

**PARALLEL-PIPELINED-MEMORY (P<sup>2</sup>M) 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<sup>2</sup>M) 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

	<b>Page</b>
<b>ACKNOWLEDGEMENT .....</b>	<b>ii</b>
<b>TABLE OF CONTENTS .....</b>	<b>iii</b>
<b>LIST OF TABLES.....</b>	<b>x</b>
<b>LIST OF FIGURES.....</b>	<b>xxii</b>
<b>LIST OF ABBREVIATIONS .....</b>	<b>xx</b>
<b>LIST OF SYMBOLS .....</b>	<b>xxiii</b>
<b>ABSTRAK.....</b>	<b>xxvi</b>
<b>ABSTRACT.....</b>	<b>xxviii</b>
<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1</b>
1.1 Introduction.....	1
1.2 Research Motivation .....	3
1.3 Problem Statements .....	7
1.4 Research Objectives.....	10
1.5 Research Contributions .....	10
1.5.1 Software.....	10
1.5.1(a) Parallel Technique .....	11
1.5.1(b) Pipelined Technique .....	11
1.5.1(c) Memory Technique.....	12
1.5.2 Hardware.....	12
1.5.3 Network .....	13
1.5.4 Test and Measurement.....	13
1.6 Research Scopes and Limitations .....	14
1.7 Thesis Organization .....	17

<b>CHAPTER 2</b>	<b>LITERATURE REVIEW .....</b>	<b>19</b>
2.1	Introduction.....	19
2.2	Overview on Symmetric Cryptography Schemes.....	19
2.3	Performance Review of Research Works on Symmetric Cryptography Schemes .....	21
2.4	Overview on AES and Blowfish Schemes.....	25
2.4.1	AES.....	25
	2.4.1(a) <i>SubBytes</i> .....	26
	2.4.1(b) <i>ShiftRows</i> .....	28
	2.4.1(c) <i>MixColumns</i> .....	28
	2.4.1(d) <i>AddRoundKey</i> .....	29
	2.4.1(e) Key Expansion .....	30
	2.4.1(f) <i>InvShiftRows</i> .....	30
	2.4.1(g) <i>InvSubBytes</i> .....	31
	2.4.1(h) <i>InvMixColumns</i> .....	31
2.4.2	Blowfish.....	32
	2.4.2(a) Subkeys .....	34
	2.4.2(b) Encryption/Decryption .....	35
	2.4.2(c) F Function .....	35
2.5	Review of Research Works on AES and Blowfish through FPGA .....	36
2.5.1	AES.....	36
2.5.2	Blowfish.....	48
2.6	Overview on Hardware Platform .....	61
2.6.1	FPGA Zynq-7000 SoC .....	61
2.6.2	FMC XM105 .....	65
2.6.3	XBee-PRO ZigBee Module.....	66
2.7	Review on Existing FPGA-based Radio Systems .....	68
2.8	Summary.....	76

<b>CHAPTER 3</b>	<b>METHODOLOGIES.....</b>	<b>78</b>
3.1	Introduction.....	78
3.2	Overview of Software-based Flow .....	79
3.3	Architectural Design of the Proposed P <sup>2</sup> M AES-128 .....	85
3.3.1	AES-128 Testbench .....	87
3.3.2	AES-128 Core.....	91
3.3.3	Data Processing Unit .....	93
3.3.3(a)	<i>SubBytes</i> Operation .....	93
3.3.3(b)	<i>ShiftRows</i> Operation .....	96
3.3.3(c)	<i>MixColumns</i> Operation .....	97
3.3.3(d)	<i>AddRoundKey</i> Operation .....	98
3.3.4	Key Expansion Unit.....	99
3.3.5	Layout Constraint .....	101
3.3.6	Timing Constraint.....	101
3.3.7	Parallel Technique .....	102
3.3.8	Pipelined Technique .....	104
3.3.9	Memory-based Technique .....	107
3.4	Architectural Design of the Proposed P <sup>2</sup> M Blowfish .....	108
3.4.1	Blowfish Data Controller.....	110
3.4.2	Blowfish Core.....	116
3.4.2(a)	Memory Operation.....	116
3.4.2(b)	Blowfish Round Operation .....	121
3.4.2(c)	FIFO Operation .....	121
3.4.2(d)	<i>S-boxes</i> Operation .....	124
3.4.2(e)	$\pi$ Data .....	125
3.4.2(f)	<i>P-Arrays</i> Operation .....	127
3.4.2(g)	Ciphertext Operation .....	128

