UNIVERSITI PUTRA MALAYSIA

A FASTER VERSION OF RIJNDAEL CRYPTOGRAPHIC ALGORITHM USING CYCLIC SHIFT AND BITWISE OPERATIONS

FAKARIAH HANI BT MOHD ALI

FSKTM 2004 5

A FASTER VERSION OF RIJNDAEL CRYPTOGRAPHIC ALGORITHM USING CYCLIC SHIFT AND BITWISE OPERATIONS

By

FAKARIAH HANI BT MOHD ALI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

February 2004

Dedicated to my husband; Mohd Rafaie Abdul Razak,

my daughter; Nurul Rusydina, my newborn baby; Muhammad Fawwaz Hadi

my parents and family

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirements for the degree of Master of Science

A FASTER VERSION OF RIJNDAEL CRYPTOGRAPHIC ALGORITHM USING CYCLIC SHIFT AND BITWISE OPERATIONS

By

FAKARIAH HANI BT MOHD ALI

February 2004

Chairman: **Associate Professor Ramlan Mahmod, Ph.D.**

Faculty: **Computer Science and Information Technology**

Doing arithmetic in finite field is the key part to the implementation of communication and coding system including the newly developed Rijndael the Advanced Encryption Standard (AES). This encryption standard uses KeyExpansion, ByteSub, Mixcolumn and Shiftrow functions which consists of XOR, inverse, multiplying and swap modules. Among them, inverse and multiplier are the most complex modules with longer delay. These modules are included in the Mixcolumn function. From the proposal of AES, the Mixcolumn function was suggested to solve the problem of delay by using look-up tables. This function can be integrated into a bigger table to replace the calculations of inverse and multiply operations, if it provides enough memory. In fact, too many tables are needed for various irreducible polynomials that this system is not flexible and expandable. The area for lookup tables becomes huge

when multiple round units are implemented. This research proposes the use of cyclic shift and bit wise XOR operation as new approach to replace the lookup table. The principle benefit of using this new approach over the transform from Rijndael block cipher is speed. This new approach has shown the excellent result, which faster then Rijndael. The new approach algorithm speed increment has consistently increased in between 18% to 22% microsecond for encryption and 30% to 34% for decryption compared to Rijndael algorithm.

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

VERSI TERLAJU ALGORITMA KRIPTOGRAFI RIJNDAEL DENGAN MENGGUNAKAN OPERASI SHIFT DAN BITWISE

Oleh

FAKARIAH HANI MOHD ALI

Februari 2004

Pengerusi: **Profesor Madya Ramlan Mahmod, Ph.D.**

Fakulti: **Sains Komputer dan Teknologi Maklumat**

Penggunaan aritmetik dalam operasi nombor yang terbatas (finite filed) adalah kunci kepada perlaksanaan sistem komunikasi dan pengkodan . Ia juga digunapakai oleh Rijndael yang dikenali sebagai Advanced Encryption Standard. Algoritma ini melaksanakan fungsi KeyExpansion, ByteSub, Mixcolumn dan Shiftrow yang mengandungi operasi XOR, songsangan, pendaraban dan pertukaran. Dalam kesemua operasi, operasi songsangan dan pendaraban adalah operasi yang dikenalpasti boleh menyebabkan kelewatan. Operasi ini dilaksanakan dalam fungsi Mixcolumn. Daripada kertas cadangan AES, fungsi Mixcolumn telah dicadangkan untuk mengatasi masalah kelewatan ini dengan menggunakan *jadual* . Fungsi ini diintegrasikan ke dalam satu *jadual* yang besar untuk menggantikan operasi songsangan dan pendaraban sekiranya cukup memori. Lagipun terlalu banyak jadual diperlukan untuk berbagai "irreducible polynomials" dan menyebabkan ianya tidak sesuai dan

