ATILIM UNIVERSITY

DEPARTMENT of MATHEMATICS

MATH 411 Seminar Studies

Project Report

Mathematics in AES

Submitted by: Mert NAR

Instructor: Burcu GULMEZ TEMUR

23 January 2015

Contents

1 ABSTRACT

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. In this report our aim is to give the mathematical background needed in advanced Encryption standard(AES). AES is a symmetric block cipher created by some mathematical knowledge, especially Finite Fields. In the Rijndael document, computational definitions and notions are emphasized and mathematics that is at background of standard is not defined comprehensively. On this document, we will try to explain the mathematical meaning of computational operations in AES.

2 DEFINITIONS And NOTIONS

Byte: Is a unit of digital information in computing and telecommunications that consists of eight bits.

Byte Level: characterize the bitwise operators' logical counterparts, the AND, OR and NOT operators.

Word: 4-byte vectors

Polynomial Representation: Bytes are shown as polynomial from the field isomorphic to $\mathbb{F}_{2^8}$

EXOR: Is a digital logic that implements an exclusive or; take bits of bytes as input

State: Is the intermediate cipher result

3 MATHEMATICAL BACKGROUND

In this section we will give all necessary definitions and results that we need in order to analyze how AES works.

3.1 Definitions and Theorems

Definition 3.1 *A **ring** R is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all a, b, c in R:*

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. *There is an additive identity 0. That is, there is an element* 0 *in* R *such that* $a + 0 = a$ *for all* a *in* R.
4. *There is an element* $-a$ *in* R *such that* $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$.

Definition 3.2 *A subset S of a ring R is called a **subring** of R provided S is closed under $+$ and $\cdot$ and forms a ring under these operations.*

Definition 3.3 *A subset J of a ring R is called an **ideal** provided J is a subring of R and for all $a \in J$ and $r \in R$ we have $ar \in J$ and $ra \in J$.*

Definition 3.4 *Let R be a commutative ring. An ideal J of R is said to be **principal** if there is an $a \in R$ such that $J = (a)$. In this case, J is also called the **principal ideal generated by** a .*

Definition 3.5 *The ring of residue classes of the ring R modulo the ideal J under the operations*

$$(a + J) + (b + J) = (a + b) + J$$

$$(a + J)(b + J) = ab + J$$

*is called the **factor ring** of R modulo J and is denoted by R/J.*

Definition 3.6 *A **field** is a commutative ring with identity in which every nonzero element has a multiplicative inverse.*

Definition 3.7 *The ring formed by the polynomials over R with the below operations is called the* ***polynomial ring*** *over R and denoted by R[x].*

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

$$g(x) = \sum_{i=0}^{m} b_i x^i$$

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k,$$

where

$$c_k = \sum_{i+j=k} a_i b_j,\ 0 \leq i \leq n, 0 \leq j \leq n$$

Definition 3.8 *A polynomial $p(x) \in F[x]$ is said to be* ***irreducible over a field*** *F* ***(or irreducible in*** *$F[x]$****, or prime in*** *$F[x]$* ***)*** *if p has positive degree and $p = bc$ with $b, c \in F[x]$ implies that either b or c is a constant polynomial.*

Theorem 3.9 *Any polynomial $f \in F[x]$ of positive degree can be written in the form*

$$f = ap_1^{e_1} ... p_k^{e_k}$$

where $a \in F$, $p_1, ...p_k$ are distinct monic irreducible polynomials in $F[x]$, and $e_1, ..., e_k$ are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.