3.4.3	Layout Constraint .....	129
3.4.4	Timing Constraint.....	129
3.4.5	ILA Operation.....	131
3.4.6	UART Operation .....	132
3.4.7	Frequency Divider Operation .....	134
3.4.8	Parallel Technique .....	136
3.4.9	Pipelined Technique .....	140
3.4.10	Memory-based Technique .....	145
3.5	Summary.....	148
<b>CHAPTER 4 DEVELOPMENT AND IMPLEMENTATION OF THE PROPOSED P<sup>2</sup>M BLOWFISH RADIO SYSTEM .....</b>		<b>150</b>
4.1	Introduction.....	150
4.2	Overview of Hardware-based Flow .....	151
4.3	Architectural Design of the P <sup>2</sup> M Blowfish Radio System.....	161
4.3.1	P <sup>2</sup> M Blowfish Implementation on FPGA .....	163
4.3.2	P <sup>2</sup> M Blowfish with Internal Memory .....	165
4.3.3	P <sup>2</sup> M Blowfish with Communication Module .....	166
4.3.4	P <sup>2</sup> M Blowfish with BER.....	168
4.3.5	P <sup>2</sup> M Blowfish with Communication and RF Modules .....	169
4.3.6	WPAN Verification .....	171
4.4	Experimental of Testing and Measurement .....	173
4.4.1	Hardware Utilization .....	176
4.4.2	Throughput .....	177
4.4.3	Power Consumption.....	178
4.4.4	BER.....	179
4.4.5	Signal Strength.....	182
4.4.6	Communication Range .....	183

4.5	Summary .....	184
<b>CHAPTER 5 RESULTS AND DISCUSSION .....</b>		<b>186</b>
5.1	Introduction .....	186
5.2	Simulation Results .....	187
5.2.1	The Proposed P <sup>2</sup> M AES-128 .....	188
5.2.2	The Proposed P <sup>2</sup> M Blowfish .....	195
5.3	Implementation Results .....	202
5.3.1	The Proposed P <sup>2</sup> M AES-128 .....	203
	5.3.1(a) Hardware Utilization .....	203
	5.3.1(b) Throughput .....	204
	5.3.1(c) Power Consumption .....	208
5.3.2	The Proposed P <sup>2</sup> M Blowfish .....	210
	5.3.2(a) Hardware Utilization .....	210
	5.3.2(b) Throughput .....	213
	5.3.2(c) Power Consumption .....	216
5.4	Real-Time Measurements .....	218
5.4.1	BER .....	220
5.4.2	Signal Strength .....	227
5.4.3	Communication Range .....	232
5.5	Analysis on Performance Comparison .....	233
5.5.1	Comparison of the Proposed P <sup>2</sup> M AES-128 with the Previous Works on FPGA .....	235
5.5.2	Comparison of the Proposed P <sup>2</sup> M Blowfish with the Previous Works on FPGA .....	245
5.5.3	Comparison between the Proposed P <sup>2</sup> M AES-128 and P <sup>2</sup> M Blowfish .....	250
	5.5.3(a) Hardware Utilization .....	253



