AES-CCM DESIGN FOR SECURITY OF BTLE CONTROLLER

HIDAYARNI HAMZAH

A thesis submitted in
fulfilment of the requirement for the award of the
Degree of Master of Electrical Engineering

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

NOVEMBER 2022

To my beloved parents and husband, thank you.

ACKNOWLEDGEMENT

First and foremost Alhamdulillah, praises and thanks to the almighty Allah S.W.T for His blessing to complete this research.

I would like to express my special thanks of gratitude to my lovely supervisor Dr. Nabihah @ Nornabihah binti Ahmad as well as my co-supervisor Dr. Mohamad Hairol Bin Jabbar for their supportive attitude, share knowledge and advise me along this Master research. A lot of difficulties in this research journey but continuous direction from Dr. Nabihah really help me to finish this thesis.

A special thanks to my UTM's colleagues Dr. Hadi, Atiqah, Aini and Ung Shin Ji for their kindness and always share their knowledge with me regarding Xilinx Vivado as well as writing HDL Verilog. Thanks also to USM CEDEC team for support and giving me the opportunity to involve in this AES in BTLE research.

I would like to dedicate my dissertation to my precious family for their fully support and always encourage me to fulfill this Master by research.

ABSTRACT

Advanced Encryption Standard in Counter with Cipher Block Chaining-Message Authentication Code (AES–CCM) functions as a security system in Bluetooth Low Energy (BTLE) Controller. There is a link layer security in the Bluetooth system that provides encryption and authentication using CCM mode. The link layer in BTLE architecture match to integrate with CCM mode as CCM requires a new temporal key whenever encryption is initiated. The proposed design was implemented using FPGA Xilinx Vivado Virtex-7 XC7VX85TFFQ1157-1 written in HDL Verilog language. The AES is a symmetric block cypher that can process data blocks of 128-bit and it can utilize cypher keys of 128, 192 and 256-bit. All AES processing in CCM encryption uses AES with a 128-bit key and a 128-bit block size. As it was intended to be used in BTLE Controller, the design of AES–CCM was developed with high throughput to achieve high-speed performance. Throughput is the rate of the output data is processed. As the size of BTLE is tiny so the area of the design should be as low as possible. In this FPGA design the area measures in term of number of slices. Slices is the number of the logics in the design, each slice contains of two 4-input functions, carry logic, arithmetic logic, storage logic and function multiplexer. The method used to achieve the high throughput is sharing data path for SubBytes, MixColumn and AddRoundKey design. Another approached is pipelined in SubBytes and MixColumn. These methods generated AES with 6.4 Gbps throughput with 2740 number of slices. AES-CCM is designed in cascaded for both Counter (CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) part with limited to three blocks input of CTR and CBC-MAC in encryption with throughput of 2.133 Gbps and area of 320 number of slices. The simulations were verified at a frequency of 16.67 MHz. The results were compared with those from previous works in order to obtain the best result. This proposed design is suitable for BTLE Controller.

