UNIVERSITI PUTRA MALAYSIA

IMPROVED SECURITY OF RIJNDAEL KEY EXPANSION FUNCTION

AI-ABADI HASSAN MANSUR HUSSIEN

FSKTM 2018 62

IMPROVED SECURITY OF RIJNDAEL KEY EXPANSION FUNCTION

By

Al-ABADI HASSAN MANSUR HUSSIEN

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

December 2017

COPYRIGHT

DEDICATION

In memory of my father

To my mother

With love and eternal appreciation

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

IMPROVED SECURITY OF RIJNDAEL KEY EXPANSION FUNCTION

By

Al-ABADI HASSAN MANSUR HUSSIEN

December 2017

Chairman : Madam Zaiton Muda
Faculty : Computer Science and Information Technology

Symmetric block ciphers are the most widely utilized cryptographic primitives. In most block ciphers, a master key of special length is manipulated to create round sub-keys. This manipulation is known as the key schedule. A strong key schedule means that a cipher will be more resistant to various forms of attacks especially in related-key model attacks. These days, the most common block cipher is Rijndael which adopted by the National Institute of Standards and Technology (NIST), USA in 2001 as an Advance Encryption Standard (AES). Some cryptanalysis studies have also revealed a security weakness of Rijndael such as its vulnerability to related-key differential attacks and the related-key boomerang attack. This is mainly due to the lack of nonlinearity in the key schedule of Rijndael. Constructing a key schedule that is both efficient and provably secure has been an open problem for a long time. This research presents a method to improve the key schedule of Rijndael cipher in order to make the cipher resist to related-key scenario attack in form of differential cryptanalysis attacks and boomerang attack. Two statistical tests are used: the first is a Frequency test that evaluates the bit confusion property and the second is the Strict Avalanche Criterion (SAC) test that evaluates the bit diffusion property. To evaluate the resistance of the proposed approach to the related-key differential attack and the related-key boomerang attacks, the MILP-based approach is developed. This method counts the minimum number of active S-boxes (finds the related-key differential characteristic) in a given number of rounds for byte-oriented block cipher in the related-key model. The results show that the proposed key expansion function of has excellent statistical properties and agrees with the concept of Shannon's diffusion and confusion bits. The proposed approach is also resistant against the latest related-key differential attacks and related-key boomerang attack found in the original Rijndael. Furthermore, the proposed approach has a software implementation speed approximate to the original Rijndael even in some applications where the key master frequently changes for each processed data block. These results prove that proposed

approach performs better than the original Rijndael 128-bit key expansion function and that of previous research.

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

MENAMBAH BAIK KESELAMATAN FUNGSI PENGEMBANGAN KUNCI RIJNDAEL

Oleh

AL-ABADI HASSAN MANSUR HUSSIEN

Disember 2017

Pengerusi : Puan Zaiton Muda
Fakulti : Sains Komputer dan Teknologi Maklumat

Sifer blok simetrik merupakan primitif kriptografi yang paling meluas digunakan. Dalam kebanyakan ciphers blok, kunci induk panjang khas dimanipulasi untuk membuat sub-kunci pusingan. Manipulasi ini dikenali sebagai jadual utama. Jadual utama yang kuat bermakna cipher akan lebih tahan terhadap pelbagai bentuk serangan terutamanya dalam serangan model utama berkaitan. Sifer blok yang paling lazim pada masa kini adalah Rijndael yang telah dipilih oleh Institut Kebangsaan dagi Piawaian dan Teknologi (NIST), USA pada tahun 2001 sebagai Piawaian Penyulitan Lanjutan (AES). Beberapa kajian kriptanalisis juga telah menemui kelemahan keselamatan dalam Rijndael seperti kerentanannya terhadap serangan kebezaan berkaitan kunci dan serangan boomerang berkaitan kunci. Ini adalah disebabkan oleh kekurangan ketaklinearan dalam penjadualan kunci bagi Rijndael. Membina jadual utama yang cekap dan aman adalah masalah terbuka untuk masa yang lama.Penyelidikan ini membentangkan satu kaedah untuk meningkatkan jadual utama cip Rijndael untuk menjadikan cipher itu menentang serangan senario utama berkaitan dalam bentuk serangan cryptanalysis differential dan serangan boomerang. Bagi menilai kerentanan pendekatan yang dicadangkan terhadap serangan kebezaan berkaitan kunci dan serangan boomerang berkaitan kunci, pendekatan berasaskan MILP digunakan. Pendekatan ini untuk mengira bilangan minimum kotak-S yang aktif (mencari ciri-ciri kebezaan berkaitan kunci) dalam bilangan pusingan yang diberikan untuk sifer dalam model berkaitan kunci. Selain itu. Keputusan telah menunjukkan bahawa fungsi pengembangan kunci yang dicadangkan mempunyai ciri-ciri statistik yang sangat baik berasaskan kepada konsep pengeliruan dan penyebaran bit oleh Shannon. juga mempunyai daya tahan terhadap serangan kebezaan berkaitan kunci dan serangan boomerang berkaitan kunci. Di samping itu, mempunyai kelajuan implementasi perisian yang menghampiri kelajuan Rijndael 128-bit yang asal walaupun dalam beberapa aplikasi di mana kunci utama sering berubah untuk setiap blok data yang diproses. Semua keputusan membuktikan bahawa yang dicadangkan

