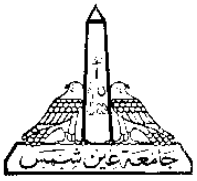


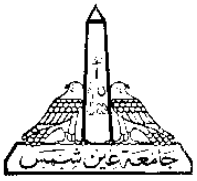
AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Engineering Physics and Mathmatics

New Algorithmic Algebraic Techniques for Cryptanalysis of Cryptographic Ciphers

A Thesis submitted in partial fulfillment of the
requirements of the degree of
Doctor of Philosophy in Physics, Engineering
Mathematics and Engineering Mechanics
(Engineering Physics and Mathmatics)
by

Wageda Ibrahim Shabaan Ahmed Elsobky
Master of Science in Physics, Engineering Mathematics
and Engineering Mechanics
(Engineering Physics and Mathmatics)
Faculty of Engineering Shobra, 2013

Supervised By
Prof**.** Dr. Reda-Elbarkouky
Dr. Ahmed Abdel Hafez
Cairo - (2017)



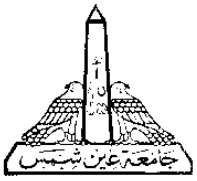
AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Engineering Physics and Mathmatics

New Algorithmic Algebraic Techniques for Cryptanalysis of Cryptographic Ciphers

A Thesis submitted in partial fulfillment of the
requirements of the degree of
Doctor of Philosophy in Physics, Engineering
Mathematics and Engineering Mechanics
(Engineering Physics and Mathmatics)
by

Wageda Ibrahim Shabaan Ahmed Elsobky
Master of Science in Physics, Engineering Mathematics
and Engineering Mechanics
(Engineering Physics and Mathmatics)
Faculty of Engineering Shobra, 2013

Supervised By
Prof**.** Dr. Reda-Elbarkouky
Dr. Ahmed Abdel Hafez



AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Physics and Mathematics

New Algorithmic Algebraic Techniques for Cryptanalysis of Cryptographic Ciphers

by

Wageda Ibrahim Shabaan Ahmed Elsobky

Master of Science in Physics, Engineering Mathematics and Engineering Mechanics

(Engineering Physics and Mathmatics)

Faculty of Engineering Shobra, 2013

Examiners' Committee

Name and Affiliation	**Signature**
Prof.	.....
Choose an item., University	
Prof.	.....
Choose an item., University	
Dr.	.....
Choose an item., University	

.Statement

This thesis is submitted as a partial fulfillment of Doctor of Philosophy in Physics, Engineering Mathematics and Engineering Mechanics Engineering, Faculty of Engineering, Ain shams University.

The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Wageda Ibrahim Shabaan Ahmed Elsobky

Signature

……...…….

Date:

Researcher Data

Name:	**Wageda Ibrahim Shabaan Ahmed Elsobky**
Date of birth:	29/01/1982
Place of birth:	Benha
Last academic degree:	Master of Science in Physics, Engineering Mathematics and Engineering Mechanics
Field of specialization:	Mathemat[pics
University issued the degree:	Faculty of Engineering Shobra
Date of issued degree:	2013
Current job:	Assistant lecture in Faculty of Engineering Benha

Thesis Summary

In our thesis we focus in Algebraic Cryptanalysis of AES ”Advanced Encryption Standard” hence Algebraic cryptanalysis is a relatively new field of cryptology. Algebraic cryptanalysis on Rijndael AES, is based on its rich algebraic structure. The basic idea is to model a cipher using a system of polynomial equations over a finite field. This approach has gained attention since Nicolas Courtois claimed that it could be used to attack AES, which has a simple algebraic structure [1]. This attack has also been attempted on other ciphers such as DES [2]. Algebraic cryptanalysis has been shown very effective for families of stream ciphers. Gröbner bases algorithms a well-known method to solve this problem. This thesis has described a description of cryptanalysis types, including Algebraic cryptanalysis type. We also describe the mathematical models of AES. There are three types of models to penetrate the AES cipher .Through this thesis we concentrate in the one which study the nonlinear part of the AES model .In general the equations of AES are divided into two groups, one linear which represents shift row , mix colum and add round key. The second group is the S-Box which is nonlinear.

