UNIVERSITI PUTRA MALAYSIA

A MODIFIED APPROACH TO IMPROVE THE PERFORMANCE OF AES USING FEISTEL STRUCTURE

AFEEF YAHYA AHMED AL-ANSI

FSKTM 2018 27

A MODIFIED APPROACH TO IMPROVE THE PERFORMANCE OF AES USING FEISTEL STRUCTURE

By

AFEEF YAHYA AHMED AL-ANSI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Information Security

JANUARY 2018

DEDICATIONS

To soul of my mother.

To my great father.

To my beloved wife.

To my children .. Ayman, Aisha and Ayoub.

To my brothers and sisters.

To all my friends.

To each of who has taught me or gave me advice.. teachers.

Dedicate this work. . .

Abstract of thesis presented to the Senate of University Putra Malaysia in fulfillment of the requirement for the degree of Master of Information Security

A MODIFIED APPROACH TO IMPROVE THE PERFORMANCE OF AES USING FEISTEL STRUCTURE

By

AFEEF YAHYA AHMED AL-ANSI

January 2018

Chair: Assoc. Prof Dr. Zurina Mohd Hanapi, Ph.D.

Faculty: Computer Science and Information Technology

In encryption algorithm design, apart from the security performance, processing performance and the cost of the implementation are very important trade-off parameters. A most popular and widely adopted symmetric encryption algorithm is the Advanced Encryption Standard (AES). It suffers from the demand for the performance efficiency. To improve its computational cost, we propose a modification of the AES technique. Having found that out of the four major operations in the AES; MixColumn is the one that takes huge amount of computing time and for which replacement with look-up table adds additional space constrain, we propose replacing the MixColumns with a Feistel Structure that exits and is the main engine of the Data Encryption Standard (DES). Empirical performance analysis on our proposed modified AES shows a significant reduction in the processing time by up to 67% on the average. The method support parallel implementation with little overhead.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master keselamatan maklumat

PENDEKATAN YANG DIUBAH SUAI BAGI MENINGKATKAN PRESTASI AES MENGGUNAKAN STRUKTUR FEISTEL

Oleh

AFEEF YAHYA AHMED AL-ANSI

Januari 2018

Pengerusi: Prof. Madya Dr. Zurina Mohd Hanapi, Ph.D.

Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Dalam reka bentuk algoritma, selain daripada prestasi keselamatan, prestasi pemprosesan dan kos pelaksanaan adalah parameter pertimbangangan yang sangat penting. Algoritma simetri yang paling popular dan digunakan secara meluas adalah Advanced Encryption Standard (AES). Namun ia menderita akibat kehendak permintaan untuk kecekapan. Untuk meningkatkan kos pengiraannya, kami mencadangkan pengubahsuaian teknik AES. Setelah mendapati bahawa daripada empat operasi utama dalam AES, MixColumn adalah salah satu yang mengambil masa pengkomputeran yang besar dan mengurangkan ruang, maka, yang mana penggantian dengan jadual paparan menambah ruang; maka kami mencadangkan penggantian MixColumns dengan Struktur Feistel, yang sedia ada, dan merupakan enjin utama dalam Data Encryption Standard (DES). Analisis prestasi empirik terhadap AES yang diubahsuai menunjukkan pengurangan yang signifikan dalam masa pemprosesan sehingga purata 67%. Kaedah ini menyokong pelaksanaan selari, dengan kos tetap yang sedikit.

ACKNOWLEDGMENTS

First all thanks are due to Allah the Lord of all worlds who said "My Lord, increase me in knowledge.". (Surat Taha 20:114). The best peace and blessing upon Mohammed, the last of prophets who said "Allah makes the way to Jannah easy for him who treads the path in search of knowledge." (Narrated by Termethi -2625).

I would like to express the deepest appreciation and sincere gratitude to my supervisor, Assc. Prof. Madya Dr. Zurina Mohd. Hanapi, for her patience and truthful guidance through all the steps of research and writing thesis. I am grateful for her for her encourage and the effort she has spent to help me accomplish this work until having a Master's degree. Special thanks are due to Assoc. Prof. Dr. Nor Fazlida Modd Sani for her valuable instructions and help during time of my study. I thank and appreciate the valuable effort of my lecturers at Faculty of Computer Science and Information Technology (FSKTM), University Putra Malaysia (UPM).

I would like to thank my dearest father. I am deeply indebted to him for his unconventional support and sacrifice for so many years.

I would like to pay special thanks to my brother, Abdulrahman, who support me during period of study.

Finally, I owe many thanks to my wife for her love, dedication, help, and encouragement in those critical moments along this journey. Words are not enough to express my gratitude.

I certify that a Thesis Examination Committee has met on (January 19, 2018) to conduct the final examination of (AFEEF YAHYA AHMED AL-ANSI) on thesis entitled "A modified approach to improve the performance of AES using Feistel structure" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the (Master of Information Security).

Members of the Thesis Examination Committee were as follows:

Zurina Mohd Hanapi, Ph.D.
Assc. Prof. Dr.
Computer Science and Information Technology
Universiti Putra Malaysia

Sharifah Md. Yasin, Ph.D.
Dr
Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at University Putra Malaysia or at any other institution.