5.5.3(b) Throughput.....	255
5.5.3(c) Power Consumption.....	256
5.5.4 Comparison of the Proposed P <sup>2</sup> M Blowfish with the Previous Works through Radio Systems.....	257
5.6 Summary.....	263
<b>CHAPTER 6 CONCLUSION AND FUTURE WORKS.....</b>	<b>266</b>
6.1 Introduction.....	266
6.2 Conclusion.....	266
6.3 Future Works.....	274
<b>REFERENCES ..</b>	<b>275</b>
<b>APPENDICES</b>	
Appendix A: The Port Functions and Description for RAMB18E1 and RAMB36E1 based on Xilinx (2016)	
Appendix B: The XM105 Features based on Xilinx (2011)	
Appendix C: The Pin Signals for the XBee-PRO Zigbee Module based on Digi International (2015)	
Appendix D: The Design Methodology of Proposed <i>SubBytes.v</i>	
Appendix E: The Design Methodology of Proposed <i>ShiftRows.v</i>	
Appendix F: The Design Methodology of Proposed <i>MixColumns.v</i>	
Appendix G: The Design Methodology of Proposed <i>AddRoundKey.v</i>	
Appendix H: The Design Methodology of Proposed <i>key_expander.v</i>	
Appendix I: Part of the IO Pins of ZYNQ-7000 XC7Z020-CLG484	
Appendix J: The <i>S-Box</i> and Inverse <i>S-Box</i> in AES-128	
Appendix K: The Design Methodology of Proposed <i>BlowfishRound.v</i>	
Appendix L: The Design Methodology of Proposed <i>BlowfishPiROM.v</i>	
Appendix M: The Design Methodology of Proposed <i>BlowfishPArray.v</i>	

- Appendix N: The Design Methodology of Proposed *BlowfishCipher.v*
- Appendix O: The  $\Pi$  Values for four *S-Boxes* of Proposed Blowfish in *BlowfishPiROM.v*
- Appendix P: The Implementation Process on Zynq-7000 SoC through Vivado Xilinx Software
- Appendix Q: Data Samples of the Proposed P<sup>2</sup>M AES-128 Design during Encryption and Decryption Modes
- Appendix R: Test Vectors for the Proposed P<sup>2</sup>M Blowfish Design during Encryption and Decryption Modes
- Appendix S: Performance Comparison of the Improved Power-Throughput AES and Blowfish Algorithms on FPGA
- Appendix T: The Schematic Diagram of the Proposed P<sup>2</sup>M AES-128 for Each Round in Xilinx Vivado
- Appendix U: Theoretical Relation between the Sequential, Pipelined and Parallel Techniques with the Throughput and Power Consumption
- Appendix V: The Power Report from Xilinx Vivado Power Tool
- Appendix W: The Schematic Diagram of the Proposed P<sup>2</sup>M Blowfish for Each Core in Xilinx Vivado
- Appendix X: Real-Time Measurement Setup for Antenna Received Power Analysis at the P<sup>2</sup>M Blowfish Radio Receiver by using Anritsu Spectrum Analyzer
- Appendix Y: The Measurement Data of BER, Antenna Received Power (dBm), SNR (dB) and Communication Range (m)

## **LIST OF PUBLICATIONS**

## LIST OF TABLES

		<b>Page</b>
Table 2.1	Performance comparison between AES and Blowfish schemes based on previous research works .....	25
Table 2.2	The hexadecimal digits of $\pi$ for <i>P-Arrays</i> (Schneier, 1993).....	34
Table 2.3	Performance comparison on AES designs from the previous research works .....	49
Table 2.4	Performance comparison on Blowfish designs from the previous research works .....	59
Table 2.5	Specification of Zynq-7000 XC7Z020-CLG484-1 SoC (Xilinx, 2015) .....	65
Table 2.6	Specifications of the XBee-PRO ZigBee module (Digi International, 2015).....	67
Table 2.7	The existing FPGA-based radio systems .....	73
Table 3.1	Conventional AES designs and proposed P <sup>2</sup> M AES-128 design .....	86
Table 3.2	IO pins functional description of the <i>test_AES128.v</i> .....	89
Table 3.3	Conventional Blowfish designs and the proposed P <sup>2</sup> M Blowfish design.....	91
Table 3.4	The 128-bit block and key data of the proposed P <sup>2</sup> M AES-128 in hexadecimal value with the expected 128-bit output data.....	109
Table 3.5	IO pins functional description of the <i>system.vhdl</i> .....	113
Table 3.6	Number of probes and its function .....	132
Table 4.1	Hardware specification of the proposed P <sup>2</sup> M Blowfish radio system .....	151
Table 4.2	Existing FPGA-based radio systems and the proposed work .....	162
Table 4.3	Existing Blowfish radio systems and the proposed work.....	163
Table 5.1	The 128-bit block and key data of the proposed P <sup>2</sup> M AES-128	