S-box is the unique nonlinear operation in Rijndael cipher, and it determines the performance of AES cipher . So much work has concentrated on Rijndael S-box. Many researchers devote time to design and improve the algebraic cryptanalysis scheme

[3, 4,]. Algebraic cryptanalysis consists of two steps. First step converts the cipher into a system of polynomial equations, usually over GF(2), or over other rings. Second step, solves the system of equations and obtain from the solution the secret key of the cipher. Many researchers focus on these two steps. Courtois and Pieprzyk [7] analyzed the over defined system . Our focus on solving nonlinear system of equations GF(2^8) applying a powerful algebraic tool; Gröbner basis; to overcome the nonlinearity features of S-Box. Finally, the analysis shows that how applying Gröbner basis of AES constructs a spare matrix which makes the system easy to be solved. Moreover, we have proved the "Resistance of Algebraic Attack" RAA value (Γ) has been reduced. We apply Gröbner basis on two models of nonlinear S-Box [7,8] .

Key words: Algebraic cryptanalysis, multivariate quadratic polynomial equation system, S-box, Gröbner bases, Rijndael AES, RAA.

Acknowledgment

First of all thanks to ALLAH Who helps me to accomplish this work. There are always some inuential people in anyone's academic life. Since this dissertation is the last written document in my student life, I would like to thank all those who changed my life and attitude during these exciting and challenging years: I can not imagine how I can thank the best teachers of my life, my two angels of God, my parents, for all their support, help, and love during my entire life; the only ones who were always there for me in both my happiness and hard time; the ones I love the most for ever and can not reciprocate even a small part of what they did for me. At any period in my academic life, it was my dream to have someone beside me who has the answer to all my questions. I never had such an opportunity before I met Prof. Reda. I have never met anyone brighter and smarter in my life. I would like to warmly thank Dr. Ahmed Abdel Hafez for his extreme kindness, help and support during the last 3 years. More importantly, he changed my attitude towards several points in life. I learned from him to follow my passion and to do research in areas which I find interesting, though other people believe what I am doing is of no interest. He was always motivating me to set ambitious goals in my research and not to give up until I achieve them all.

Thank you

List of Figures

Chapter 2: Cryptanalysis types

Fig 2. 1 Egyptians Cryptography ..... **Error! Bookmark not defined.**
Fig 2. 2 Cryptographic Model..... **Error! Bookmark not defined.**
Fig 2. 3 Transposition column ..... **Error! Bookmark not defined.**
Fig 2. 4 Example of transposition..... **Error! Bookmark not defined.**
Fig 2. 5 Caesar Substitution..... **Error! Bookmark not defined.**
Fig 2. 6 Monoalphabetic substitution..... **Error! Bookmark not defined.**
Fig 2. 7 Hash Functions ..... **Error! Bookmark not defined.**
Fig 2. 8 Asymmetric Key Cryptography..... **Error! Bookmark not defined.**
Fig 2. 9 Symmetric Key Cryptography..... **Error! Bookmark not defined.**

Chapter 3: Gröbner bases

Fig 3. 1 The original System..... **Error! Bookmark not defined.**
Fig 3. 2 Three Polynomial of the Ideal ..... **Error! Bookmark not defined.**
Fig 3. 3 The original system 107xy+y^2+29,x^2+80xy+114**Error! Bookmark not defined**
Fig 3. 4 The ideal obtained by F4 ..... **Error! Bookmark not defined.**

Chapter 4: Description of The AES

Fig 4. 1 AES 128 Schematic..... **Error! Bookmark not defined.**
Fig 4. 2 Encryption and Decryption of AES **Error! Bookmark not defined.**
Fig 4. 3 AESwith different Keys..... **Error! Bookmark not defined.**
Fig 4. 4 The internal structure of AES..... **Error! Bookmark not defined.**
Fig 4. 5 The AES array of bytes ..... **Error! Bookmark not defined.**
Fig 4. 6 The famous AES S-box. ..... **Error! Bookmark not defined.**
Fig 4. 7 How S-Box operate ..... **Error! Bookmark not defined.**
Fig 4. 8 Shift row matrix..... **Error! Bookmark not defined.**
Fig 4. 9 Internal shift row operation ..... **Error! Bookmark not defined.**
Fig 4. 10 Mix column..... **Error! Bookmark not defined.**
Fig 4. 11 Internal operation of mix column .. **Error! Bookmark not defined.**
Fig 4. 12 Add Round Key..... **Error! Bookmark not defined.**