mempunyai prestasi yang lebih baik daripada fungsi pengembangan kunci Rijndael 128-bit dan juga berbanding dengan kajian yang terdahulu .

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my advisor, Madam Zaiton Muda, and University committee member, Dr. Sharifah Md. Yasin, for their continuous encouragement, valuable advice, and guidance throughout this research. The freedom given and open encouragement to new ideas for my research are the main drivers towards finishing this thesis.

Special thanks goes to my dearest friends who are always willing to help and share their ideas and knowledge even when they are busy with their own research. I will always treasure their friendship.

Most of all, I would like to express my deepest appreciation to my lovely family for their affectionate support, patience, and encouragement. Their prayers and good wishes constantly help me to be strong, especially in difficult times. I am forever grateful and indebted. To my late father, thank you for everything that you have given to me. You are proud of me, I know it. To my brothers and sisters, thank you for your support. And finally, the one person who has made this all possible has been my mum. She has been a constant source of support and encouragement and has made an untold number of sacrifices for the entire family, and specifically for me to continue my schooling. She is a great inspiration to me. Hence, great appreciation and enormous thanks are due to her, for without her understanding, I am sure this thesis would never have been completed. I thank you all.

I certify that a Thesis Examination Committee has met on 5 December 2017 to conduct the final examination of Al-Abadi Hassan Mansur Hussien on his thesis entitled "Improved Security of Rijndael Key Expansion Function" 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 Science.

Members of the Thesis Examination Committee were as follows:

Azizol bin Hj. Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zuriati binti Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Rabiah binti Ahmad, PhD
Professor
Universiti Teknikal Malaysia
Malaysia
(External Examiner)

NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 29 January 2018

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science.The members of the Supervisory Committee were as follows:

Zaiton binti Muda
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Sharifah binti Md. Yasin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: ____________________ Date: ________________

Name and Matric NO: AL-Abadi Hassan Mansur Hussien, GS43692

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: ______________________
Name of Chairman of Supervisory Committee: Madam Zaiton binti Muda

Signature: ______________________
Name of Member of Supervisory Committee: Dr. Sharifah binti Md. Yasin

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF THE ALGORITHMS

LIST OF ABBREVIATIONS

IBM ILOG CPLEX	Optimization Software Package (Studio)
RDTSC	Time Stamp Counter
AES-IN	Advanced Encryption Standard Instruction Set in Intel
SAES	New Advanced Encryption Sandard (tweak-aes-128-bit)
TAES	Shiftcolumn Proposed of Muda, z., et al., (2015)
MITM	Meet-in-the-middle Attack
SPSS	Statistical Product and Service Solution
MILP	Mixed Integer Linear Programming
NIST	National Institute of Standards and Technology
MDS	Maximum Distance Separable Code
DDT	Difference Distribution Table
SPN	Substitution-Permutation Network
CBC	Cipher Block Chaining
SAC	Strict Avalanche Criterion
AES	Advanced Encryption Standard
DM	Davies-Meyer Construction
GF	Galois Filed
DF	Differential Probability
ID	Impossible Differential Attacks
LP	Linear Programing
CP	Constraint Programming

CHAPTER 1

INTRODUCTION

1.1 Background

A secret key block cipher is crucial in primitive cryptography. One fundamental motivation behind the use of a block cipher is to provide protection to information transmitted in insecure communication environments. Block ciphers are applied as a component in different security domains in which other secret key cryptographic primitives may have to be constructed. This includes cryptographic pseudorandom number generators, message authentication codes, and hash functions. Nowadays, the most common block cipher is Rijndael, which is used as a standard for symmetric encryption in many countries (Lu, 2015). It is also the most extensively applied and significant symmetric block cipher algorithm in the computer security field.

