T.R.
BOLU ABANT İZZET BAYSAL UNIVERSITY
INSTITUTE OF GRADUATE STUDIES
Department of Mathematics

GRÖBNER BASES FOR SOME VARIANTS OF ADVANCED ENCRYPTION STANDARD

MASTER OF SCIENCE

DILSHAD RAHEEM KAREEM BAJALAN

ACADEMIC SUPERVISOR
Prof. Dr. Erol YILMAZ

BOLU, AĞUSTOS - 2021

APPROVAL OF THE THESIS

GRÖBNER BASES FOR SOME VARIANTS OF ADVANCED ENCRYPTION STANDARD submitted by **Dilshad Raheem Kereem BAJALAN** and defended before the Examining Committe Members listed below in partial fulfillment of the requirements for the degree of **Master of Science** in **Department of Mathematics, Institute of Graduate Studies of Bolu** Abant **İzzet Baysal University in 5.08.2021** by

Examining Committee Members	**Signature**
Supervisor Prof. Dr. Erol YILMAZ Bolu Abant İzzet Baysal University	.....
Member Assoc. Prof. Dr. Ergun YARANERI İstanbul Technical University	.....
Member Asist. Prof. Dr. Ali Öztürk Bolu Abant İzzet Baysal University	.....

Prof. Dr. Osman GÖRÜR

Director of Instıtute of Graduate Studies

ETHICAL DECLARATION

In this thesis dissertation that was properly prepared according to the Thesis Writing Rules of Bolu Abant İzzet Baysal University of the Institute of Graduates Studies, I hereby declare that;

- All data, information, and documents presented in the thesis were obtained in accordance with the academic and ethical rules,
- All data, documents, assessments, and results were presented in accordance with the scientific ethical and moral rules,
- All works that were benefitted in the thesis were appropriately cited,
- No alteration was made in the data used,
- Study presented in this thesis is original,

Otherwise, I declare that I accept the loss of all my rights in case any contradiction that may arise against me.

Based on the plagiarism report that was generated on the date of 16/08/2021 by using predetermined filtrations set by Directorate of Institute of Graduate Studies of the Turnitin programme, a plagiarism detection sofware, the rate of plagiarism detected was 25 %.

_____

Dilshad Raheem Kereem BAJALAN

ABSTRACT

GRÖBNER BASES FOR SOME VARIANTS OF ADVANCED ENCRYPTION STANDARD
MSC THESIS
DILSHAD RAHEEM KAREEM BAJALAN
INSTITUTE OF GRADUATE STUDIES
BOLU ABANT IZZET BAYSAL UNIVERSITY
DEPARTMENT OF MATHEMATICS
(SUPERVISOR: PROF.DR. EROL YILMAZ)

BOLU, AUGUST 2021
(x + 32)

The some different variants of the Advanced Encryption Standard are investigated. Algebraic equations and Gröbner basis for them are obtained in two different setting of the polynomial ring.

KEYWORDS: Block ciphers, AES, S-boxes, Lagrange polynomails, Gröbner bases, Crytanalysis.

ÖZET

İLERİ ŞİFRELEME STANDARTLARININ BAZI TÜRLERİ İÇİN GRÖBNER TABANLARI
YÜKSEK LİSANS TEZİ
DILSHAD RAHEEM KAREEM BAJALAN
BOLU ABANT İZZET BAYSAL ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

(TEZ DANIŞMANI: PROF. DR. EROL YILMAZ)

BOLU, AĞUSTOS - 2021
(x + 32)

Gelişmiş Şifreleme Standardının bazı farklı çeşitleri incelendi. Bu varyantlar için cebirsel denklemler ve Gröbner tabanları polinom halkasının iki farklı durumu için elde edildi.

ANAHTAR KELİMELER: Blok şifreler, AES, S-kutuları, Lagrange polinomları, Gröbner tabanları, Kriptanaliz.

TABLE OF CONTENTS

APPROVAL OF THE THESIS ..... **iv**
ETHICAL DECLARATION ..... **v**
ABSTRACT ..... **vi**
ÖZET ..... **vii**
TABLE OF CONTENTS ..... **viii**
LIST OF TABLES ..... **ixi**
LIST OF ABBREVIATIONS AND SYMBOLS ..... **ix**
1. INTRODUCTION **1**
2. AIM AND SCOPE OF THE STUDY **3**
3. GRÖBNER BASES **4**
3.1. Monomial Ordering and Division Algorithm 4
3.2. Gröbner Bases 7
3.3. Zero Dimensional Ideals 8
4. SMALL SCALE VARIANTS OF AES **10**
4.1 Parameters 10
4.2 Round Operations 12
5. ALGEBRAIC EQUATIONS FOR SMALL SCALE AES **17**
5.1 Algebraic Equations Over $GF(2^4)$ 17
5.2 Algebraic Equations Over $GF(2)$ 22
6. CONCLUSIONS AND RECOMMENDATIONS **29**
7. REFERENCES **30**
8. APPENDICES **31**

LIST OF TABLES

Page

Table 3.1. Division Algorithm ……..…….....5
Table 3.2. Buchberger's Algorithm……..7
Table 4.1. The Addition Table of $GF(2^4)$…….....10
Table 4.2. The Multiplication Table of $GF(2^4)$……...……..10
Table 0.3. S-box Substition Table….……11
Table 0.4. MixColumns Multiplication Matrices……...12
Table 0.5. Key Schedule…….13
Table 4.6. An Example of $SR^*(4,2,2,4)$…….15
Table 5.1. Inverse Map Substition Table……22

LIST OF ABBREVIATIONS AND SYMBOLS

DES **:** Data Encryption Standard

AES **:** Advanced Encryption Standard

S-box **:** Substition Box

XSL **:** Extended Sparse Linearization

GF(2) **:** The Galois field of two elements

GF(2^4) **:** The Galois field of 16 elements with the irreducible polynomial $x^4 + x + 1$ over GF(2).

ACKNOWLEDGEMENTS

First of all, and above all, the author expresses his biggest thank to the almighty Allah.

The author wishes to express his deepest gratitude to his supervisor Prof. Dr. EROL YILMAZ for his guidance, advice, criticism, encouragements and insight throughout the research.

The author would also like to thank Prof. Dr. Harun KARSLI, Prof. Dr. Zafer ERCAN, and Assist. Prof. Dr. Serpil KARAGÖZ and Assoc. Prof. Dr. Tahire ÖZEN for their guidance.

It is the right time and the right place for the author, to thank the most generous and kind parents in the world, his father (Raheem), and his mother (Shukriya) for their being such amazing parents and educator; and his brothers for their being in his life, Mohammed, Ahmed, Azad, and Nawzad.

1. INTRODUCTION

Cryptography is the process of converting plaintext into ciphertext and vice-versa. Converting the plaintext into ciphertext is called encryption. The breaking of the ciphertext is called decryption. An algorithm for performing encryption and decryption is called cipher. There are basically two types of ciphers. While symmetric cipher has a single key used for both encryption and decryption, asymmetric cipher contains two keys, a public key for encryption and a secret key for decryption. Symmetric ciphers split into block ciphers and stream ciphers. Data is broken up into blocks and each block is encrypted and decrypted with the secret key in block ciphers. Each character is individually encrypted and decypted with a keystream varies in each step in stream ciphers.

The best known examples of block ciphers are the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). DES is published by USA National Bureau of Standards in 1977. After the DES was broken by using differential and linear attacks, it was replaced by the AES in 2000. The AES is still the most used block cipher.

Cryptanalysis is a branch of cryptography which focuses on breaking ciphers. Like many block ciphers, the design of AES contains highly algebraic structures. The algebraic properties of block ciphers have attracted the attention of cryptanalysts. They designed different algebraic attacks against block ciphers. The main idea is to write the encryption operations as a system of multivariate polynomial equations and then solve this system to recover the secret key. Algebraic attacks gave new perspectives in block cipher cryptanalysis.