CHAPTER 6: Algebraic cryptanalysis of AES using Gröbner Basis

Fig 6. 1 Gröbner result as a matrix ..... **Error! Bookmark not defined.**
Fig 6. 2 Matrix with zero white colour ..... **Error! Bookmark not defined.**
Fig 6. 3 model 4with coloured result ..... **Error! Bookmark not defined.**
Fig 6. 4 Model 4 with zero white colour..... **Error! Bookmark not defined.**

List of Abbreviations

AES	**Advanced Encryption Standard**
$x_1, \ldots, x_n$.	variables
AA	Algebraic Attack
BES	Big Encryption System
BFA	Brute Force Attack
COA	Cipher text Only Attacks
CPA	Chosen Plaintext Attack
DES	Data Encryption Standard
GB	Gröbner basis
GF	Galois field
G-J	Gauss-Jordan (elimination)
grevlex	graded reverse lexicographic ordering of monomials
HT	Heading term of a polynomial
KPA	Known Plaintext Attack
LC	leading coefficient of a polynomial
lex	lexicographic ordering of monomials
LM	leading monomial of a polynomial
LT	leading term of a polynomial
MIM	Man in Middle Attack
MQ	Multivariate Quadratic Equations
RAA	Resistance against Algebraic Attack

$\mathbf{S}\ (\mathbf{g_p}, \mathbf{g_q})$	The S-Polynomial of f
XSL	Extended Sparse Linearization
$\boldsymbol{I}$	ideal
$\boldsymbol{f1}, \ldots, \boldsymbol{fm}$	polynomials

Glossary of Terms and Acronyms

Affine transformation	**A transformation consisting of multiplication by matrix followed by the addition of a vector**
Bit	A binary digit having a value of 0or 1
Cryptology	is the study of two branches cryptography and cryptanalysis
Cryptanalysis	is the study of mathematical tools trying to break the cipher
Plaintext	It is the original data to be encrypted.
Cipher text	It is the output text after the encryption of the original data.
Key	It is a word or value used in the cryptographic model to cipher the message / decipher the encrypted data.
Encryption	A process of manipulating a message in such a way that it hides its content with the help of key.
Decryption	The operation of turning the encrypted data into its original form.
Crypto Analyst	It is a specialist person in analyzing and breaking codes.
Array	An enumerated collection of identical entities (e.g., an array of bytes).
Block	Sequence of binary bits that comprise the input, output, State, and Round Key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes.
Byte	A group of eight bits that is treated either as a single entity or as an array of 8 individual bits.
Round Key	Round keys are values derived from the Cipher Key using the Key Expansion routine; they are applied to the State in

	the Cipher and Inverse Cipher.
S-box	Non-linear substitution table used in several byte substitution transformations and in the Key Expansion routine to perform a one-for-one substitution of a byte value.
Word	A group of 32 bits that is treated either as a single entity or as an array of 4 bytes
IDEA	The International Data Encryption Algorithm
Add Round Key	Transformation in the Cipher and Inverse Cipher in which a Round Key is added to the State using an XOR operation. The length of a Round Key equals the size of the State (i.e., for Nb = 4, the Round Key length equals 128 bits/16 bytes).
SubBytes	Transformation in the Cipher that processes the State using a non¬ linear byte substitution table (S-box) that operates on each of the State bytes independently
XOR	Exclusive-OR operation.
Nk	Number of 32-bit words comprising the Cipher Key. For this standard, Nk = 4, 6, or 8.
Nr	Number of rounds, which is a function of Nk and Nb (which is fixed). For this standard, Nr = 10, 12, or 14.
Nb	Number of columns (32-bit words) comprising the State. For this standard, Nb = 4.
Mix Columns	Transformation in the Cipher that takes all of the columns of the State and mixes their data (independently of one another) to produce new columns.

شكر

فى البداية أود أن أحمد الله عز وجل على إعانتى لإتمام هذا العمل.

وأتقدم بخالص الشكر والإمتنان للسادة المشرفين على الرسالة أ.د. رضا امين البرقوقى وأ.م.د. أحمد عبد الحافظ للدعم المستمر طوال فترة البحث والدراسة والتوجيه أثناء كتابة هذا العمل.

.ومما لاشك فيه أن الدعم المعنوى المستمر من والدى والدتى وزوجى وأولادى واخواتى خلال فترة الدراسة له أكبر مردود على إنجاح وإنجاز هذا العمل.

وفى النهاية لايسعنى إلا أن أتقدم بخالص الشكر والعرفان فى كل من ساهم بعلمه أو جهده أو دعمه بطريقة مباشرة أو غير مباشرة فى إنجاز هذا العمل.