The Rijndael algorithm encryption is a block cipher that was adopted by the National Institute of Standards and Technology (NIST) as an Advanced Encryption Standard (AES) in 2001 (Daemen & Rijmen, 2013). As a result, Rijndael became vastly utilized for commercial and governmental purposes, where both hardware and software implementation was targeted. Furthermore, it is an agile design with an extremely effective and efficient performance cipher. A recent cryptanalysis unearthed certain security weaknesses in the Rijndael. Further cryptanalysis on the security of Rijndael was at most focused on either related-key scenario or secret-key scenario attacks. In the secret-key scenario, attacks relied on the vulnerabilities of the state transformation function of Rijndael (Nikolić, 2011; Tao & Wu, 2015) . Accordingly, some cryptanalyses also found the security weakness of the Rijndael key expansion function such as related-key differential attacks, related sub-key attacks, and related-key boomerang attacks (Biryukov & Khovratovich, 2009; Biryukov et al., 2010; Biryukov & Nikolić, 2010; Jean, 2013; Cui et al., 2015) . Nevertheless, these attacks are ultimately hypothetical and hence need a higher computational complexity potential, which is beyond our reach. To implement ideal resistance in the cryptographic standards of Rijndael, a better solution must be determined through changing or modifying the key schedule algorithm.

Consequently, an extremely important component of a block cipher is the key schedule. In most ciphers, a master key of special length is manipulated to create round sub-keys. This manipulation is known as the key schedule. A strong key schedule means that a cipher will be more resistant to various forms of attacks especially in related-key model attacks. Since the recent attacks are found to arise from the property of the key expansion function for Rijndael, this research will tweak only the key part of Rijndael, in which the state transformation rounds of the function will remain unchanged.

1.2 Motivation

Security in Computing has become an essential domain in Information Technology (IT). More importantly, IT security has introduced ways to shield serious documents and communications from risk of exposure. The operation of hiding information, Automated Teller Machine (ATM) credit and debit cards, web browsing, and transfer of data from one point to another can be performed via cryptographic algorithms. The most utilized cryptography algorithm is the Rijndael 128-bit. This is due to its elegant design besides being an extremely securely and efficient cipher. Unfortunately, several studies have found a theoretical attack that could exploit the weakness of the Rijndael key expansion algorithm, which allows a significant reduction in the time required to break the cipher, compared to brute force attack. Rijndael is the most trusted algorithm that is widely used for security purposes. However, the new theoretical attacks such as related-key attacks and related-key boomerang attacks could give rise to a more practical technique based on this theoretical one. Dunkelman et al . (2014) present a practical-time related-key attack on the KASUMI cryptosystem in Global System for Mobile Communications (GSM) and 3-G telephony.

The redesign of the key expansion function of Rijndael has become a major challenge for the cryptographer in which the issue is to determine a method to create a new key schedule for Rijndael to ensure there is no leakage in each sub-key that would prevent a theoretical related-key attack scenario from occurring. Besides that, the efficiency of the encryption performance must also be taken into account so that the change in the key expansion function does not adversely affect the performance of the whole cipher and the results are obtained in a speed that is entirely the speed of the original algorithm, especially when using a re-key for each block message in some application modes. Most of the studies on the enhancement of the key expansion function have not presented a formally proven security solution for the key expansion function or even the whole block cipher after the change has been made. Therefore, in this research, in addition to redesigning the key expansion function of Rijndael, an automatic tool is also developed to evaluate the security of the symmetric block cipher either in the secret-key model attacks or related-key model attacks using Mixed Integer Linear Programming (MILP).