ABSTRAK

Piawaian Penyulitan maju dalam Kaunter dengan Kod Pengesahan Mesej Berantai Blok Cipher (AES–CCM) berfungsi sebagai sistem keselamatan dalam Pengawal Tenaga Rendah *Bluetooth* (BTLE*)*. Terdapat sistem keselamatan di dalam lapisan pautan *Bluetooth* yang menyediakan penyulitan dan pengesahan menggunakan mod CCM. Lapisan pautan dalam seni bina BTLE sepadan untuk disepadukan dengan mod CCM kerana CCM memerlukan kunci sementara baharu apabila penyulitan dimulakan. Projek ini telah dilaksanakan menggunakan FPGA Xilinx Vivado Virtex-7 XC7VX85TFFQ1157-1 yang ditulis dalam bahasa HDL Verilog. AES telah direka menggunakan blok cipher simetri yang boleh memproses blok data 128-bit dan boleh menggunakan kekunci cipher 128, 192 dan 256-bit. Semua pemprosesan AES dalam CCM menggunakan kekunci 128-bit dan saiz blok 128-bit. Memandangkan ia bertujuan untuk digunakan dalam Pengawal BTLE, ia telah dibangunkan dengan daya pemprosesan yang tinggi untuk mencapai prestasi berkelajuan tinggi. Oleh kerana saiz BTLE adalah kecil, kawasan reka bentuk hendaklah serendah mungkin. Dalam reka bentuk FPGA, ukuran keluasan kawasan diukur dalam bilangan kepingan iaitu bilangan logik dalam reka bentuk. Setiap kepingan mengandungi dua fungsi 4-masukan, logik pembawa, logik aritmetik, logik storan dan fungsi pemultipleks. Kaedah yang digunakan untuk mencapai daya pemprosesan yang tinggi ialah berkongsi laluan data untuk reka bentuk *SubBytes*, *MixColumn* dan *AddRoundKey*. Teknik seterusnya adalah talian paip bagi rekaan *SubBytes* dan *MixColumn*. Kaedah ini menjana AES dengan daya pemprosesan 6.4 Gbps dan keluasan sebanyak 2740 kepingan. AES-CCM ini direka secara melata untuk bahagian Pembilang (CTR) dan Kod Pengesahan Mesej Berantai Blok Cipher (CBC-MAC) dengan masukan input terhad kepada tiga blok CTR dan CBC-MAC dengan daya pemprosesan 2.133 Gbps dan keluasan sebanyak 320 kepingan berfrekuensi 16.67 MHz. Perbandingan dengan rekaan terdahulu telah dibuat bagi mencapai keputusan keluaran yang terbaik. Reka bentuk AES-CCM ini sesuai digunakan bagi aplikasi Pengawal BTLE.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAD	–	Additional Authentication Data
AES	–	Advanced Encryption Standard
AES-CCM	–	Advanced Encryption Standard Counter with Cipher block chaining-Message
ASIC	–	Application-Specific Integrated Circuit
BR/EDR	–	Basic Rate/ Enhanced Data Rate
BRAMs		Broadcast Recognition Access Method
BTLE	–	Bluetooth Low Energy
CAD	–	CAD Computer Aided Design
CBC	–	Cipher Block Chaining Mode
CBC-MAC	–	Cipher Block Chaining Message Authentication Code
CCM	–	Counter with Cipher Block Chaining - Message Authentication Code
CFB	–	Cipher Feedback Mode
CMOS	–	Complementary Metal Oxide Semiconductor
CTR	–	Counter Mode
DES	–	Data Encryption Standard
ECB	–	Electronic Code Book Mode
FIPS	–	Federal International Processing Standard
FPGA	–	Field Programmable Gate Array
FSM	–	Finite State Machine
GUI	–	Graphical User Interface
HDL	–	Hardware Description Languages
IETF	–	Internet Engineering Task Force
IoT	–	Internet of Things
ISM	–	Industrial, Scientific and Medical

IV	–	Initialization Vector
LUT	–	Look Up Table
LLC	–	Link Layer Construct
MAC	–	Media Access Control
MIC	–	Message Integrity Code
MPDU	–	Medium-Access-Control Protocol Data Unit
NRE	–	Non Recurring Engineering
NIST	–	National Institute of Standards and Technology
OFB	–	Output Feedback Mode
PDU	–	Protocol data Unit
P.E	–	Payload Extraction
PN	–	Packet Number
RC	–	Re-Construction
RFC	–	Request for Comments
RFID	–	Radio Frequency Identification
RTL	–	Register Transfer Level
S-box	–	Substitution Table
SoC	–	System on Chip
TK	–	Temporal Key
VHDL	–	Very High Speed Integrated Circuit Hardware Description
WBAN	–	Wireless Body Area Network
WPAN	–	Wireless Personal Area Network
XOR	–	Exclusive-OR

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background

Bluetooth Low Energy (BTLE) is an element of Bluetooth version 4.0. The Classic Bluetooth application was designed to connect separate worlds of computing and communications, such as linking cell phones to laptops. Then, its application was broadened to link cell phones to headsets. As the technology matures, the use of Bluetooth has become a part of human lives – from streaming stereo music to wireless printing and file transfering, as well as downloading phone book from phones to cars. Even though BTLE functions are similar to Bluetooth standard protocols, it is designed for very low-power applications that can operate using a coin-cell battery for several months to years. For the band radio frequencies, BTLE uses the same 2.4 GHz Industrial, Scientific and Medical (ISM) as the Classic Bluetooth. It allows dual-mode devices to share a single radio antenna. However, BTLE uses a much simpler modulation system.

As compared to the Classic Bluetooth, BTLE offers new opportunities in designing and developing Bluetooth applications, which include several key advantages such as ultra-low peak, average and idle power consumption modes, low-power requirements, compact size, low cost, multi-vendor interoperability, compatibility with a large base of mobile phones, computers, tablets and communication range [1]. Advanced Encryption Standard (AES) is required for security services in many applications, such as Wireless Network, Radio Frequency Identification (RFID) tags and many more. It was selected as the United States (US) standard for encryption of unclassified information in 2001. After the announcement

of AES, it has replaced the Data Encryption Standard (DES), which was the US standard since 1977. AES is the currently employed specification for encrypting electronic data from the United States National Institute of Standards and Technology (NIST) [2].

Bluetooth wireless technology provides peer-to-peer communications over short distances. To ensure usage protection and information confidentiality, the system provides security measures at both the application and the link layers. These measures are designed to be appropriate for a peer environment. This means that in each device, the authentication and encryption routines are implemented in the same way.

