

UNIVERSITI PUTRA MALAYSIA

KEY TRANSFORMATION APPROACH FOR RIJNDAEL SECURITY

MEK RAHMAH BINTI SULONG.

FSKTM 2008 3



KEY TRANSFORMATION APPROACH FOR RIJNDAEL SECURITY

By

MEK RAHMAH BINTI SULONG

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

February 2008



Dedicated to my honorable supervisor; Associate Professor Ramlan Mahmod, my supportive co-supervisor; Mrs. Zaiton Muda, my friends, and my beloved family.



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

KEY TRANSFORMATION APPROACH FOR RIJNDAEL SECURITY

By

MEK RAHMAH BINTI SULONG

February 2008

Chairman:Associate Professor Ramlan Mahmod, Phd.Faculty:Computer Science and Information Technology

Rijndael is a block cipher designed by Joan Daemen and Vincent Rijmen in 1999. It is a combination of security, performance, efficiency, implementability and flexibility that makes it the best selection for Advanced Encryption Standard (AES). However, the 128bit Rijndael Key Schedule does not satisfy the frequency (bit confusion) test for majority of Subkeys and does not satisfy the avalanche (bit diffusion) test for any Subkeys. These contribute to some attacks in the Key Schedule. Thus, a new transformation method which is called "ShiftRow" is proposed into the 128-bit Rijndael Key Schedule based upon information principles (bit confusion and diffusion properties). The new method shifts the rows of the Rijndael Subkey after the RCon function is being applied to the Subkey. This method improves the security of Rijndael Key Scheduling by increasing the bit confusion and diffusion of the Rijndael Subkey. The new method has shown positive results in terms of the bit confusion and diffusion of Subkey and it has increased bit confusion and diffusion compared to the Subkey of the original Rijndael Key Schedule.



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

PENDEKATAN KUNCI TRANSFORMASI UNTUK KESELAMATAN RIJNDAEL

Oleh

MEK RAHMAH BINTI SULONG

Februari 2008

Pengerusi:Professor Madya Ramlan Mahmod, Ph.d.Fakulti:Sains Komputer dan Teknologi Maklumat

Rijndael adalah sebuah blok cipher yang telah direkabentuk oleh Joan Daemen dan Vincent Rijmen pada tahun 1999. Ia merupakan suatu kombinasi keselamatan, persembahan, keefisyenan, perlaksanaan dan kesesuaian menjadikannya sebagai pilihan yang terbaik untuk Advanced Encryption Standard (AES). Bagaimanapun, Penjadualan Kunci Rijndael tidak berjaya melepasi ujian frekuensi (pengeliruan bit) bagi kebanyakan Sub-Kekunci dan tidak berjaya melepasi ujian avalanche (pencampuran bit) bagi sebarang Sub-Kekunci. Hal ini akan menyumbang kepada pencerobohan ke atas Penjadualan Kunci. Oleh itu, satu kaedah transformasi baharu yang dinamakan "ShiftRow" telah diajukan untuk ditambah ke dalam Penjadualan Kunci Rijndael yang mana ianya berdasarkan prinsip maklumat (ciri-ciri pengeliruan dan pencampuran bit). Kaedah baru ini menganjak baris Sub-Kekunci Rijndael setelah fungsi RCon



diaplikasikan pada Sub-Kekunci. Kaedah ini memperelokkan keselamatan bagi Penjadualan Kunci Rijndael dengan meningkatkan pengeliruan dan pencampuran bit pada Sub-Kekunci Rijndael. Kaedah baru ini telah menunjukkan keputusan yang positif dari segi pengeliruan dan pencampuran bit bagi Sub-Kekunci dan ianya telah meningkatkan pengeliruan dan pencampuran bit dibandingkan dengan Sub-Kekunci Jadual Kunci Rijndael asal.





ACKNOWLEDGEMENT

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

My deepest appreciation and gratitude is dedicated to the research committee lead by Associate Professor Ramlan Mahmod and Mrs. Zaiton Muda for their motivation, guidance, encouragement, support, and assistance throughout the research.

My deepest thank go to my family and colleagues at the Faculty of Computer Science and Information Technology, UPM, for their supports during the process of completing this research.

As for financial support, I am grateful to PASCA for giving me the scholarship while I was completing this research. Thank you all and may God bless all these individuals for their kindness.