1.3 Problem Statement

The security analysis of Rijndael has been the objective of numerous cryptographic papers. The designers of Rijndael adapted the security features of the block cipher by looking at the property of the MixColumns transformation. However, further analysis of the security of Rijndael is at most focused on either secret-key attacks or related-key (or differential-key) attacks. The secret-key model attacks are established on the exposure of the state transformation round of Rijndael and are not established on vulnerabilities of the Rijndael key expansion function. Accordingly, the decreased number of rounds for Rijndael is due to the omitted MixColumns from the last rounds. This includes the Partial Sums Technique Attacks on six rounds (Tunstall, 2012) , Boomerang Technique Attacks on six rounds (Biryukov, 2005), and Impossible

Differential Technique Attacks on seven rounds of Rijndael 128-bit (Mala et al.,2010) . Li & Jin (2016) introduced the Meet-in-the-middle Technique Attack on ten rounds of Rijndael 256-bit. In addition, improving upon seven-, eight-, and twelve-round attacks on the 128-bit, 192-bit, and 256-bit key variants, respectively, using the Biclique cryptanalysis in the Meet-in-the-middle Technique Attack, was conducted on Rijndael in light of the omitted MixColumns from the last rounds (Bogdanov et al., 2011; Tao & Wu, 2015).

Recently, some of the cryptanalysts have found weaknesses in the Rijndael key expansion function, such as related-key differential attacks and related-key boomerang attacks (Biryukov & Khovratovich, 2009; Biryukov et al., 2010; Biryukov & Nikolić, 2010; Jean, 2013; Cui et al., 2015). This is mainly due to the lack of nonlinearity in the key schedule of the Rijndael, which has not enough active bytes into each sub-key and has slow diffusion into the key expansion function. The main reason for the slow diffusion into the key expansion function is because of a too linear function existing in the structural constraints of the original algorithm. The related-key model scenario attacks arises as a result of leaks into the key expansion function. Confusion and diffusion are two properties of the operation of a secure cipher. Therefore, these properties and substitution-permutation are applied just on the main-part of the Rijndael algorithm, but there is no strong security for the key expansion function. According to Cui et al., (2015), the diffusion in the key schedule is slow enough that related-key attacks can track all the differences in the round keys for which the lesser nonlinearity (too linear) into the Rijndael key expansion is not as claimed by the Rijndael designer.

Specifically, this thesis addresses the following issues:

1. The related-key differential attack on the 10-round Rijndael 128-bit. The attacker aims to recover the keys and to work only with the sub-keys of the Rijndael key schedule. This is done by looking for the differences in the differential characteristic (active S-boxes bytes) of the sub-keys bytes of the Rijndael key schedule. Meanwhile, the attacker works only on the class of the sub-key, in which the maximum differential propagation probability of an S-box in Rijndael is ${}^{4}/_{256}$, which approximately equals 2^{-6}. Hence, according to Gérault et al. (2017) and Khoo el al. (2017) , the level of security regarding a valid differential characteristic of Rijndael 128-bit is 2^{-114}, which is higher than the wanted threshold of 2^{-128} for a 128-bit block cipher. Thus, this is an open problem of locating an exact minimum number of active S-boxes for the Rijndael 128-bit in the related-key model attacks.

2. The related-key boomerang attacks aims to recover the keys, which will work for all the keys in the Rijndael cipher. The attacker uses differential characteristics on the smaller number of rounds to attack. This is because the lower bound of active S-boxes bytes into the Rijndael 128-bit at all the differential characteristics is 19 active S-boxes. Thus, Rijndael 128-bit has a 0 active S-box for the top characteristics for round 1 and 19 active S-boxes for the bottom characteristic of round 9. The attacker has a 2^{-114} −probability, which is higher than the valid probability of 2^{-128}. Hence, this would allow room for a boomerang attack. This is because 22-19 = 3 active S-boxes remainder is sufficient for an attack that could recover the key for 10 rounds.

1.4 Research Questions

This thesis proposes an enhancement to the security of the Rijndael 128-bit block cipher by redesigning the key expansion function to be more secure to the related-key differential attacks and related-key boomerang attack that exploit the weakness of the original Rijndael key schedule. The proposed approach examines the following questions:

1. Do diffusion and confusion statistical tests determine the weakness of the key expansion function?

2. Does the Mixed Integer Linear Programming analysis prove the security of the proposed approach in terms of the related-key model attacks?

