Some Mathematical Preliminaries in AES

Zhaohui Cheng
School of Computing Science@Middlesex University
m.z.cheng@mdx.ac.uk
April 2003

Abstract: The notes just explain some basic operations applied in AES.

1. The field GF(2^8)

The elements of a finite field can be represented in several different ways. For any prime power there is a single finite field, hence all representations of GF(2^8) are isomorphic. Despite this equivalence, the representation methods affect the implementation complexity (efficiency). AES has chosen the polynomial representation: $F_2[x]/g(x)$ (deg(g(x))=8, $g(x) \in F_2[x]$ which is irreducible on $F_2[x]$).

F_2 is a field (F; $\oplus$,$\otimes$). F={0,1}, $a \oplus b = a+b \bmod 2$, $a \otimes b = a*b \bmod 2 = a*b$

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

$F_2[x]/g(x)$ is a field (G; +,$*$) where

$$G=\{ b_7 x^7+ b_6 x^6+ b_5 x^5+ b_4 x^4+ b_3 x^3+ b_2 x^2+ b_1 x + b_0 : b_0 \in F_2=\{0,1\}\}.$$

+ is the polynomial addition; the coefficient addition is the operation $\oplus$ on F_2.
$*$ is the polynomial multiplication with modulo g(x); the coefficient multiplication is the operation $\otimes$ on F_2

Isomorphism: GF(2^8) $\cong F_2[x]/g(x)$

Isomorphism mapping f: GF(2^8)$\rightarrow F_2[x]/g(x)$
For each byte $b \in$ GF(2^8), represented with bits $b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0$, is considered as a polynomial in $F_2[x]/g(x)$ with coefficient in F_2={0,1}:

$$b_7 x^7+ b_6 x^6+ b_5 x^5+ b_4 x^4+ b_3 x^3+ b_2 x^2+ b_1 x + b_0$$

For example, the byte of hexadecimal value '57' (binary 01010111) corresponds to the polynomial

$$x^6+ x^4+ x^2+ x +1$$

Addition: + can be calculated with XOR.

Multiplication: $x*m(x)$ can be calculated with a left shift. $x*m(x) \bmod g(x) = x*m(x)$ XOR 11B. If b_7 is 1, then the value after left shifting is bitwised with 1B.

$$a(x)*b(x)= a(x) * (b_7 x^7+ b_6 x^6+ b_5 x^5+ b_4 x^4+ b_3 x^3+ b_2 x^2+ b_1 x + b_0)$$
$$=(((((((a(x)+b_7)*x+ b_6)*x+b_5)*x+b_4)*x+b_3)*x+b_2)*x+b_1)*x+b_0$$

$a^{-1}(x)$ can be computed with extended Euclid algorithm.

In a field we can use the generator theory to simplify multiplication. The multiplication can be computed by the exponent addition. For a finite field, every element in the field can be represented by the generator with exponent format. g is the generator of a finite field GF. For each b$\in$ the finite field GF, $b=g^i$, i is natural number, $0 \le i < |GF|$. AES selects the generator x+1 ({03}) (Note that $F_2[x]/g(x)$ has more than one generator).
The computation can be done using the fomular

$$a*b=g^j * g^k = g^{(j+k) \bmod 255}. \; a^{-1} = g^{255-j} .$$

For example,

$\{03\} \leftrightarrow (x+1). \; \{03\}^{02} \leftrightarrow (x+1)^{02} = x^2+2x+1 = x^2+1 \leftrightarrow \{05\}$
$\{03\}*\{05\} = \{03\}*\{03\}^{02} = \{03\}^{03} = \{0f\}.$
$\{02\} = \{03\}^{19}, \{02\}^{-1} = \{03\}^{ff-19} = \{03\}^{e6} = \{8d\}$