tidak boleh dikembangkan. Jadual juga akan melibatkan penggunaan ruang yang amat besar apabila dilaksanakan pada banyak pusingan . Penyelidikan ini mencadangkan untuk menggunakan operasi *shift* dan *XOR* untuk menggantikan penggunaan jadual tersebut. Kelebihan penggunaan pendekatan baru ini ialah pertambahan dari sudut kelajuan. Pendekatan ini telah menunjukkan keputusan yang agak memberansangkan apabila ia di adaptasikan kepada algoritma Rijndael. Keseluruhannya pendekatan baru ini telah menyebabkan kelajuan algoritma Rijndael bertambah secara konsisten sebanyak diantara 18% hingga 22% mikrosaat untuk proses enkripsi dan 30% hingga 34% untuk proses dekripsi.

ACKNOWLEDGEMENTS

Praise to ALLAH S.W.T for giving me strength, patience, and motivation to complete this research work.

My deepest appreciation and gratitude go to the research committee lead by *Prof.Madya Dr. Ramlan Mahmod*, *Dr. Muhammad Rushdan Mohd. Said* and *Dr Ismail Abdullah* for providing me inspiration for this work and also for their virtuous guidance, encouragement, support and help during the time of doing the research.

My deepest thanks go to my husband, parents, family, and colleagues at the Faculty of Computer Science and Information Technology, UPM, for their supports and encouragement during the time of doing the research.

For financial support, I was grateful to Universiti Teknologi MARA for giving me the scholarship while I was carrying out this research. Thank you all and may God bless all these individuals for their kindness.

Fakariah Hani Mohd Ali

February 2004

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

NIST	-	National Institute of Standards and Technology
AES	-	Advanced Encryption Standard
DES	-	Data Encryption Standard
GF	-	Galois Field
XOR	-	Exclusive XOR
ATM	-	Automated Teller Machine
NBS	-	National Bureau of Standard
DEA	-	Data Encryption Algorithm
RSA	-	Rivest Shamir Adlemen
VCR	-	Video cassette recorders
ISO	-	International Organization for Standardization
IEEE	-	Institute of Electric Electronic Engineering
ANSI	-	American National Standards Institute
IETF	-	Internet Engineering Task Force

CHAPTER 1

INTRODUCTION

1.1 Background

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables us to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Cryptography is the science of secret writing. It has been used since the dawn of writing itself to conceal messages from an adversary. Cryptography distinguishes between two types of cryptographic system: symmetric and public key. Both encrypt messages using computer algorithm, and both provide users with secrecy through the use of cryptographic keys. The difference between the two cryptosystems lies in the way keys are used. A symmetric cryptosystem has a single key (see Figure 1), which is used to both encrypt and decrypt messages. The algorithm is a mathematical process that transforms plaintext into ciphertext and back again, and each transformation depends on the value of the key.

