유한체(Finite Field)

김상원

https://youtu.be/ENceJt8VW8Y

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

유한체 활용 알고리즘

유한체 정의

유한체 표기

유한체 표현 예시

활용

- AES (Advanced Encryption Standard)
  - SubBytes 변환
    - AES의 SubBytes 단계에서는 S-box라는 치환 표를 사용하여 각 바이트를 대체
    - S-box는 유한체 **GF(2^8)**에서의 역원을 사용하여 정의됨
    - 즉, 바이트 단위의 값은 **GF(2^8)**의 원소로 취급되며, 이들에 대한 비선형 변환은 유한체 연산을 통해 수행됨
  - MixColumns 변환
    - AES의 MixColumns 단계에서는 **GF(2^8)**에서의 행렬 곱셈을 사용하여 데이터 블록의 각 열을 다른 열과 섞음
    - 이 과정에서 사용되는 행렬은 유한체 **GF(2^8)**에서 정의된 다항식으로 이루어져 있어, 바이트 단위의 값을 다항식 계수로 취급하여 연산을 수행
- RSA (Rivest-Shamir-Adleman)
  - 모듈러 거듭제곱 연산
    - RSA에서 암호화와 복호화는 큰 소수 p와 q를 곱하여 얻은 모듈로 n = pq에 대해 모듈러 거듭제곱 연산을 필요로 함
    - 이러한 연산은 유한체 GF(n)에서 수행됨
  - 모듈러 역원 계산
    - RSA 알고리즘에서 개인 키를 계산할 때, 모듈러 역원을 계산하는 것이 필요하며, 이는 유한체 GF(n)에서의 연산임
- AIMER

정의

- **유한체 (Finite Field)**
  - 유한개 원소 만을 갖고, 그 안에서 대수적 구조를 형성하는 체
  - 유한체를 '갈루아 체(Galois Field)' 라고도 부름
    - 갈루아 이론 : 체의 대칭성 구조를 군의 구조로 바라다 볼 수 있게 한 이론
  - 특히, 코드(부호) 등을 기술하는데 유용한 수학적 '대수 구조(Algebraic Structure)'를 가짐
    - 유한체는 부호화 이론, 암호학 등에서 많이 응용되는 '대수적 구조 ' 임
      - 실수체 R, 복소수체 C 등은 그 요소 수가 무한 개인 무한 체이나, 갈루아 체는 유한체라고 해서 그 요소 수가 유한개임
- 체 (Field)
  - 원소들 간의 덧셈, 곱셈의 연산 결과가 다시 그 안에 있는 닫힘성을 갖는 대수적 구조
  - 닫힘성 : 집합 A가 어떤 연산 *에 대해서 닫혀있다 함은, 집합 A의 임의의 원소 a,b에 대한 연산 a*b의 결과 역시 집합 A의 원소가 되는 성질
    - 예 1 : 자연수는 덧셈과 곱셈에 대해서 닫혀 있음
      - 두 자연수를 더하거나 곱하면 그 또한 자연수가 되기 때문
    - 예 2 : 자연수는 뺄셈과 나눗셈에 대해서 닫혀 있지 않음
      - 두 자연수를 빼거나 나누면 항상 자연수가 되지 않음 (음수나 분수는 자연수가 아님)

- 대수 구조 (Algebraic Structure)
  - 원소의 집합 및 연산을 함께 묶어낸 수학적 개념
  - 대수적 구조를 갖는 집합 예 : 군(Group), 환(Ring), 체(Field), 벡터공간 등