There is a significant difference from a cryptographic point of view between Numeric Comparison and the PIN entry model used by Bluetooth Core Specification and the earlier versions. In a Numeric Comparison association model, the six-digit number is a structure of the security algorithm, as compared to the Bluetooth security model, in which the number is used as an input. Learning the displayed number is unbenefited in decrypting the encoded data exchanged between two devices [3].

BTLE requires Advanced Encryption Standard (AES) as the default security service in its application. Encryption in BTLE System utilizes Advanced Encryption Standard–Counter with Cipher block chaining–Message Authentication Code (AES–CCM) cryptography. Similar to Basic Rate/Enhanced Data Rate (BR/EDR), the encryption in BTLE System uses cryptography of Counter with Cipher Block Chaining–Message Authentication Code (CCM). Another term for CCM is Cipher Block Chaining Message Authentication Code (CBC–MAC) [3].

In the IEEE 802.11i-2004 standard, the Wired Equivalent Privacy (WEP) in the original IEEE 802.11 standard is replaced with the AES–CCM. In general, two different cryptographic algorithms are used to provide privacy and authentication. The AES–CCM algorithm, on the other hand, provides these two security services with the same algorithm by using the AES block cypher and the same key.

CTR with CBC–MAC (CCM) mode utilizes the Counter (CTR) mode and CBC–MAC mode. Privacy is provided by this algorithm in CTR mode, which requires a value that ensures uniqueness, whereas the authentication is performed in CBC–MAC mode. An additional capability of CBC–MAC mode is in its integrity method, which ensures that every cypher block depends on every preceding part of the plain text, where ciphering two identical blocks results in different cypher blocks. The use of cryptographic algorithms in demanding applications that transmit huge amounts of data is essential. As AES–CCM is used in BTLE Controller, its design should be high-throughput in order to achieve high-speed performance.

FPGAs are reprogrammable platforms, which are widely used in various designs and diverse target applications. They are progressively used as final product platforms for low-volume production. In an FPGA-based system design, there is no manufacturing turnaround time. Thus, the design can be tested and evaluated quickly, allowing shorter development cycles, shorter time to market and lower Non-Recurring Engineering (NRE) costs. NRE refers to the one-time cost to research, design, develop and test a new product or product enhancement [4].

As for budgeting new product, a planned NRE must be considered to determine if the new product would be profitable or not. In addition, there is no mask making as compared to Application-Specific Integrated Circuit (ASIC). Regarding the Computer-Aided Design (CAD) tools, the FPGA vendors provide tools that help designers to take the steps involved in the FPGA design flow. FPGA can be bought off the shelf and reconfigured by designers themselves. Regarding the FPGA design flow, it is usually a Graphical User Interface (GUI)-based tool [5].

1.2 Problem statement

The design needs higher throughput due to higher speed of output data is produced. Throughput is the rate of the output data is processed. BTLE is a small type controller as its function for small electronic devices such as mobile phone and many more. As the size of BTLE is small so the area of the design should be as low as possible. In this Field Gate Programmable Array (FPGA) design the area measures

in term of number of slices. Slices is the number of the logics in the design, each slice contains of two 4-input functions, carry logic, arithmetic logic, storage logic and function multiplexer. AES–CCM functions as a security system in BTLE Controller. In the BTLE System, a link-layer security provides encryption and authentication in CCM mode as this mode shall be implemented in accordance with the algorithm as defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 3610 [5], in conjunction with the AES-128 block cypher as defined in NIST Publication Federal International Processing Standard (FIPS) [6]. The link-layer match to integrate with CCM mode as CCM requires a new temporal key whenever encryption is started, which is not available in other AES modes. CCM also requires a unique nonce value for each Data Channel of Protocol Data Unit (PDU) protected by a given temporal key.

The problem with the existing AES–CCM is the previous design does not achieve high throughput and low area. Several AES–CCM optimization techniques have been explored for BTLE Controller with high throughput performance by using FPGA Xilinx Vivado and Verilog HDL language. This design aim to achieve greater than 2.06 Gbps throughput and less than 900 number of slices compare to previous work.

As more and more hacking and cybercrime are being reported all over the world, people are extremely concerned about their privacy. Sensitive data that falls into the wrong hands without user consent may lead to significant damages. For example, if devices with serious security flaws are deployed in the military, sensitive military information could be leaked to the enemies [1].

1.3 Objectives of the study

The objectives of this study are as follows:

1. To design and develop an AES–CCM for BTLE Controller with high throughput and low area using FPGA implementation.

2. To evaluate and verify the functionality of the AES-CCM.

1.4 Scopes of the Study

The scope of this research is limited to the architecture of AES–CCM based on the methods to achieve the objectives. BTLE Controller application requires a compact AES–CCM with high throughput and low area design suitable for the small design of BTLE Controller with high speed data transfer. In BTLE Controller the frequency range is 10 Mhz to 25 Mhz [3] as the link layer packet is using 16.67 Mhz, this AES-CCM is also design at similar frequency. This design is a hardware implementation with 20 ns latency in eight clock cycle per encrypted in AES design and 60 ns in twenty four clock cycle per encrypted in AES-CCM design.