L(xy)	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0		00	19	01	32	02	1a	c6	4b	c7	1b	68	33	ee	df	03
1	64	04	e0	0e	34	8d	81	ef	4c	71	08	c8	f8	69	1c	c1
2	7d	c2	1d	b5	f9	b9	27	6a	4d	e4	a6	72	9a	c9	09	78
3	65	2f	8a	05	21	0f	e1	24	12	f0	82	45	35	93	da	8e
4	96	8f	db	bd	36	d0	ce	94	13	5c	d2	f1	40	46	83	38
5	66	dd	fd	30	bf	06	8b	62	b3	25	e2	98	22	88	91	10
6	7e	6e	48	c3	a3	b6	1e	42	3a	6b	28	54	fa	85	3d	ba
7	2b	79	0a	15	9b	9f	5e	ca	4e	d4	ac	e5	f3	73	a7	57
8	af	58	a8	50	f4	ea	d6	74	4f	ae	e9	d5	e7	e6	ad	e8
9	2c	d7	75	7a	eb	16	0b	f5	59	cb	5f	b0	9c	a9	51	a0
a	7f	0c	f6	6f	17	c4	49	ec	d8	43	1f	2d	a4	76	7b	b7
b	cc	bb	3e	5a	fb	60	b1	86	3b	52	a1	6c	aa	55	29	9d
c	97	b2	87	90	61	be	dc	fc	bc	95	cf	cd	37	3f	5b	d1
d	53	39	84	3c	41	a2	6d	47	14	2a	9e	5d	56	f2	d3	ab
e	44	11	92	d9	23	20	2e	89	b4	7c	b8	26	77	99	e3	a5
f	67	4a	ed	de	c5	31	fe	18	0d	63	8c	80	c0	f7	70	07

x

Table 1 – 'Logs' – L values such that $\{xy\}=\{03\}^L$ for a given a finite field element {xy}

E(xy)	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	01	03	05	0f	11	33	55	ff	1a	2e	72	96	a1	f8	13	35
1	5f	e1	38	48	d8	73	95	a4	f7	02	06	0a	1e	22	66	aa
2	e5	34	5c	e4	37	59	eb	26	6a	be	d9	70	90	ab	e6	31
3	53	f5	04	0c	14	3c	44	cc	4f	d1	68	b8	d3	6e	b2	cd
4	4c	d4	67	a9	e0	3b	4d	d7	62	a6	f1	08	18	28	78	88
5	83	9e	b9	d0	6b	bd	dc	7f	81	98	b3	ce	49	db	76	9a
6	b5	c4	57	f9	10	30	50	f0	0b	1d	27	69	bb	d6	61	a3
7	fe	19	2b	7d	87	92	ad	ec	2f	71	93	ae	e9	20	60	a0
8	fb	16	3a	4e	d2	6d	b7	c2	5d	e7	32	56	fa	15	3f	41
9	c3	5e	e2	3d	47	c9	40	c0	5b	ed	2c	74	9c	bf	da	75
a	9f	ba	d5	64	ac	ef	2a	7e	82	9d	bc	df	7a	8e	89	80
b	9b	b6	c1	58	e8	23	65	af	ea	25	6f	b1	c8	43	c5	54
c	fc	1f	21	63	a5	f4	07	09	1b	2d	77	99	b0	cb	46	ca
d	45	cf	4a	de	79	8b	86	91	a8	e3	3e	42	c6	51	f3	0e
e	12	36	5a	ee	29	7b	8d	8c	8f	8a	85	94	a7	f2	0d	17
f	39	4b	dd	7c	84	97	a2	fd	1c	24	6c	b4	c7	52	f6	01

x

Table 2 – 'Antilogs' – field elements {E } such that $\{E\} = \{03\}^{(xy)}$ given the power (xy)

2. Polynomials with Coefficients in GF(2^8)

The elements in GF(2^{32}) can be represented by polynomials over GF(2^8) using an isomorphism mapping in the following way.

$$GF(2^{32}) \cong GF(2^8)[x]/m(x) \cong (F_2[y]/g(y))[x]/m(x)$$

where $F_2[y]/g(y) \cong GF(256)$; $deg(g(y))=8$; $g(y) \in F_2[y]$ and is irreducible on $F_2[y]$; $deg(m(x))=4$; $m(x) \in GF(256)[x]$ and is irreducible on $GF(256)[x]$).