Courtois and Peiprzyk developed an algebraic attack on AES [1]. They try to solve a large system of quadratic equations using Extended Sparse Linearization (XSL). Although it was later realized that the XSL method was useless, this study pioneered the use of computational algebra techniques in attacks on block ciphers. At this stage, Gröbner bases techniques came to the forward. Gröbner bases, introduced by Bucberger in his Ph. D. thesis [2], are special generating sets of polynomial ideals that can be used for solving systems of polynomial equations. Two block ciphers, Flurry and Curry, which are resistant against linear and

differential attacks but vulnerable to Gröbner bases attacks are developed in [3]. A zero dimensional Gröbner basis for AES-128 over $GF(2^8)$ is obtained in [4]. Similar studies have been done for AES-196 and AES-256 in [5] and [6] respectively. They all use a degree lexicographic order which can not be used for solving the system of polynomial equation. Hence these bases can not directly used for cryptanalysis of the AES systems. Although they proposed algebraic cryptanalysis schemes based on a Gröbner basis conversion, they have no practical use. Hence these Gröbner bases has no security implications for AES.

In cryptanalysis, one of the best ways to measure the performance of an attack is to test it on reduced versions of the cipher. The small scale variants of the AES is defined in [7]. After that, some of these variants were cryptanalyzed in [7] and [8]. Gröbner bases over $GF(2)$ for small scale variants variants are obtained in [9]. Using these Gröbner bases the authors were also go further in cryptanalyzing of the small scale variants of AES.

2. AIM AND SCOPE OF THE STUDY

In this thesis, it is aimed to compute Gröbner bases for small scale variants of AES to be used in cryptanalysis. We investigate the smale scale variants of AES in details in chapter 4. Then we obtain algebraic equations for them over $GF(2^4)$ in the first section of chapter 5. Since S-boxes are the only non-linear part of block ciphers, finding the polynomials that represent them is the most important part of finding algebraic equations. We use the Lagrange interpolation polynomials for S-box as they did in [4]. We also get algebraic equations over $GF(2)$ in the second section of chapter 5. We find the quadratic polynomials for S-box using linear algebra techniques. Then we use elimination theorem via Gröbner bases and express output variables as polynomials of input variables of S-box. Although the methods we used in this section show some similarities with [9], our study includes more detailed results.

3. GRÖBNER BASES

In this chapter, we will give a brief introduction to Gröbner bases. We refer the interested readers to [10] for a more detailed information about this topic.

3.1. Monomial Ordering and Division Algorithm

Definition 3.1. *A monomial in $x_1, x_2, \dots, x_n$ is the product of the form*

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$$

Where all exponents are non-negative integers. The total degree of this monomial is the sum $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

We can simplify the notation for monomials as follows: let $\alpha = (\alpha_1, \dots, \alpha_n)$ be the n-tuple of non-negative integers. Then we set

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}.$$

Definition 3.2. *A monomial ordering on $K[x_1, \dots, x_n]$ is any relation $>$ on $\mathbb{Z}_{\geq 0}^n$, or equivalently, any relation on set of monomials $x^\alpha, \alpha \in \mathbb{Z}_{\geq 0}^n$ satisfying*

- *$>$ is total order,*
- *If $\alpha > \beta$, then $\alpha + \gamma > \beta + \gamma$ for $\gamma \in \mathbb{Z}_{\geq 0}^n$,*
- *$>$ is a well ordering on $\mathbb{Z}_{\geq 0}^n$. That means every non empty set of $\mathbb{Z}_{\geq 0}^n$ has a smallest element*

The well ordering is important because

Lemma 3.3. *A monomial ordering $>$ is a well ordering on $\mathbb{Z}_{\geq 0}^n$ if and only if every decreasing sequence must terminate after finitely many steps.*

This lemma will guarantee that the division algorithm on $K[x_1, \dots, x_n]$ stops after finitely many steps.

There are several monomial orderings on $K[x_1, \dots, x_n]$ unlike polynomials of single variables where there is only one ordering. Now, we will define three of them.

Definition 3.4 (Lexicographic Order). *Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ we say $\alpha >_{lex} \beta$ if the first nonzero entry of $\alpha - \beta$ is positive.*

For example, $\alpha = (2,3,1) >_{lex} \beta = (1,2,5)$ since $\alpha - \beta = (1,1,-4)$.

Definition 3.5 (Graded Lexicographic Order). *Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ we say $\alpha >_{grlex} \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$.*

For example, $\alpha = (2,3,2) >_{grlex} \beta = (4,1,1)$ since $|\alpha| = 2 + 3 + 2 > |\beta| = 4 + +1 + 1$ or $\alpha = (2,3,5) >_{grlex} \beta = (2,2,6)$ since $|\alpha| = |\beta|$ but $\alpha >_{lex} \beta$.

Definition 3.5 (Graded Reverse Lexicographic Order). *Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ we say $\alpha >_{grevlex} \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the last nonzero entry of $\alpha - \beta$ is negative.*

For example, $\alpha = (2,6,3) >_{grlex} \beta = (5,2,4)$ since $|\alpha| = |\beta|$ and $\alpha - \beta = (-3,4,-1)$.

Definition 3.6. *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial and $>$ be monomial ordering*

- *The multidegree of f*

$$\text{multideg}\,(f) = \max\{\alpha : a_\alpha \neq 0\}$$

- *The leading coefficient of f*

$$\text{LC}\,(f) = a_{\text{multideg}(f)}$$

- *The leading monomial of f*

$$\text{LM}(f) = x^{\text{multideg}(f)}$$

- *The leading term of f*

$$\text{LT}(f) = \text{LC}(f)\text{LM}(f)$$

For example if $f = 5x^2y^3z^2 + 5z^3 - 6x^4 + 8x^3z^3$, then

order	multideg(f)	LC(f)	LM(f)	LT(f)
lex	(4,0,0)	-6	x^4	$-6x^4$
grlex	(3,0,3)	8	x^3z^3	$8x^3z^3$
grevlex	(2,3,2)	5	$x^2y^3z^2$	$5x^2y^3z^2$

Theorem 3.7 (Division Algorithm). *Fix a monomial ordering Let* $F = (f_1, \dots, f_s)$ *be the s-tuple of polynomials in* $K[x_1, \dots, x_n]$. *Then every* $f \in K[x_1, \dots, x_n]$ *can be written as*

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

Where $a_i, r \in K[x_1, \dots, x_n]$ *and either* $r = 0$ *or no term of* r *is divisible by* $LT(f_i)$ *for* $i = 1, \dots, s$. *Furthermore if* $a_i f_i \neq 0$, *then multideg*$(a_i f_i)$ < *multideg (f).*

The polynomial r is called the remainder of f upon division by F. the polynomials $a_1, \dots, a_s$ and the reaminder r can be computed by the following algorithm.

Table 3.1. Division Algorithm

Input: $f_1, \dots, f_s, f$

Output: $a_1, \dots, a_s, r$

$a_1 := 0, \dots, a_s := 0, \mathrm{h} := f$

WHILE h $\neq 0$ DO

IF there are $i's$ such that LT(f_i) |LT(h) THEN

Choose the least i satisfying this

$$a_i := a_i + \frac{\mathrm{LT(h)}}{\mathrm{LT}(f_i)}$$

$$\mathrm{h} := \mathrm{h} - \frac{\mathrm{LT(h)}}{\mathrm{LT}(f_i)} f$$

ELSE

$$r := r + \mathrm{LT}(f_i)$$
$$\mathrm{h} := \mathrm{h} - \mathrm{LT}(f_i)$$

3.2. Gröbner Bases

Definition 3.8. *Fix a monomial ordering. Let* $I \subset K[x_1, \dots, x_n]$ *be a non-zero ideal. The ideal of leading terms of* I *is the ideal generated by the set*

$$\mathrm{LT}(I) = \{\mathrm{LT}(f) : f \in I\}$$

And it is denoted by $\langle \mathrm{LT}(I) \rangle$.

If $I = \langle f_1, \dots, f_s \rangle$, then clearly $\langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s) \subset \langle \mathrm{LT}(I) \rangle$ but converse is not always true.

Definition 3.9. *Fix a monomial ordering. Let* $I \subset k[x_1, \dots, x_n]$ *be a non-zero ideal. A set of polynomials* $\{g_1, \dots, g_t\} \subset I$ *is called a Gröbner Basis for* I *if*

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t) \rangle.$$

The most important property of a Gröbner basis is that the reaminder of division of a polynomial by a Gröbner basis is unique. This is not always true for a general division on a several variable polynomial ring.

