# ANALYSIS AND IMPROVEMENT OF S-BOX IN RIJNDAEL- AES ALGORITHM

JULIET NYOKABI GAITHURU

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

SEPTEMBER 2013

This dissertation is dedicated to my father Samuel Gaithuru, mother Esther Njeru and brothers Robert Njeru and Robin Muigai for their fervent support and encouragement.

## ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisor Dr. Majid Bakhtiari for his tremendous support during my study at UTM. He inspired me greatly to work on this project. His willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I needed during the process.

# ABSTRACT

The internet has become a part of everyday life and is used as a communication tool, a way to bank, invest, shop and an educational and entertainment medium. As the importance and popularity of the internet has grown over the years, so has the number of threats from hackers on the internet which has necessitated the need for the encryption of confidential data. Various methods of data encryption have been used over time, with developments being made to improve these techniques as hackers develop improved ways of attacking the algorithms used for encryption. This process of continued improvement of cryptographic security brought about the development and acceptance of the Advanced Encryption Standard (AES), which is a National Institute of Standards and Technology specification for the encryption of electronic data including financial, telecommunications, and government data. The Rijndael algorithm was selected as the encryption algorithm for AES in October 2001 and is currently used by government agencies and the private sector to secure sensitive unclassified information. Research has shown that Rijndael is susceptible to differential/ linear cryptanalysis for 7 and 8-round Rijndael, saturation attacks, algebraic attacks and side channel attacks on reduced versions of Rijndael, which could pave the way for a full-blown attack on the Rijndael algorithm in the future. This research investigates the weaknesses present in the Rijndael algorithm using various custom-made testing tools and then using the results of this investigation to improve the security of the algorithm. The improvement is provided in the form a technique of generating highly non-linear output using a non-linear random number generator which uses the recursive inverse congruential method. The research will comprise of three phases; literature review, analysis of the Rijndael algorithm using custom-made tools and development of an improvement whose performance will be evaluated in comparison to the current algorithm.

## TABLE OF CONTENTS

# LIST OF TABLES

## TABLE OF FIGURES

## LIST OF APPENDICES

# CHAPTER 1

# INTRODUCTION

## 1.0 Introduction

The internet, which started off as a communications system for scientists and the military, has now become a gateway to a lot of knowledge and information, and is used in everyday life. It is used as a tool that enables communication among millions of people; a means of banking, shopping, investing, entertainment and education (Project, 2005).

As the importance and popularity of the internet has grown over the years, the number of threats from hackers has grown with it, thus necessitating the need for the encryption of confidential data. Presently, there are many hackers on the internet therefore rendering our data insecure without the use of encryption technology. It is very important to safeguard financial and business information from these hackers, and this is made possible through the use of encryption technology.

Encryption is a useful technique for hiding information so as to keep it secure. It is applicable in email communication and chat sessions with friends. Encryption breaks up the data sequence and scrambles it thus making it inaccessible to hackers because it is converted into unintelligible symbols called cipher-text.

In this way, personal data is stored safely on the hard disk, when being transferred over the internet while at the same time hiding the owner's identity as well as personal information including details of the information processed over the internet.

Various methods of data encryption have been used over time, with developments being made to improve these techniques as hackers develop improved ways of attacking the algorithms used for encryption. This process of continued improvement of cryptographic security brought about the development and acceptance of the Advanced Encryption Standard (AES). AES is a National Institute of Standards and Technology (NIST) specification used for encrypting electronic data and has since been used to encrypt digital information ranging from telecommunication to financial and government data.

Today AES is applied in over 1700 NIST-validated products and has also been approved by NIST, International Standards Organization (ISO), IEEE and also come to be known as the US government standard. It is used by the U.S. National Security Agency (NSA) for providing security of top secret information. Due to its high level application, there is a need to ensure its security. In the past few years, there have been numerous attempts to attack the algorithm and show its vulnerabilities. This has therefore created a need to evaluate the algorithm and discover its weaknesses and therefore develop an improvement of the algorithm so as to safeguard top secret information.

## 1.1 Problem background

Rijndael is the block cipher algorithm recently chosen by the NIST as the Advanced Encryption Standard (AES). Rijndael was selected as the standard symmetric key encryption algorithm for encrypting sensitive American federal information. The selection of Rijndael was done following a selection process which began with 15 candidate algorithms which were then narrowed down to 5 finalists whose comparative performance is as shown in the Table 1.1.