Isomorphism mapping h: GF(2^{32})$\rightarrow$ GF(2^8)[x]/m(x)
For each double word B with bytes B_3 B_2 B_1 B_0

$$B_3 x^3 + B_2 x^2 + B_1 x + B_0$$

For example, {03010502}$\rightarrow$f(x) = $00000011x^3+00000001x^2+00000101x+00000010$

Isomorphism mapping f: GF(2^8)$\rightarrow$ $F_2[y]/g(y)$.

$$\{03\}=00000011 \rightarrow y+1$$

Field GF(2^{32}) defines two operations $\boldsymbol{\Phi}$, $\boldsymbol{\Gamma}$. $\boldsymbol{\Phi}$ is the polynomial addition, whose coefficient addition is the addition operation + on GF(2^8). This + operation is the same operation as XOR of bits. $\boldsymbol{\Gamma}$ is the polynomial multiplication with modulo m(x) whose coefficient multiplication is the multiplication $*$ on field GF(2^8).

If m(x) is not irreducible, GF(2^8)[x]/m(x) is not a field that isomorphic with GF(2^{32}). But if $a(x) \in$ GF(2^8)[x]/m(x) is coprime with m(x), a(x) has inverse under the modulo m(x). That means, mapping p: GF(2^{32}) $\rightarrow$ GF(2^{32}), $p(b)=a\boldsymbol{\Gamma}b$, is bijection and has inverse function, $p^{-1}(b) = a^{-1}\boldsymbol{\Gamma}b$.

3. MixColumn

The following part shows how MixColumn operation proceeds in AES. AES chooses $m(x)=x^4+1$ as the modulo, because $x^j \bmod m(x) = x^{j \bmod 4}$, which simplifies the computing of modulo and AES only needs to create one bijection to mix the columns (bijection enables decryption). The multiplication can be computed by multiply one 4×4 matrix. AES selects $a(x)=\{03\}x^3+\{01\}x^2+\{01\}+\{02\}$, which is coprime with m(x) and has two coefficients as {01} without computing during multiplication. But a(x)'s inverse $a^{-1}(x)=\{0b\}x^3+\{0d\}x^2+\{09\}+\{0e\}$ is more complex than a(x) when computing multiplication. This is reason that decryption needs more cycles than encryption in AES. The following computation shows that the MixColumn is a bijection.

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$$
$$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$$
$$d(x) = a(x) \bullet b(x) \bmod x^4 + 1$$
$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$
$$d(x) = a(x) \bullet b(x) \bmod x^4 + 1$$
$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

$$a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$$
$$b(x) = a^{-1}(x) \bullet d(x) = a^{-1}(x) \bullet a(x) \bullet b(x) \bmod x^4 + 1$$
$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$
$$= \begin{bmatrix} h_{00} & h_{01} & h_{02} & h_{03} \\ h_{10} & h_{11} & h_{12} & h_{13} \\ h_{20} & h_{21} & h_{22} & h_{23} \\ h_{30} & h_{31} & h_{32} & h_{33} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$
$$h_{00} = 0e \bullet 02 \oplus 0b \bullet 01 \oplus 0d \bullet 01 \oplus 09 \bullet 03$$
$$0e \bullet 02 = \{03\}^{df} \bullet \{03\}^{19} = \{03\}^{(df+19) \bmod 255} = \{03\}^{f8} = 1c$$
$$0b \bullet 01 = \{03\}^{68} \bullet \{03\}^{00} = \{03\}^{68} = 0b$$
$$0d \bullet 01 = 0d$$
$$09 \bullet 03 = \{03\}^{c7} \bullet \{03\}^{01} = \{03\}^{c8} = 1b$$
$$h_{00} = 1c \oplus 0b \oplus 0d \oplus 1b = 1c \oplus (0b \oplus 1b) \oplus 0d = 1c \oplus 10 \oplus 0d = 0c \oplus 0d = 01$$
$$h_{01} = 0e \bullet 03 \oplus 0b \bullet 02 \oplus 0d \bullet 01 \oplus 09 \bullet 01$$
$$0e \bullet 03 = \{03\}^{df} \bullet \{03\}^{01} = \{03\}^{(df+01) \bmod 255} = \{03\}^{e0} = 12$$
$$0b \bullet 02 = \{03\}^{68} \bullet \{03\}^{19} = \{03\}^{(68+19) \bmod 255} = \{03\}^{81} = 16$$
$$h_{01} = 12 \oplus 16 \oplus 0d \oplus 09 = \oplus 0d \oplus 09 = 0$$
.....