Definition 3.10. *Let* $f, g \in K[x_1, \dots, x_n]$ *be two nonzero polynomials. Fix a monomial ordering. Let* $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$. *The S-polynomial of* f *and* g *is*

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} f - \frac{x^\gamma}{\mathrm{LT}(g)} g.$$

Theorem 3.11 (Buchberger's Criterion). *The set* $G = \{g_1, g_2, \dots, g_s\} \subset K[x_1, \dots, x_n]$ *is a Gröbner basis for the ideal generated by* G *if and only if the remainder of the division of* $S(g_i, g_j)$ *by* G *is zero for* $1 \leq i < j \leq s$.

Lemma 3.12. *Let* $f, g \in K[x_1, \dots, x_n]$ *be two nonzero monic polynomials. Fix a monomial ordering. If* $\mathrm{LM}(f)$ *and* $\mathrm{LM}(g)$ *are relatively prime, then the remainder of the division of* $S(f, g)$ *by* $\{f, g\}$ *is zero.*

Proof. Since $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ are relatively prime,

$$\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{LM}(f)\mathrm{LM}(g).$$

Therefore

$$S(f, g) = \mathrm{LM}(g)f - \mathrm{LM}(f)g = -(g - \mathrm{LM}(g))f + (f - \mathrm{LM}(f))g.$$

Corollary 3.13. *If the leading monomials of the the monic polynomials* $G = \{g_1, g_2, \dots, g_s\}$ *are pairwise relatively prime, then* G *is a Gröbner basis.*

The following algorithm finds a Gröbner basis for an ideal starting from a given generating set of that ideal.

Table 3.2. Buchberger's Algorithm

Input: $F: = (f_1, f_2, \dots, f_s)$
Output: G, a Göbner Basis for $\langle F \rangle$
$G := F$
$B: = \{(i, j): 1 \leq i \leq j \leq s\}$
$t := s$
WHILE $B \neq \emptyset$
    Choose $(i, j) \in B$
    B: $= B - \{(i, j)\}$
    $r :=$ remainder of the division of $S(g_i, g_j)$ by G
    IF $r \neq 0$ THEN
        t: =t+1, B: $= B \cup \{(i, t): 1 \leq i < t\}$
        G: =G$\cup \{r\}$.

3.3. Zero Dimensional Ideals

Let $I \subseteq K[x_1, x_2, \dots, x_n]$ be an ideal and let G be a Gröbner basis for I. then $K[x_1, x_2, \dots, x_n]/I$ forms a vector space with a basis

$$B = \{x^\alpha : x^\alpha \notin \mathrm{LT}(I)\}.$$

Theorem 3.14. *Let* K *be algebraically closed field and let* $I \subseteq K[x_1, x_2, \dots, x_n]$ *be an ideal. Then the followings are equivalent*

i. *$K[x_1, x_2, \dots, x_n]/I$ is a finite dimensional vector space over K.*

ii. *If G is a Gröbner basis for I, then there are $g \in G$ and $\alpha_i \geq 0$ such that $LT(g) = x_i^{\alpha_i}$ for $1 \leq i \leq n$.*

iii. *The zero set $V(I) = \{a \in K^n : \forall f \in I, f(a) = 0\}$ is a finite set.*

Definition 3.15. *An ideal satisfying conditions given above theorem is called zero dimensional ideal.*

Definition 3.16. *If $I \subseteq K[x_1, x_2, \dots, x_n]$ is an ideal, then the i-th elimination ideal is*

$$I_i = I \cap K[x_{i+1}, x_{i+2}, \dots, x_n].$$

Theorem 3.17 (Elimination Theorem). If G is a Gröbner basis for $I \subseteq K[x_1, x_2, \dots, x_n]$ with respect to lex order with $x_1 > x_2 > \cdots > x_n$, then

$$G_i = G \cap K[x_{i+1}, x_{i+2}, \dots, x_n]$$

is a Gröbner basis for the elimination ideal I_i.

The Elimination theorem implies that a Gröbner basis induced by a lex order successively variables. This theorem therefore suggests the following strategy to solve a zero dimensional system of polynomial equation: Starting with the single variable equations, solve them. Then replace these solutions to other equations of the system. Apply the same process again and again until reaching the whole solution.

4. SMALL SCALE VARIANTS OF AES

In this chapter, the small scale variants of AES given in [7] will be examined in detail. While the number of variables and number of steps were reduced, the structure of AES preserved in these variants. Thus it will be possible to investigate the applicability of various algebraic cryptoanalysis methods on AES.

4.1 Parameters

We define two small scale variants of AES: SR(n, r, c, e) and SR$^*(n, r, c, e)$ which differ in the form of the final round. The parameters are

- n is number of rounds where $1 \leq n \leq 10$.
- r is number of rows of the input matrix where $r = 1,2$ or 4.
- c is number of columns of the input matrix where $c = 1,2$ or 4.
- e is the length (in bits) of each element of the input matrix where $e = 4$ or $e = 8$.

When $e = 8$, we use the field

$$GF(2^8) = {GF(2)[x]}\Big/{\langle x^8 + x^4 + x^3 + x + 1\rangle} \cong GF(2)(\theta)$$

where θ is a root of the Rijndael polynomial $x^8 + x^4 + x^3 + x + 1$ over $GF(2)$.

When $e = 4$, we use the field

$$GF(2^4) = {GF(2)[x]}\Big/{\langle x^4 + x + 1\rangle} \cong GF(2)(\rho)$$

where ρ is a root of the primitive polynomial $x^4 + x + 1$ over $GF(2)$. Let us take a closer look to this field.

We use hexadecimal notation when refering the elements of $GF(2^4)$ as follows: The coefficient vector of $\rho^3 + \rho + 1 \in GF(2)(\rho)$ is 1011 which corresponds to B in hexadecimal notation.

Let us give an example of multiplication of elements

$$B \otimes D = (\rho^3 + \rho + 1)(\rho^3 + \rho^2 + 1) = \rho^6 + \rho^5 + \rho^4 + \rho^3 + \rho^2 + \rho + 1$$

Now divide $\rho^6 + \rho^5 + \rho^4 + \rho^3 + \rho^2 + \rho + 1$ by $\rho^4 + \rho + 1$.

$$\rho^6 + \rho^5 + \rho^4 + \rho^3 + \rho^2 + \rho + 1 = (\rho^2 + \rho + 1)(\rho^4 + \rho + 1) + \rho^2 + \rho.$$

Hence

$$B \otimes D = \rho^6 + \rho^5 + \rho^4 + \rho^3 + \rho^2 + \rho + 1 \equiv \rho^2 + \rho \equiv 6$$

The complete addition and multiplication table of $GF(2^4)$ are given below.

Table 4.1. The Addition Table of $GF(2^4)$.

$\oplus$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Table 4.2. The Multiplication Table of $GF(2^4)$.

$\otimes$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

4.2 Round Operations

Each round in a scaled AES consists of some combination of the following operations:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

We will explain these operations only for $e = 4$. The case $e = 8$ uses the original AES 128 operations.

SubBytes operation applies an S-box operation to each element of the input matrix. S-box takes a 4-bit input $c_3c_2c_1c_0$ and return a 4-bit output $s_3s_2s_1s_0$ using the following transformation.

$$\begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Where $b_3b_2b_1b_0$ is multiplicative inverse of $c_3c_2c_1c_0$. Here we assume the inverse of 0000 is itself for the sake of completeness.

For example, take $5 \equiv 0101$ as an input. Its inverse is $B \equiv 1011$. Then

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Hence S-box maps 5 to $1110 \equiv E$. The following table gives S-box maps of each element.