**Table 1.1:** Comparative performances of the 5 AES candidate algorithms

| **Algorithm** | **Developer** | **Key length** | **Performance** |
|---|---|---|---|
| MARS | IBM | 128-256 bits | Has numerous operations-most expensive |
| RC6 | RSA Labs | 128-256 bits | Has multiplication operations-less applicable in smart cards & hardware |
| Serpent | Anderson, Biham, Knudsen | 128-256 bits | Slow speed- $^{1}{}_{3}$ of AES |
| Twofish | Schneier | 128-256 bits | Expensive to change its key; key dependent S-Box |
| Rijndael | Rijmen, Daemen | 128-256 bits | High speed, simple design, low memory requirements (smartcard) |

As shown in the Table 1.1, Rijndael was designed on the basis of three criteria: resistance to attacks; high speed and code compactness suitable for a variety of platforms; and simplicity in design. Rijndael was chosen in favour of four other candidate algorithms; Serpent, MARS, Two-fish and RC6, This was due to its superior performance in comparison to candidates. Its performance during encryption and decryption was ranked as the highest for 64-bit and 8-bit (C and assembler), in the 32-bit smartcard as well as in Digital Signal Processors. It ranked second when implemented in 32-bit C or Java. Its performance in key scheduling was rated as the best on each platform. NIST proceeded to rank Rijndael as having the highest overall performance (Molloy, 2009).

AES is used in applications by hundreds of millions of users all over the world to provide security in wireless communications, for internet banking transactions, as well as keeping data on hard disks secure coupled with the approval of NSA for its use in protecting top secret information.

In the last decade, there have been many researchers who have tried to unearth weaknesses in AES, but none have been found so far. Research has shown that attacks on the Rijndael AES algorithm are dependent upon the generation of 2119-2128 plaintext-ciphertext pairs (Răcuciu et al. 2008). It has been discovered that an attack is possible by exploiting weaknesses in its structure, non-structural properties as well as weaknesses present during implementation.

**i.** Weaknesses in the structure are prone to:

> **a)** Saturation attacks- also referred to as the square attack. It is the most powerful cryptanalysis of AES and can break down a 7-round reduced version.
>
> **b)** Algebraic attacks- which try to exploit the round transformation following the revelation by W.Millan and J.Fuller that the S-Box can be described by 8 Boolean functions (J. F. a. W. Millan, 2003).
>
> **c)** Weaknesses in non-structural properties are prone to the exhaustive key search attack-which is possible for 56-bit key DES, but not for 128-bit AES due to the significant financial investment in hardware required (Daemen *et al.*, 2002). However, if the cost of processing power is halved every six months according to the current trend, then this attack may be plausible at the end of the century.

**ii.** Implementation weaknesses which pave the way for side-channel attacks- which could be in the form of timing analysis, differential & simple power analysis. AES has shown resistance due to its binary XOR and table look-up process

In 2009, some weaknesses were observed in the case where AES was used for encryption of data using less than four related keys chosen by an attacker. The results of the attack proved that finding AES key may be four times easier than was previously thought. However, due to the key sizes of AES, a full blown attack is not practical. To break a 128-bit AES key it would take at least 2 billion years using a trillion machines, each testing a billion keys per second. This therefore means that there is no practical threat on the security of user data yet although this discovery may pave the way for further research which may lead to the discovery of new attack strategies on the AES algorithm. Therefore due to this revelation, it is necessary to develop a way to improve the security of the Rijndael-AES algorithm.

## 1.2 Problem Statement

Rijndeal was selected as the first AES algorithm by NIST in 2001, due to its security cost and implementation benefits and has since been used to encrypt sensitive information. However, many attempts have been made to uncover weaknesses in AES including possible susceptibility to the algebraic attack, side channel attack and saturation (square) attack (Atasu *et al.*, 2004). These efforts have not produced a practical threat to the security of Rijndael AES algorithm, but have provided new insights which might mean there is a possibility of exploiting the security of Rijndael and thus expose sensitive top secret information. This research therefore explores the weaknesses in AES particularly focusing on the S-Box used in the sub-bytes transformation and improve these weaknesses.

## 1.3 Purpose of the Study

To analyze and reveal the weaknesses of the Rijndael algorithm in AES with the use of various tools and mathematical techniques, and thus facilitate the development of an improvement of the algorithm which ensures improved security of the algorithm.

## 1.4 Project Objectives

This project aims at achieving three objectives:

i. To study the AES algorithm (Rijndael).
ii. To analyze the weaknesses of the main S-Box in Rijndael AES algorithm, by using customized tools and mathematical tests.
iii. To suggest a technique for generating a customized secure S-Box.