(Signature)

AFEEF YAHAY A. AL-ANSI
Date: JANUARY 23, 2018

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Meaning
ASIC	Application-Specific Integrated Circuit
BRAM	Block Random Access Memory
CBC	Cypher Block Chaining
CIA	Confidentiality Integrity and Availability
CFB	Cipher FeedBack
CTR	Counter
CUDA	Computing Unified Device Architecture
DES	Data Encryption Standard
ECB	Electronic Code Book
FPGA	Field Programmable Gate Array
GF	Galois Field
GPU	Graphic Processing Unit
IDEA	International Data Encryption Algorithm
IV	Initialization Vector
LSW	Least Significant Word
NIST	National Institute of Standards and Technology
OFB	Output FeedBack
PKC	Public-Key Cryptography
RC4	Rivest Cipher Four
PRN	Pseudo-Random Numbers
S-box	Substitution Box
SKC	Symmetric-Key Cryptography
SPN	Substitution-Permutation Network
SCA	Side-Channel Attack
XOR	Exclusive Or

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

There are three main goals to ensure system security: Confidentiality of the information stored and/or shared; Integrity of the system and its associated data; and the system Availability as at when needed (Perrin, 2008). These cardinal goals are often refers to as Confidentiality, Integrity and Availability (CIA) triad. To achieve the Confidentiality and Integrity, cryptography is a main techniques on which the security protocols are built (Almorsy, Grundy & Müller, 2016). Cryptographic techniques are classified into two, based on the keying type: symmetric-key cry cryptography (SKC) that utilizes single key for both of the encryption and decryption process and asymmetric, also known as public-key cryptography (PKC) in which each of the process utilizes different key. The symmetric (also called private key) cryptography could operate on block form or on character stream of information. Some of the private key cryptography includes data encryption standard (DES) (FIPS, 1999), Advance Encryption Standard (AES) (NSIT, 2001), Blowfish (Schneier, 1993), the International Data Encryption Algorithm (IDEA) (Leong, Cheung, Tsoi & Leong, 2000) and Rivest Cipher Four (RC4) (Mousa & Hamad, 2006). DES was de facto among them. AES being an advancement of the DES is considered more secured due to utilizing large key sizes, and is suitable for both 8-bit microprocessor platforms and 32-bit processors (Daemen & Rijmen, 2013). Thus, as standardized by the National Institute of Standards and Technology (NIST), it is accepted as an appropriate replacement for DES.

In the encryption algorithm design, apart from the security performance, the algorithm efficiency is a significant factor that is given serious consideration by researchers. The cost of the implementation is very important because of the varying applications/platform on which the algorithm are deployed, such as embedded systems, sensor networks, e-commerce, banking, and online transaction processing applications. AES remains the most popular and widely adopted symmetric encryption algorithm.

In the AES, all computations are performed on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows of bytes for processing as a matrix. The matrix undergoes rounds of four sets transformations. Among which is what is referred to as MixColumns transformation. Even as AES is efficient, the MixColumn process involves a huge computing overheads in the whole transformation, for which a lookup table substitute also leads to additional large space overhead (Daemen & Rijmen, 2013).

1.2 Problem Statement

In general, apart from its security, various works on cryptography tries to overcome varied various performance challenges such as execution time (throughput), memory requirement and system's computation power. The power consumption depend mainly on the two other metrics. Classic AES and latest modified AES (Fei et al. 2016) are taken too much resources that lead to poor processes performance.

The major factor that determines speed of the implementations comes from the four basic building blocks operations in the Substitution-Permutation Network (SPN) of the AES – the RowShift, MixColumn, the AddRoundKey and the SubBytes. Among them the MixColumn is the most computationally involved symmetric operation for which table substitution also leads to large additional space requirement (Kawle et al. 2014).

Considering the essence of the MixColumn operation, replacing it with a similar but more efficient Feistel structure in the DES network, to suit the operations in the AES, could greatly improve the implementation efficiency in terms of processing time. In addition, adopting parallel operation in the cryptographic process is also of great benefit in boosting the efficiency. We consider the Feistel network also suitable for parallelizing the implementation.

1.3 Study Objectives

The main objective of this research is to improve the AES performance by reducing the computation overhead in the implementation. This, we expect to achieve by achieving the following objectives:

i. To propose a new AES implementation by integrating, , Feistel Network as a substitution to the more computationally involved MixColumn operation, in order to improve the performance over the classic implementation;

ii. To analyze the performance of parallel implementation of the proposed AES in order to improve further the processing time.

1.4 Scope and Limitation of the Study

In this project, we optimize the efficiency of the AES implementation in term of processing time. We integrate into the SPN, a modified Feistel Network of the DES to achieve computing time, and parallelization technique to further enhance the computing efficiency.

We use processing time to measure the AES algorithm performance. We have not explicitly considered the computational security.

We implement a fully functional algorithm that takes any kind of file, using C, for the proposal.

