UNIVERSITI PUTRA MALAYSIA

IMPROVED ALGEBRAIC CRYPTANALYSIS OF THE REDUCED-ROUND ADVANCED ENCRYPTION STANDARD

DAVOOD REZAEIPOUR

IPM 2011 4

IMPROVED ALGEBRAIC CRYPTANALYSIS OF THE REDUCED-ROUND ADVANCED ENCRYPTION STANDARD

By

DAVOOD REZAEIPOUR

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

January 2011

DEDICATION

To

My wife and my children

Manijeh , Mahsa and Sina

For their great patience

and

My Dear Teachers

Abstract of thesis presented to the senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

IMPROVED ALGEBRAIC CRYPTANALYSIS OF THE REDUCED-ROUND ADVANCED ENCRYPTION STANDARD

By

DAVOOD REZAEIPOUR

January 2011

Chair: Assoc. Prof. Mohamad Rushdan Md. Said, PhD

Faculty: Institute for Mathematical Research

As we know Cryptology is divided into two parts: “Cryptography” and “Cryptanalysis”. Since block ciphers can be deployed in many different applications, so we focus on Advanced Encryption Standard (AES) which is the successor of Data Encryption Standard (DES).

In cryptography, we purpose new block cipher (NBC08) in order to understand the inner structure and other known properties. NBC08 accepts an variable-length key up to 512 bits, which is an improved security/performance tradeoff over existing block ciphers. It cannot be analyzed by known cryptanalytic attacks.

We study AES specifications and also the algebraic structure for AES over Galois Fields GF(2) and GF(2^8). We describe the most common cryptanalytic techniques on block ciphers, such as Differential, Linear and Integral cryptanalysis.

We study the different solving methods for system of equations of AES in both fields, GF(2) and GF(2^8). The process of performing these methods on AES acts as Algebraic attack.

In cryptanalysis, we improve the algebraic cryptanalysis attack on the reduced-round AES. It’s called Ground Algebraic attack. The notable property of Ground attack is that less requirements to any information for analyzing AES. Ground Algebraic attack is the first attack on reduced-round AES which can break 4-round and 5-round AES by respectively 2^{56} and $2^{113.5}$ computational complexities. The number of required chosen plaintexts for cryptanalysis 4-round and 5-round AES is 8 and 15, respectively.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagi memenuhi keperluan untuk ijazah Doktor Falsafah

KRIPTANALISIS ALJABAR YANG DIPERTINGKATKAN KE ATAS PUSINGAN TERTURUN PENYULITAN PIAWAI LANJUTAN

Oleh

DAVOOD REZAEIPOUR

Januari 2011

Pengerusi: Assoc. Prof. Mohamad Rushdan Md. Said, PhD

Fakulti: Institut Penyelidikan Matematik

Populariti saifer blok adalah berdasarkan kepada rekaan-rekaan berjaya (seperti DES dan pengganti nya, AES) yang diseragamkan, boleh didapati dengan percuma, dan boleh diatur kedudukannya dalam banyak aplikasi yang berbeza. Dalam tesis ini kami mencadangkan saifer blok baru (NBC08) yang menerima kunci panjang berubah-ubah sehingga 512 bit, yang mana adalah sesuai untuk dilaksanakan dalam pelbagai jenis persekitaran. NBC08 ialah satu sekuriti yang dipertingkatkan dari segi keselamatan/prestasi dibanding dengan saifer blok yang sedia wujud, yang tidak boleh dianalisis dengan mana-mana serangan kriptanalisis.

Kami mengkaji semula spesifikasi AES dan kekuatannya menentang serangan-serangan yang diketahui. Disebabkan oleh jidar keselamatan besar AES menentang kriptanalisis linear dan pembezaan dan penggunaan takrif aljabar mudah, penyelidik-penyelidik cenderung mengeksploitasi ciri-ciri aljabar AES. Kami juga mengkaji struktur aljabar untuk AES ke atas GF(2) dan GF(2^8). Kami menghuraikan teknik-teknik lazim kriptanalisis saifer blok – Kriptanalisis pembezaan, kriptanalisis Linear dan kriptanalisis kamiran.