	in hexadecimal value during encryption and decryption modes.....	191
Table 5.2	The 128-bit block data of P <sup>2</sup> M Blowfish in hexadecimal value during encryption and decryption modes.....	199
Table 5.3	FPGA hardware requirement for the proposed P <sup>2</sup> M AES-128 .....	204
Table 5.4	Performance data of the proposed P <sup>2</sup> M AES-128 .....	206
Table 5.5	The value of $t_{hd}$ and $t_{su}$ at different clock frequency.....	208
Table 5.6	Power consumption of the proposed AES-128 design .....	209
Table 5.7	FPGA hardware requirement for the proposed research work .....	212
Table 5.8	Performance data of the proposed P <sup>2</sup> M Blowfish .....	214
Table 5.9	The value of $t_{hd}$ and $t_{su}$ at different clock frequency .....	215
Table 5.10	The power consumption of the proposed P <sup>2</sup> M Blowfish radio system.....	216
Table 5.11	Hexadecimal value of encrypted data in <i>mem_enc</i> .....	224
Table 5.12	Summary of performance analysis between the existing AES from previous research works and the proposed P <sup>2</sup> M AES-128.....	242
Table 5.13	Summary of performance analysis between the existing Blowfish from previous research works and the proposed P <sup>2</sup> M Blowfish.....	251
Table 5.14	Implementation of Blowfish schemes on different radio systems for real-time validation at 2.4 GHz ZigBee standard.....	262
Table 5.15	The performance comparison between the proposed P <sup>2</sup> M Blowfish and reference designs including the proposed P <sup>2</sup> M AES-128.....	265
Table 6.1	The gap between the proposed P <sup>2</sup> M AES-128 and P <sup>2</sup> M Blowfish with the related research works.....	271

## LIST OF FIGURES

		<b>Page</b>
Figure 1.1	50 billion connected IoT devices in 2020 (CISCO, 2019) .....	2
Figure 1.2	Overview of different IoT wireless communication standards at three horizontal layers (Links, 2015).....	3
Figure 1.3	The future of the connected devices for the IoT (Tudosoiu, 2014; Rodriguez and Stamatati, 2018) .....	4
Figure 1.4	Evolution of communication technology.....	5
Figure 1.5	Research contributions of the proposed research work .....	14
Figure 2.1	Overview of cryptography types (Kessler, 2010).....	20
Figure 2.2	The structure of AES-128: (a)Encryption Round; (b)Decryption Round (NIST, 2001) .....	27
Figure 2.3	The <i>SubBytes</i> process using <i>S-box</i> in hexadecimal format (NIST, 2001).....	27
Figure 2.4	The <i>ShiftRows</i> process (NIST, 2001).....	28
Figure 2.5	<i>MixColumns</i> operates on the <i>State</i> column-by-column (NIST, 2001).....	28
Figure 2.6	<i>AddRoundKey</i> XOR of each column of the <i>State</i> using word from the key schedule (NIST, 2001) .....	29
Figure 2.7	The <i>InvShiftRows</i> cyclically shifts the last three rows of the <i>State</i> (NIST, 2001).....	31
Figure 2.8	The inverse <i>S-box</i> used in the <i>InvSubBytes</i> transformation (NIST, 2001).....	31
Figure 2.9	The operation of <i>InvMixColumns</i> (NIST, 2001) .....	32
Figure 2.10	Blowfish scheme with F function for encryption and decryption modes (Schneier, 1993) .....	33