TABLE OF CONTENTS

DED ABST	ICATI [RAC]	ON Γ	ii iii
ACK	I KAK NOWI	LEDGEMENT	v
APPI	ROVA	L	viii
DEC	LARA	TION	x
LIST	OF T	ABLES	xiii
LIST	OF F	IGURES	XV
LIST LIST	OF A	LGORITHMS BBREVIATIONS	xix xxi
СНА	PTER		
1	INT	RODUCTION	1
	1.1	Introduction	1
	1.2	Problem Statement	4
	1.3	Objective	6
	1.4	Scope	6
	1.5	Thesis Organization	7
2	LITI	ERATURE REVIEW	8
	2.1	Introduction	8
	2.2	The Basic of Cryptography	8
	2.3	Asymmetric / Public Key Cryptosystem	10
		2.3.1 Discrete Logarithm Based System	11
		2.3.2 Rivest-Shamir-Adelman (RSA)	13
		2.3.3 Elliptic Curve	15
	2.4	Rijndael/AES	18
	2.5	The Advances of Rijndael	60
3	RES	EARCH METHODOLOGY	67
	., 1	Introduction	67
	3.1		67 (7
	3.1 3.2	Problem Analysis	67





		3.2.2 Input Requirement	68
		3.2.3 Performance Measurement	69
	3.3	Design	70
		3.3.1 Description of ShiftRows	71
	3.4	Implementation	72
	3.5	Analysis of Result	83
	3.6	Security Measurement	84
		3.6.1 The Frequency (Monobit) Test	85
		3.6.2 The Strict Avalanche Criterion (SAC) Test	88
4	KEY	SCHEDULING TRANSFORMATION	96
-	4.1	Introduction	96
	4.2	The Proposed New Approach Specification of the Key Expansion	97
		4.2.1 Shift Row Transformation of the New Approach	103
	4.3	The Proposed New Approach Specification of	104
		the Inverse Key Expansion	10.
		4.3.1 Inverse Shift Row Transformation of the New Approach	108
5	RESI	ULTS AND DISCUSSION	110
	5.1	Introduction	110
	5.2	Input and Output	110
	5.3	Test	111
		5.3.1 Frequency Test and Result Analysis	112
		5.3.2 Strict Avalanche Criterion (SAC) Test and Result Analysis	122
6	CON	CLUSION AND FUTURE WORK	126
	6.1	Introduction	126
	6.2	Conclusion	126
	6.3	Suggestion for Future Work	128
REFE	RENC	CES	130
			100
APPE	NDIC	ES	137
DIOP			167
RIOD	AIA(JF SIUDENI	157



LIST OF TABLES

Table		Page
Table 2.1:	'Logs' – L Values Such that $\{xy\} = \{03\}^{L}$ for a Given a Finite Field Element $\{xy\}$	29
Table 2.2:	'Antilogs' – Field Elements {E} Such that {E} = {03} ^(xy) Given the Power (xy)	30
Table 2.3:	The Substitution Box (S-Box) – S-Box[xy] (in Hexadecimal)	42
Table 2.4:	Shift Offsets for Different Block Lengths	43
Table 2.5:	The Inverse Substitution Box (Inverse S-Box) – InvS-Box[xy] (in Hexadecimal)	57
Table 3.1:	Kolmo <mark>gorov-Smirnov Table (a, b, and c)</mark>	91
Table 4.1:	The Offsets of 128-Bit Key Length	103
Table 5.1:	The Input and Output of Rijndael Key Schedule	111
Table 5.2:	Frequency Test Table	113
Table 5.3:	r1_1 to r1_10 Represent Ten Subkeys in Binary Form	116
Table 5.4:	The Example of Frequency Table of Subkey 1 for random Cipher Key	119
Table 5.5:	P-Values of 180 Random Subkeys	120

Table 5.6:	P-Values of 180 Non-Random Subkeys	120
Table 5.7:	The Result of Ten Subkeys of Poisson Test Distribution	123
Table 5.8:	D-Values of 180 Random Subkeys	124
Table 5.9:	D-Values of 180 Non-Random Subkeys	124





LIST OF FIGURES

Figure		Page
Figure 1.1:	A Symmetric Cryptosystem	2
Figure 1.2:	A Public-Key Cryptosystem	2
Figure 2.1:	Basic Scenario for Two Communicating Parties	9
Figure 2.2:	Operation of A Cipher	10
Figure 2.3:	Public Key Encryption Process	11
Figure 2.4:	Substitution-Permutation Networks (SPN) Structure	18
Figure 2.5:	The Rijndael Round Steps	21
Figure 2.6:	The Two-Dimensional AES State Array	22
Figure 2.7:	State Array Representation of Input Bytes	23
Figure 2.8:	State Array Representation of Output Bytes	23
Figure 2.9:	The AES State Array	25
Figure 2.10:	SubBytes Acts on the Individual Bytes of the State	42
Figure 2.11:	ShiftRow Operates on the Rows of the State	44
Figure 2.12:	MixColumn Operates on the Columns of the State	46

