PARALLEL-PIPELINED-MEMORY (P^2M) OF BLOWFISH FPGA-BASED RADIO SYSTEM WITH IMPROVED POWER-THROUGHPUT FOR SECURE ZIGBEE TRANSMISSION

RAFIDAH BINTI AHMAD

UNIVERSITI SAINS MALAYSIA

2020

PARALLEL-PIPELINED-MEMORY (P^2M) OF BLOWFISH FPGA-BASED RADIO SYSTEM WITH IMPROVED POWER-THROUGHPUT FOR SECURE ZIGBEE TRANSMISSION

by

RAFIDAH BINTI AHMAD

Thesis submitted in fulfilment of the
requirements for the degree of
Doctor of Philosophy

January 2020

ACKNOWLEDGEMENT

Firstly, I would like to express my humble gratitude to Allah SWT for giving me opportunity and help me endlessly in finishing this research work. I am deeply indebted to my supervisor, Professor Dr. Widad Ismail for her guidance, advice, help and support from the beginning towards completing this PhD thesis. Her suggestions and unfailing patient have been a great motivation for me to success in my study. I would also like to thank the Director of CEDEC and USM for giving me a chance to pursue my study at PhD level. A special dedication to the entire School of Electrical and Electronic Engineering for the facilities and equipments provided for making this research work achieved its objective. Many thanks for the support of administrative and technical staff especially Mr. Latip, Mdm. Zammira and Mr. Jamal who have helped me a lot during the test and measurement. A very special gratitude also goes out to my parents Ahmad Geni and Rukiah Ajis, and my siblings Fauziah, Mohd. Azlan, Mohd. Faris and Mohd. Ismail for their prayers, blessings and moral supports since the beginning. Special dedicated thanks to my dearest sons Tg. Muhd. Luqman, Tg. Muhd. Arif, Tg. Muhd. Zafri and Tg. Muhd. Adam for being always there and gave me a lot of moral supports, encouragement as well as patience for me to go through all the ups and downs. Last but not least, my appreciation and thanks to my friends for their valuable ideas, comments and critics throughout the preparation of my research work. Thank you all for the tremendous help and support to make the production of this thesis a success.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

ADC	Analog-to-digital converter
ADD	Addition
AES	Advanced Encryption Standard
ALU	Arithmetic logic unit
ARM	Advanced reduced instruction set computer machine
ASM	Algorithmic state machine
BER	Bit-error-rate
BIT	Bit stream
BRAM	Block random access memory
CAST	Carlisle Adams Stafford Tavares
CFB	Cipher feedback
CLB	Configurable logic block
CPLD	Complex programmable logic device
CPU	Central processing unit
DAC	Digital-to-analog converter
DES	Data Encryption Standard
DOMT	Digital ortho-mode transducer
DRIL	Dynamic reconfiguration, replication, inner-loop pipelining and loop-folding
DSP	Digital signal processing
F	Feistal
FF	Flip-flop
FFT	Fast Fourier Transform
FIFO	First-in-first-out
FIPS	Federal Information Processing Standard
FIR	Finite impulse response
FMC	FPGA mezzanine card
FPGA	Field programmable gate array
FSM	Finite state machine
GPIO	General purpose input output
HDL	Hardware description language
HF	High frequency

I2C	Inter-integrated circuit
IDE	Integrated development environment
IDEA	International data encryption algorithm
IEEE	The Institute of Electrical and Electronics Engineers
IIR	Infinite impulse response
ILA	Integrated logic analyzer
IO	Input output
IoT	Internet of things
IP	Intellectual property
ISE	Integrated synthesis environment
ISM	Industrial, scientific and medical
LSB	Least significant bit
LUT	Look-up-table
MDS	Minimum detectable signal
MIT	Massachusetts Institute of Technology
MMCM	Mixed-mode clock manager
MSB	Most significant bit
NIST	National Institute of Standards and Technology
NLOS	Non-line-of-sight
NVIS	Near vertical incidence sounding
OMAP	Open multimedia applications platform
P^2M	Parallel-pipelined-memory
P2P	Point-to-point
PL	Programmable logic
PS	Processing system
QAM	Quadrature amplitude modulation
RAM	Random access memory
RC	Rivest's cipher
RF	Radio frequency
RHINO	Reconfigurable hardware interface for computation and radio
ROM	Read only memory
RTL	Register transfer level
SDR	Software defined radio
SNR	Signal-to-noise ratio

SoC	System-on-chip
SOF	Start-of-frame
SPI	Serial peripheral interface
SSR	Sideband rejection ratio
UART	Universal asynchronous receiver transmitter
UHF	Ultra high frequency
ULK	Unified learning kit
USB	Universal serial bus
USM	Universiti Sains Malaysia
UUT	Unit under test
VHDL	Very high speed integrated circuit hardware description language
VHF	Very high frequency
WARP	Wireless open-access research platform
WPAN	Wireless personal area network

LIST OF SYMBOLS

a	4-byte word of AES-128
AddRoundKey	Addition of a round key in AES-128 architecture
B	Bandwidth
c	Column of *state* in AES-128
C	Total effective capacitance being switched per clock cycle
dataCntr	Transmitted data counter
E_b	Bit energy
erf(x)	Gauss error function
errorCntr	Error data counter
F_{max}	Maximum clock frequency in MHz unit
GF	Galois polynomial
ibufds	Differential input buffer
InvMixColumns	Inverse mix-columns in AES-128
InvShiftRows	Inverse shift rows in AES-128
InvSubBytes	Inverse byte substitution in AES-128
L	Number of parallel system
M	Number of level in pipelined system
Max	Maximum
mem_dec	Memory for decrypted data of Blowfish
mem_enc	Memory for encrypted data of Blowfish
minicom	UART terminal window in CPU
MixColumns	Mix-columns in AES-128
mode	Selector for encryption or decryption process
n	Number of clock cycles
N_b	Number of columns