Figure 2.11	The pipelined AES-128 for encryption process (Yoo <i>et al.</i> , 2005)...	39
Figure 2.12	Circuit architecture of sequential, parallel and pipelined key expansions (Fan and Hwang, 2008).....	40
Figure 2.13	The architecture of AES through sequential and pipelined techniques (Prasanthi and Reddy, 2012).....	41
Figure 2.14	The operation of key expansion unit (Adib and Raissouni, 2012)....	42
Figure 2.15	The masked AES with pipelined technique: (a)Masked AES; (b)Masked <i>S-box</i> (Wang and Ha, 2013).....	43
Figure 2.16	<i>MixColumn</i> operation by using registers (Neenu and Bonifus, 2016).....	45
Figure 2.17	Implementation of <i>AddRoundKey</i> and key expansion unit (Nuray <i>et al.</i> , 2017).....	46
Figure 2.18	Division of one stage of F function into 5-stage pipelined technique (Sudarshan <i>et al.</i> , 2005).....	52
Figure 2.19	Partial pipelined in the F function (Karthigaikumar and Baskaran, 2010).....	53
Figure 2.20	The architecture of pipelined Blowfish (Oukili and Bri, 2016).....	55
Figure 2.21	The F function with parallel technique (Suresh and Neema, 2016)....	55
Figure 2.22	The block diagram of Blowfish design (Bansal and Jassal, 2016)....	56
Figure 2.23	The pipelined and parallel techniques in the Blowfish architecture (Chatterjee and Chakraborty, 2017).....	57
Figure 2.24	Structure of the PL (Xilinx, 2015).....	62
Figure 2.25	Composition of the CLB (Xilinx, 2015).....	63
Figure 2.26	Block diagram of BRAM: (a)RAMB18E1; (b)RAMB36E1 (Xilinx, 2016) .....	64
Figure 2.27	The FMC XM105 card as communication module (Xilinx, 2011).....	66
Figure 2.28	Block diagram of XBee-PRO ZigBee module (Digi International, 2015).....	67

Figure 3.1	Conceptual framework of the proposed P <sup>2</sup> M AES-128 and P <sup>2</sup> M Blowfish designs.....	79
Figure 3.2	Structure of software-based P <sup>2</sup> M AES-128 and P <sup>2</sup> M Blowfish architectures.....	80
Figure 3.3	Structure of software-based P <sup>2</sup> M Blowfish FPGA-based radio system.....	81
Figure 3.4	Software-based work flow: (a)P <sup>2</sup> M AES-128 and P <sup>2</sup> M Blowfish architectures; (b)P <sup>2</sup> M Blowfish FPGA-based radio system.....	84
Figure 3.5	Design methodology of the proposed AES-128 based on standard process provided by NIST (2001).....	88
Figure 3.6	The top module <i>test_AES128.v</i> .....	89
Figure 3.7	The proposed design methodology of <i>test_AES128.v</i> .....	90
Figure 3.8	The proposed design methodology of <i>subencrypt_key.v</i> .....	92
Figure 3.9	The ASM for proposed <i>sub_encrypt.v</i> .....	94
Figure 3.10	The ASM for proposed <i>SubBytes.v</i> .....	95
Figure 3.11	Part of the transformation process in proposed <i>SubBytes.v</i> .....	95
Figure 3.12	The ASM for proposed <i>ShiftRows.v</i> .....	96
Figure 3.13	Part of Verilog code in the proposed <i>ShiftRows.v</i> .....	97
Figure 3.14	The ASM for proposed <i>MixColumns.v</i> .....	98
Figure 3.15	The ASM for proposed <i>AddRoundKey.v</i> .....	99
Figure 3.16	The ASM for proposed <i>key_expander.v</i> .....	100
Figure 3.17	Part of <i>Layout.xdc</i> .....	101
Figure 3.18	Part of <i>Timing.xdc</i> .....	101
Figure 3.19	Parallel process in the proposed P <sup>2</sup> M AES-128 design.....	103
Figure 3.20	The pipelined process in the architecture of proposed P <sup>2</sup> M AES-128 design.....	105
Figure 3.21	Internal pipelining in single round of the proposed P <sup>2</sup> M AES-128 design.....	106