The AES–CCM was designed with 128-bit data blocks and keys for both AES and CCM for encryption purposes. The CCM consists of Cipher Block Chaining Mode (CBC) and Counter Mode (CTR). These modes were designed using Vivado Design Suite by Xilinx for synthesis and analysis of Verilog Hardware Description Languages (HDL) designs.

The design needs higher throughput due to higher speed of output data is produced. The aim of throughput in greater than 2.06 Gbps with less than 900 number of slices. As the size of BTLE is tiny so the area of the design should be as low as possible. In this FPGA design the area measures in term of number of slices. Slices is the number of the logics in the design.

1.5 Thesis Organization

The thesis is organized into five chapters. In Chapter 2, the literature review explains the flow of encryption and decryption processes in the AES algorithm. The four main operations in AES are also described in detail. Moreover, the operation of CBC–MAC mode and current design of hardware implementation of AES and optimization method are compared with those of previous work.

In Chapter 3, the design to be implemented is proposed after reviewing related work in Chapter 2. The implementation of each method is explained in detail for each operation. The architecture is also presented in diagrams and formulas.

In Chapter 4, the results of this research are presented and discussed. Simulation and synthesis results of the implemented design that was proposed in Chapter 3 are presented. The performance and resource usage of the design are portrayed in tables and figures. In addition, the proposed design is compared with related work in terms of performance.

Chapter 5 concludes the research by summarizing the achieved objectives, the impact of this research and recommendations as well the challenges for future work to provide possible direction for future researcher.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

This chapter describes the AES–CCM algorithm, Encryption Standard AES mode operation, AES-CCM algorithm, design parameters and hardware implementation. FPGA implementation, AES design and AES-CCM design will also briefly elaborated.

2.2 AES algorithm

AES-Rijndael algorithm is a symmetric block cypher. It operates on a 128-bit block of data supports with 128-bit, 192-bit and 256-bit of key size. Different types of information require different key sizes. The design and strength of all key lengths of the AES algorithm are crucial to protect the information. The top-secret information requires the use of a 192 or 256-bit key in acquiring the highest level of protection.

A 128-bit data or key is divided into 16 bytes. Each byte is labelled with an ‘A’, namely A0 to A15, and is arranged in a 4×4 array called ‘state’, as presented in Figure 2.1 and Equation (2.1). Each byte in the state consists of an 8-bit data or key. For instant, A15 = 32 (hexadecimal) = 00110010 (binary) [2].

Figure 2.1: 128-bit data in a 4×4 state [6]

$A = \{A_{15}, A_{14}, A_{13}, A_{12}, A_{11}, A_{10}, A_9, A_8, A_7, A_6, A_5, A_4, A_3, A_2, A_1, A_0\}$ (2.1)

where A_{15} = The most significant byte of the 128-bit data

A_0 = The least significant byte of the 128-bit data

The AES data is processed iteratively based on a round function and is executed multiple times as AES is an iterative algorithm. The number of rounds depends on the key size, as shown in Table 2.1. The key sizes of 128, 192 and 256 bits require 10, 12 and 14 rounds of iteration respectively.

Table 2.1: AES key size and the number of rounds of iteration [6]

AES Key Size	Number of Rounds
128-bit	10
192-bit	12
256-bit	14

The process flow of AES-128 requires 10 rounds of operations per 128-bit data, as displayed in Figure 2.2. In each cypher round, there are four elementary operations, namely SubBytes, ShiftRows, MixColumns and AddRoundKeys, which are performed on a two-dimensional array of bytes called state matrix. SubBytes transform individual bytes of the state matrix into the values stored in a non-linear byte substitution table (S-box). ShiftRows cyclically shifts the last three rows of the state matrix, each by a different offset. MixColumns mixes all the 4 bytes of a column of the state matrix to form a new column. AddRoundKeys is simply the exclusive-OR (XOR) operation between the state matrix and RoundKey with 128-bit data. After 10 rounds of iterations of the four operations, a plaintext is converted to a

ciphertext, which could be decrypted through an inverse flow of Figure 2.2. In Figure 2.2, a module is seen parallel to the main encrypting operations. This module, which is called Key Expansion, is used to generate a series of RoundKeys from the SeedKey, which are then applied to the state matrix in the AddRoundKeys operation. The structure of AES encryption and decryption rounds are shown in Figure 2.3.