Table 4.3. S-box Substition Table.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
6	B	5	4	2	E	7	A	9	D	F	C	3	1	0	8

The ShiftRows operation rotate row i of the input matrix by i positions to the left for $0 \leq i \leq r - 1$. For example if input matrix

$$\begin{bmatrix} A & 5 & E & 7 \\ 6 & C & 0 & 4 \\ F & 8 & 3 & D \\ 2 & B & 1 & 9 \end{bmatrix} \begin{matrix} \\ \rightarrow row1 \\ \rightarrow row2 \\ \rightarrow row3 \end{matrix} \rightarrow row0$$

Then after the ShiftRows operation the ouput matrix is

$$\begin{bmatrix} A & 5 & E & 7 \\ C & 0 & 4 & 6 \\ 3 & D & F & 8 \\ 9 & 2 & B & 1 \end{bmatrix}.$$

MixColumns operation multiplies of data by an invertible matrix which varies according to number of the rows of the data.

Table 4.4. MixColumns Multiplication Matrices.

Number of Rows	Matrix
1	(1)
2	$\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$
4	$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$

For example, take input matrix

$$\begin{bmatrix} A & 5 & E & 7 \\ C & 0 & 4 & 6 \\ 3 & D & F & 8 \\ 9 & 2 & B & 1 \end{bmatrix}.$$

Now apply MixColumns operation to each column of the input matrix.

$$\begin{pmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{pmatrix}\begin{pmatrix}A\\C\\3\\9\end{pmatrix}=\begin{pmatrix}(2\otimes A)\oplus(3\otimes C)\oplus(1\otimes 3)\oplus(1\otimes 9)\\(1\otimes A)\oplus(2\otimes C)\oplus(3\otimes 3)\oplus(1\otimes 9)\\(1\otimes A)\oplus(1\otimes C)\oplus(2\otimes 3)\oplus(3\otimes 9)\\(3\otimes A)\oplus(1\otimes C)\oplus(1\otimes 3)\oplus(2\otimes 9)\end{pmatrix}=\begin{pmatrix}A\\D\\8\\3\end{pmatrix}$$

$$\begin{pmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{pmatrix}\begin{pmatrix}5\\0\\D\\2\end{pmatrix}=\begin{pmatrix}(2\otimes 5)\oplus(3\otimes 0)\oplus(1\otimes D)\oplus(1\otimes 2)\\(1\otimes 5)\oplus(2\otimes 0)\oplus(3\otimes D)\oplus(1\otimes 2)\\(1\otimes 5)\oplus(1\otimes 0)\oplus(2\otimes D)\oplus(3\otimes 2)\\(3\otimes 5)\oplus(1\otimes 0)\oplus(1\otimes D)\oplus(2\otimes 2)\end{pmatrix}=\begin{pmatrix}5\\D\\A\\6\end{pmatrix}$$

$$\begin{pmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{pmatrix}\begin{pmatrix}E\\4\\F\\B\end{pmatrix}=\begin{pmatrix}(2\otimes E)\oplus(3\otimes 4)\oplus(1\otimes F)\oplus(1\otimes B)\\(1\otimes E)\oplus(2\otimes 4)\oplus(3\otimes F)\oplus(1\otimes B)\\(1\otimes E)\oplus(1\otimes 4)\oplus(2\otimes F)\oplus(3\otimes B)\\(3\otimes E)\oplus(1\otimes 4)\oplus(1\otimes F)\oplus(2\otimes B)\end{pmatrix}=\begin{pmatrix}7\\F\\9\\F\end{pmatrix}$$

$$\begin{pmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{pmatrix}\begin{pmatrix}7\\6\\8\\1\end{pmatrix}=\begin{pmatrix}(2\otimes 7)\oplus(3\otimes 6)\oplus(1\otimes 8)\oplus(1\otimes 1)\\(1\otimes 7)\oplus(2\otimes 6)\oplus(3\otimes 8)\oplus(1\otimes 1)\\(1\otimes 7)\oplus(1\otimes 6)\oplus(2\otimes 8)\oplus(3\otimes 1)\\(3\otimes 7)\oplus(1\otimes 6)\oplus(1\otimes 8)\oplus(2\otimes 1)\end{pmatrix}=\begin{pmatrix}D\\1\\1\\6\end{pmatrix}$$

Hence the output after MixColumns operation is

$$\begin{pmatrix}A&5&7&D\\D&D&F&1\\8&A&9&1\\3&6&F&6\end{pmatrix}.$$

AddRoundKey operation simultaneously adds a roundkey matrix to some intermediate matrix. Each SR(n,r,c,e) or SR$^*(n,r,c,e)$ has a initial roundkey matrix of size $r\times c$. Then each roundkey is then used to define the next roundkey as described below. The definition of the roundkey depends on the number of columns (c) in the array.

Table 4.5. Key Schedule.

Number of Columns	Input	Output
1	c_0	$l_0 = F_i(c_0)$
2	c_0, c_1	$l_0 = F_i(c_1)\oplus c_0$ $l_1 = l_0\oplus c_1$
4	c_0, c_1, c_2, c_3	$l_0 = F_i(c_3)\oplus c_0$ $l_1 = l_0\oplus c_1$ $l_2 = l_1\oplus c_2$ $l_3 = l_2\oplus c_3$

where

$$F_i(c_j) = \begin{pmatrix} \text{sbox}(c_{j0}) \\ \vdots \\ \vdots \\ \text{sbox}(c_{j,r-1}) \end{pmatrix} \oplus \begin{pmatrix} \kappa_i \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad \kappa_i = \rho^{i-1} \mod \rho^4 + \rho + 1.$$

Each small scaled AES has a user provided key of $r \times c \times e$ bits which is called initial sub key. The round keys can be found by using key schedule explained above. Let us start with the initial subkey

$$\begin{pmatrix} 1 & C & F & 7 \\ 3 & 0 & A & 2 \\ D & 4 & 9 & B \\ 8 & E & 5 & 6 \end{pmatrix}.$$

$$\ell_0 = \begin{pmatrix} \text{sbox}(7) \\ \text{sbox}(2) \\ \text{sbox}(B) \\ \text{sbox}(6) \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 3 \\ D \\ 8 \end{pmatrix} = \begin{pmatrix} A \\ 5 \\ C \\ 7 \end{pmatrix} \oplus \begin{pmatrix} 2 \\ 3 \\ D \\ 8 \end{pmatrix} = \begin{pmatrix} A \\ 6 \\ 1 \\ F \end{pmatrix},$$

$$\ell_1 = \begin{pmatrix} A \\ 6 \\ 1 \\ F \end{pmatrix} \oplus \begin{pmatrix} C \\ 0 \\ 4 \\ E \end{pmatrix} = \begin{pmatrix} 6 \\ 6 \\ 5 \\ 1 \end{pmatrix}, \ell_2 = \begin{pmatrix} 6 \\ 6 \\ 5 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} F \\ A \\ 9 \\ 5 \end{pmatrix} = \begin{pmatrix} 9 \\ C \\ C \\ 4 \end{pmatrix},$$

$$\ell_3 = \begin{pmatrix} 9 \\ C \\ C \\ 4 \end{pmatrix} \oplus \begin{pmatrix} 7 \\ 2 \\ B \\ 6 \end{pmatrix} = \begin{pmatrix} E \\ E \\ 7 \\ 2 \end{pmatrix}.$$

Hence the first round subkey is

$$\begin{pmatrix} A & 6 & 9 & E \\ 6 & 6 & C & E \\ 1 & 5 & C & 7 \\ F & 1 & 4 & 2 \end{pmatrix}.$$

The second round subkey can be similarly obtained from the first round subkey using the above formulas. This process repeat itself for n rounds.

Like in the original AES, the operation MixColumns is omitted on the last round of $\text{SR}^*(n, r, c, e)$ whereas MixColumns is contained in the final round of

SR(n, r, c, e). Hence AES is identical to SR$^*(10,4,4,8)$. We finish this chapter with a complete example of SR$^*(4,2,2,4)$.