Figure 2.13:	In the Key Addition the Round Key is Bitwise EXORed to the State.	48
Figure 2.14:	Round Key Selection for Nb = 6 and Nk = 4	54
Figure 3.1:	The Performance Comparison between the Original and the New Rijndael Key Scheduling Algorithm.	74
Figure 3.2:	The Input of 128-bit Random Cipher Key	75
Figure 3.3:	The RotWord Process	76
Figure 3.4:	The SubBytes Process	76
Figure 3.5:	The XOR Process	77
Figure 3.6:	The Intermediate Output Result of 32 Bit Keys	77
Figure 3.7:	The XOR Process	78
Figure 3.8:	The Intermediate Output Result of 64 Bit Keys	78
Figure 3.9:	The XOR Process	78
Figure 3.10:	The Intermediate Output Result of 96 Bit Keys	78
Figure 3.11:	The XOR Process	78
Figure 3.12:	The Output Result of 128 Bit Keys	79
Figure 3.13:	The Shift Row (New Approach) Applied to the 128 Bit Keys	80

Figure 3.14:	The Final Output Result of 128-Bit Subkey 1 for the Application of ShiftRow to 128 Bit Keys	80
Figure 3.15:	The Final Output Result of 128-Bit Subkey 2 for the Application of ShiftRow to 128 Bit Keys	81
Figure 3.16:	The Final Output Result of 128-Bit Subkey 3 for the Application of ShiftRow to 128 Bit Keys	81
Figure 3.17:	The Final Output Result of 128-Bit Subkey 4 for the Application of ShiftRow to 128 Bit Keys	81
Figure 3.18:	The Final Output Result of 128-Bit Subkey 5 for the Application of ShiftRow to 128 Bit Keys	81
Figure 3.19:	The Final Output Result of 128-Bit Subkey 6 for the Application of ShiftRow to 128 Bit Keys	82
Figure 3.20:	The Final Output Result of 128-Bit Subkey 7 for the Application of ShiftRow to 128 Bit Keys	82
Figure 3.21:	The Final Output Result of 128-Bit Subkey 8 for the Application of ShiftRow to 128 Bit Keys	82
Figure 3.22:	The Final Output Result of 128-Bit Subkey 9 for the Application of ShiftRow to 128 Bit Keys	82
Figure 3.23 :	The Final Output Result of 128-Bit Subkey 10 for the Application of ShiftRow to 128 Bit Keys	82
Figure 4.1:	The Original Structure of Rijndael Key Expansion	96
Figure 4.2:	The New Structure of Rijndael Key Expansion	97
Figure 4.3:	The Effect of the ShiftRow Transformation on the Word	104



Figure 4.4:	The New Structure of Inverse Key Expansion Transmission	104
Figure 4.5:	The Effect of the ShiftRow Transformation on the Word	108
Figure 5.1:	Cipher Key 1 in Hexadecimal Form	114
Figure 5.2:	r1_1 Represent Subkey 1 in Hexadecimal Form	114
Figure 5.3:	r1_2 Represent Subkey 2 in Hexadecimal Form	114
Figure 5.4:	r1_3 Represent Subkey 3 in Hexadecimal Form	114
Figure 5.5:	r1_4 Represent Subkey 4 in Hexadecimal Form	115
Figure 5.6:	r1_5 Represent Subkey <mark>5</mark> in Hexadecimal Form	115
Figure 5.7:	r1_6 Represent Subkey 6 in Hexadecimal Form	115
Figure 5.8:	r1_7 Represent Subkey 7 in Hexadecimal Form	115
Figure 5.9:	r1_8 Represent Subkey 8 in Hexadecimal Form	115
Figure 5.10:	r1_9 Represent Subkey 9 in Hexadecimal Form	115
Figure 5.11:	r1_10 Represent Subkey 10 in Hexadecimal Form	115
Figure 5.12:	The Selected Subkeys of the New Approach (Random Cipherkey) and Original Approach	121
Figure 5.13:	The Selected Subkeys of the New Approach (Non-Random Cipher Key) and Original Approach	125