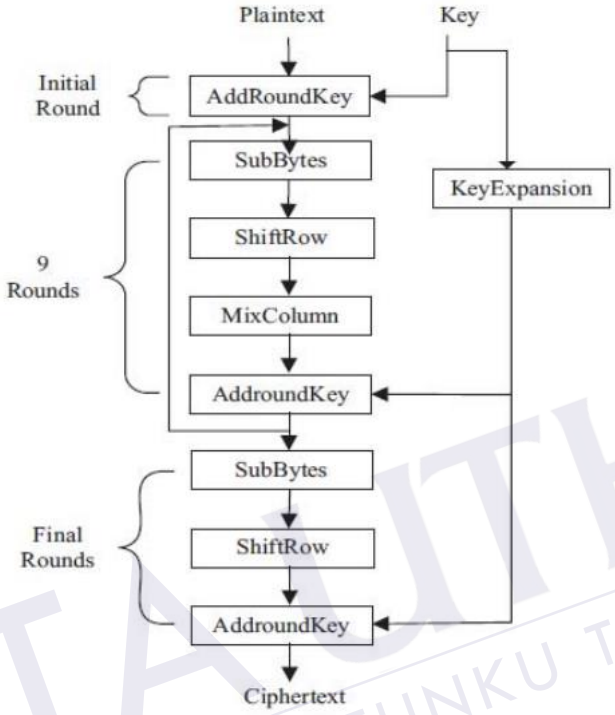

Figure 2.2: 128-bit AES encryption flow [7]

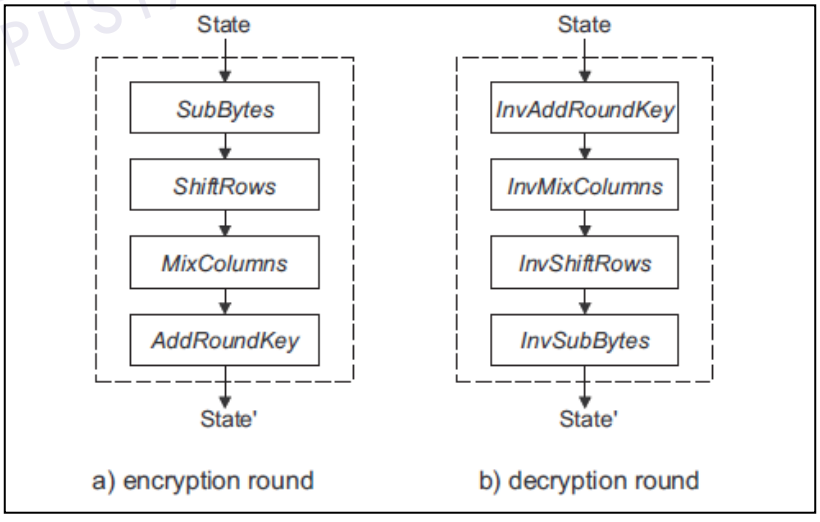

Figure 2.3: The structure of AES encryption and decryption rounds [8]

During the encryption of a 128-bit plain text, round key schedules and produces the 128-bit encrypted ciphertext, depending on the control signals. For example, in encryption mode, a 128-bit plaintext will be loaded when the load pin gives the logic '1'. After the data is loaded, reset will be made logic '1'. At the end of 10 rounds of internal blocks, SubBytes, ShiftRows and MixColumn processing, the done signal will be made logic '1' and the output register now holds the encrypted output, as shown in Figure 2.4.

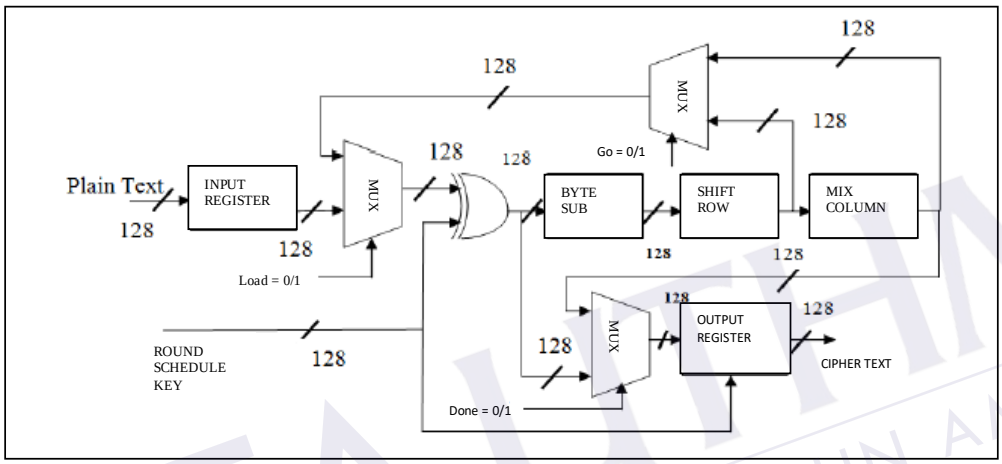

Figure 2.4: AES encryption block diagram [9]

The decryption block processes the 128-bit ciphertext and encrypts 128-bit key obtained from the final stage of the encryption. It reproduces the original data as the decrypted output of 128 bits along with the 128-bit key as in Figure 2.5.

