research Contributions

1. UTM will own its encryption soft core IP that supports multiple AES architectures (128-bit and 256-bit key length), thus enables future works on System-On-Chip (SoC) researches.

2. The soft core is modeled at system level for easier debug and upgrade in SoC design, and implemented in Verilog language thus provides wider options in backend tools.

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 work begins with the literature review on cryptography with AES algorithm and specification between 128-bit and 256-bit architectures, RTL modeling with Verilog HDL, and fundamental of pipeline design.

After literature review, problem formulation and scope identification are done to extend the UTM-Crypto128 to 256-bit architecture (UTM-Crypto256) with implementation done in the Altera FPGA device. Applications for UTM-Crypto256 are targeted at security devices and secured SoC, such as smart card reader.

The most important part before designing the hardware is to understand the AES algorithm and specification thoroughly, 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 AES (M. H. Jing *et al.*, 2001).

In this research, most of the efforts are focus on architectural design of the UTM-Crypto256 processor core with consideration on all resources possibly needed.

Architecture designs of the UTM-Crypto256 processor are coded in Verilog by hand. The compilation, synthesis and simulation are performed using the Mentor Graphics Modelsim simulator and Altera Quartus II Web-Edition 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.

Along with the development, exploration will be made on enabling pipelining capabilities to the encryption core, which will improve the performance without cost on power. This attempt is also to re-use whatever learnt in the UTM MEHA1BPA Master Course back to the project, such as the pipeline knowledge which was taught in the Advanced Computer Architectures subject.

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 the Thesis

This report is organized into seven chapters. The first chapter is the introduction which covers the background, problem statement, objectives, scopes, the significant and contributions of the project, and at the 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 2 covers high level overview of the AES algorithm and key differences between its 128-bit and 256-bit architectures. It also presents the reason for modeling the design in Verilog HDL, as well as brief introduction to pipelining.

Chapter 3 elaborates the specification of AES algorithm. It covers all the functions and transformation in AES in details, based on the 256-bit architecture.

Chapter 4 summarizes the work done in migrating the VHDL UTM-Crypto128 into Verilog HDL modeling, as well as the efficiency gain from the HDL migration.

Chapter 5 discusses the design and development of the UTM-Crypto256 processor core. 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 UTM-Crypto256 processor core are clearly identified and defined.

Chapter 6 presents the validation and performance analysis of the UTM-Crypto256 processor core. It presents the results obtained from running the performance analysis with artificially generated data. Both Functional and Timing simulations using Modelsim and Quartus-II simulators are used to proof the design correctness.

Finally in Chapter 7, the research work is summarized and ended with potential improvements, extensions and suggestions of future works for this project.