Table 4.6. An Example of SR$^*(4,2,2,4)$

	Start of Round	After SubBytes	After ShiftRows	After MixColums		RoundKey
Round 0	$\begin{pmatrix} A & 3 \\ 7 & D \end{pmatrix}$				$\oplus$	$\begin{pmatrix} 5 & B \\ E & 2 \end{pmatrix}$
Round 1	$\begin{pmatrix} F & 8 \\ 9 & F \end{pmatrix}$	$\begin{pmatrix} 8 & 9 \\ D & 8 \end{pmatrix}$	$\begin{pmatrix} 8 & 9 \\ 8 & D \end{pmatrix}$	$\begin{pmatrix} 8 & 1 \\ 8 & 1 \end{pmatrix}$	$\oplus$	$\begin{pmatrix} 8 & 3 \\ B & 9 \end{pmatrix}$
Round 2	$\begin{pmatrix} 7 & B \\ 2 & 6 \end{pmatrix}$	$\begin{pmatrix} A & C \\ 5 & 7 \end{pmatrix}$	$\begin{pmatrix} A & C \\ 7 & 5 \end{pmatrix}$	$\begin{pmatrix} 3 & D \\ E & 4 \end{pmatrix}$	$\oplus$	$\begin{pmatrix} E & D \\ 6 & F \end{pmatrix}$
Round 3	$\begin{pmatrix} 9 & 6 \\ 4 & 9 \end{pmatrix}$	$\begin{pmatrix} D & 7 \\ 2 & D \end{pmatrix}$	$\begin{pmatrix} D & 7 \\ D & 2 \end{pmatrix}$	$\begin{pmatrix} D & D \\ D & 8 \end{pmatrix}$	$\oplus$	$\begin{pmatrix} B & 1 \\ E & 6 \end{pmatrix}$
Round 4	$\begin{pmatrix} 3 & 7 \\ A & F \end{pmatrix}$	$\begin{pmatrix} 4 & A \\ F & 8 \end{pmatrix}$	$\begin{pmatrix} 4 & A \\ 8 & F \end{pmatrix}$	No MixColumns on the final round	$\oplus$	$\begin{pmatrix} 5 & 4 \\ 9 & F \end{pmatrix}$

Output is

$$\begin{pmatrix} 1 & E \\ 1 & 0 \end{pmatrix}$$

5. ALGEBRAIC EQUATIONS FOR SMALL SCALE AES

For the small scaled AES, two different multivariate polynomial systems of equations can be considered. One can write polynomials over $GF(2^4)$ another is over $GF(2)$.

5.1 Algebraic Equations Over $GF(2^4)$

Since the S-box is the only non-linear part of AES, we start with writing an interpolation polynomial for the S-box.

Definition 5.1. *The Lagrange interpolation polynomial $L(x)$ that passes through $(x_0, y_0), (x_1, y_1), \dots, (x_k, y_k)$ is given by*

$$L(x) = \sum_{j=0}^{k} y_j \ell_j(x)$$

where

$$\ell_j(x) = \prod_{\substack{i=0 \\ i \neq j}}^{k} \frac{x - x_i}{x_j - x_i}.$$

Hence the interpolation polynomial for S-box can be found by

$$L(x) = \sum_{j=0}^{15} y_j \prod_{\substack{i=0 \\ i \neq j}}^{15} \frac{x - x_i}{x_j - x_i}$$

where

x_j	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
y_j	6	B	5	4	2	E	7	A	9	D	F	C	3	1	0	8

After making the necessary calculations over $GF(2^4)$,

$$L(x) = 5x^{14} + x^{13} + Cx^{11} + 5x^7 + 6.$$

We also need two find the interpolation polynomial for inverse of S-box. Interchanging roles of x_j's and y_j's in the above table the interpolation polynomial for inverse of S-box is

$$L^{-1}(x) = 5x^{14} + 2x^{13} + 2x^{12} + Ax^{11} + x^{10} + 7x^8 + x^6 + Bx^5 + Bx^4 + 6x^3 + Fx^2 + 3x + E$$

We will use a column vector instead of a matrix for the internal state and the round keys. This notation will allows us to express the MixColumns and ShiftRows operations as a single matrix multiplication. For example if we have the matrix

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix},$$

then we will represent it by the column vector

$$\begin{pmatrix} a_{00} \\ a_{10} \\ a_{01} \\ a_{11} \end{pmatrix}.$$

Therefore ShiftRow operation for $SR(n, 2,2,4)$ can be express as

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_{00} \\ a_{10} \\ a_{01} \\ a_{11} \end{pmatrix} = \begin{pmatrix} a_{00} \\ a_{11} \\ a_{01} \\ a_{10} \end{pmatrix}$$

and MixColumn operation can be express as multiplying by the matrix

$$\begin{pmatrix} 3 & 2 & 0 & 0 \\ 2 & 3 & 0 & 0 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 2 & 3 \end{pmatrix}.$$

The combination of two operation can be express as multiplying by the matrix

$$D = \begin{pmatrix} 3 & 2 & 0 & 0 \\ 2 & 3 & 0 & 0 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 & 2 \\ 2 & 0 & 0 & 3 \\ 0 & 2 & 3 & 0 \\ 0 & 3 & 2 & 0 \end{pmatrix}.$$

The inverse of D is

$$D^{-1} = \begin{pmatrix} 3 & 2 & 0 & 0 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 3 & 2 \\ 2 & 3 & 0 & 0 \end{pmatrix}$$

If the Mix column operation is omitted on the last round, then we use the matrix

$$\widetilde{D} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Notice that $\widetilde{D}^{-1} = \widetilde{D}$.

Similarly, ShiftRow operation for $SR(n, 4,4,4)$ can be express as

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_{00} \\ a_{10} \\ a_{20} \\ a_{30} \\ a_{01} \\ a_{11} \\ a_{21} \\ a_{31} \\ a_{02} \\ a_{12} \\ a_{22} \\ a_{32} \\ a_{03} \\ a_{13} \\ a_{23} \\ a_{33} \end{pmatrix} = \begin{pmatrix} a_{00} \\ a_{11} \\ a_{22} \\ a_{33} \\ a_{01} \\ a_{12} \\ a_{23} \\ a_{30} \\ a_{02} \\ a_{13} \\ a_{20} \\ a_{31} \\ a_{03} \\ a_{10} \\ a_{21} \\ a_{32} \end{pmatrix}$$

and MixColumn operation can be express as multiplying by the matrix

$$\begin{pmatrix} M & 0 & 0 & 0 \\ 0 & M & 0 & 0 \\ 0 & 0 & M & 0 \\ 0 & 0 & 0 & M \end{pmatrix}$$

where

$$M = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}.$$

Then

$$D = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 3 \\ 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 \end{pmatrix}$$

and

$$D^{-1} = \begin{pmatrix} 2 & 3 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 3 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 3 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 3 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Let $K = GF(2^4)$. Define the polynomial ring R as

$$R = K[x_{ij}: 0 \leq i \leq r \times c, 0 \leq j \leq n-1]$$

where $x_{ij}$is the ith component of the state vector after jth round and k_{ij} are key variables with same concept. In particular we call x_{i0}'s as plaintext variables, x_{in}'s as ciphertext variable and k_{i0}'s as cipher key variables.

One round operation can be described as

$$\begin{pmatrix} x_{0,j} \\ \vdots \\ x_{rc-1,j} \end{pmatrix} = D.\begin{pmatrix} L\left(x_{0,j-1} + k_{0,j-1}\right) \\ \vdots \\ L\left(x_{rc-1,j-1} + k_{rc-1,j-1}\right) \end{pmatrix}.$$

Hence the round polynomials for $1 \leq j \leq n-1$ can be written as

$$\begin{pmatrix} L\left(x_{0,j-1} + k_{0,j-1}\right) \\ \vdots \\ L\left(x_{rc-1,j-1} + k_{rc-1,j-1}\right) \end{pmatrix} + D^{-1}\begin{pmatrix} x_{0j} \\ \vdots \\ x_{rc-1,j} \end{pmatrix} \tag{5.1}$$

For the last round we also considering adding the final key

$$\begin{pmatrix} L\left(x_{0,n-1} + k_{0,n-1}\right) \\ \vdots \\ L\left(x_{rc-1,n-1} + k_{rc-1,n-1}\right) \end{pmatrix} + D^{-1}\begin{pmatrix} x_{0,n} + k_{0,n} \\ \vdots \\ x_{rc-1,n} + k_{rc-1,n} \end{pmatrix} \tag{5.2}$$

Notice that in SR$^*(n,r,c,4)$ we use the matrix $\widetilde{D}^{-1}$ instead of D^{-1} for the last round.

