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 4.23µW/MHz power consumption. The area of the chip is 640µm×325µm (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

TABLE OF FIGURES

LIST OF TABLES

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

Vt	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