Proof. reference to [[1], 1.59, p.23] ■

Theorem 3.10 *For $f \in F[x]$, the factor ring $F[x]/(f)$ is a field if and only if f is irreducible over F.*

Proof. reference to [[1], 1.61, p.25] ■

Definition 3.11 *Let K be a subfield of F and $\theta \in F$. If θ satisfies a nontrivial polynomial equation with coefficients in K, that is, if*

$$a_n\theta^n + ... + a_1\theta + a_0 = 0$$

*with $a_i \in K$ not all being 0, then θ is said to be **algebraic over** K . An extension L of K is called algebraic over K (or an algebraic extension of K) if every element of L is algebraic over K.*

Definition 3.12 *If $\theta \in F$ is algebraic over K, then the uniquely determined monic polynomial $g \in K[x]$ generating the ideal $J = \{f \in K[x] : f(\theta) = 0\}$ of $K[x]$ is called the **minimal polynomial (or defining polynomial, or irreducible polynomial)** of θ over K. By the degree of θ over K we mean the degree of g.*

Theorem 3.13 *If $\theta \in F$ is algebraic over K, then its minimal polynomial g over K has the following properties:*

1. *g is irreducible in $K[x]$*
2. *For $f \in K[x]$ we have $f(\theta) = 0$ if and only if g divides f.*
3. *g is the monic polynomial in $K[x]$ of least degree having θ as a root.*

Proof. reference to [[1], 1.82, p.31] ■

Definition 3.14 *Let L be an extension field of K. If L, considered as a vector space over K, is finite dimensional, then L is called a **finite extension of** K . The dimension of the vector space L over K is then called the degree of L over K, in symbol $[L : K]$*

Theorem 3.15 *Let $\theta \in F$ be algebraic of degree n over K and let g be the minimal polynomial of θ over K. Then:*

1. *$K(\theta)$ is isomorphic to $K[x]/(g)$.*
2. *$[K(\theta) : K] = n$ and $\{1, \theta, ..., \theta^{n-1}\}$ is a basis of $K(\theta)$ over K.*

3. Every $\alpha \in K(\theta)$ is algebraic over K and its degree over K is a divisor of n.

Proof. reference to [[1], 1.86, p.33] ■

Definition 3.16 *For a prime p, let $\mathbb{F}_p$ be the set $\{0, 1, ..., p-1\}$ of integers and let*

$$\varphi : \mathbb{Z}/(p) \to \mathbb{F}_p$$

*be the mapping defined by $\varphi([a]) = a$ for $a = \{0, 1, ..., p-1\}$. Then $\mathbb{F}_p$, endowed with the field structure induced by φ , is a finite field, called the **Galois field of order** p .*

Definition 3.17 *A primitive element of a finite field is a generator of the multiplicative group of the field.*

Theorem 3.18 *For every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.*

Proof. reference to [[1], 2.8, p.47] ■

3.2 Construction of $\mathbb{F}_{2^8}$ by $m(x)$

$m(x) \in F_2[x]$ is given as:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

3.2.1 $m(x)$ is Irreducible

Assume that $m(x) = f(x)g(x)$, for some $f, g \in \mathbb{F}_2[x]$; $f \neq g$ and f is irreducible without loss of generally. Then we have the following possibilities:

- $degf(x) = 1, degg(x) = 7$
- $degf(x) = 2, degg(x) = 6$
- $degf(x) = 3, degg(x) = 5$
- $degf(x) = 4, degg(x) = 4$

If $deg(f(x)) = n$ then irreducible polynomials over $\mathbb{F}_2[x]$ are;

for $n = 1$; $1 + x$, x

for $n = 2$; $1 + x + x^2$

for $n = 3$; $1 + x + x^3$, $1 + x^2 + x^3$

for $n = 4$; $1 + x + x^4$, $1 + x + x^2 + x^3 + x^4$, $1 + x^3 + x^4$

We need to show m(x) = f(x)g(x) + r(x) where r(x) is not the zero polynomial in $\mathbb{F}_2[x]$.

If $f(x) = x+1$ then $x^8 + x^4 + x^3 + x + 1 = (x+1)(x^7 + x^6 + x^5 + x^4 + x^2 + x) + 1$ so $r(x) = 1$ is not zero polynomial.

If $f(x) = x$ then $x^8 + x^4 + x^3 + x + 1 = (x)(x^7 + x^3 + x^2 + 1) + 1$ so $r(x) = 1$ is not zero polynomial.

If $f(x) = 1 + x + x^2$ then $x^8 + x^4 + x^3 + x + 1 = (x^2 + x + 1)(x^6 + x^5 + x^3) + x + 1$ so $r(x) = x + 1$ is not zero polynomial.

