갈루아체(Galois Field)

https://youtu.be/uH-ZMunbrBM

HSU 한성대학교
HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

군(Group)과 체(Fields)

갈루아체=유한체(Finite Fields)

소체(Prime Fields)

확대체(Extension Fields)

AES에서 GF(2^8) 적용

CryptoCraft LAB

군(Group)과 체(Fields)

- 군(Group): 원소 G와 G의 두 원소를 결합하는 연산 o의 집합이다.
  - 군 연산은 닫혀있다. a,b∈G -> a o b =c ∈G
  - 결합법칙 성립
  - 모든 a ∈ G에 대해 a o e = e o $a = a$ 인 항등원 e∈G
  - a ∈ G에 대해 a^{-1} o $a = a$ o $a^{-1} = e$인 a의 역원 a^{-1} ∈G존재

- 체(Fileds): 덧셈군(additive group)과 곱셈군(multiplicative group)을 포함하는 집합
  - F의 모든원소는 군 연산 '+'과 항등원 0이 존재하고 교환법칙이 성립하는 덧셈군 구성
  - F의 모든원소는 군 연산 'x'과 항등원 1이 존재하고 교환법칙이 성립하는 곱셈군 구성
  - 두 군연산이 결합되면 분배법칙 성립.

유한체(Finite Field)=갈루아체(Galois Field)

- 유한체 = 갈루아체(Galois Field)
  :거의 항상 유한의 원소를 갖는 체
  GF(m)
- 위수(order) : 체의 원소의 수

ex) p(prime number):소수 n():양의 정수
m=p^n 일 때만 order가 m인 유한체 존재.

ex)81(= 3^4)개의 원소를 갖는 유한체 존재
$12(= 2^3$x 3) 개의 원소를 갖는 유한체 존재 x

소체(Prime Fields)

- Order이 소수인 체 = GF(p)
- GF(p)의 원소 : GF(p)={0,1, …. p-1}
- GF(p)의 연산은 모듈러 p에서 수행. (mod p)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	2
3	3	4	0	1	2
4	4	0	1	2	3

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

ex)GF(5)={1,2,3,4}
모듈러 5에서의 연산

확대체(Extension Fields - ($GF(2^m)$))

- 유한체의 order ≠ prime number or

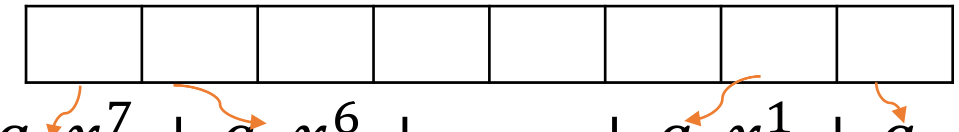
  2^m이 명확하게 소수 x ->

  덧셈,곱셈 연산이 mod 2^m 의 정수의 덧셈과 곱셈으로 표현 x

- M>1인 GF(2^m) =확대체

- GF(2)의 계수를 갖는 다항식으로 표현하여 계산 (즉 0과 1,차수는 m-1)

ex)GF(2^8)



$$a_7x^7 + a_6x^6 + \ \ldots\ldots + a_1x^1 + a_0$$

0110010 = $x^6 + x^5 + x$

$GF(2^m)$에서 덧셈과 뺄셈

- GF(2)에서의 수행

  - mod 2에서의 덧셈과 뺄셈은 동일

  - XOR 와 동일

Ex) GF(2^8)

$$
\begin{array}{rl}
A(x) = & x^7 + x^5 + x^4 + 1 \\
\pm\ B(x) = & x^7 + x^4 + x^2 + 1 \\
\hline
C(x) = & x^5 + \quad + x^2
\end{array}
$$

$GF(2^m)$에서 곱셈

AES MixColumn 의 핵심

Ex) m=8

A(x)= $a_7x^7 + a_6x^6 + \ldots\ldots + a_1x^1 + a_0$

B(x)= $b_7x^7 + b_6x^6 + \ldots\ldots + b_1x^1 + b_0$

C(x)= $c_{14}x^{14} + c_{13}x^{13} + \ldots\ldots + c_1x^1 + c_0$ -15bit ->8bit 축소

모듈러 축소 필요 -> 기약다항식 P(x) 필요

C(x) = A(x)·B(x) mod P(x)

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

A(x)=$x^7 + x^4 + x^1$

x B(x)=$x^3 + 1$

$C'(x)$=$x^{10} + x^4 + x^3 + 1$

x^2

$x^8 + x^4 + x^3 + 1$ | $x^{10} + \quad + x^4 + x^3 + \quad + 1$

$x^{10} + x^6 + x^5 + \quad + x^2$

$x^6 + x^5 + x^4 + x^3 + x^2 + 1$

C(x) $\equiv x^{10} + x^4 + x^3 + 1 \; mod \; x^8 + x^4 + x^3 + x + 1$

$= \quad x^6 + x^5 + x^4 + x^3 + x^2 + 1$

$GF(2^m)$에서 역원

AES S-Box를 포함하는 바이트 대체 변형의 핵심 연산.

Ex) P(x)=$x^8 + x^4 + x^3 + x + 1$

$x^7 + x^6 + x = (11000010)_2 = (C2)_{hex}$

$(C2)_{hex}$의 역원 $x^5 + x^3 + x^2 + x + 1 = (00101111)_2 = (2F)_{hex}$

$(x^7+x^6 + x)(x^5 + x^3 + x^2 + x + 1) \equiv 1 \, mod \; P(x)$

AES에서 GF(2^8) 적용

- S_BOX

$A_i \longrightarrow$ GF(2^8) 역원 $\longrightarrow$ 아파인 대응 $\longrightarrow B_i$

- MixColumn

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \overbrace{\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}}^{GF(2^8)} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

Q & A