Figure 3.22	Structure of memory-based technique for byte-by-byte data process in the <i>S-box</i> and inverse <i>S-box</i> .....	108
Figure 3.23	Design methodology of the proposed P <sup>2</sup> M Blowfish architecture....	111
Figure 3.24	The proposed top module of <i>system.vhdl</i> .....	113
Figure 3.25	The proposed design methodology of <i>system.vhdl</i> .....	114
Figure 3.26	The proposed design methodology of <i>Blowfish_core.v</i> .....	117
Figure 3.27	Part of Verilog code for the proposed <i>Blowfish_core.v</i> .....	119
Figure 3.28	The proposed design methodology of <i>DualReadPortRAM.v</i> .....	120
Figure 3.29	Part of Verilog code in the proposed <i>DualReadPortRAM.v</i> .....	120
Figure 3.30	Part of Verilog code in the proposed <i>BlowfishRound.v</i> .....	121
Figure 3.31	The ASM for proposed <i>BlowfishRound.v</i> .....	122
Figure 3.32	The proposed design methodology of <i>MiniFIFO.v</i> .....	123
Figure 3.33	The input data of proposed Blowfish is sent to the output port via FIFO approach.....	123
Figure 3.34	The ASM for proposed <i>BlowfishSBox.v</i> .....	124
Figure 3.35	Four 32-bit <i>S-boxes</i> with 256 entries each are stored in BRAM of the proposed Blowfish.....	125
Figure 3.36	The address and 32-bit $\pi$ values for <i>S-boxes</i> of the proposed Blowfish.....	126
Figure 3.37	The ASM for proposed <i>BlowfishPiROM.v</i> .....	126
Figure 3.38	The ASM for proposed <i>BlowfishPArray.v</i> .....	127
Figure 3.39	Part of Verilog code in the proposed <i>BlowfishPArray.v</i> .....	128
Figure 3.40	The ASM for proposed <i>BlowfishCipher.v</i> .....	129
Figure 3.41	Part of Verilog code in the proposed <i>BlowfishCipher.v</i> .....	130
Figure 3.42	Setting the pin numbers of FPGA device for input ports of the proposed Blowfish in <i>layout.xdc</i> .....	130
Figure 3.43	Part of timing constraint in the proposed <i>timing.xdc</i> for ZC702 platform.....	131



Figure 3.44	Setting the clock frequency in <i>ila.xdc</i> of the proposed Blowfish.....	131
Figure 3.45	The proposed design methodology of <i>UART.vhdl</i> .....	133
Figure 3.46	Part of RTL code in the proposed <i>UART.vhdl</i> .....	134
Figure 3.47	The proposed design methodology of <i>FrequencyDivider.vhdl</i> .....	135
Figure 3.48	Clock frequency for ZC702 and ZedBoard platforms of the proposed Blowfish.....	136
Figure 3.49	The implementation of parallel technique in the proposed P <sup>2</sup> M Blowfish design.....	137
Figure 3.50	The schematic diagram of parallel blocks in the proposed P <sup>2</sup> M Blowfish design.....	138
Figure 3.51	The parallel technique in F function of the proposed Blowfish .....	139
Figure 3.52	The parallel and pipelining paths in the proposed P <sup>2</sup> M Blowfish architecture.....	141
Figure 3.53	The proposed pipelining path of F function.....	142
Figure 3.54	The proposed pipelining path in the architecture of key expansion unit for generating 18 subkeys.....	142
Figure 3.55	The internal pipelined process in the architecture of P <sup>2</sup> M Blowfish radio system.....	144
Figure 3.56	The pipelined process for UART data counter.....	144
Figure 3.57	Structure of different techniques for <i>S-boxes</i> in a Blowfish block: (a) The proposed memory-based technique in this work; (b) The registers for data storage as conventional design technique in previous works .....	147
Figure 4.1	The proposed P <sup>2</sup> M Blowfish FPGA-based radio system for secured IoT application.....	152
Figure 4.2	Hardware-based work flow for the proposed P <sup>2</sup> M Blowfish radio system.....	155
Figure 4.3	Schematic diagram of the proposed FPGA-based radio system.....	162