The key schedule operation can described as

$$\begin{pmatrix} k_{0,j} \\ \vdots \\ k_{c-1,j} \\ k_{c,j} \\ \vdots \\ k_{rc-1,j} \end{pmatrix} = \begin{pmatrix} k_{0,j-1} \\ \vdots \\ k_{c-1,j-1} \\ k_{c,j-1} \\ \vdots \\ k_{rc-1,j-1} \end{pmatrix} + \begin{pmatrix} L(k_{(r-1)c-1,j-1}) \\ \vdots \\ L(k_{rc-1,j-1}) \\ k_{0j} \\ \vdots \\ k_{(r-1)c-1,j-1} \end{pmatrix} + \begin{pmatrix} \rho^{j-1} \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

for $1 \leq j \leq n$. Therefore key schedule polynomials are

$$\begin{pmatrix} L^{-1}(k_{0,j} + k_{0,j-1} + \rho^{j-1}) \\ \vdots \\ L^{-1}(k_{c-1,j} + k_{c-1,j-1}) \\ k_{c,j} + k_{c,j-1} \\ \vdots \\ k_{rc-1,j} + k_{rc-1,j-1} \end{pmatrix} + \begin{pmatrix} k_{rc-1,j-1} \\ \vdots \\ k_{(r-1)c,j-1} \\ k_{0,j} \\ \vdots \\ k_{(r-1)c-1,j} \end{pmatrix} \tag{5.3}$$

for $1 \leq j \leq n$.

Let us order the variables as follows:

1. plaintext variables $x_{0,0} < \cdots < x_{rc-1,0}$
2. ciphertext variables $x_{0,n} < \cdots < x_{rc-1,n}$
3. key variables $k_{00} < k_{1,0} < \cdots < k_{rc-1,n}$
4. interstate variables $x_{1,0} < x_{2,0} < \cdots < x_{rc-2,n}$

Theorem 5.2. *The polynomials given in (5.1), (5.2) and (5.3) forms a Gröbner basis for the small scaled AES with respect to degree lexicographic ordering where variables are in the above given order. Moreover, the ideal generated by these polynomials is zero dimensional.*

Proof. Polynomials in (5.1), (5.2) and (5.3) has either x_{ij}^{14} or k_{ij}^{14} as a leading term. Furthermore, the leading terms are relatively prime. Hence Corollary 3.13 implies that they form a Gröbner basis and Theorem 3.13 implies that the ideal generated by these polynomials is zero dimensional.

5.2 Algebraic Equations Over $GF(2)$

A general quadratic polynomial in the polynomial ring

$$GF(2)[x, y] = GF(2)[x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3]$$

is of the form

$$f(x, y) = \sum_{j,k=0}^{3} a_{jk} x_j y_k + \sum_{j=0}^{3} b_j x_j + \sum_{k=0}^{3} c_k y_k + d$$

where $a_{jk}, b_j, c_k, d \in GF(2)$. Notice that since $u^2 = 1$ for all $u \in GF(2)$ we omit the terms x_j^2 and y_k^2 from the quadratic polynomial.

We say a map $T: GF(2)^4 \to GF(2)^4$ satisfied by the quadratic polynomial $f(x, y)$ if $f(u, v) = 0$ for all input u and corresponding output v of T. To find the system of quadratic equations satisfying T, we can use linear algebraic techniques. A quadratic polynomial $f(x, y)$ satisfies the T if and only if coffecients a_{jk}, b_j, c_k, d forms a solution to the following linear system.

$$f(u^{(i)}, v^{(i)}) = \sum_{j,k=0}^{3} a_{jk} u_j^{(i)} v_k^{(i)} + \sum_{j=0}^{3} b_j u_j^{(i)} + \sum_{k=0}^{3} c_k v_k^{(i)} + d$$

for $i = 0,1, \dots, 15$.

Inverse map in $GF(2^4)$ with binary representation for the small scaled AES given by the following table.

Table 5.1. Inverse Map Substition Table.

i	$u^{(i)}$	$v^{(i)}$	i	$u^{(i)}$	$v^{(i)}$
0	0000	0000	8	1000	1111
1	0001	0001	9	1001	0010
2	0010	1001	10	1010	1100
3	0011	1110	11	1011	0101
4	0100	1101	12	1100	1010
5	0101	1011	13	1101	0100
6	0110	0111	14	1110	0011
7	0111	0110	15	1111	1000

Hence the coefficient matrix of the linear system is

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&1&0&0&1&1\\
0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&1&1&1&1&1&0&1\\
0&0&0&0&1&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&1&1&0&1&1\\
0&0&0&0&1&0&1&1&0&0&0&0&1&0&1&1&0&1&0&1&1&0&1&1&1\\
0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&0&0&1&1&0&0&1&1&1&1\\
0&0&0&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&1&0&1&1&0&1\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&1&0&1\\
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&1&0&1&1&0&0&1\\
0&1&0&1&0&0&0&0&0&1&0&1&0&1&0&1&1&0&1&1&0&1&0&1&1\\
1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&1&0&1\\
0&1&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&1&0&1&0&1&0&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&0&0&1&1&1&0&0&0&1&1&1\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&1&1&1&1&0&0&0&1
\end{pmatrix}.$$

The null space of the matrix generated by the rows of the following matrix

$$Q = \begin{pmatrix}
1&0&0&0&0&0&1&1&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&1&0&1&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&1&0&0\\
1&1&0&1&0&0&1&1&1&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&1&0&0&0&1&1&0&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&1&0&1&0&0&1&0&1&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0\\
1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&0&0&1&1&1&1&1&1&0&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&1&1&0&1&1&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

Let $v = (x_j y_k, x_j, y_k, 1)$ for $0 \leq j, k \leq 3$. Then the quadratic polynomials satisfting the inverse map given by $Q.v$ which are

$$\{x_0y_0 + x_2y_0 + x_1y_1 + x_2y_1 + x_1y_3 + x_3y_3 + y_0,$$
$$x_1y_0 + x_2y_0 + x_1y_1 + x_2y_1 + x_3y_1 + x_1y_2 + x_1y_3 + x_2y_3 + y_1,$$
$$x_1y_0 + x_2y_0 + x_3y_0 + x_2y_1 + x_3y_2 + x_1y_3 + x_3y_3 + y_2,$$
$$x_1y_1 + x_2y_1 + x_1y_2 + x_2y_2 + x_3y_2 + x_1y_3 + y_3,$$
$$x_0y_0 + x_2y_0 + x_3y_1 + x_1y_2 + x_3y_2 + x_2y_3 + x_0,$$
$$x_1y_0 + x_1y_2 + x_2y_0 + x_2y_1 + x_2y_2 + x_3y_2 + x_3y_3 + x_1,$$
$$x_2y_0 + x_2y_1 + x_2y_2 + x_2y_3 + x_1y_0 + x_3y_0 + x_1y_1 + x_1y_3 + x_3y_3 + x_2,$$
$$x_3y_1 + x_1y_1 + x_2y_1 + x_1y_2 + x_2y_2 + x_2y_3 + x_3,$$
$$x_1y_0 + x_0y_1 + x_3y_1 + x_2y_2 + x_3y_2 + x_1y_3 + x_2y_3,$$
$$x_2y_0 + x_1y_1 + x_0y_2 + x_3y_2 + x_2y_3 + x_3y_3,$$
$$x_3y_0 + x_2y_1 + x_1y_2 + x_0y_3 + x_3y_3\ \}.$$

The Gröbner basis for ideal generated by these polynomials with respect to lex order $y_3 > y_2 > y_1 > y_0 > x_3 > x_2 > x_1 > x_0$ is

$$G = \{x_3^2 + x_3, x_2^2 + x_2, x_1^2 + x_1, x_0^2 + x_0, x_1x_2x_0 + x_2x_0 + x_0 + x_1 + x_1x_2 + x_2 + x_1x_2x_3 + x_3 + y_0,\ x_0x_1 + x_2x_1 + x_0x_3x_1 + x_3x_1 + x_0x_2 + x_3 + y_1, x_0x_1 + x_0x_2 + x_2 + x_0x_3 + x_0x_2x_3 + x_3 + y_2, x_2x_3x_1 + x_3x_1 + x_1 + x_2 + x_0x_3 + x_2x_3 + x_3 + y_3\}.$$