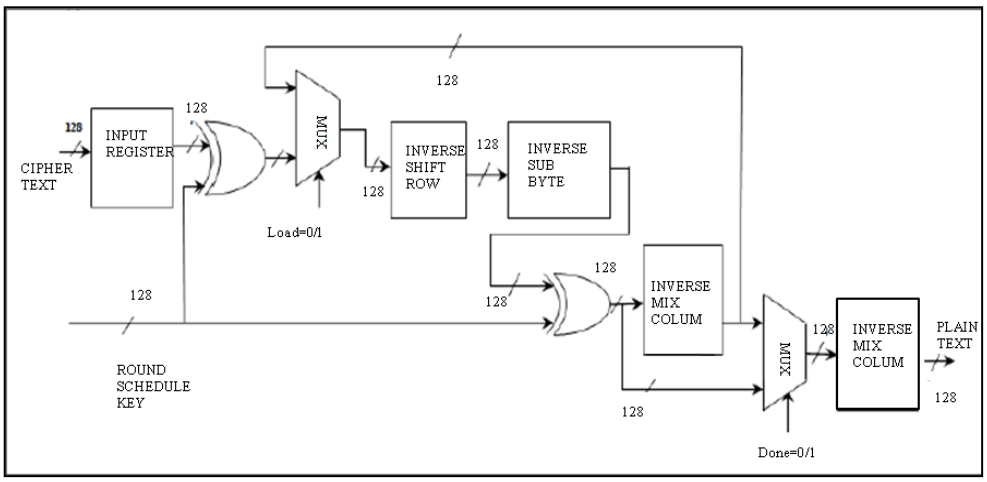

Figure 2.5: AES decryption block diagram [9]

REFERENCES

[1] Robin Heydon. “Bluetooth Low Energy, The Developer’s Handbook.” Crawfordsville, Indiana: Prentice hall. 2012.

[2] Tech Faq (2016). "AES (Rijndael).” Retrieved on 25 Sept. 16, from http://www.tech-faq.com/aes-rijndael.html.

[3] “Covered Core Package version 4.2: Bluetooth Specification Version 4.2”, [Vol 3, Part H] 3.6.2 Encryption Information,” Covered Core Package version: 4.2, Publication date: Dec 02 2014.

[4] G. Leelavathi, S. Prakasha, K. Shaila, K. R.Venugopal, L. M. Patnaik. " Design and Implementation of Advanced Encryption Algorithm with FPGA and ASIC." IJREAT International Journal of Research in Engineering & Advanced Technology. 2013, 1(3):1-8.

[5] IETF RFC3610 (2016). “RFC3610” Retrieved on Oct. 16, from (http://www.ietf.org/rfc/rfc3610.txt).

[6] NIST Publication FIPS-197 (2016). “FIPS-197” Retrieved on Oct. 16, from (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf).

[7] S. U. Jonwal and P. P. Shingare. "Advanced Encryption Standard (AES) implementation on FPGA with hardware in loop," 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, 2017, pp. 64-67.

[8] K. Gaj and P. Chodowiec. “FPGA and ASIC Implementations of AES.” In: Çetin Kaya Koç. Cryptographic Engineering. Spring Street, New York: Springer, page 235; 2009.

[9] M. Walunjkar, M. M. Mujahid, S. A. Ahmed and A. Jadhav. "An AES-Core Development by Using Verilog." JIRCCE International Journal of Innovative Research in Computer and Communication Engineering. 2013, 1(8): 1642-1648.

[10] N. Ahmad. “New Architecture of Low Area AES S-Box/ Inv Sbox Using VLSI Implementation.” Jurnal Teknologi. 2016, 5(9): 21-25.

[11] D. Yadav and A. Rajawat. "Area and Throughput Analysis of Different AES Architectures for FPGA Implementations," 2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Gwalior, 2016, pp. 67-71.

[12] C. W. Huang, S. W. Kuo and C. J. Chang. "Embedded 8-bit AES in wireless Bluetooth application," 2013 International Conference on System Science and Engineering (ICSSE), Budapest: IEEE 2013, pp. 87-92.

[13] NIST Special Publication 800-38A (2001). "Recommendation for Block Cipher Modes of Operation, Methods and Techniques” Retrieved on 16 Dec. 17, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf.

[14] “Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality,” NIST Special Publication 800-38C, May 2004.