If $f(x) = 1 + x + x^3$ then $x^8 + x^4 + x^3 + x + 1 = (1 + x + x^3)(x^5 + x^3 + x^2 + 1) + x^2$ so $r(x) = x^2$ is not zero polynomial.

If $f(x) = 1 + x^2 + x^3$ then $x^8 + x^4 + x^3 + x + 1 = (1 + x^2 + x^3)(x^5 + x^4 + x^3) + x + 1$ so $r(x) = x + 1$ is not zero polynomial.

If $f(x) = 1+x+x^4$ then $x^8+x^4+x^3+x+1 = (1+x+x^4)(x^4)+x^3+x^2+1$ so $r(x) =)x^3+x^2+1$ is not zero polynomial.

If $f(x) = 1+x+x^2+x^3+x^4$ then $x^8+x^4+x^3+x+1 = (1+x+x^2+x^3+x^4)(x^4+x^3+x+1)+x^2$ so $r(x) = x^2$ is not zero polynomial.

If $f(x) = 1 + x^3 + x^4$ then $x^8 + x^4 + x^3 + x + 1 = (1 + x^3 + x^4)(x^4 + x^3 + x + 1) + x^3 + x^2$ so $r(x) = x^3 + x^2$ is not zero polynomial.

Therefore m(x) is irreducible. Let α be a root of m(x), that is $m(\alpha) = 0$, then we have;

$$\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$$

$$\alpha^9 = \alpha^5 + \alpha^4 + \alpha^2 + \alpha$$

$$\alpha^{10} = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2$$

$$\alpha^{11} = \alpha^7 + \alpha^6 + \alpha^4 + \alpha^3$$

$$\alpha^{12} = \alpha^8 + \alpha^7 + \alpha^5 + \alpha^4 = \alpha^7 + \alpha + 1$$

$$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + 1$$

$$\alpha^{14} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$$

.

.

.

$$\alpha^{255} = 1$$

$$\alpha^{256} = \alpha$$

So α is a primitive element of $\mathbb{F}_{2^8}$, that is

$$\mathbb{F}_{2^8}^* = \mathbb{F}_{2^8} - \{0\} =< \alpha >,$$

and we have

$$\mathbb{F}_{2^8} = \mathbb{F}_2(\alpha) = \{a_7\alpha^7 + a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha^1 + a_0 | a_i \in \mathbb{F}_2\}$$

Thus, by Theorem 3.16 we obtain

$$\mathbb{F}_2[x]/(m(x)) \cong \mathbb{F}_2(\alpha) = \mathbb{F}_{2^8}$$

3.3 Polynomial Representation of a Byte and Operations

All byte can be represented as a polynomial in $\mathbb{F}_2[x]/(m(x))$. Bytes are elements of ${\mathbb{F}_2}^8$. We define a map

$$\Psi : \mathbb{F}_2^8 \to \mathbb{F}_2[x]/(m(x))$$

$$s = (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7) \longmapsto b(x)$$

where $b(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$.

3.3.1 Addition

In the polynomial representation, the sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 (i.e., $1 + 1 = 0$) of the coefficients of the two terms[2].

Example 3.19 *In hexadecimal notation A7 + 83 = 24, or with the polynomial notation:*

$$(x^7 + x^5 + x^2 + x + 1) + (x^7 + x + 1) = x^5 + x^2$$

In binary notation we have: 10100111 + 10000011 = 00100100. Clearly, the addition corresponds with the simple bitwise EXOR at the byte level.

3.3.2 Multiplication

Unlike for addition, there is no simple operation at byte level. In the polynomial representation, multiplication in $\mathbb{F}_{2^8}$ corresponds with multiplication of polynomials modulo an irreducible binary polynomial of degree 8. For Rijndael, this polynomial is called $m(x)$ and given by

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

or 11B in hexadecimal representation [2].

Example 3.20 $57 \bullet 83 = C1$*, or:*

$$(x^6+x^4+x^2+x+1)(x^7+x+1) = x^{13}+x^{11}+x^9+x^8+x^7+x^7+x^5+x^3+x^2+x+x^6+x^4+x^2+x+1$$

$$= x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1(mod\ m(x))$$

$$= x7 + x6 + 1$$

Clearly, the result will be a binary polynomial of degree below 8.