From G, output variables can be express as polynomial functions of input variables as follows:

$$y_0 = f_0(x_0, x_1, x_2, x_3) = x_1x_2x_0 + x_2x_0 + x_0 + x_1 + x_1x_2 + x_2 + x_1x_2x_3 + x_3$$
$$y_1 = f_1(x_0, x_1, x_2, x_3) = x_0x_1 + x_2x_1 + x_0x_3x_1 + x_3x_1 + x_0x_2 + x_3$$
$$y_2 = f_2(x_0, x_1, x_2, x_3) = x_0x_1 + x_0x_2 + x_2 + x_0x_3 + x_0x_2x_3 + x_3$$
$$y_3 = f_3(x_0, x_1, x_2, x_3) = x_2x_3x_1 + x_3x_1 + x_1 + x_2 + x_0x_3 + x_2x_3 + x_3$$

Hence S-box operation is

$$\text{sbox}\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} f_0(x_0, x_1, x_2, x_3) \\ f_1(x_0, x_1, x_2, x_3) \\ f_2(x_0, x_1, x_2, x_3) \\ f_3(x_0, x_1, x_2, x_3) \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

Each element of $GF(2^4)$ can be represented by a 4×1 column vector in $GF(2)$. Therefore the corresponding matrices for ShiftRow operations in $\text{SR}(n, 1,1,4), \text{SR}(n, 1,2,4)$ and $\text{SR}(n, 2,2,4)$ respectively are

$$I_4,\ \begin{pmatrix} I_4 & 0 \\ 0 & I_4 \end{pmatrix},\ \begin{pmatrix} I_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & I_4 \\ 0 & 0 & I_4 & 0 \\ 0 & I_4 & 0 & 0 \end{pmatrix}$$

where 0 is 4×4 zero matrix and I_4 is 4×4 identity matrix. Similarly, the Corresponding matrices for ShiftRow operations for $r = 1, r = 2$ and $r = 4$ respectively are

$$I_4,\ \begin{pmatrix} M_2 & M_3 \\ M_3 & M_2 \end{pmatrix},\ \begin{pmatrix} M_2 & M_3 & I_4 & I_4 \\ I_4 & M_2 & M_3 & I_4 \\ I_4 & I_4 & M_2 & M_3 \\ M_3 & I_4 & I_4 & M_2 \end{pmatrix}$$

where M_2 and M_3 are 4×4 matrices which carry the multiplication by 2 and 3 in $GF(2^4)$ into $GF(2)$. Let us find these matrices. Suppose that

$$M_2 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}.$$

Since $2 \otimes 1 = 1$,

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \Longrightarrow a_{11} = a_{31} = a_{41} = 0, a_{21} = 1.$$

Since $2 \otimes 2 = 4$,

$$\begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ 1 & a_{22} & a_{23} & a_{24} \\ 0 & a_{32} & a_{33} & a_{34} \\ 0 & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \Longrightarrow a_{12} = a_{22} = a_{42} = 0, a_{32} = 1.$$

Since $2 \otimes 4 = 8$,

$$\begin{pmatrix} 0 & 0 & a_{13} & a_{14} \\ 1 & 0 & a_{23} & a_{24} \\ 0 & 1 & a_{33} & a_{34} \\ 0 & 0 & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \Longrightarrow a_{13} = a_{23} = a_{33} = 0, a_{43} = 1.$$

Since $2 \otimes 8 = 3$,

$$\begin{pmatrix} 0 & 0 & 0 & a_{14} \\ 1 & 0 & 0 & a_{24} \\ 0 & 1 & 0 & a_{34} \\ 0 & 0 & 1 & a_{44} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \Longrightarrow a_{14} = a_{24} = 1, a_{34} = a_{44} = 0.$$

So

$$M_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

One can check that this matrix satisfies all other multiplication operations. Similarly

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Then corresponding matrices for combination of ShiftRow and MixColumn operations in $\mathrm{SR}(n, 1,1,4), \mathrm{SR}(n, 1,2,4)$ and $\mathrm{SR}(n, 2,2,4)$ respectively are

$$D = I_4, \qquad D = \begin{pmatrix} M_2 & M_3 \\ M_3 & M_2 \end{pmatrix}, \qquad D = \begin{pmatrix} M_2 & I_4 & I_4 & M_3 \\ I_4 & I_4 & M_3 & M_2 \\ I_4 & M_3 & M_2 & I_4 \\ M_3 & M_2 & I_4 & I_4 \end{pmatrix}.$$

Let $K = GF(2)$. Define the polynomial ring

$$R = K[x_i, y_i, k_i : 0 \le i \le n]$$

where y_0 is plaintext variable, y_n is ciphertext variable, x_i's are intermediate varibles corresponding beginning value of each round, y_i's are intermediate varibles corresponding value after SubBytes operation of each round and k_i's are key variables. Notice that each variable is in fact a vector of variables. For example

$$x_0 = (x_{0,0,0}, \dots, x_{0,0,3}, \dots, x_{0,rc-1,0}, \dots, x_{0,rc-1,3}).$$

Then the following algebraic equation represent $\mathrm{SR}(n, r, c, 4)$.

$$x_0 = y_0 + k_0 \tag{5.4}$$

$$y_i = \mathrm{sbox}(x_{i-1}) \qquad 1 \le i \le n \tag{5.5}$$

$$k_i = T(k_{i-1}) \qquad 1 \le i \le n \tag{5.6}$$

$$x_i = Dy_i + k_i \qquad 1 \le i \le n \tag{5.7}$$

$$y_n = x_n + k_n \tag{5.8}$$

where T is given by

$$\begin{pmatrix} k_{0,j-1} \\ \vdots \\ k_{c-1,j-1} \\ k_{c,j-1} \\ \vdots \\ k_{rc-1,j-1} \end{pmatrix} + \begin{pmatrix} \mathrm{sbox}(k_{(r-1)c-1,j-1}) \\ \vdots \\ \mathrm{sbox}(k_{rc-1,j-1}) \\ k_{0j} \\ \vdots \\ k_{(r-1)c-1,j-1} \end{pmatrix} + \begin{pmatrix} \rho^{j-1} \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}.$$

Theorem 5.3. *The equations (5.4) to (5.8) forms a Gröbner basis for the small scaled AES with respect to lexicographic ordering with* $k_0 < y_0 < x_0 < \cdots < k_n < y_n < x_n$. *Moreover, the ideal generated by these polynomials is zero dimensional.*

Proof. Equations (5.4) to (5.8) has either x_i, y_i or k_i as a leading term. Furthermore, the leading terms are relatively prime. Hence Corollary 3.13 implies that they form a Gröbner basis and Theorem 3.13 implies that the ideal generated by these polynomials is zero dimensional.

6. CONCLUSIONS AND RECOMMENDATIONS

One of the purposes of cryptanalysis is to obtain the key of the cipher using known plaintexts and ciphertexts. For this, it is necessary to compute the Gröbner base under the lexicographic order of the corresponding polynomial system. Gröbner basis given in [4] with respect to degree lexicographic order. They failed to convert the existing Gröbner basis to a Gröbner basis under the lex order because this base contains high degree polynomials that depend on many variables. They were not able to translate their findings into a successful cryptanalysis.

Similar to what they did, we were able to obtain Gröbner bases for small scale variants of AES under the degree lexicographic order. Naturally, our polynomials are of lower degree and contain fewer variables. However, despite trying various conversion techniques, we were also unable to obtain a Gröbner basis with respect to lexicographic order. We think that the reason for this is that the processors and memory of the computers we have are not sufficient for this kind of computations. We believe that the desired results can be achieved by using more powerful computers and more advanced techniques. The results obtained in this thesis will be a starting point for such a study.

7. REFERENCES

Vancouver citation system was used in this thesis.