3. Is the analysis of software implementation enough to describe the efficiency of the proposed approach?

1.5 Objectives of the Research

This research suggests a new technique for Rijndael, which only changes the cipher in the key expansion function. However, the security of the proposed method is the major focus of this research. Hence, as researchers, we would like to achieve an efficiency implementation as well. There are Two main objectives for this research:

1. Propose a new key expansion function for the Rijndael 128-bit block cipher.
   a. To make the Rijndael 128-bit be more resistant to related-key differential attacks and related-key boomerang attacks.
   b. To achieve a standardized speed in software implementation that is approximate to the original algorithm

2. Propose an automatic tool based on Mixed Integer Linear Programing (MILP) to analyze the security of the Rijndael 128-bit cipher regarding related-key model attacks.

1.6 Scope of the Research

This research focuses on the Rijndael block cipher. In this block cipher, there are two main parts: the round function, and the key scheduling transformation. The main concern of this research is the key scheduling transformation where enhancement is made by modifying the core function in the current key transformation to improve the requirement of bit confusion and diffusion properties and through making the cipher more resistant against related-key differential attacks and related-key boomerang attacks.

In addition, the proposed approach should prove efficient with a speed that is comparable to the speed of the original Rijndael algorithm. In most symmetric-key ciphers, key agility is the main way to evaluate the symmetric block cipher speed. Basically, the speed of a block cipher is measured in two directions. The first case is where the master key is fixed and the sub-keys are expanded once and the same set of keys to encrypt multiple blocks of data are used. The second case is when the master key keeps changing consecutively in each of the encrypted blocks data and the sub-keys have to re-key in each block of data, especially where the block cipher is utilized as the cryptographic primitive constructions. Consequently, this research will concentrate on testing the key agility of the proposed approach whereby the master key keeps changing on each block data.

1.7 Research Contributions

The major contribution of this study is an improvement to the security of the Rijndael 128-bit cipher. In the proposed approach, the core function of the key schedule algorithm is modified. By altering RotWord and adding additional SubBytes, the Rijndael 128-bit is able to resist related-key scenario attacks in the form of differential attacks and boomerang attacks. An automatic tool based on MILP is developed to determine the lower bounds of the active bytes S-boxes corresponding to the characteristic of the Rijndael 128-bit cipher (including the round function and key parts), by adopting the methods of Mouha et al., (2012) and Sun et al., (2014).

The following are the contributions of this study:

1. The proposed approach has excellent statistical properties using the concept of Shannon's diffusion and confusion bits. This has led to the development of a new cipher, which is named as SAES 128-bit, and more secure against related-key differential attacks and related-key boomerang attacks.

2. The proposed SAES has a benchmark speed in software implementation approximate to the original Rijndael or AES even in some applications where the master key frequently changes for each processed data block.

3. A statistical method that can be used to prove the security of the cipher in related-key model attacks based on the MILP-based approach is developed.

1.8 Organization of the Thesis

This section presents an outline of the entire thesis, which is organized as follows:

Chapter 1 presents the introduction and includes—among others—the background, problem statement, objectives of the research, and questions and contributions of the study.

Chapter 2 reviews related works of the subject matter, which include the Advanced Encryption Standard (AES) Competition that choose Rijndael as a new AES, and the description of the security of Rijndael regarding differential cryptanalysis along with the efficiency of the cipher. Thus, the security issues of Rijndael in related-key differential attacks and related-key boomerang attacks are described. The end of the chapter discusses related works that are compared with the security and efficiency of the alternative 128-bit Rijndael key expansion function in tabular format.

Chapter 3 provides a brief explanation of the research methodology adopted in this research. The requirement analysis for this research is discussed as well as the design of the new key expansion function. The implementation stages are shown in detail and experimental evaluation in terms of security and efficiency and analysis of the proposed key expansion function algorithm are also highlighted.

Chapter 4 describes the proposed key expansion function (SAES) along with previously proposed approach on Rijndael 128-bit (TAES) and original Rijndael 128-bit (AES) ciphers.

Chapter 5 presents the mechanism of the MILP-based approach in constructing the SAES, TAES, and AES, so as to determine the lower bounds of the active S-boxes of the bytes in related-key model attacks.