## 1.5 Project Scope

This research focused on analyzing and revealing the weaknesses of the Rijndael algorithm in AES and therefore use these findings to develop an improvement of the algorithm which ensures improved security of the algorithm. The scope of this research is as follows:

i. Initially, an analysis of the operation of the Rijndeal AES algorithm was carried out.
ii. The study was conducted on the 128-bit key length version of the Rijndael AES algorithm which implements 10 rounds and encrypts a plaintext data block of 128-bits at a time.
iii. The evaluation of the randomness of sequences of the S-Box output bits was carried out using the following tests: frequency test, serial test, correlation test and non-linearity test.
iv. An analysis of the results was carried out.

v. A technique for generating a more secure S-Box was proposed that satisfies three S-Box design principles: non-linearity, bit independence criterion (BIC) and the correlation analysis under the majority logic criterion.

vi. A qualitative analysis of the suggested solution was carried out.

## 1.6 The Significance of the Study

Today, the growing use of the internet for banking, communication and business purposes has necessitated the use of a secure encryption algorithm. The Rijndael algorithm in AES is implemented for this purpose and is even used to protect top secret government information. In the past decade, there have been numerous attempts by researchers to uncover the weaknesses of AES (Atasu *et al.*, 2004). In this study, an evaluation of the weaknesses in the Rijndael algorithm in AES is done and for these weaknesses; a suggestion is given for the improvement of the security of the algorithm. This study helps to ensure more secure e-banking, communication and electronic transactions. Given the use of AES as the US government standard, the development of an improved AES algorithm provides assurance of the security of US government information. This study also provides significant contribution in the growing trend of cloud computing, by ensuring CIA (confidentiality, integrity and availability) when accessing data to and from data centres, in peer transactions as well as in providing secure user authentication (Ali, 2011)

## 1.7 Organization of Report

The thesis consists of 4 chapters. Chapter one describes the introduction, background of the study, study objectives and problem statement, the scope of the study and its significant. The second chapter reviews available and related literature on the security of the Rijndael algorithm in AES. Chapter three describes the methodology of the study along with the appropriate framework. The fourth chapter provides the analysis of the preliminary findings of the study and conclusion of initial work.

# REFERENCES

Ali, H. A., Firkhan Mohd Saman, Md Yazid. (2011). Rijndael encryption technique for user authentication in cloud computing.

Atasu, K., Breveglieri, L., & Macchetti, M. (2004). *Efficient AES implementations for ARM based platforms.* Paper presented at the Proceedings of the 2004 ACM symposium on Applied computing.

Bubicz, J. S., Janusz. Compound Inversive Congruential Generator Design Algorithm. *parameters, 2*(4), 6.

Chun, Y., & Yanxia, G. (2009). *A Research and Improvement Based on Rijndael Algorithm.* Paper presented at the Information Science and Engineering (ICISE), 2009 1st International Conference on.

Cui, L., & Cao, Y. (2007). A new S-box structure named Affine-Power-Affine. *International Journal of Innovative Computing, Information and Control, 3*(3), 751-759.

Daemen, J., Rijmen, V., & Barreto, P. S. (2002). *Rijndael: beyond the AES.* Paper presented at the Mikulášská kryptobesídka 2002--3rd Czech and Slovak cryptography workshop.

Desmedt, Y., Van Le, T., Marrotte, M., & Quisquater, J.-J. (2002). *Algebraic Structures and Cycling Test of Rijndael*.

Enterprises, I. (2012). Time Division Multiplexing: InetDaemon Enterprises.

Gentle, J. E., Härdle, W. K., & Mori, Y. (2012). *Handbook of computational statistics: concepts and methods*: Springer.

Gille-Genest, A. (2012). Pseudo-Random Numbers Generators. *Premia 14*. Retrieved from

Gregory Gordon Rose, D. D., CA, (US); Alexander Gantman, P., CA, & (US); Lu Xiao, S. D., CA (US). (2011). United States Patent No. 11/509,215: U. States.

Hellekalek, P. (1995a). *Inversive pseudorandom number generators: concepts, results and links*. Paper presented at the Proceedings of the 27th conference on Winter simulation, Arlington, Virginia, USA.

Hellekalek, P. (1995b). *Inversive pseudorandom number generators: concepts, results and links.* Paper presented at the Proceedings of the 27th conference on Winter simulation.