3.3.3 Multiplication Inverse

The multiplication defined above is associative and there is a neutral element (01). For any binary polynomial $b(x)$ of degree below 8, the extended algorithm of Euclid can be used to compute polynomials $a(x)$, $c(x)$ such that

$$b(x)a(x) + m(x)c(x) = 1$$

. Hence,

$$a(x)b(x)\ (mod\ m(x))\ = 1$$

or

$$b^{-1}(x) = a(x)(mod\ m(x))$$

Moreover, it holds that $a(x)(b(x)+c(x)) = a(x)b(x)+a(x)c(x)$. It follows that the set of 256 possible byte values, with the EXOR as addition and the multiplication defined as above has the structure of the finite field $\mathbb{F}_{2^8}$ [2].

3.3.4 Multiplication by x

If we multiply b(x) by the polynomial x, we have:

$$b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x$$

$xb(x)$ is obtained by reducing the above result modulo $m(x)$.This operation is reflecting to computation as shifting byte left and If $b_7 = 1$, $m(x)$ must be subtracted (i.e., EXORed) [2].

Example 3.21 *In polynomial notation, let* $b(x) = x^7 + x^5 + x^2 + x + 1$.*By multiplying by x,*

$$b'(x) = x^8 + x^6 + x^3 + x^2 + x$$

$$b''(x) = x^6 + x^4 + x^2 + 1(mod\ m(x))$$

$$b'(x) - m(x) = x^8 + x^6 + x^3 + x^2 + x - (x^8 + x^4 + x^3 + x + 1)$$

We are working on $\mathbb{F}_2$ *so subtraction means EXOR, then*

$$b'(x) - m(x) = x^6 + x^4 + x^2 + 1$$

3.4 Construction of Factorial Ring $\mathbb{F}(\alpha)[x]/(x^4 + 1)$

There are four words of a state, say that

$$w_0 = (s_0, s_1, s_2, s_3)$$

$$w_1 = (s_4, s_5, s_6, s_3)$$

$$w_2 = (s_8, s_9, s_{10}, s_{11})$$

$$w_3 = (s_{12}, s_{13}, s_{14}, s_{15}),$$

where s_i are bytes of state.

Each word, say w_i, consists of 4 byte, i.e. $w_i \in \mathbb{F}_{2^8}^4$

However, we need to consider word as polynomial for word based transformations(such as mixColumn). So there is another need of ring to work on. By using same primitive element α, we define a map

$$\mathbb{F}_{2^8}^4 \longrightarrow \mathbb{F}(\alpha)[x]/(x^4+1)$$

$$w_0 \longmapsto w_0(x) = s_3(\alpha)x^3 + s_2(\alpha)x^2 + s_1(\alpha)x + s_0(\alpha)$$

$$w_1 \longmapsto w_1(x) = s_7(\alpha)x^3 + s_6(\alpha)x^2 + s_5(\alpha)x + s_4(\alpha)$$

$$w_2 \longmapsto w_2(x) = s_{11}(\alpha)x^3 + s_{10}(\alpha)x^2 + s_9(\alpha)x + s_8(\alpha)$$

$$w_3 \longmapsto w_3(x) = s_{15}(\alpha)x^3 + s_{14}(\alpha)x^2 + s_{13}(\alpha)x + s_{12}(\alpha)$$

Next operations are analyzed by using this map.

Note:Byte level transformations are analyzed by using this map.

3.4.1 Addition

Take $a(x), b(x) \in \mathbb{F}(\alpha)[x]/(x^4+1)$

$$a(x) = a_3(\alpha)x^3 + a_2(\alpha)x^2 + a_1(\alpha)x + a_0(\alpha)$$

and

$$b(x) = b_3(\alpha)x^3 + b_2(\alpha)x^2 + b_1(\alpha)x + b_0(\alpha).$$

$$a(x) + b(x) = [a_3(\alpha) \oplus b_3(\alpha)]x^3 + [a_2(\alpha) \oplus \oplus b_2(\alpha)]x^2 + [a_1(\alpha) \oplus b_1(\alpha)]x + [a_0(\alpha) \oplus b_0(\alpha)]$$

where $\oplus$ is byte EXOR, which is addition in $\mathbb{F}_2(\alpha)$ [2].