Chapter 6 provides an analysis of the results and a general discussion of the research reviewed.

Chapter 7 summarizes the entire thesis and provides recommendation on possible extensions or future work for this research.

REFERENCES

AlMarashda, K., AlSalami, Y., Salah, K., & Martin, T. (2011). On the security of inclusion or omission of MixColumns in AES cipher. In *2011 International Conference for Internet Technology and Secured Transactions* (pp. 34–39).

Adams, C., & Gilchrist, J. (1999). *The CAST-256 encryption algorithm* (No. RFC 2612).

Bernstein, D. J., & Schwabe, P. (2008). New AES software speed records. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5365 LNCS*, 322–336. https://doi.org/10.1007/978-3-540-89754-5_25

Biham, E., Dunkelman, O., & Keller, N. (2005). Related-Key Boomerang and Rectangle Attacks. In *Cramer R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science* (Vol. 3494, pp. 507–525). Springer, Berlin,: Springer, Berlin, Heidelberg. https://doi.org/10.1007/11426639_30

Biham, E., & Shamir, A. (1993). Differential Cryptanalysis of the Full 16-round DES. *Advances in Cryptology — CRYPTO' 92*, 487–496. https://doi.org/10.1007/3-540-48071-4_34

Biryukov, A. (2005). The Boomerang Attack on 5 and 6-Round Reduced AES Boomerang Attack. In *In International Conference on Advanced Encryption Standard* (pp. 11–15). https://doi.org/10.1007/11506447

Biryukov, A., & Khovratovich, D. (2009). Related-key cryptanalysis of the full AES-192 and AES-256. In *Advances in Cryptology – ASIACRYPT 2009. ASIACRYPT 2009. Lecture Notes in Computer Science* (Vol. 5912, pp. 1–18). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-10366-7_1

Biryukov, A., Khovratovich, D., & Nikolić, I. (2010). Distinguisher and related-key attack on the full AES-256. In *Advances in Cryptology - CRYPTO 2010. Lecture Notes in Computer Science* (Vol. 5677, pp. 231–249). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03356-8_14

Biryukov, A., & Nikolić, I. (2010). Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to AES, Camellia, Khazad and others. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6110 LNCS*, 322–344. https://doi.org/10.1007/978-3-642-13190-5_17

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011). Biclique Cryptanalysis of the Full AES. *Advances in cryptology–ASIACRYPT*, 344–371.

Bos, J. W., & Özen, O. (2012). Efficient Hashing using the AES Instruction Set. In *In International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 507–522).

Brown, L., & Pieprzyk, J. (1998). Introducing the new LOKI97 block cipher. *In First AES Candidate Conference* (pp. 20-22).

Biham, E., Anderson, R., & Knudsen, L. (1998). Serpent: A new block cipher proposal. *In Fast Software Encryption* (pp. 222-238). Springer Berlin/Heidelberg.

Choy, J., Zhang, A., Khoo, K., Henricksen, M., & Poschmann, A. (2011). AES variants secure against related-key differential and boomerang attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6633 LNCS*, 191–207. https://doi.org/10.1007/978-3-642-21040-2_13

CPLEX, I. I. (2011). IBM ILOG CPLEX Optimization Studio V12. 4 Documentation.

Cui, J., Zhong, H., Shi, R., & Wang, J. (2015). Related-key cryptanalysis on 7-round AES-128/192. *International Journal of Electronic Security and Digital Forensics*, *7*(2), 166–178. https://doi.org/10.1504/IJESDF.2015.069609

Daemen, J., & Rijmen, V. (2013). *The Design of Rijndael: AES - The Advanced Encryption Standard. Springer Science & Business Media*. https://doi.org/10.1007/978-3-662-04722-4

Dunkelman, O., & Keller, N. (2010). The effects of the omission of last round's MixColumns on AES. *Information Processing Letters*, *110*(8–9), 304–308. https://doi.org/10.1016/j.ipl.2010.02.007

Dunkelman, O., Keller, N., & Shamir, A. (2014). A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. *Journal of Cryptology*, *27*(4), 824–849. https://doi.org/10.1007/s00145-013-9154-9

Fouque, P., Jean, J., & Peyrin, T. (2013). Structural Evaluation ofAES and Chosen-Key Distinguisher of 9-round AES-128. *In Advances in Cryptology–CRYPTO .Springer Berlin Heidelberg*, 183–203.

