

Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

**NOVEL DIGITAL VLSI IMPLEMENTATION OF DATA ENCRYPTION
ALGORITHM USING NANO-METRIC CMOS TECHNOLOGY**

A THESIS PRESENTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE

OF

DOCTOR OF PHILOSOPHY

IN

ENGINEERING

AT

MASSEY UNIVERSITY

AUCKLAND

NEW ZEALAND

NABIHAH @ NORNABIHAH AHMAD

2013

ABSTRACT

Implementations of the Advanced Encryption Standard (AES) have rapidly grown in various applications including telecommunications, finance and networks that require a low power consumption and low cost design. Presented in this thesis is a new 8-bit stream cipher architecture core for an application specific integrated circuit AES crypto-processor. The chip area and power are optimised along with high throughput by employing circuit-level techniques, resource sharing and low supply voltage. The proposed design includes a novel S-box/ InvS-box, MixColumn/ InvMixColumn and ShiftRow/ InvShiftRow with a novel low power Exclusive OR (XOR) gate applied to all sub systems to minimise the power consumption. It is implemented in a 130nm CMOS process and supports both encryption and decryption in Electronic Codebook Mode (EBC) using 128-bit keys with a throughput of 0.05Gbit/s (at 100MHz clock). This design utilises 3152 gate equivalents, including an on-the-fly key scheduling unit along with 4.23 μ W/MHz power consumption. The area of the chip is 640 μ m \times 325 μ m (0.208 square mm), excluding the bonding pads. Compared to other 8-bit implementations, the proposed design achieves a smaller chip size along with higher throughput and lower power dissipation. This thesis also describes a new fault detection scheme for S-box/ InvS-box that is parity prediction based to protect the key from fault attacks.

ACKNOWLEDGEMENTS

I would firstly like to profoundly thank my supervisor Dr. Rezaul Hasan for his endless support, encouragement, guidance and advice throughout my doctoral studies. There were many difficulties during the theoretical and experimental aspects of the work, but Rezaul's direction and never ending patience with me has helped me to finally accomplish this thesis. Rezaul's deep knowledge of VLSI and integrated circuit design along with his research insights facilitated me to achieve the research goals. Without him this work could not have been brought to its final accomplishment. In addition, his guidance and effort through long days and long hours of authorship work has resulted in several high standard international journal publications during the course of this research.

Thanks are also due to the staff and senior students at the School of Engineering and Advanced Technology (SEAT) for their friendship and continuous cooperation in dealing with the issues arising during my studies. I would like to especially thank Ananiah Sundararajan, Robert Fisk, Jack Li, Sadia Alam, Stepan Lapshav, Dmitri Roukin, Loke Chun Eng and Muhammad Khurram for their time in helping me with the software and my research design, as well as, their advice and suggestions. The support of the MOSIS academic research program is also gratefully acknowledged for covering the cost of my prototype fabrication.

I would also like to thank my family for their unconditional support and encouragement during the course of my doctoral studies.

DECLARATION

The author declares that this is her own work except where due acknowledgement has been given. It is being submitted for the PhD in Engineering to Massey University, New Zealand.

This thesis describes the research carried out by the author at the School of Engineering, Massey University, New Zealand from March 2009 to July 2013, supervised by Dr. Rezaul Hasan.

TABLE OF CONTENTS

Abstract.....	i
Acknowledgements.....	ii
Declaration.....	iii
Table of Contents.....	iv
Table of Figures.....	viii
List of Tables.....	xi
Definitions and Abbreviations.....	xii
CHAPTER 1.....	14
Introduction.....	14
1.1 Introduction.....	14
1.2 Motivation.....	17
1.3 Research Objectives.....	19
1.4 Contributions to Knowledge.....	19
1.5 Thesis Organisation.....	21
CHAPTER 2.....	22
Literature Review.....	22
2.1 Introduction.....	22
2.2 Mathematical Background.....	22
2.2.1 Finite Fields.....	22
2.2.2 Operations over Binary Finite Fields $GF(2^8)$	24
2.3 AES System and Architecture.....	25
2.3.1 Round Transformation.....	27
2.4 Mode of operation.....	34
2.4.1 Electronic Codebook Mode (ECB).....	34
2.4.2 Counter Mode (CTR).....	35
2.4.3 Cipher-block Chaining mode (CBC).....	36
2.4.4 Cipher Feedback mode (CFB).....	36
2.4.5 Output Feedback mode (OFB).....	37
2.5 Design Evaluation Criteria and Specifications.....	37
2.5.1 Speed of operation.....	38
2.5.2 Power Consumption.....	39