[15] L. Huai, X. Zou, Z. Liu and Y. Han. "An Energy-Efficient AES-CCM Implementation for IEEE802.15.4 Wireless Sensor Networks." Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09 International Conference,Wuhan, Hubei: IEEE. 2009. pp. 394-397.

[16] V. P. Hoang, T. T. D. Phan, V. L. Dao. "A Compact, Ultra-Low Power AES-CCM IP Core for Wireless Body Area Networks." 2016 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Tallinn, 2016, pp. 1-4.

[17] I. A. Badillo, C. F. Uribe, R. Cumplido and M. M. Sandoval. "Efficient hardware architecture for the AES-CCM protocol of the IEEE 802.11i standard." Computers & Electrical Engineering. 2010, 36(3): 565-577.

[18] Y. Liu, H. Zhang and T. Feng. "Design of an Encryption-Decryption Module Oriented for Internet Information Security SOC Design." International Journal of Soft Computing And Software Engineering (JSCSE). 2012, 2(7): 26-36.

[19] A. Aziz and N. Ikram. "An FPGA-based AES-CCM Crypto Core For IEEE 802.11i Architecture. " International Journal of Network Security. 2007, 5(2): 224–232.

[20] S. E. Adib and N. Raissouni. "AES Encryption Algorithm Hardware Implementation:Throughput and Area Comparison of 128, 192 and 256-bits Key." International Journal of Reconfigurable and Embedded Systems (IJRES). 2012,1(2): 67-74.

[21] N. Ahmad and S.M. Rezaul Hasan. "Efficient integrated AES crypto-processor architecture for 8-bit stream cipher." Electronics Letters. 2012, 48(23): 1456-1457.

[22] T. Hongsongkiat and P. Chongstitvatana. "AES Implementation for RFID Tags: The Hardware and Software Approaches." 2014 International Computer Science and Engineering Conference (ICSEC). Khon Kaen: IEEE. 2014. Pp. 118-123.

[23] M. Rao, A. Kaknjo, E. Omerdic, D. Toal and T. Newe. "An Efficient High Speed AES Implementation Using Traditional FPGA and LabVIEW FPGA Platforms," 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Zhengzhou, China, 2018, pp. 93-937.

[24] Z. Kouser, M. Singhal and A. M. Joshi. "FPGA implementation of advanced Encryption Standard algorithm," 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, 2016, pp. 1-5.

[25] N. S. S. Srinivas and M. Akramuddin. "FPGA based hardware implementation of AES Rijndael algorithm for Encryption and Decryption," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 1769-1776.

[26] J. Yewale and M. A. Sayyad. "Implementation of AES on FPGA,"IOSR Journal of VLSI and Signal Processing (IOSR-JVSP).2014, 4(5): PP 65-69.

[27] D. K. Nguyen, L. Lanante and H Ochi. "High Throughput– Resource Saving Hardware Implementation of AES-CCM for Robust Security Network." Journal of Automation and Control Engineering. 2013, 1(3): 250-254.

[28] K. Nguyen, L. Lanante, Y. Nagao, M. Kurosaki and H. Ochi. "Implementation of 2.6 Gbps Super-high Speed AES-CCM Security Protocol

for IEEE 802.11i." 13th International Symposium on Communications and Information Technologies (ISCIT). International Symposium, Surat Thani: IEEE. 2013. pp. 669-673.

[29] I. Choi and Ji-Hoon Kim. "Area-Optimized Multi-Standard AES-CCM Security Engine for IEEE 802.15.4 / 802.15.6." Journal Of Semiconductor Technology and Science. 2016, 16(3): 293-299.

[30] A. Hodjat, P. Schaumont and I. Verbauwhede. "Architectural design features of a programmable high throughput AES coprocessor." International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC: IEEE. 2004. pp. 498-502.

[31] E. Trejo, F. Henr´ıquez, and A. D. P´erez. "An Efficient FPGA implementation of CCM." Information Security and Cryptology - ICISC 2005, 8th International Conference. Seoul: 2005, pp. 1-14.

[32] I. A. Badillo, C. F. Uribe, R. Cumplido and M. Morales-Sandoval. "FPGA Implementation and Performance Evaluation of AES-CCM Cores for Wireless Networks," 2008 International Conference on Reconfigurable Computing and FPGAs, Cancun, 2008, pp. 421-42.

[33] K. Vu and D. Zier. "FPGA Implementation AES for CCM Mode Encryption Using Xilinx Spartan-II." ECE 679, ADVANCED CRYPTOGRAPHY, OREGON STATE UNIVERSITY SPRING. 2003. pp. 1-5.

[34] "AES-CCM Advanced Encryption Standard Core." CAST Specification, Publication date: June 2016.

[35] J. D. Ji, S. W. Jung, E. A. Jun and J. Lim. "Efficient Sequential Architecture for the AES CCM Mode in the 802.16e Standard." 2009 Second International Conference on Intelligent Networks and Intelligent Systems. Tianjin: IEEE. 2009, pp. 253-256.