Gérault, D, P. L., Minier, M., & Solnon, C. (2017). Revisiting AES Related-Key Differential Attacks with Constraint Programming. *IACR Cryptology ePrint Archive*, 139. Retrieved from http://dblp.uni-trier.de/db/journals/iacr/iacr2017.html#GeraultLMS17

Georgoudis, D., Leroux, D., & Chaves, B. S. (1998). The "FROG" encryption algorithm. AES submission, 8.

Gilbert, H., & Minier, M. (2000). A Collision Attack on 7 Rounds of Rijndael. *In AES Candidate Conference* (Vol. 230, p. 241).

Gilbert, H., Girault, M., Hoogvorst, P., Pornin, T., Poupard, G., Stern, J., & Vaudenay, S. (1998). Decorrelated Fast Cipher: an AES Candidate. *In CDROM1 of the Advanced Encryption Standard Candidate Conference* (No. LASEC-CONF-2007-025).

Gorski, M., & Lucks, S. (2008). New Related-Key Boomerang Attacks on AES. In *Lecture Notes in Computer Science* (Vol. vol 5365). Springer, Berlin, Heidelberg. https://doi.org/https://doi.org/10.1007/978-3-540-89754-5_21

Gueron, S. (2012). *Intel Advanced Encryption Standard (AES) New Instructions Set*. Retrieved from http://software.intel.com/sites/default/files/article/165683/aes-wp-2012-09-22-v01.pdf

Huang, J., & Lai, X. (2016). Transposition of AES Key Schedule. In *International Conference on Information Security and Cryptology.* (p. 260). Springer, Cham.

Jacobson Jr, M. J., & Huber, K. (1998). The MAGENTA Block Cipher Algorithm. *NIST AES Proposal, 94.*

Isa, H., Bahari, I., Sufian, H., & Z'Aba, M. R. (2012). AES: Current security and efficiency analysis of its alternatives. *In Information Assurance and Security (IAS)*, *7*(1), 52. https://doi.org/10.1109/ISIAS.2011.6122831

Jean, J. (2013). *Cryptanalysis of Symmetric-Key Primitives Based on the AES Block Cipher. Cryptography and Security [cs.CR]. (Doctoral dissertation, Ecole Normale Supérieure de Paris-ENS Paris).*

Jean, J., & Nikolić, I. (2016). Efficient design strategies based on the AES round function. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9783*, 334–353. https://doi.org/10.1007/978-3-662-52993-5_17

Jean, J., Nikolic, I., & Peyrin, T. (2014). Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In *International Conference on the Theory and Application of Cryptology and Information Security* (Vol. 8874, pp. 274–288). https://doi.org/10.1007/978-3-662-45608-8_15

Kaidalov, D., Oliynykov, R., & Kazymyrov, O. (2014). A method for security estimation of the SPN-based block cipher against related-key attacks. *Tatra Mountains Mathematical Publications*, *60*(1), 25–45. https://doi.org/10.2478/tmmp-2014-0023

Khoo, K., Lee, E., Peyrin, T., & Sim, S. M. (2017). Human-readable Proof of the Related-Key Security of AES-128. *IACR Transactions on Symmetric Cryptology*, *2*, 59–83. https://doi.org/10.13154/tosc.v2017.i2.59-83

Khovratovich, D. (2012). *Related-key cryptanalysis of AES, Hierocrypt-3, and CipherUnicorn-A*. *Investigation Reports on Cryptographic Techniques*.No.2201

Kim, J., Hong, S., & Preneel, B. (2007). Related-Key Rectangle Attacks on Reduced AES-192 and AES-256. In *In International Workshop on Fast Software Encryption* (pp. 225–241). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74619-5_155

Knudsen, L. (1998). DEAL-a 128-bit block cipher. *Complexity*, 258(2), 216.