2.5.3	Delay	42
2.5.4	Area	43
2.6	AES architecture	43
2.6.1	AES 128-bit datapath	43
2.6.2	AES 32-bit datapath	44
2.6.3	AES 8-bit datapath	45
CHAPTER 3	48
Novel XOR Gate Low-Power Low-Voltage Full Swing Output Voltage for CMOS		
Galois Field Arithmetic		
3.1	Introduction.....	48
3.2	Novel XOR Topology	50
3.3	Performance and simulation results in 65nm CMOS.....	52
3.4	Performance analyses and simulation results in 130nm CMOS	57
3.5	XOR gate chip and experimental results	62
3.6	Conclusions.....	66
CHAPTER 4	68
A Compact Combinational Logic Design of S-box/ InvS-box for AES crypto-		
processor.....		
4.1	Introduction	68
4.2	S-box/ InvS-box design methodology	69
4.2.1	Multiplication of nibble with constant, λ	74
4.2.2	Squaring nibbles.....	75
4.2.3	Multiplication of nibbles in $GF(2^4)$	75
4.2.4	Multiplication of bit-pairs in $GF(2^2)$	76
4.2.5	Multiplication of bit-pairs with constant ϕ in $GF(2^2)$	76
4.2.6	Multiplicative inverse of nibble in $GF(2^4)$	77
4.3	Proposed S-box/ InvS-box architecture	77
4.3.1	Stage 1	78
4.3.2	Simplification of multiplicative inverse of nibble in $GF(2^4)$	79
4.3.3	CombineXAXB.....	81
4.4	Hardware Implementation of S-box/ InvS-box	83
4.5	Evaluation and comparison with other designs	84
4.6	Conclusions	88

CHAPTER 5	90
Fault Detection Scheme of AES S-box/ InvS-box using Parity Prediction Based Method.....	91
5.1 Introduction	91
5.2 Proposed Fault Detection Scheme for AES S-box/ InvS-box architecture.....	93
5.2.1 Blocks 1 and 6: Predicted Parity of Isomorphic and Inverse Isomorphic Mapping	95
5.2.2 Block 3: Parity Stage 1	97
5.2.3 Block 4: Parity Inversion.....	98
5.2.4 Block 5: Parity CombineXAXB	99
5.2.5 Blocks 2 and 7: Parity Affine and Inverse Affine.....	101
5.3 Hardware Complexity Analysis	102
5.4 Fault coverage of the proposed fault detection scheme	103
5.5 Conclusions	104
CHAPTER 6	105
Efficient Integrated AES Crypto-Processor Architecture for 8-bit Stream Cipher	105
6.1 Introduction	105
6.2 AES Architecture.....	105
6.3 SubBytes and InvSubBytes Architecture	107
6.4 New Topology of MixColumns/ InvMixColumns	108
6.5 ShiftRows/ InvShiftRows Architecture Implementation	113
6.6 Add Round Key Implementation.....	116
6.7 Key Scheduling Unit.....	116
6.8 Conclusions	121
CHAPTER 7	122
Implementation, Verification and Results of AES Crypto-Processor.....	122
7.1 Introduction.....	122
7.2 Physical implementation.....	122
7.2.1 Layout consideration for design	122
7.3 Verification Methodologies	125
7.3.1 Functional Verification	126
7.3.2 Physical verification.....	126
7.4 Simulation and Measurement results	127

7.4.1	Composite result and discussions	127
7.4.2	Circuit Simulation Results.....	130
7.5	Measurement testing setup for AES chip	132
7.6	Experimental Results.....	137
7.7	Conclusions.....	139
CHAPTER 8	140
Conclusions and Recommendations.....		140
8.1	Introduction	140
8.2	Thesis Summary	140
BIBLIOGRAPHY	144
Appendices	151
List of Publications	163
Journal Paper I	165
Journal Paper II	171
Journal Paper III.....		173
Conference Proceeding I	185
Conference Proceeding II	188
Conference Proceeding III.....		192
Conference Proceeding IV.....		197
Conference Proceeding V	202

