Galois Field

https://youtu.be/FnyfcjDskB8

송경주

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Galois Field($GF(p)$)

$GF(2^n)$

암호에서의 Galois Field($GF(2^n)$)

Galois Field($GF(p)$)

- 유한체 = Galois Field (Z_p, p는 소수)

- 사칙연산(+, − ,×, ÷)에 대해 자유로운 유한 집합.
- 원소들의 연산 결과도 포함하는 집합.
- Galois Field 라고도 부름.
- Z_p = $\{0, 1\ \cdots, (p-1)\}$
- Z_p = $GF(p)$

Galois Field($GF(p)$)

- 유한체 성질
  1. **유한성 (finiteness)** : 원소의 개수가 유한함.
  2. **폐쇄성 (closure)** : 연산의 결과도 동일한 집합에 존재.
  3. **결합성 (associativity)** : 연산의 결합법칙 성립 a+(b+c) = (a+b)+c
  4. **교환성 (community)** : 연산의 교환법칙 성립 ex)a+b = b+a, axb = bxa
  5. **분배성 (distribution)** : 연산의 분배법칙 성립 a· $(b+c) = a \cdot b + a \cdot c$
  6. **항등원이 존재** : 각 원소에 대한 덧셈 항등원과 곱셈 항등원이 존재
  7. **역원이 존재** : 0을 제외한 각 원소에 대한 덧셈과 곱셈의 역원이 존재

     · 덧셈의 역원 : 더해서 0이 되는 원소　　· 곱셈의 역원 : 곱한 값의 mod P가 1이 되는 원소.

Galois Field($GF(p)$)

- Galois Field

<수학자 갈루아(Galois)>

- 유한체의 원소 개수 : 항상 p^n개 임을 증명, p는 소수
- 유한체 : $GF(p^n)$로 표시, $GF(p^n) = \{0,1,\cdots,(p^n-1)\}$

- 암호에서 쓰이는 $GF(2^n)$

- 현재 사용하는 암호에서는 n비트 단위의 블록으로 평문을 암호화
- 암호화 된 평문은 n비트 암호문 출력 → n비트 블록이 가질 수 있는 수 = 2^n개

원소의 수가 2^n로 정해진 암호에 대해서 암호화 및 복호화 연산을 진행하기 위해 $GF(2^n)$사용이 적합.

Galois Field($GF(2^n)$)

- 암호에서의 $GF(2^n)$

- mod 2^n 연산 사용
- $GF(2^n)$에서 2^n은 소수가 아님 → 역원이 존재하지 않는 값 발생

Ex) $n = 2$, $GF(4) = \{0, 1, 2, 3\}$ 에서 2의 역원은?

(2 x ☆) mod 4 = 1 을 만족할 때, ☆=2의 역원 (☆은 원소)

☆ = 0, (2 x 0) mod 4 = 0

☆ = 1, (2 x 1) mod 4 = 2

☆ = 2, (2 x 2) mod 4 = 0

☆ = 3, (2 x 3) mod 4 = 2

→ (2 x ☆) mod 4 = 1 을 만족하는 ☆이 없으므로 역원이 없다.

- 위와 같은 이유로 평문에 대한 암호 연산 불가능 (연원이 있는 값에 대해서만 암호화 가능)
- 이 문제를 해결하기 위해 다항식에 모듈러 연산을 적용하는 polynomial GF 개발

Galois Field($GF(2^n)$)

- 다항식 $GF(2^n)$

- $GF(2^n) = \{0,1,\cdots,(2^n-1)\}$ 의 요소들을 $(n-1)$차 다항식으로 표현
- $(n-1)$차 다항식의 항의 수 : n개 → n비트 블록과 대응

  승수 : 해당 비트의 위치

  계수 : 해당 위치의 비트 값 (0 or 1, 즉 $GF(2)$)

- 암호에서 다항식을 사용할 때는 다항식에 대한 모듈러 연산을 수행.
- 모듈러 연산에는 기약 다항식을 사용 ($GF(2^n)$에서는 n차 기약 다항식 사용)
  - 기약 다항식 :
    - 차수가 0보다 큰 두개 이상의 다항식의 곱으로 나타낼 수 없는 것.
    - 여러 차수에 대한 기약 다항식은 이미 계산되어 있으므로 찾아서 쓰면 된다..!!