Hussain, I., Shah, T., Gondal, M., Khan, W., & Mahmood, H. (2012a). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, *23*(1), 97-104. doi: 10.1007/s00521-012-0914-5

Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2012b). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, 1-8.

Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2012). A projective general linear group based algorithm for the construction of substitution box for block ciphers. *Neural Computing and Applications*, 1-9.

Hussain, I. S., Tariq Gondal, Muhammad Asif Khan, Waqar Ahmad Mahmood, Hasan. (2012). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, 1-8.

Hussain, I. S., Tariq Mahmood, Hasan Gondal, Muhammad Asif. (2012). A projective general linear group based algorithm for the construction of substitution box for block ciphers. *Neural Computing and Applications*, 1-9.

Inc, T. C. L. C. (1981- 2013). PCMAG Encyclopedia *PCMAG Encyclopedia*.

Joan Daemen, V. R. (2002). *The Design of Rijndael: The Advanced Encryption Standard*. Verlag Berlin, Germany: Springer.

Kinga Márton, A. S., Christian Săcărea, Octavian Creț. (2011). Generation and Testing of Random Numbers for Cryptographic Applications. *international conference Romanian Cryptology Days, RCD-2011*(Proceedings of the Romanian Academy, Series A).

Krishnamurthy, G., & Ramaswamy, V. (2008). Making AES stronger: AES with key dependent S-box. *IJCSNS International Journal of Computer Science and Network Security, 8*(9), 388-398.

Li, L. (2011). *Testing Several Types Of Random Number Generator*. MS, Master of Science, The Florida State University. (Electronic Theses, Treatises and Dissertations. Paper 5393)

Li, X. C., Junli Liu, Weixiao Wan, Wanggen. (2009). *An improved AES encryption algorithm.* Paper presented at the Wireless Mobile and Computing (CCWMC 2009), IET International Communication Conference on.

Meidl, W., & Topuzoğlu, A. (2010). On the Inversive Pseudorandom Number Generator. In L. Devroye, B. Karasözen, M. Kohler & R. Korn (Eds.), *Recent Developments in Applied Probability and Statistics* (pp. 103-125): Physica-Verlag HD.

Millan, J. F. a. W. (2003). Linear Redundancy in S-Boxes. *International Association for Cryptologic Research, FSE 2003, LNCS 2887*, pp. 74–86.

Millan, W. (1998). How to improve the nonlinearity of bijective S-boxes. In C. Boyd & E. Dawson (Eds.), *Information Security and Privacy* (Vol. 1438, pp. 181-192): Springer Berlin Heidelberg.

Molloy, P. (2009). *Multiprocessing-ASMP vs SMP*.

Niels Ferguson, B. S., Tadayoshi Kohno. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Indianapolis, United States of America: Wiley Publishing, Inc.

NIST. (2001). A statistical test suite for random and pseudo-random number generators for cryptographic applications *NIST Special Publication 800-22*.

Pierre L'ecuyer, R. S. (2007). TestU01: A C Library for Empirical Testing of Random Number Generators (Vol. ACM Transactions on Mathematical Software, Vol. 33, No. 4, Article 22): Universit ´e de Montr ´ea.

Project, T. L. I. (2005). PID.

Răcuciu, C. G., Dan Medeleanu, Florin Jula, Nicolae Raducanu, Dan. (2008). *Comparative analisys for the new generation of encryption algorithms involved in NESSIE and CRYPTREC projects.* Paper presented at the The 38th International Symposium of the Military Equipment & Technologies Research Agency, Bucureşti.

Rizwan Jameel Qureshi, M. H., SA. (2008). An adaptive software development process model. *Advances in Engineering Software, 39*(8), 654-658.

Rukhin, A. S., Juan Nechvatal, James Smid, Miles Barker, Elaine. (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications: DTIC Document.

Solutions, C. T. (2004). *Operating Systems*. 500 Glen Pointe Center West
Teaneck, NJ 07666

Ph: 201-801-0233: Cognizant Academy.

Sulak, F. (2011). *Statistical Analysis of Block Ciphers and Hash Algorithms.* Philisophy of Doctorate in Cryptography, Middle East Technical University.

T Kean, M. M., JV McCanny, S McMillan, C Patterson. (2001). *Field-Programmable Logic and Applications: 11th International Conference*. Verlag Berlin Hedelberg, Germany: Springer.

Tran, M.-T. B., Doan Khanh Duong, Anh Duc. (2008). *Gray S-box for advanced encryption standard.* Paper presented at the Computational Intelligence and Security, 2008. CIS'08. International Conference on.