Figure 4.4	Design methodology of the proposed P <sup>2</sup> M Blowfish radio system.....	164
Figure 4.5	Implementation setup of the proposed P <sup>2</sup> M Blowfish design through Zynq-7000 FPGA.....	165
Figure 4.6	The proposed block diagram of memories for encrypted and decrypted data.....	166
Figure 4.7	Schematic diagram of UART interface between the Blowfish transmitter and Blowfish receiver.....	167
Figure 4.8	Implementation setup of communication module with UART interface.....	168
Figure 4.9	Schematic diagram of BER flow at the Blowfish receiver.....	169
Figure 4.10	Schematic diagram of the proposed P <sup>2</sup> M Blowfish design with communication and ZigBee RF modules.....	170
Figure 4.11	Implementation setup of the proposed P <sup>2</sup> M Blowfish FPGA-based radio system for real-time transmission.....	172
Figure 4.12	The proposed methodology of P2P communication flow for the P <sup>2</sup> M Blowfish FPGA-based radio system as transmitter and receiver within WPAN environment.....	174
Figure 4.13	The Zynq-7000 XC7Z020-CLG484-1 is employed in both ZedBoard and ZC702 platforms.....	176
Figure 4.14	SNR for wireless communication (Cisco System, 2017).....	181
Figure 4.15	The MDS and noise level (Wolff, 2017).....	182
Figure 4.16	The communication range test setup for NLOS indoor environment at laboratories of School of Electrical and Electronic Engineering.....	184
Figure 5.1	Simulation waveform of the proposed P <sup>2</sup> M AES-128 during encryption and decryption modes: (a) The 128-bit data and key at the input ports; (b)The 128-bit data and key at the output ports...	189
Figure 5.2	Output data of the proposed P <sup>2</sup> M AES-128 during encryption and decryption modes: (a) The 128-bit encrypted and decrypted	

	data; (b) The latency during encryption mode; (c) The latency during decryption mode.....	192
Figure 5.3	Data during encryption mode: (a)Input data; (b)Output data.....	196
Figure 5.4	Data during decryption mode: (a)Input data; (b)Output data.....	198
Figure 5.5	The length of latency: (a)Encryption mode; (b)Decryption mode...	200
Figure 5.6	Definition of the hold time, $t_{hd}$ and setup time, $t_{su}$ (EDN Network, 2012).....	207
Figure 5.7	The difference of FPGA hardware requirement between the P <sup>2</sup> M Blowfish core and P <sup>2</sup> M Blowfish radio system.....	213
Figure 5.8	Setting the port parameters of ZigBee RF module via XCTU.....	221
Figure 5.9	The centre frequency for the ZigBee RF module via XCTU.....	221
Figure 5.10	The BER analysis via ChipScope ILA and the encrypted data received from the transmitter via <i>minicom</i> .....	222
Figure 5.11	The encrypted data stored in the memory <i>mem_enc</i> before transmission process.....	223
Figure 5.12	The transmitted and received signals via oscilloscope at 0% BER...	224
Figure 5.13	The transmitted and received signals via ChipScope ILA and <i>minicom</i> at BER of $1.56 \times 10^{-3}$ .....	225
Figure 5.14	Port of the transmitted and received signals via oscilloscope at BER of $1.56 \times 10^{-3}$ .....	226
Figure 5.15	BER vs Communication Range (m).....	227
Figure 5.16	Measurement setup for antenna received power analysis at the P <sup>2</sup> M Blowfish radio receiver by using the Anritsu Spectrum Analyzer.....	228
Figure 5.17	BER vs Received Power (dBm).....	229
Figure 5.18	The strongest antenna received power of -24.98 dBm with 0% BER.....	229
Figure 5.19	Noise floor at 2.405 GHz.....	230

Figure 5.20	BER vs SNR (dB): (a)Theory; (b)The proposed design.....	231
Figure 5.21	Received power (dBm) vs Communcation Range (m).....	233
Figure 5.22	Comparison of the slices used between the proposed P <sup>2</sup> M AES-128 and previous research works.....	238
Figure 5.23	Comparison of the throughput between the proposed P <sup>2</sup> M AES-128 and previous research works .....	239
Figure 5.24	Comparison of the power consumption between the proposed P <sup>2</sup> M AES-128 and previous research works.....	241
Figure 5.25	Comparison of slices requirement between the proposed P <sup>2</sup> M Blowfish core and reference works.....	247
Figure 5.26	Comparison of throughput between the proposed P <sup>2</sup> M Blowfish core and reference works.....	248
Figure 5.27	Comparison of power consumption between the proposed P <sup>2</sup> M Blowfish and reference works.....	249
Figure 5.28	Hardware utilization between the proposed P <sup>2</sup> M AES-128 and P <sup>2</sup> M Blowfish core.....	254
Figure 5.29	Throughput vs power consumption between the proposed P <sup>2</sup> M Blowfish and P <sup>2</sup> M AES-128.....	257

## 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	Feistel
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 <sup>2</sup> M	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