VERILOG DESIGN OF BIST ON AES256 PROCESSOR CORE WITH FPGA IMPLEMENTATION

HEW KEAN YUNG

UNIVERSITI TEKNOLOGI MALAYSIA

VERILOG DESIGN OF BIST ON AES256 PROCESSOR CORE WITH FPGA IMPLEMENTATION

HEW KEAN YUNG

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering (Computer & Microelectronic System)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

OCTOBER 2008

To my beloved father and mother, sister and brother, and friends.

ACKNOWLEDGEMENT

The project entitled “Verilog Design of BIST on AES256 Processor Core with FPGA Implementation” was completed due to cooperation and assistance of a number of people. Hence, I would like to take this opportunity to express my gratitude and appreciation to anyone and everyone who has contributed explicitly or implicitly towards the success of this project. Acknowledgment is particularly given to my project supervisor, Professor Dr. Mohamed Khalil bin Hj. Mohd Hani, for encouragement, guidance, critics, advice and support.

I am indebted to Intel Microelectronics (M) Sdn. Bhd for funding my part-time Master study. My Intel manager and my fellow postgraduate coursemates should also deserve special thanks for their encouragement and assistance throughout the research. Special appreciation to Lai Yit Pin and Vishnu Param for their advice and previous works done on AES256 processor core as well.

Last but not least, a really big thank you to my parents, who are always by my side offering me moral support and motivating me the most throughout this research. Without their encouragement, I would not have gone so far.

ABSTRACT

Cryptography is very important to ensure secured data storage and transmission through encryption technique in this digital world. The most widely used cryptography algorithm is the Advanced Encryption Standard (AES) published in 2001. AES algorithm is fast and easy to be implemented, and it aims to protect data and ensure privacy. Hence, AES hardware cannot afford any encryption failure which will corrupt the whole system. Built-In-Self-Test (BIST) introduced into the AES system will increase the system testability and reliability, which in turn will protect the system from attack and will incur less testing cost. This project aims to continue previous UTM student's research on FPGA implementation of AES system in System-on-Chip (SoC) design. By extending further, a proposed AES hardware BIST design is incorporated into the AES processor core in Verilog RTL and FGPA implementation. This will be a valuable asset to UTM for future SoC researches on AES and BIST design.

ABSTRAK

Kriptografi adalah sangat penting untuk menjaminkan keselamatan penyimpanan and pertukaran maklumat melalui teknik penyulitan (*encryption*) dalam dunia digital ini. Algorithm yang paling luas digunakan ialah *Advanced Encryption Standard* (AES) yang diterbitkan pada tahun 2001. Algorithm AES adalah pantas dan mudah dilaksanakan dan tujuannya adalah untuk melindungi maklumat dan memastikan privasi maklumat. Dengan ini, perkakasan AES mesti mengelakan kegagalan penyulitan yang akan meruntuhkan seluruh system. *Built-In-Self-Test* (BIST) diperkenalkan dalam sistem AES akan meningkatkan kebolehujian dan kebolehpercayaan sistem, yang seterusnya mempertahankan sistem daripada pencerobohan and menyebabkan kurang kos ujian. Maklamat project ini adalah untuk meneruskan penyelidikan pelajar UTM yang lalu dengan penggunaan FPGA dalam rekabentuk *System-on-Chip* (SoC). Project ini juga dilanjutkan lagi dengan mencadangkan rekabentuk BIST untuk perkakasan AES digabungkan dalam prosessor AES dengan *Verilog RTL* dan penggunaan FPGA. Rekabentuk ini akan menjadikan satu asset yang amat berharga kepada UTM untuk penyelidikan SoC pada masa depan dalam rekabentuk AES dan BIST.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	–	Advanced Encryption Standard
AES128	–	AES specification in 128-bit architecture
AES256	–	AES specification in 256-bit architecture
BIST	–	Built-In Self Test
SBOX	–	SubByte Transformation
FPGA	–	Field Programmable Gate Array
VHDL	–	Very-High-Speed-Integrated-Circuit Hardware Description Language

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

This project proposes system level modeling of Built-In-Self-Test (BIST) capability using Verilog hardware description language on Advanced Encryption Standard (AES) core. The whole system will be implemented on Field-Programmable Gate Array (FPGA) in System-on-Chip (SoC) design. The design is to ensure the reliability and testability of digital data encryption and decryption in AES core. This chapter covers the project background, project objectives, followed by scope of work, project contributions and finally the report outline.

1.1 Project Background

In this paperless twenty-first century, almost all data processing or information processing are in digital formats. Means to guarantee the secrecy of this information has become very crucial and lot of researches have been made across the centuries. In other words, in order to protect the data and keep privacy, the information system should be equipped with cryptography which is the practice and study of hiding information. Cryptography enables to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

In October 2000, the NIST (National Institute of Standards and Technology) announced the approval of a new secret key cipher standard chosen among 15 candidates. This new standard algorithm was meant to replace the old DES algorithm, whose key sizes were becoming too small. Rijndael – a compressed name taken from its inventors Rijmen and Daemen - was chosen to become the future AES. This cryptography AES standard has been designed in UTM-Crypto256 Processor Core on hardware implementation (FPGA) with key RAM, which can make not only a forward key scheduling for encryption but also a reversed key scheduling for decryption. Therefore, this hardware implementation enhances the physical security as well as higher speed and outside attackers cannot easily attack, interrupt or modify its operation.

However, with the increasing growth of sub-micron technology has resulted in the difficulty of testing. Manufacturing processes are extremely complex, making the manufacturers to consider testability as a requirement to assure the reliability and the functionality of each of their designed circuits. Also, specific attacks are possible because the attacker has access to the physical cryptographic device to compromise secret keys of cryptographic algorithms by using standard statistical tools. As a result, a good cryptographic device must therefore ensure high reliability and dependability and, in addition, it must implement some countermeasures to prevent the possibility of gathering the secret code by mean of any attack.