TABLE OF FIGURES

Figure 2.1 <i>AES flow for encryption and decryption</i>	26
Figure 2.2 <i>Electronic Codebook (ECB) mode for Encryption and Decryption[39]</i>	35
Figure 2.3 <i>Counter Mode (CTR) mode for Encryption and Decryption[39]</i>	35
Figure 2.4 <i>Cipher-block Chaining (CBC) mode for Encryption and Decryption[39]</i> ..	36
Figure 2.5 <i>Cipher Feedback (CFB) mode for Encryption and Decryption[39]</i>	37
Figure 2.6 <i>Output Feedback (OFB) mode for Encryption and Decryption[39]</i>	37
Figure 2.7 <i>Static CMOS leakage sources[42]</i>	40
Figure 3.1 <i>Proposed XOR1 circuit for low-power Galois field arithmetic</i>	51
Figure 3.2 <i>Proposed XOR2 gate circuit</i>	52
Figure 3.3 <i>Full swing output voltage of the proposed (a) XOR1 gate (b) XOR2 gate</i>	53
Figure 3.4 <i>Propagation delay with supply voltage scaling for different XOR gates in 65nm CMOS technology</i>	55
Figure 3.5 <i>Power dissipation with supply voltage scaling for different XOR gates in 65nm CMOS technology</i>	56
Figure 3.6 <i>Power-delay product (PDP) with supply voltage scaling for different XOR gates in 65nm CMOS technology</i>	56
Figure 3.7 <i>Propagation delay with supply voltage scaling for different XOR gates in 130nm CMOS technology</i>	59
Figure 3.8 <i>Power dissipation with supply voltage scaling for different XOR gates in 130nm CMOS technology</i>	60
Figure 3.9 <i>Power-delay product (PDP) with supply voltage scaling for different XOR gates in 130nm CMOS technology</i>	60
Figure 3.10 <i>Propagation Delay vs. output load</i>	61
Figure 3.11 <i>Layout of the 2-input XOR gate (a) XOR1 gate (b) XOR2 gate</i>	63
Figure 3.12 <i>Microphotograph of the fabricated novel CMOS pass-transistor based full swing output voltage XOR2 gate along with bonding pads and XOR gate inset view</i>	64
Figure 3.13 <i>Logic Analyzer waveform of the inputs and the output for the fabricated XOR2 gate</i>	65

Figure 3.14 Oscilloscope waveforms for the fabricated XOR2 gate (Yellow = input A, Blue= input B and Green=output Y).....	65
Figure 3.15 Rise time of output signal.....	66
Figure 3.16 Fall time of output signal.....	66
Figure 4.1 Multiplicative Inverse in $GF(2^8)$ as extension of degree 2 over $GF((2^2)^2)$	74
Figure 4.2 Proposed Multiplicative Inverse in $GF(2^8)$ architecture.....	84
Figure 4.3 Complete layout of the S-box/ InvS-box.....	85
Figure 4.4 Complete chip die of the S-box/ InvS-box with bonding pads.	85
Figure 4.5 S-box functional test verification of the SubBytes operation.	87
Figure 4.6 InvS-box functional test verification of the Inverse SubBytes operation....	87
Figure 5.1 Proposed parity prediction fault detection blocks for the composite field S-box and InvS-box.....	94
Figure 5.4 Predicted Parity circuit for Stage 1 implementation.....	98
Figure 5.5 Predicted Parity circuit for inversion in $GF(2^4)$ implementation.....	99
Figure 5.6 Predicted parity circuit of CombineXAXB implementation.....	100
Figure 5.7 Predicted parity circuit of affine implementation.....	101
Figure 5.8 Predicted parity circuit of inverse affine implementation.....	102
Figure 6.1 Block diagram of AES crypto-processor.....	106
Figure 6.2 High level architecture of the AES crypto-processor.....	107
Figure 6.3 Proposed Multiplicative Inverse in $GF(2^8)$ transformation architecture.	108
Figure 6.4 MixColumns and InvMixColumns circuit.....	112
Figure 6.5 ShiftRows and InvShiftRows circuit for 8-bit datapath.....	115
Figure 6.6 RCON[i] Generator.....	118
Figure 6.7 Key Scheduling unit.....	120
Figure 7.1 External connections of AES crypto-processor on the 108-pin PGA package.....	124
Figure 7.2 Packaged AES microchip in PGA108M.....	124
Figure 7.3 Complete layout of active circuitry for the AES crypto-processor.....	125
Figure 7.4 Photomicrograph of the AES fabricated die.....	125
Figure 7.5 Waveform simulation for SubByte transformation.....	130
Figure 7.6 Waveform simulation for ShiftRow transformation.....	131
Figure 7.7 Waveform simulation for MixColumns and key round transformation....	131
Figure 7.8 Waveform simulation for last key round and data output of AES encryption.....	132