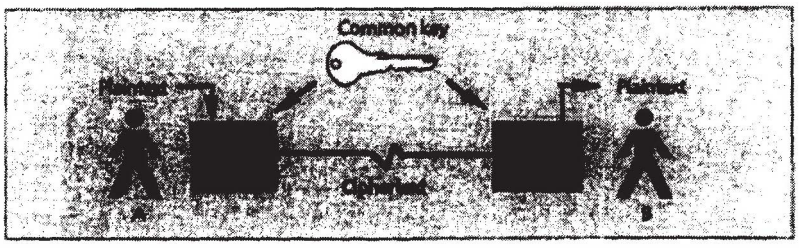

Figure 1: A symmetric cryptosystem

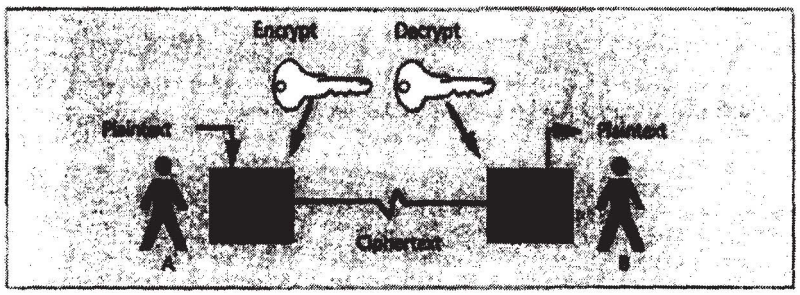

Figure 1.1: A public key cryptosystem

A well-known example of a symmetric cryptosystem is Data Encryption Standard (Federal Information Processing Standards Publication (FIPS PUB) 46,1977) (Coppersmith et. al., 1997). Other schemes include Triple DES, IDEA, RC4, RC5 and Blowfish. The new technology known as public key cryptography was introduced in 1976. In contrast to symmetric cryptosystems, public-key cryptosystems use complementary pairs of keys to separate the functions of encryption and decryptions as shown in Figure 1.1. One key is in a pair, and the private key is kept secret but the other is made publicly. Detail description for both cryptosystems will be explained in chapter 2. This research focused on symmetric cryptosystem only.

Improvement in the speed and power of microprocessor chips has made the Data Encryption Standard with its 56-bit key becomes subject to brute-force attack that can be carried out by organizations of moderate size. In 1997, the National Institute of Standards and Technology (NIST) US (an agency of the U.S Department of Commerce's Technology Administration) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) Federal information in furtherance of NIST's statutory responsibilities and to be adopted as Advanced Encryption Standard

(AES). This new algorithm will replace Data Encryption Standard, which has been standard since 1977. In 1998, NIST announced the acceptance of fifteen candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. NIST reviewed the results of this preliminary research and selected MARS, RC6™, Rijndael, Serpent and Twofish as finalists. Having reviewed further public analysis of the finalists, NIST has decided to propose Rijndael (Daemen et. al., 1999) as the Advanced Encryption Standard (AES) (Nechvatal et. al., 2000) (AES Development Effort, 2001).

Rijndael is a block cipher designed by Joan Daemen and Vincent Rijmen. According to Nechvatal et. al. (2000), Rijndael's combination of security, performance, efficiency, implementability and flexibility makes it an appropriate selection for the AES for use in the technology of today and in the future. Detail description on Rijndael will be explained in chapter 3. There are many further analyses and improvements have been done on Rijndael (Daemen et. al., 1999) (Federal Information Processing Standards Publication (FIPS) 197,2001). McLoone et. al. (2001) proposed a Field Programmable Gate Arrays (FPGAs) Rijndael encryption design which utilizes look-up tables to implement the entire Rijndael Round function. Jing et. al. (2001) proposed a new algorithm for computing inverse in GF (2^m) on the standard basis. They proposed a set of multiplier and inverse in GF (2^m) to increase the computing speed. Sklavos et. al. (2002) proposed an alternative architectures and VLSI implementation designs. These designs operate for both encryption and decryption process in the same device. Xinmiao et. al.

(2002) addresses various approaches for efficient hardware implementation of the AES algorithm.

1.2 Problem Statement

Speed is very important to perform encryption on data in real time (McLoone et. al., 2001). Different applications of the Advanced Encryption Standard (Rijndael) algorithm may require different speed / area trade-offs. Some applications, such as smart cards and cellular phones, require small area. Other applications such as WWW servers and ATMs are speed critical (Xinmiao et. al., 2002). In the computational operation in AES, several steps have to use inverse and multiplication functions. Those function include in the Mixcolumn transformation which is one of the transformation in the AES algorithm. Inverse and multiplier are the most complex modules with longer delay. Mixcolumn transformation is suggested to use look-up tables to solve the problem of delay. That function can be integrated into a bigger table to replace the calculations of inverse and multiply operations, if it provides enough memory. In fact, too many tables are needed for various irreducible polynomials so that this system is not flexible and expandable (Jing et. al., 2001). According to Xinmiao et. al. (2002), the area for lookup tables becomes huge when multiple round units are implemented. In this research we proposed the use of cyclic shift and XOR operation to replace the use of look-up tables. This approach is used to speed up Mixcolumn transformation. Detail description will be explained in chapter 4.