LIST OF ALGORITHMS

Α	lgorithm		Page
А	lgorithm 2.1:	Cipher Algorithm	39
А	lgorithm 2.2:	Round Transformation Algorithm	40
А	lgorithm 2.3:	Final Round Transformation Algorithm	40
A	lgorithm 2.4:	SubBytes Algorithm	43
A	lgorithm 2.5:	ShiftRows Algorithm	45
A	lgorithm 2.6:	MixColumns Algorithm	47
A	lgorithm 2.7:	RoundKey Algorithm	48
A	lgorithm 2.8:	Key Schedule Algorithm	50
Al	lgorithm 2.9:	KeyExpansion Algorithm for Nk ≤ 6	51
Al	lgorithm 2.10:	KeyExpansion Algorithm for Nk > 6	53
Al	lgorithm 2.11:	InvCipher Algorithm	55
Al	gorithm 2.12:	InvSubBytes Algorithm	56
Al	gorithm 2.13:	InvShiftRows Algorithm	58
Al	gorithm 2.14:	InvMixColumns Algorithm	59

Algorithm 4.1:	KeyExpansion Algorithm	100
Algorithm 4.2:	InvKeyExpansion Algorithm	105





LIST OF ABBREVIATIONS

NIST	-	National Institute OF Standards and Technology
AES	-	Advanced Encryption Standard
DES	-	Data Encryption Standard
GF	-	Galois Field
XOR		Exclusive XOR
NBS		National Bureau of Standard
DEA	-	Data Encryption Algorithm
RSA		Rivest Shamir Adlemen
IEEE	-	Institute of Electric Electronic Engineering
ANSI		American National Standards Institute



G

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cryptography is the science of encoding and decoding secret messages (Alex Brennen V., 2004). The term *cryptanalysis* is the study of cryptographic algorithms or resulting Ciphertext in order to determine their strengths and potential weaknesses. Often such analysis is performed to break an encryption algorithm or in order to perform key recovery (Alex Brennen V., 2004). *Cryptology* is the science of making and breaking secure codes. *Cryptosystem* is a protocol or method of performing encryption (Alex Brennen V., 2004). There are two types of cryptosystems: symmetric and asymmetric key. Both encrypt messages use computer algorithm and provide users with the secrecy through the use of cryptographic keys but still, there are differences in the way the keys are being used. A symmetric cryptosystem has a single key (see Figure 1.1), which is used for both encrypting and decrypting messages. Mathematical process is used in an algorithm to transform Plaintext into Ciphertext and vice versa, with each transformation depending on the value of the key.





Figure 1.1: A Symmetric Cryptosystem

Data Encryption Standard (DES) is a well-known example of symmetric cryptosystem. Others are Triple DES, IDEA, RC2, RC4, RC5, and Blowfish. In contrast to symmetric cryptosystem, public-key cryptosystem uses complementary pair of keys to separate the process of encryption and decryption as shown in Figure 1.2. One key is considered a pair, with the private key kept secret while the other is made public. However, this research focuses on symmetric-key cryptosystem only. Hereinafter, detailed description for both cryptosystems will be explained in Chapter 2.



The growth of cryptology has made the variety of algorithms, including DES being exposed to various types of attack. In 1997, the National Institute of Standards and



Technology (NIST) US (an agency of the US Department of Commerce's Technology Administration), initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitivity (unclassified) of Federal information in furtherance of NIST's statutory responsibilities and to be adopted as Advanced Encryption Standard (AES).

In the same year, NIST announced the acceptance of fifteen candidate algorithms and requested assistance of the cryptographic research community in analyzing the candidates. NIST reviewed the results of the preliminary research and selected Rijndael, Twofish, RC6TM, MARS and Serpent as finalists. Having reviewed further public analysis of the finalists, NIST has decided to propose Rijndael as the Advanced Encryption Standard (AES) (Nechvatal et. al., 2000). Rijndael is a block cipher designed by Joan Daemen and Vincent Rijmen. According to Nechvatal et. al. (2000), it is a combination of security, performance, efficiency, implementability and flexibility that makes it an appropriate selection for AES for the purpose of usage in the current and future technology.

There are many other further analysis and improvements that have been done on Rijndael (Daemen et. al., 1999). McLoon W. et. al. (2001) proposed Field Programmable Gate Arrays (FPGAs) Rijndael encryption design, utilizes look-up tables to implement entire Rijndael round function. In the same year, Jing et. al. (2001) derived a new algorithm for computing inverse in GF(2^m) on the standard basis. Sklavos et. al. (2002) designed alternative architectures and VLSI implementation designs. These designs operate for both encryption and decryption processes in the same device. Xinmiao et. al. (2002) addressed various approaches for efficient hardware