[36] P. Rajasekar and H. Mangalam. "Efficient FPGA Implementation of AES 128 Bit for IEEE 802.16e Mobile WiMax Standard". Circuits and Systems. Scientific Research an academic Publisher. 2016. pp. 371-380.

[37] A. G. Dev and P. Srinathan. "ASIC Implementation of Switchable Key Advanced Encryption Standard Algorithm Encryption." International Journal of Science, Technology & Management. 2013, 2(5): 15-23.

[38] Nordic Semiconductor."nRF51822 Multiprotocol Bluetooth® low energy/2.4 GHz RF System on Chip." Trondheim Norway: Product Specification v3.1. 2014.

[39] N. Ahmad. "Parity Based Fault Detection Techniques For S-Box/ Inv S-Box Advanced Encryption System." ARPN Journal of Engineering and Applied Sciences. 2015, 10(19): 9088-9092

[40] C. Sivakumar and A. Velmurugan. "High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11i)." 2007 International Conference on Signal Processing, Communications and Networking. Chennai: IEEE. 2007. pp. 398-403.

[41] A. A. Kamal and A. M. Youssef. "An area optimized implementation of the Advanced Encryption Standard." 2008 International Conference on Microelectronics. Sharjah: IEEE. 2008. pp. 159-162

[42] R. Ahmad, A. A. Manaf and W. Ismail. "Development of an improved power-throughput Blowfish algorithm on FPGA." 2016 IEEE 12th International Colloquium on Signal Processing & Its Applications (CSPA). Malacca City: IEEE. 2016, pp. 237-241.

[43] S. Chakrabarty and D. W. Engels. "Black networks for Bluetooth Low Energy." 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas: IEEE. 2016, pp. 11-14.

[44] N. Ahmad, R. Hasan and W. M. Jubadi. "Design of AES S-box using combinational logic optimization." 2010 IEEE Symposium on Industrial Electronics and Applications (ISIEA), Penang, 2010, pp. 696-699.

[45] R. Borhan and R. M. Fuad Tengku Aziz. "Successful implementation of AES algorithm in hardware." 2012 IEEE International Conference on Electronics Design, Systems and Applications (ICEDSA). Kuala Lumpur: IEEE, 2012, pp. 27-32.

[46] Q. Liu, Z. Xu and Y. Yuan. "High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion." in IET Computers & Digital Techniques. 2015, 9(3): 175-184.

[47] Synopsys (2016). "Design" Retrieved on 16 Dec. 16, from https://www.synopsys.com/silicon-design.html.

[48] M. Chávez1, F. Henríquez, and E. Trejo. "AES-CCM Implementations For The IEEE 802.15.4 Devices." 2007 IFAC. Maxico: IEEE, 2007, PP. 223-229.

[49] Mohamed Khalil-Hani. “RTL Design of Digital Systems with Verilog.” Johor, Malaysia: UTM. 2015.

[50] Xilinx (2020). "Design” Retrieved on 8 Oct. 2021, from https://docs.xilinx.com/v/u/en-US/ds180_7Series_Overview.

APPENDIX D

VITA

The author was born in February 6, 1988, in Kota Bharu, Kelantan, Malaysia. She went to St. David's High school Malacca and Tuanku Jaafar Technical Institute, Negeri Sembilan for her secondary school. Then, she furthered her study to University of Technology Mara (UiTM), Penang majoring in Diploma of Electrical Engineering (Instrumentation). After her diploma graduation, she joined a robotic and automation skill development program with funded by Ministry of Finance Malaysia at Terengganu Advanced Technology University College (TATIUC). As she completed the program, she was offered a job at On Semiconductor Malaysia as a failure analysis technician. She had working in failure analysis's laboratory handling with machines and chemicals. After 2 years working experienced, she pursued her study to University of Tun Hussein Onn Malaysia (UTHM) and successfully completed her Bachelor of Electronic Engineering (Microelectronics). She worked as a sales engineer at Nippo Mechatronics Malaysia after graduating in 2015. She has experience with various semiconductor company on business and development. After a year working as a sales engineer, she further her study in Master's Degree as a full-time researcher at UTHM with a 3D program, sponsored by Telentcorp and technically supported by Collaborative Microelectronic Design Excellence Centre (CEDEC), University of Science Malaysia (USM). Furthermore, her research papers was accepted for presentation at the Journal of Telecommunication, Electronic and Computer Engineering (JTEC), on November 30, 2017 in Johor Bahru, Malaysia. In addition, her second research paper was presented at 2nd Joint International Conferences on Emerging Computing Technology and Sports (2nd JICETS) from November 25 until 27, 2019 in Bandung, Indonesia.