Degree	*Irreducible Polynomials*
1	$(x+1)$, (x)
2	(x^2+x+1)
3	(x^3+x^2+1), (x^3+x+1)
4	$(x^4+x^3+x^2+x+1)$, (x^4+x^3+1), (x^4+x+1)
5	(x^5+x^2+1), $(x^5+x^3+x^2+x+1)$, $(x^5+x^4+x^3+x+1)$, $(x^5+x^4+x^3+x^2+1)$, $(x^5+x^4+x^2+x+1)$

Galois Field($GF(2^n)$)

- mod (n차 기약 다항식) → (n-1)차 다항식으로 표현됨.
- (n-1)차 다항식으로 표현할 수 있는 원소의 개수 : 2^n
- (n-1)차 다항식은 유한체의 성질을 만족함.
- mod (n차 기약 다항식) 의 결과로 나온 (n-1)차 다항식은 $GF(2^n)$를 만듦.
- $\mathrm{GF}(2^n) = \{0, 1,\ \mathrm{x},\ \mathrm{x}+1,\ \ x^2, \cdots\}$

- Encryption에서 사용 (n비트 암호문)
- n비트 블록의 평문 : (n-1) 차 다항식으로 표현
- 연산에 mod (n차 기약 다항식) 을 적용하여 n비트 블록으로 유지.
- (n-1)차 다항식 암호문 생성

- Decryption에서 사용
- n비트 블록의 평문 : (n-1) 차 다항식으로 표현
- 연산에 mod (n차 기약 다항식) 을 적용하여 n비트 블록으로 유지.'
- (n-1)차 다항식 평문의 블록 생성

Galois Field($GF(2^n)$)

- 다항식 $\mathrm{GF}(2^n)$의 덧셈연산

Ex) $\mathrm{GF}(2^6) = \{0, 1, x+1, \cdots, x^5+x^4+x^3+x^2+x+1\}$ 일 때,

두 다항식 x^4+x^2, $x^5+x^4+x^3+1$ 의 덧셈.

$$
\begin{array}{r}
+\ x^4 + \quad + x^2 \\
+\ \ x^5 + x^4 + x^3 + \quad + 1 \\
\hline
x^5 + 2x^4 + x^3 + x^2 + 1
\end{array}
$$

각 계수는 $\mathrm{GF}(2^n)$이므로 mod 2 계산.

$\rightarrow\ x^5 + x^3 + x^2 + 1$

Galois Field($GF(2^n)$)

- 다항식 $GF(2^n)$의 곱셈연산

Ex) $GF(2^5)$, 두 다항식 x^2+1, x^4+x^2+1 의 곱셈. (5차 기약 다항식 mod (x^5+x^2+1) 로 계산.)

$$(x^2+1)(x^4+x^2+1) = x^2(x^4+x^2+1)+(x^4+x^2+1)$$

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

$$x^6+1$$

곱한 결과에 대해 mod (x^5+x^2+1)연산

$$\begin{array}{r|l} & x \\ \hline x^5+x^2+1 & x^6+1 \\ & x^6+x^3+x \\ \hline & \boxed{x^3+x+1} \end{array}$$

$(x^2+1)(x^4+x^2+1)$ mod (x^5+x^2+1) = x^3+x+1

암호에서의 Galois Field($GF(2^n)$)

- AES

- 기약 다항식 $x^8 + x^4 + x^3 + x + 1$ 이용

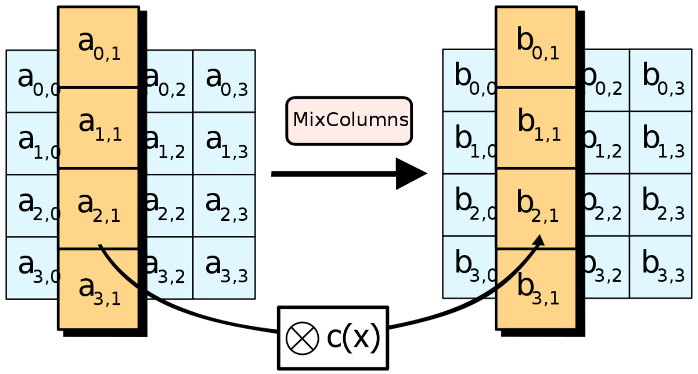
- Mixcolumns : addition과 multiplication 수행.

  Addition : 단순 XOR

  Multiplication : $GF(2^8)$에서 연산

- S-box : $GF(2^8)$상에서 입력에 대한 곱셈의 역원 사용하여 연산

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$



- SEED

- 기약 다항식 $x^8 + x^6 + x^5 + x + 1$ 이용

- S-box : $GF(2^8)$ 상에서 입력에 대한 곱셈 수행.

$$S_i : Z_{2^8} \to Z_{2^8}, S_i(x) = A^{(i)} \bullet x^{n_i} \oplus b_i$$

Q & A