3.4.2 Multiplication

Multiplication is more complicated. Assume we have two polynomials over $\mathbb{F}(\alpha)[x]/(x^4+1)$

$$a(x) = a_3(\alpha)x^3 + a_2(\alpha)x^2 + a_1(\alpha)x + a_0(\alpha)$$

and

$$b(x) = b_3(\alpha)x^3 + b_2(\alpha)x^2 + b_1(\alpha)x + b_0(\alpha).$$

Their product $c(\alpha)(x) = a(\alpha)(x)b(\alpha)(x)(mod(x^4+1))$ is given by

$$c(x) = c_6(\alpha)x^6 + c_5(\alpha)x^5 + c_4(\alpha)x^4 + c_3(\alpha)x^3 + c_2(\alpha)x^2 + c_1(\alpha)x + c_0(\alpha)$$

$$\equiv c_3(\alpha)x^3 + [c_6(\alpha) + c_2(\alpha)]x^2 + [c_5(\alpha) + c_1(\alpha)]x + [c_4(\alpha) + c_0(\alpha)]\ (mod(x^4+1))$$

Let $d(x) = c(x)\ (mod(x^4+1))$, then

$$d(x) = d_3(\alpha)x^3 + d_2(\alpha)x^2 + d_1(\alpha)x + d_0(\alpha)$$

with

$$d_0(\alpha) = c_4(\alpha) + c_0(\alpha)$$

$$d_1(\alpha) = c_5(\alpha) + c_1(\alpha)$$

$$d_2(\alpha) = c_6(\alpha) + c_2(\alpha)$$

$$d_3(\alpha) = c_3(\alpha)$$

that is

$$d_0(\alpha) = a_0(\alpha)b_0(\alpha) + a_3(\alpha)b_1(\alpha) + a_2(\alpha)b_2(\alpha) + a_1(\alpha)b_3(\alpha)$$

$$d_1(\alpha) = a_1(\alpha)b_0(\alpha) + a_0(\alpha)b_1(\alpha) + a_3(\alpha)b_2(\alpha) + a_2(\alpha)b_3(\alpha)$$

$$d_2(\alpha) = a_2(\alpha)b_0(\alpha) + a_1(\alpha)b_1(\alpha) + a_0(\alpha)b_2(\alpha) + d_{14}(\alpha) + a_3(\alpha)b_3(\alpha)$$

$$d_3(\alpha) = a_3(\alpha)b_0(\alpha) + d_7(\alpha) + a_2(\alpha)b_1(\alpha) + a_1(\alpha)b_2(\alpha) + a_0(\alpha)b_3(\alpha)$$

3.4.3 Matrix Representation

The operation consisting of multiplication by a fixed polynomial a(x) can be written as matrix multiplication where the matrix is a circulant matrix [2]. We have

$$\begin{bmatrix} d_0(\alpha) \\ d_1(\alpha) \\ d_2(\alpha) \\ d_3(\alpha) \end{bmatrix} = \begin{bmatrix} a_0(\alpha) & a_3(\alpha) & a_2(\alpha) & a_1(\alpha) \\ a_1(\alpha) & a_0(\alpha) & a_3(\alpha) & a_2(\alpha) \\ a_2(\alpha) & a_1(\alpha) & a_0(\alpha) & a_3(\alpha) \\ a_3(\alpha) & a_2(\alpha) & a_1(\alpha) & a_0(\alpha) \end{bmatrix} . \begin{bmatrix} b_0(\alpha) \\ b_1(\alpha) \\ b_2(\alpha) \\ b_3(\alpha) \end{bmatrix}$$

References

[1] Rudolf Lidl, Harald Niederreiter, Introduction to Finite Fields and Their Applications Tasmania, Launceston, Australia Revised Edition, 1994.

[2] FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf