اونيۏرسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

SECURITY ANALYSIS TECHNIQUES USING DIFFERENTIAL RELATIONSHIPS FOR BLOCK CIPHERS

ALYA GEOGIANA BINTI BUJA

DOCTOR OF PHILOSOPHY

2018

Faculty of Information and Communication Technology

SECURITY ANALYSIS TECHNIQUES USING DIFFERENTIAL RELATIONSHIPS FOR BLOCK CIPHERS

Alya Geogiana binti Buja

Doctor of Philosophy

2018

SECURITY ANALYSIS TECHNIQUES USING DIFFERENTIAL RELATIONSHIPS FOR BLOCK CIPHERS

ALYA GEOGIANA BINTI BUJA

A thesis submitted
in fulfillment of the requirements for the degree of Doctor of Philosophy

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2018

DECLARATION

I declare that this thesis entitled "Security Analysis Techniques using Differential Relationships for Block Ciphers" is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	:	…………………………….
Name	:	Alya Geogiana binti Buja
Date	:	…………………………….

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of Doctor of Philosophy.

Signature	:	……………………………
Supervisor Name	:	Dr Shekh Faisal bin Abdul Latip
Date	:	………………..………..

DEDICATION

To my family.

ABSTRACT

The uses of block cipher has become crucial in nowadays' computing era as well as the information security. Information must be available only for authenticated and authorized users. However, flaws and weaknesses in the cryptosystem can breach the security of stored and transmitted information. A weak key in the key schedule is well-known issues which may affect several round keys have same bits in common. Besides, information leaked from the implementation also affects the security of block ciphers. Based on the flaws and leakage, the adversary is able to assess the differential relationships in block cipher using differential cryptanalysis technique. Firstly, the existing differential cryptanalysis techniques have been evaluated. Secondly, based on the gaps that have to be filled in the existing differential cryptanalysis techniques, new frameworks of differential cryptanalysis techniques have been proposed and designed by using *Pearson* correlation coefficient, Hamming-weight leakage assumption and reference point. The *Pearson* correlation coefficient is used to determine the repeated differential properties in the key schedules. Meanwhile, reference point and Hamming-weight leakage assumption are used to assess the security of the implementation of block ciphers against side-channel cube attack and differential fault analysis. Thirdly, all proposed frameworks have been assessed. The results show that the repeated differential properties are found for AES, PRESENT and Simeck key schedules. However, AES key schedule is definitely ideal to be adopted in the design for the future cryptographic algorithm. In addition, the newly designed frameworks for side-channel differential analysis techniques have been able to reduce the attack complexities for Simeck32/64, KATAN32 and KTANTAN32 compared to previous work. In conclusion, the proposed frameworks are effective in analyzing the security of block ciphers using differential cryptanalysis techniques.

ABSTRAK

Penggunaan sifer blok menjadi penting dalam era pengkomputeran masa kini serta keselamatan maklumat. Maklumat mesti disediakan untuk pengguna yang telah disahkan dan dibenarkan sahaja. Walau bagaimanapun, kelemahan dan kesilapan dalam sistem kriptografi boleh menyebabkan maklumat yang disimpan dan dihantar adalah tidak selamat. Kunci lemah yang terdapat di dalam penjadualan kunci mungkin menyebabkan beberapa kunci mempunyai bit yang sama. Selain itu, kebocoran maklumat dari pelaksanaan juga boleh mempengaruhi kekuatan sifer blok. Berdasarkan kelemahan dan kebocoran dalam pelaksanaan, musuh dapat menilai hubungan pembezaan dalam sifer blok. Pertama, teknik analisa pembezaan yang sedia ada telah dinilai berdasarkan aplikasi ke atas sifer blok. Kedua, beberapa rangka kerja baru untuk teknik analisa pembeza telah dicadangkan dan direka dengan menggunakan pekali korelasi Pearson, tanggapan kebocoran nilai berat Hamming dan titik rujukan. Pekali korelasi Pearson digunakan untuk menentukan sifat-sifat pembeza yang berulang di dalam penjadualan kunci. Sementara itu, titik rujukan dan tanggapan kebocoran nilai berat Hamming digunakan untuk menilai keselamatan pelaksanaan sifer blok terhadap serangan kiub saluran sisi dan analisis pembeza kesalahan. Ketiganya, semua rangka kerja yang baru telah dinilai. Hasil kajian menunjukkan bahawa sifat pembezaan berulang dijumpai untuk penjadualan kunci AES, PRESENT dan Simeck. Walau bagaimanapun, penjadualan kunci AES pastinya sesuai untuk digunakan dalam reka bentuk untuk algoritma kriptografi masa depan. Di samping itu, rangka kerja baru yang direka untuk teknik analisis pembezaan secara saluran sisi telah dapat mengurangkan kompleksiti serangan untuk Simeck32 / 64, KATAN32 dan KTANTAN32 berbanding kompleksiti bagi serangan sebelum ini. Kesimpulannya, rangka kerja baru yang direka di dalam tesis ini telah menilai keselamatan sifer blok dengan sangat efektif.

ACKNOWLEDGEMENTS

Alhamdulillah. Thank you Allah.

First and foremost I would like to express my sincere gratitude to my main supervisor, Dr. Shekh Faisal Bin Abdul Latip and my co-supervisor Prof. Dr. Rabiah Binti Ahmad for their continuous support, for their patience, motivation, and immense knowledge. Their guidance, insightful comments and encouragement helped me in all the time of research and writing of this thesis. Special thanks to both the external and internal examiners, Prof. Dr. Kamaruzzaman Bin Seman, Associate Prof. Dr. Sapiee Bin Jamel and Prof. Datuk Dr. Shahrin Bin Sahib for spending their time in reading, evaluating and giving their constructive comments on my thesis. Besides, I would like to thank Prof. Dr. Sazilah Binti Salam for chairing my viva-voce.

Last but not least, I would like to thank my family especially my beloved mom Doris Banta anak Mangi, my dad Buja anak Merang, my husband Mohamad Radhi bin Md Yasin and my two beloved sisters Gracia and Oliviana. My hardworking parents have sacrificed their lives for my sister and me with unconditional love and care. Thank you too to my family in laws. I would also like to thank all who directly and indirectly help me towards the accomplishment of this thesis.

Thank you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
GF(2)	Galois Field of Two Elements
ARX	Addition-Rotation-XOR
BLR	Blum-Luby-Rubinfield
DES	Data Encryption Standard
DFA	Differential Fault Analysis
HW	Hamming-weight
LSB	Least Significant Bit
MSB	Most Significant Bit
RDP	Repeated Differential Pattern
SPN	Substitution-Permutation Network

LIST OF SYMBOLS

¬	-	NOT
∧	-	AND
∨	-	OR
≤	-	Less than or equal to
∈	-	Element of
<<	-	Left shift
>>	-	Right shift
<<<	-	Left rotation
>>>	-	Right rotation
+	-	XOR logical operation
=	-	Equal
≠	-	Not equal
∑	-	Summation
{ }	-	Set
⊆	-	Subset

LIST OF PUBLICATIONS

1. Buja, A.G., Abdul-Latip, S.F. and Ahmad, R., 2018. A Security Analysis of IoT Encryption: Side-channel Cube Attack on Simeck32/64. *International Journal of Computer Networks and Communications (IJCNC) Vol 10 (4)*, AIRCC Publishing Corporation, pp. 79-90.

2. Buja, A.G., Abdul-Latip, S.F. and Ahmad, R., 2018. Fault Analysis of the KTANTAN Family of Block Ciphers: A Revisited Work on KATAN/KTANTAN Family of Block Ciphers. *Journal of Telecommuncation, Electronic and Computer Engineering (JTEC) Vol 10. (1-4),* Universiti Teknikal Malaysia Melaka (UTeM), pp. 95-100.

3. Buja, A.G., Abdul-Latip, S.F. and Ahmad, R., 2016. Repeated Differential Properties of the PRESENT Key Schedules. In Hameed, S.A et al. (Eds.), *4th International Conference on Information and Network Security, ICINS 16', Kuala Lumpur, Malaysia, December 2016, ACM,* pp. 24-28.

4. Buja, A. G., Abdul-Latip, S. F. and Ahmad, R., 2015. The Direction of Lightweight Ciphers in Mobile Big Data Computing. In Bordea, G. (Ed.), *Procedia Computer Scienc*e, 72, Elsevier, pp. 469-476.

CHAPTER 1

INTRODUCTION

Computing technology is evolving too fast. Beginning with the first gigantic machine in 1950 - 1960's, ten years later in 1970's the first networked mainframe-based machine was developed (Davis, 1977). Within that period, data was processed and stored in large, heavy and expensive machines. From time to time, data or information can be stored in larger capacity of storage, transmitted and retrieved everywhere at any time by using small, light and less expensive devices without being connected to a fixed physical link (Chen et al, 2000). Nowadays, utilizing network connectivity and computing capabilities, enable objects, sensors and any items generate, exchange and consume data with minimal human intervention (Rose, 2015).

Advances in information and computing technologies have caused many organizations to employ symmetric block ciphers to provide confidentiality, data integrity and authentication and verification (Menezes et al, 1997). U.S. National Institute of Standards and Technology (NIST) had initiated a call for the encryption primitives and finally in 1974, NIST had chosen LUCIFER as the successful candidate. LUCIFER was designed by IBM in 1971 (Feistel, 1973). After a year of collaboration between National Security Agency (NSA) and IBM, LUCIFER had been turned into Data Encryption Standard (DES) (NIST, 1977). However, after the specification of DES was announced publicly, NIST had received feedbacks regarding the length of secret key. The proposed key length was 128 bits however the one stated in the specification is only 56 bits which can be considered broken by using brute force attack. DES had been studied intensively by the researcher for better understanding on the design and strength.

In 1991, Biham and Shamir had analyzed the DES block cipher by using differential cryptanalysis which faster than brute force search (Biham and Shamir, 1993). A year later, in 1994, Matsui had introduced an attack called linear cryptanalysis that was applied on the DES block cipher (Matsui, 1994). Due to the security issues in DES, thus in 1997 NIST had made a call for Advanced Encryption Standard (AES) (NIST, 1997). The search for AES started in 1997 until 2000. Rijndael family of block ciphers had been chosen by NIST as the Advanced Encryption Standard (AES) in 2001. AES was then included in *ISO/IEC 18033-3* standard (NIST, 2001). Advanced Encryption Standard (AES) also known by its original proposed name, Rijndael was developed by Joan Daemen and Vincent Rijmen to avoid differential and linear cryptanalysis and submitted to NIST in 1998 (Daemen and Rijmen, 1998). There are three variants of AES (based on the key size); AES-128, AES-192 and AES-256 with 10, 12 and 14 rounds respectively. AES is designed by using substitution-permutation network (SPN) with four steps namely *SubBytes* (substitution), *ShiftRows* (shift), *MixColumns* (permutation) and *AddRoundKey*.

There were several initiatives had been conducted to identify secure cryptographic algorithms such as NESSIE project from 2000 - 2003 (European Commission, 2000), CRYPTREC in May 2000 (The Ministry of Internal Affairs and Communication and The Ministry of Economy, Trade and Industry, 2003) and eSTREAM in 2004 - 2008 (EU CRYPT, 2005). When this thesis was being written, Malaysia is in its initial stage of organizing National Trusted Cryptographic Algorithm List (MySEAL) Project. The project was initiated by CyberSecurity, an agency under Ministry of Science, Technology and Innovation (MOSTI). By 2020, the project is expected to have a list of cryptographic algorithms. However, the project will continue to accept the submission of cryptographic algorithms. The project aims to welcome and later promote new cryptographic algorithms