The main performance metric we considered here is execution time in the form of throughput. The space utilization comes from the elimination of any lookup table for MixColumn. As in the original AES, the design of the proposed modification is also intended to be scalable (or even better) with both 8-bits and 32-bit processors. The main target in the parallelization is software imple3mentation

1.5 Thesis organization

This project is organized into the following five chapters.

Chapter 1 establishes the background of the study. The problem studied is stated and the objectives to be achieved is also enumerated. The Chapter ends with detailed scope and limitation of this project.

In Chapter 2, begins with background on AES and its implementation. Literature related to symmetric key encryption in general and specific to AES implementation is critically reviewed. The Chapter concludes with identification of the limitations of the current works on the implementation and proffers means of addressing the limitation.

Chapter 3 detailed the methodology adopted in this project.

In Chapter 4, we discuss the results from the new method implantation and the parallelization carried out. The implication of the result in the real AES is evaluated and discussed.

In Chapter 6, we conclude the project and recommend on future enhancements of this work.

REFERENCES

Ahmad, Rafidah, and Widad Ismail. 2015. "Implementation of High Performance Advanced Encryption Standard-128 for WiMAX Application on FPGA." In ISTT 2014 - 2014 IEEE 2nd International Symposium on Telecommunication Technologies, 262–67. IEEE. doi:10.1109/ISTT.2014.7238216.

Clement, Jeremie, Bruno Mussard, David Naccache, and Lionel Torres. 2015. "Implementation of AES Using NVM Memories Based on Comparison Function." Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI 07–10–July: 356–61. doi:10.1109/ISVLSI.2015.37.

Daemen, Joan, Vincent Rijmen, and Katholieke Universiteit Leuven. 1999. "AES Proposal : Rijndael." Complexity, 1–45. http://ftp.csci.csusb.edu/ykarant/courses/w2005/csci531/papers/Rijndael.pdf.

Farooq, Umer, and M. Faisal Aslam. 2016. "Comparative Analysis of Different AES Implementation Techniques for Efficient Resource Usage and Better Performance of an FPGA." Journal of King Saud University - Computer and Information Sciences, March. King Saud University. doi:10.1016/j.jksuci.2016.01.004.

Fei, Xiongwei, Kenli Li, Wangdong Yang, and Keqin Li. 2016. "Practical Parallel AES Algorithms on Cloud for Massive Users and Their Performance Evaluation." Concurrency and Computation: Practice and Experience 28 (16): 4246–63. doi:10.1002/cpe.3734.

Garcia, Daniel F. 2015. "Performance Evaluation of Advanced Encryption Standard Algorithm." 2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 247–52. doi:10.1109/MCSI.2015.61.

Hossain, FS, Liakot Ali, and Niranjan Roy. 2010. "Design and Analysis of a High Performance AES Processor." In Electrical and Computer …, 18–20. IEEE. doi:10.1109/ICELCE.2010.5700754.

Kawle, Pravin, Avinash Hiwase, Gautam Bagde, Ekant Tekam, and Rahul Kalbande. 2014. "Modified Advanced Encryption Standard," no. 1: 21–23.

Kundi, D. S., Arshad Aziz, and Nassar Ikram. 2016. "A High Performance ST-Box Based Unified AES Encryption/decryption Architecture on FPGA." Microprocessors and Microsystems 41 (March). Elsevier B.V.: 37–46. doi:10.1016/j.micpro.2015.11.015.

Lim, Rone Kwei, Linda Ruth Petzold, and Çetin Kaya Koç. 2016. "Bitsliced High-Performance AES-ECB on GPUs." In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), edited by Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater, 9100:125–33. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-662-49301-4_8.

Parikh, Priyesh. 2016. "High Performance Implementation of Mixing of Column and Inv Mixing of Column for AES on FPGA." In 2016 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), 174–79. IEEE. doi:10.1109/ICCPEIC.2016.7557244.

Pendli, Vandan, Mokshitha Pathuri, and Subhakar Yandrathi. 2016. "Improvising Performance of Advanced Encryption Standard Algorithm." In Mobile and Secure Services (MobiSecServ), 1–5. IEEE. doi:10.1109/MOBISECSERV.2016.7440224.

Vishnu, M.B., S.K. Tiong, M. Zaini, and S.P. Koh. 2008. "Security Enhancement of Digital

Motion Image Transmission Using Hybrid AES-DES Algorithm." 2008 14th Asia-Pacific Conference on Communications.

Wadi, Salim M., and Nasharuddin Zainal. 2013. "A Low Cost Implementation of Modified Advanced Encryption Standard Algorithm Using 8085A Microprocessor." Journal of Engineering Science and Technology 8 (4): 406–15.

Williams, A. (2012). C++ concurrency in action: practical multithreading. Manning Publication.

Williams, T., & Kelley, C., (2015). An Interactive Plotting Program," in gnuplot 5.0, 5ed., E. A. Merritt and many others, Eds. gnuplot Development Team, 2015, vol. 5, pp. 1–253. [Online]. Available: http://www.gnuplot.info/