Sebetulnya, satu pendekatan penting adalah bagi menyatakan operasi penyulitan sebagai satu sistem persamaan-persamaan polinomial. AES boleh digambarkan sebagai sistem persamaan-persamaan kuadratik ke atas GF(2) atau GF(2^8), yang tidak diketahuinya bit kunci dan satu jumlah besar pembolehubah-pembolehubah pertengahan yang terhasil dari operasi penyulitan. Kami boleh menulis penyulitan AES sebagai satu formula algebra tertutup mudah ke atas medan terhingga.

Kami mengkaji kaedah-kaedah penyelesaian berbeza untuk sistem persamaan AES dalam kedua-dua medan GF(2) dan GF(2^8). Sebenar nya, hasil dari menjalankan kaedah-kaedah ini pada AES bertindak sebagai serangan aljabar, tetapi tidak satu-satunya serangan yang mungkin. Kami menghuraikan serangan penyisipan menentang AES yang digunakan daripada ciri-ciri aljabar AES. Kami kemudian memberikan versi AES S-box yang tahan menentang serangan penyisipan.

Sifat terpenting serangan baru ini ialah kurang syarat-syarat untuk apa-apa maklumat untuk mengkaji. Serangan aljabar Ground baru boleh memecahkan 4-pusingan dan 5-pusingan AES oleh masing-masing 2^{56} dan $2^{113.5}$ kerumitan-kerumitan pengiraan. Jumlah teks asal terpilih yang dikehendaki untuk kriptanalisis 4-pusingan dan 5-pusingan AES ialah 8 dan 15, masing-masing.

ACKNOWLEDGEMENTS

First and foremost, all praise to the almighty ALLAH for His blessing and merciful which enables me to complete my study.

This thesis is the result of three years of work which I have been accompanied by some people. I now have the pleasant opportunity to express my sincere appreciation to all of them.

I would like to express my deepest gratitude, appreciation and thanks to Assoc. Prof. Mohamad Rushdan Md. Said, chairman of my supervisory committee for his helpful advices and valuable guidance during this study. I am deeply indebted to him, who has read and re-read many versions of this thesis, and every other research paper I have written to date, provided me with countless hours of his time, and given me sound advice, on matters technical, professional and personal. I would not have been able to continue my study without his supports and encouragements.

I appreciate the helps of my supervisory committee members, Prof. Kamel Ariffin M. Atan and Prof. Mohamed Othman for their supports and assistance.

The last not the least, Special Thanks to my wife Manijeh, my daughter Mahsa and my son Sina for their prayers, encouragements and spiritual supports during my whole life. I dedicate this work to them, with love and gratitude.

I certify that a Thesis Examination Committee has met on 17 January 2011 to conduct the final examination of Davood Rezaeipour on his thesis entitled "**IMPROVED ALGEBRAIC CRYPTANALYSIS OF THE REDUCED-ROUND ADVANCED ENCRYPTION STANDARD**" 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 Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Isamiddin S.Rakhimov, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Zuriati Ahmad Zulkarnain, PhD
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Zainidin Eshkuvatov, PhD
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Tor Helleseth, PhD
Professor
Department of Informatics
University of Bergen
Norway
(External Examiner)

BUJANG KIM HUAT, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 27 January 2011

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of **Doctor of Philosophy**. The members of Supervisory Committee were as follows:

Mohamad Rushdan Md. Said, PhD
Associate Professor
University Putra Malaysia
(Chairman)

Kamel Ariffin M. Atan, PhD
Professor
University Putra Malaysia
(Member)

Mohamed Othman, PhD
Professor
University Putra Malaysia
(Member)

HASANAH MOHD GHAZALI, PhD
Professor and Dean
School of Graduate Studies
University Putra Malaysia
Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at University Putra Malaysia or at any other institution.

DAVOOD REZAEIPOUR

Date:

TABLE OF CONTENTS