Li, R., & Jin, C. (2016). Meet-in-the-middle attacks on 10-round AES-256. *Designs, Codes, and Cryptography*, *80*(3), 459–471. https://doi.org/10.1007/s10623-015-0113-3

Lim, C. H. (1998). CRYPTON: A new 128-bit block cipher. *NIsT AEs Proposal.*

Lu, J. (2011). The (related-key) impossible boomerang attack and its application to the AES block cipher. *Designs, Codes, and Cryptography*, *60*(2), 123–143. https://doi.org/10.1007/s10623-010-9421-9

Lu, J. (2015). A methodology for differential-linear cryptanalysis and its applications. *Designs, Codes, and Cryptography*, *77*(1), 11–48. https://doi.org/10.1007/s10623-014-9985-x

Mahmod, R., Ali, S. A., Azim, A., & Ghani, A. (2009). A Shift Column with Different Offset for Better Rijndael Security. *International Journal of Cryptology Research*, *1*(2), 245–255.

Mala, H., Dakhilalian, M., Rijmen, V., & Modarres-Hashemi, M. (2010). Improved impossible differential cryptanalysis of 7-round AES-128. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6498*, 282–291. https://doi.org/10.1007/978-3-642-17401-8_20

Massey, J. L. (1993). SAFER K-64: A byte-oriented block-ciphering algorithm. *In International Workshop on Fast Software Encryption* (pp. 1-17). Springer, Berlin, Heidelberg.

Matsui, M. (1994). The first experimental cryptanalysis of the data encryption standard. *14th Annual International Cryptology Conference*, 1–11. https://doi.org/10.1007/3-540-48658-5_1

May, L., Henricksen, M., Millan, W., Carter, G., & Dawson, E. (2002). Strengthening the Key Schedule of the AES. In *Proceedings of the 7th Australian Conference on Information Security and Privacy* (pp. 226–240). https://doi.org/10.1007/3-540-45450-0_19

Mouha, N., Wang, Q., Gu, D., & Preneel, B. (2012). Differential and Linear Cryptanalysis using Mixed-Integer Linear Programming. *In International Conference on Information Security and Cryptology*, 57–76. https://doi.org/10.1007/978-3-642-34704-7_5

Muda, Z., Mahmod, R., & M.R. Sulong. (2010). key transformation Approch for Rijndael Secuirty. *Information Technology Journal*, *9*(2), 290–297.

Muda, Z., Sulaiman, S., Yasin, S. M., & Mahmod, R. (2015). Tshiftcolumn: A new transformation in 128-bit Rijndael key expansion to improve security requirements. *Journal of Theoretical and Applied Information Technology*, *73*(1), 130–136.

Settia. N. (2010). Cryptanalysis of Modern Cryptographic Algorithms. *International Journal of Computer Science and Technology*, *VOL. 1*(ISSUE 2).

Nikolić, I. (2011). Tweaking AES. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6544 LNCS*, 198–210. https://doi.org/10.1007/978-3-642-19574-7_14

Rivest, R. L., Robshaw, M. J. B., Sidney, R., & Yin, Y. L. (1998). The RC6TM block cipher. *In First Advanced Encryption Standard (AES) Conference* (p. 16).

Sajadieh, M., Mirzaei, A., Mala, H., & Rijmen, V. (2016). A new counting method to bound the number of active S-boxes in Rijndael and 3D. *Designs, Codes and Cryptography*, 1-17.

Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., & Song, L. (2014). Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers, (L), 158–178. https://doi.org/10.1007/978-3-662-45611-8_9

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1999). The Twofish encryption algorithm: a 128-bit block cipher. *John Wiley & Sons, Inc*.

Schroeppel, R., & Orman, H. (1998). The hasty pudding cipher. *AES candidate submitted to NIST, M1.*

Tao Biaoshuai, & Hongjun Wu. (2015). Improving the Biclique Cryptanalysis of AES. In *Australasian Conference on Information Security and Privacy* (pp. 39–56). Springer, Cham.

Tunstall, M. (2012). Improved “Partial Sums”-based Square Attack on AES. In *International Conference on Security and Cryptography - SECRYPT 2012* (pp. 25–34). https://doi.org/10.5220/0003990300250034

Wagner, D., & Berkeley, U. C. (1999). The Boomerang Attack. In *In International Workshop on Fast Software Encryption* (pp. 156–170).

Yan, J., & Chen, F. (2016). An Improved AES Key Expansion Algorithm. In *International Conference on Electrical, Mechanical and Industrial Engineering* (pp. 113–116).