Figure 7.9 <i>Next set of test vectors for AES simulation after encryption process was completed</i>	132
Figure 7.10 <i>ML505 FPGA board for test vectors generator</i>	133
Figure 7.11 <i>Hardware connection setup for AES testing</i>	135
Figure 7.12 <i>Circuit testing for AES (a) PCB with the test socket for AES and 4-bit dual supply translating transceiver, (b) Logic analyzer to display the output, and (c) Circuit setup with FPGA interface and AES chip</i>	136
Figure 7.12 <i>Sel_data and q44 connection in the AES circuit</i>	137
Figure 7.13 <i>Outputs for MixColumns and first key round generated</i>	138
Figure 7.14 <i>Data output generated after 264 clock cycles and the next test vector input</i>	138

LIST OF TABLES

Table 2.1 AES Key Block Round Combinations in FIPS-197	26
Table 2.2 AES architecture of different datapath	46
Table 3.1 Comparison of simulation results for the XOR gate in 65nm CMOS technology.....	54
Table 3.2 Simulation results of XOR gate in 130nm CMOS technology.....	58
Table 3.3 Noise Margin of different XOR gate	62
Table 4.1 Gate count comparison between typical composite field architecture and proposed Stage 1	79
Table 4.2 Gate count comparison between typical inversion in $GF(2^4)$ composite field architecture and proposed inversion in $GF(2^4)$	81
Table 4.3 Gate count comparison between typical multiplication in $GF(2^4)$ and proposed CombineXAXB	83
Table 4.4 Complexity of proposed S-box/ InvS-box implementation	87
Table 4.5 AES S-box performance and comparison with previous work.	89
Table 5.1 Hardware complexities for proposed predicted parity of S-box/ InvS-box	103
Table 5.2 Fault coverage for fault detection scheme	104
Table 6.1 Comparison of different MixColumn/ InvMixColumn designs	113
Table 6.2 ShiftRow offset values	114
Table 6.3 Comparison of total hardware cost for different ShiftRows/ InvShiftRows designs	116
Table 6.4 Expanded Key Sizes in Words	118
Table 6.5 RCON[i] for key generation.....	118
Table 7.1 Complete list of input and output ports on the implemented design.	123
Table 7.2 Comparison with previous 8-bit AES design.....	129

DEFINITIONS AND ABBREVIATIONS

AES	Advanced Encryption Standard (AES),
DES	Data Encryption Standard (DES)
NIST	National Institute of Standards and Technology
WLAN	Wireless Local Area Networks
FPGA	Field Programmable Gate Array
ASIC	Application-Specific Integrated Circuits
VHDL	VHSIC Hardware Description Language
VLSI	Very Large Scale Integration
RFID	Radio-Frequency Identification Devices
CMOS	Complementary MOS
XOR	Exclusive OR
EBC	Electronic Codebook
LUT	Lookup Tables
ROM	Read-Only-Memory
ANF	Algebraic Normal Form
CSE	Common Sub expression Elimination
BDD	Binary Decision Diagram
TBDD	Twisted Binary Decision Diagram
DSE	Decoder-Switch-Encoder structure
SOP	Sum of Product
SABL	Sense Amplifier Based Logic
CTR	Counter Mode
CBC	Cipher-block Chaining
CFB	Cipher feedback
OFB	Output feedback
IV	Initialisation vector
MOSFET	Metal-Oxide Semiconductor Field-Effect Transistor
LP	Low Power
GP	General Purpose

V _t	Threshold voltage
CLB	Configurable Logic Blocks
GE	Gate Equivalent
ASIP	Application-Specific-Instruction-Processor
RAM	Random-access memory
SOC	System-on-chip
CC	Cross-coupled
P-XOR	Powerless XOR gate
GDI	Gate-Diffusion-Input
PDP	Power-Delay Product
DRC	Design Rule Checking
LVS	Layout vs. Schematic
EDP	Energy-Delay Product
PAP	Power-Area Product
PAT	Power-Area-Latency
ESD	Electrostatic Discharge