1. Buchbergers, B., Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal, J. Symb. Comput. 2006; 41(3-4), 475–511.

2. Courtois, N. and Pieprzyk, J., Cryptanalysis of block ciphers with overdefined systems of equations, In Proc. of ASIACRYPT, Lecture Notes in Computer Science (2501). 2002; p 267–287.

3. Buchmann, J., Pyshkin, A., Weinmann, RP. Block ciphers sensitive to Gröbner basis attacks, In Proc. of CT-RSA 2006, Lecture Notes in Computer Science(3806). 2006; p 313–331.

4. Buchmann, J., Pyshkin, A., Weinmann, RP. A zero-dimensional Groebner basis for AES-128; In: FSE 2006, Lecture Notes in Computer Science (4047); 2006. p. 78–88.

5. Cui, J., Huang, L., Zhong, H., Yang, W. Algebraic attack on Rijndael-192 based on Grobner basis; Acta Electronica Sinica. 2013; 41(5), 833–839.

6. Zhao, K., Cui, J., Xie, Z., Algebraic Cryptanalysis Scheme of AES-256 Using Gröbner Basis, Journal of Electrical and Computer Engineering. 2017; Article ID 9828967, 9 pages.

7. Cid, C., Murphy, S., Robshaw, M., Small Scale Variants of the AES, In: FSE2005, Lecture Notes in Computer Science (3557). 2005; p. 145-162.

8. Cid, C., Murphy, S., Robshaw, M., Algebraic Aspects of the Advanced Encryption Standard. Springer-Verlag, 2006.

9. Bulygin, S., Brickenstein, M., Obtaining and solving systems of equations in key variables only for the small variants of AES, Mathematics in Computer Science. 2010; 4 (2), 359-383.

10. Cox, DA., Little, JB., O'Shea, D., Ideals, Varieties and Algorithms. Springer-Verlag, 2007.

8. APPENDICES

Appendix 1: The Mathematica Codes for Lagrange Interpolation Polynomial Computations.

```
list = { 0, 1, y, y + 1, y^2, y^2 + 1, y^2 + y, y^2 + y + 1, y^3, y^3 + 1, y^3 + y,
   y^3 + y + 1, y^3 + y^2, y^3 + y^2 + 1, y^3 + y^2 + y, y^3 + y^2 + y + 1} ;

k[ j_] := (∏_{i=1}^{16} (list[[i]] + list[[j]])) / (2 list[[j]]) ;

l[ j_] := (∏_{i=1}^{16} (x + list[[i]])) / (x + list[[j]])

llist = Table[ Table[ PolynomialMod[ Coefficient[ l[ j] , x, i] , y^4 + y + 1, Modulus → 2] ,
    {i, 0, 15}] , {j, 1, 16}] ;

slist = list[[{7, 12, 6, 5, 3, 15, 8, 11, 10, 14, 16, 13, 4, 2, 1, 9}]] ;

table = Table[ PolynomialMod[ slist[[i]] llist[[i]] , y^4 + y + 1, Modulus → 2] , {i, 1, 16}] ;

q = PolynomialMod[ Apply[ Plus, table] , y^4 + y + 1, Modulus → 2]
{y + y^2, 0, 0, 0, 0, 0, 0, 1 + y^2, 0, 0, 0, y^2 + y^3, 0, 1, 1 + y^2, 0}

poly[ x_] := (1 + y^2) x^14 + x^13 + (y^2 + y^3) x^11 + (1 + y^2) x^7 + y + y^2

poly[ x] /. y → 2
6 + 5 x^7 + 12 x^11 + x^13 + 5 x^14

slist1 = list[[{15, 14, 5, 13, 4, 3, 1, 7, 16, 9, 8, 2, 12, 10, 6, 11}]] ;

table1 = Table[ PolynomialMod[ slist1[[i]] llist[[i]] , y^4 + y + 1, Modulus → 2] ,
   {i, 1, 16}] ;

q1 = PolynomialMod[ Apply[ Plus, table1] , y^4 + y + 1, Modulus → 2] ;

poly1[ x_] := Sum[ q1[[i + 1]] x^i , {i, 1, 15}] + y + y^2 + y^3

poly1[ x] /. y → 2
14 + 3 x + 15 x^2 + 6 x^3 + 11 x^4 + 11 x^5 + x^6 + x^7 + 7 x^8 + x^10 + 10 x^11 + 2 x^12 + 2 x^13 + 5 x^14
```

Appendix 2: The Mathematica Codes for Quadratic Polynomial and Gröbner Basis Computations for Inverse Map.

```
W = {{0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1},
     {0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1},
     {0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1},
     {0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1},
     {0,0,1,1,1,1,0,0,1,0,1,0,1,0,0,1},
     {0,0,0,1,1,0,1,1,1,0,1,1,0,1,0,0},
     {0,0,0,1,0,1,1,1,1,1,0,0,1,0,1,0},
     {0,1,1,0,1,1,1,0,1,0,0,1,0,0,1,0}};

T = Join[Join[Flatten[Table[W[[i]] W[[j]], {i, 1, 4}, {j, 5, 8}], 1], W],
   {Table[1, {16}]}];

Q = NullSpace[Transpose[T], Modulus -> 2];

list = {x3 y3, x3 y2, x3 y1, x3 y0, x2 y3, x2 y2, x2 y1, x2 y0, x1 y3, x1 y2, x1 y1,
   x1 y0, x0 y3, x0 y2, x0 y1, x0 y0, x3, x2, x1, x0, y3, y2, y1, y0, 1};

p = Q.list
```

$$\{y_0,\ x_0y_0,\ x_2y_0,\ x_1y_1,\ x_2y_1,\ x_1y_3,\ x_3y_3,$$
$$x_1y_0,\ x_2y_0,\ y_1,\ x_1y_1,\ x_2y_1,\ x_3y_1,\ x_1y_2,\ x_1y_3,\ x_2y_3,$$
$$x_1y_0,\ x_2y_0,\ x_3y_0,\ x_2y_1,\ y_2,\ x_3y_2,\ x_1y_3,\ x_3y_3,$$
$$x_1y_1,\ x_2y_1,\ x_1y_2,\ x_2y_2,\ x_3y_2,\ y_3,\ x_1y_3,\ x_0,\ x_0y_0,\ x_2y_0,\ x_3y_1,\ x_1y_2,\ x_3y_2,\ x_2y_3,$$
$$x_1,\ x_1y_0,\ x_2y_0,\ x_2y_1,\ x_1y_2,\ x_2y_2,\ x_3y_2,\ x_3y_3,$$
$$x_2,\ x_1y_0,\ x_2y_0,\ x_3y_0,\ x_1y_1,\ x_2y_1,\ x_2y_2,\ x_1y_3,\ x_2y_3,\ x_3y_3,$$
$$x_3,\ x_1y_1,\ x_2y_1,\ x_3y_1,\ x_1y_2,\ x_2y_2,\ x_2y_3,\ x_1y_0,\ x_0y_1,\ x_3y_1,\ x_2y_2,\ x_3y_2,\ x_1y_3,\ x_2y_3,$$
$$x_2y_0,\ x_1y_1,\ x_0y_2,\ x_3y_2,\ x_2y_3,\ x_3y_3,\ x_3y_0,\ x_2y_1,\ x_1y_2,\ x_0y_3,\ x_3y_3\}$$

```
GroebnerBasis[p, {y3, y2, y1, y0, x0, x1, x2, x3}, Modulus -> 2]
```

$$\{x_3,\ x_3^2,\ x_2,\ x_2^2,\ x_1,\ x_1^2,\ x_0,\ x_0^2,\ x_1,\ x_2,\ x_0x_2,\ x_1x_2,\ x_0x_1x_2,\ x_3,\ x_1x_2x_3,\ y_0,$$
$$x_0x_1,\ x_0x_2,\ x_1x_2,\ x_3,\ x_1x_3,\ x_0x_1x_3,\ y_1,\ x_0x_1,\ x_2,\ x_0x_2,\ x_3,\ x_0x_3,\ x_0x_2x_3,\ y_2,$$
$$x_1,\ x_2,\ x_3,\ x_0x_3,\ x_1x_3,\ x_2x_3,\ x_1x_2x_3,\ y_3\}$$