Built-In-Self-Test (BIST) is one of the most popular test technique used to ensure the testability of device. With further detailed BIST design down to module level, although not specifically designed to protect against tampering, this design will makes more difficult being attacked based on power analysis. However, drawback of BIST is that it introduced additional implementation hardware overhead, design cycle time, design resources and degradation.

This project focuses on the design of the embedded BIST architecture on SBOX hardware inside AES core. AES core is a cryptography core which can make not only a forward key scheduling for encryption but also a reversed key scheduling for decryption. The BIST design will be implemented using Verilog Hardware Description Language at the Register Transfer Level (RTL) abreaction level. SBOX BIST technique is incorporated into the AES core on system level and implemented on hardware (FPGA) in System-on-Chip (SoC) design.

1.2 Project Objectives

From the discussion from previous section, this report set out two main objectives for the research:

1. To design Built-in Self Test (BIST) down to AES Sbox level to further enhance the security of stored information on AES core.

2. To incorporate AES core with generic system Built-In Self Test (BIST) design on AES encryption processor core.

3. To implement AES core with Built-In Self Test (BIST) capability on Field-Programmable Gate Array (FPGA) in System-on-Chip (SoC) 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:

(i) This project is not to design the AES core but to understand the architecture and implementation of existing UTM-Crypto256 AES Processor Core.

(ii) Enhance AES core with system generic BIST capability to increase the testability.

(iii) Design BIST down to SBOX module level to increase the security of device.

(iv) The design is to be modeled at system level and then translate to RTL abstraction level (verilog coding).

(v) Logic and functional validation, synthesis and timing simulation for verify the design correctness will be performed using Altera Quartus 6.1.

(vi) The hardware implementation will be on Altera APEX20KE FPGA, using EP20K200EFC484-2X device with Nios processor embedded inside.

1.4 Project Contributions

(i) With the implementation of BIST, expensive tester requirements and testing procedures starting from circuit or logic level to field level testing are minimized. The reduction of the test cost will lead to the reduction of overall production cost.

(ii) BIST will also increase the security of encrypted information and prevent being attacked and thus ensure the reliability of AES core.

(iii) UTM will own this embedded BIST on AES core and thus enables future works on System-On-Chip (SoC) researches such as upgrade the whole system into Nios II FPGA board.

1.5 Report Outline

This report is organized into seven chapters. Chapter 1 basically gives an overview on the project, objectives, scope of works and project contribution.

Chapter 2 gives the literature review on AES architecture, Sbox BIST and FPGA architecture aiming to have a greater understanding of the overall idea of this project. Chapter 3 mainly concentrates on the Design Workflow, Verilog overview, Altera's Quartus tool and SOPC builder tool.

Chapter 4 discusses on the design implementation of Sbox BIST in simulation and end with generic system BIST idea. Chapter 5 focuses on FPGA implementation which covers from top level design, Avalon bus down to APEX device configuration.

Chapter 6 mainly discusses simulation results and some performance analysis. The report will end with the conclusion and future works in Chapter 7.

This report also enclosed with references and the appendix which consists of the Verilog coding.

REFERENCES

1. Yit Pin, Lai (2007). *Verilog Design of 256-bits AES Crypto Processor Core*. Master Thesis. Universiti Teknologi Malaysia; 2007.

2. G. Di Natale, M. L. Flottes, B. Rouzeyre. *On-Line Self-Test of AES Hardware Implementations.* France : Université Montpellier II

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

4. Pierre Loidreau (2005). *Introduction To Cryptography*

5. Svante Seleborg (2007). *About AES – Advanced Encryption Standard*

6. Dr Mohammad Khalil Hani (2008). *Digital Systems – VHDL & Verilog Design*

7. Jasmine Hau Yuan Wen. *Nios Avalon Bus In Slave Transfer Tutorial*

8. Altera (2004). *Avalon Interface Specification Reference Manual*

9. Altera (2003). *Nios Embeded Processor Development Board Datasheet*

10. Altera (2002). *Excalibur Nios Tutorial*

11. Altera (2008). *Quartus II Version 8.0 Handbook Volume 4: SOPC Builder*

12. Altera. *Introduction to the Altera SOPC Builder Using Verilog Design*

13. Alam, M., Badawy, W., and Jullien, G. (2002). *A Novel Pipelined Threads*

14. Architecture for AES Encryption Algoritma. *IEEE International Conference on Application-Specific System, Architectures, and Processors (ASAP'02)*: IEEE, 1063-6862/02.

15. Brown, S. (2000). *Fundamentals of Digital Logic With VHDL Design*. New York: McGraw-Hill.

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

17. John D.Carpinelli (2000), *Computer Systems Organization & Architecture*, Pearson Education

18. N. Kranitis. *An Effective Deterministic BIST Scheme for Shifter/Accumulator Pairs in Datapaths.* Greece: Institute of Informatics & Telecommunications

19. National Institute of Standards and Technology (2001). *Advanced Encryption Standard*, National Institute of Standards and Technology : Federal Information Processing Standards Publication 197.

20. Panato, A., Barcelos, M., and Reis, R. (2002). *An IP of an Advanced Encryption*

21. Standard for Altera^{TM} Devices. *15 th Symposium on Integrated Circuit and System Design (SBCCI'02)*: IEEE, 0-7695-1807-9/02.

22. Paul Kocher, Joshua Ja_e, and Benjamin Jun. *Differential Power Analysis*. USA: Cryptography Research, Inc