정의

- 유한체의 표기
  - q개의 원소를 갖는 유한체 표기
    - GF(q) 또는 F_q 또는 GF(p^n) 또는 $(F_q)^n$ 또는 F_q^n
- GF(p^n) : q = p^n개의 유한개 원소를 갖는 유한체(Galois체)
  - q : 위수 (位數, Order : 유한 체 내 원소의 갯수)
    - 유한개 원소 수 : p^n = q 개 (0 포함)
    - [참고] 유한 체의 원소 수는,
      - 소수 또는 소수의 멱(prime power) 만 가능하다고, 갈로이스가 밝힘
    - 즉, 유한체의 크기(원소 수)는, 항상 소수 p(표수)의 거듭제곱(p^n)의 형태 임
  - p : 표수 (標數, Characteristic), 때론 기수(base)라고도 함
    - 유한체는, 항상 양의 표수 p를 가짐
    - 여기서, p가 소수이면, 이를 소수 체(Prime Field)라고 함
  - N : 양의 정수(dimension)
  - GF(q) : 위수(order) q를 갖는 유한체
- 유한체의 위수/길이/차수 (Order) q
  - 원소의 개수가 항상 소수(p)의 거듭제곱(p^n=q)이 됨 (갈로이스가 밝힘)
    - 예 : GF(5), GF(8) => 유한체 존재
    - 예 : GF(6), GF(10) => 유한체 존재 안함
  - 전영(0) 원소를 뺀 나머지 원소들은, 순환 군(Cyclic Group)을 이룸

정의

- 유한체의 표현 예
  - 유한체는,
    - 비록 다른 연산 형식도 가능하나
    - 주로, 아래와 같이 모듈러 연산에 적용시켜 표현하는 경우가 많음
  - GF(2) 또는 ({0,1}, +, x)
    - 2^1=2개의 유한개 원소 {0,1}을 갖는, 단순 2진 유한체 (binary field)

덧셈 연산 (+)

+	0	1
0	0	1
1	1	0

XOR 연산과 같음

곱셈 연산 (+)

X	0	1
0	0	0
1	0	1

AND 연산과 같음

덧셈 역원(+)

a	0	1
-a	1	0

곱셈 역원 (+)

a	0	1
a^{-1}		1

  - 성질
    - 정수 modulo 2의 환(Ring)과 같음

정의

- 유한체의 표현 예
  - **GF(2^n)** 또는 F_2^n : 대부분 응용에 사용되는, 2진 부호화 형식이 이 형태를 취함
    - '0', '1', 2개 요소의 n-tuple로써 이루어진, n 튜플 2진 유한체 (n-tuple binary field)
      - 2^n개(위수, 位數 : $p^n = q$)의 유한개 원소들이, 어떤 벡터공간을 생성(Span)함
      - {0,1} 즉, 2개의 기수(base)로써 구성되는, 2진 n-tuple로써 표현 가능
      - {(0,1, ･･･,1),(1,0, ･･･,1),(1,1, ･･･,0), ･･･,(0,0, ･･･,0)}
        (n개, 2^n개)
      - 예 : (7,4) 해밍코드에서, 부호화(매핑)에 대해, 유한체에 의한 수학 기호 표현은,
      - f : GF(2^4) -> GF(2^7)
  - GF(3)
    - 3개의 유한개 원소 {0,1,2}를 갖는 3진 유한체 (ternary field)
    - 성질 : 정수 modulo 3 환(Ring)과 같음
  - GF(4)
    - 4개의 유한개 원소 {0,1,β, β^2}를 갖는 4진 유한체 (quaternary field)
    - 성질 : 정수 modulo 4 환(Ring)과 같지 않음
    - $x + x = 0$, $\beta^2 = \beta + 1$, $\beta^3 = 1$,
    - $\beta^4 = \beta^2\beta^2 = (\beta + 1)(\beta + 1) = \beta^2 + \beta + \beta + 1 = \beta$

덧셈 연산 (+)

+	0	1	2
0	0	1	2
1	1	0	0
2	2	0	1

곱셈 연산 (x)

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

덧셈 연산 (+)

+	0	1	β	β^2
0	0	1	β	β^2
1	1	0	β^2	β
β	β	β^2	0	1
β^2	β^2	β	1	0

곱셈 연산 (x)

+	0	1	β	β^2
0	0	1	0	0
1	0	0	β	β^2
β	0	β	β^2	1
β^2	0	β^2	1	β

Q & A