zero knowledge proof
&
Homomorphic Encryption

https://youtu.be/LE4k8QbyeHs

한성대학교
HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

동형암호 함수

❖ 동형암호

- 데이터를 암호화한 상태에서 각종 연산 작업 수행 가능
- 빅데이터, 인공지능, 블록체인 등의 분야 활용

동형암호 함수

❖ 특성

- $x = E^{-1}(y)$ 연산이 어려움
- $x \neq y$ 라면 $E(x) \neq E(y)$
- E(x) 와 E(y)를 알고 있다면, x와 y를 모르더라도 $E(x) + E(y) = E(x+y)$를 만들어낼 수 있음

➢ 비밀 정보인 x와 y의 값을 노출하지 않으면서 암호화된 상태로 올바른 연산 가능

나머지 연산 활용하여 동형암호 함수 만드는 법

	10	+	15	=	25
% 4	2	+	3	= 1	1
% 7	3	+	1	= 4	4

	12	+	13	=	25
% 4	0	+	1	= 1	1
% 7	5	+	6	= 4	4

- 10 + 15 → E(x) + E(y), 25 → E(x+y) : E(x) + E(y) = E(x+y)
- 10 + 15와 12 + 13의 연산 결과 값은 25로 같지만 10 ≠ 12, 15 ≠ 13 → 두 경우의 x와 y의 값은 다름
- X와 y의 값을 숨긴 채로 덧셈 연산 가능

동형암호 함수

❖ 덧셈 및 곱셈 집합의 재정의

- 덧셈이 재정의된 집합 Z_n

  덧셈의 결과를 나머지 연산하여 Z_n에 속하도록 함 : Z_n = {0,1, …, n-1}

  ex) n = 7 : 4 + 6 = 10, 10 ≡ 3 mod 7 >> {0,1, … 6}

- 곱셈이 재정의된 집합 Z^*_p

  제수를 소수로 가정 → Z^*_p : Z_n에서 0 제외한 집합 (∵곱셈에 대한 역원)

  곱셈의 결과를 나머지 연산하여 Z^*_p 에 속하도록 함 : Z^*_p = {1, … p-1}

  ex) p = 7 : 4 * 6 = 24, 24 ≡ 3 mod 7 >> {1, 2, 3, … 6}

동형암호 함수

❖ $Z^{*}p$ = {1, … , p-1}

- 순환군(Cyclic group)

해당 집합의 모든 원소에 대해 $a \in \{0, \dots, p\text{-}2\}$인 a를 사용하여 표현한 g^{a} 가 집합 Z^{*}_{p} 의 모든 원소를 표현

➢ g는 생성자이며, 이때의 g^{a} 는 해당 집합의 모든 원소를 표현하게 됨 : $g \in Z^{*}_{p}$, $g^{a} \in Z^{*}_{p}$

Ex) p = 7, Z^{*}_{7} = {1,2,3,4,5,6}, a = {0,1,2,3,4,5}

g : ‘ 군의 위수(군의 원소의 개수(p-1)와 같음) = 원소의 위수 ’를 만족하는 해당 집합 내의 원소

$g \in Z^{*}_{7}$ 인 g에 대해 $g^{a} \equiv 1 \bmod 7$ 일 때의 a가 해당 원소의 위수

→ 1의 위수 : 1 / 2의 위수 : 3 / 3의 위수 : 6 / 4의 위수 : 3 / 5의 위수 : 6 / 6의 위수 : 2

→ g = 3 : a = {0,…, 5} : $3^0\ 3^1\ 3^2\ 3^3\ 3^4\ 3^5$ → 1 3 2 6 4 5 : Z^{*}_{7} 의 모든 원소 표현 가능

→ g = 6 : a = {0, …,5} : $5^0\ 5^1\ 5^2\ 5^3\ 5^4\ 5^5$ → 1 5 4 6 2 3 : Z^{*}_{7} 의 모든 원소 표현 가능

* 위수 : 2 이상의 정수 m에 대해 a가 (x,m) =인 정수일 때, $x^{r} \equiv 1 \bmod m$ 인 가장 작은 양의 정수 r을 법 m에대한 x의 위수라고 함

동형암호 함수

❖ $Z^{*}p$ = {1, … , p-1}

- p가 충분히 크다면 $g^a = h$를 만족하는 a 값을 찾기 어려워짐

  이산로그 문제를 풀면 비밀값(a)을 알아낼 수 있음 → 이산로그의 효율성과 보안성은 반비례

  P가 커질수록 만족하는 a값을 찾아야할 범위가 커지고 연산이 많아지며, 시간복잡도는 군의 크기에 비례

  ➢ 이산로그 문제를 풀기 어려워짐

- 곱셈시 지수의 덧셈 적용

  $g^a \cdot g^b = g^{(a+b) \bmod p-1}$

  mod p-1 ? 곱셈 연산의 결과도 Z^{*}_{p} 에 속해야하므로 (a+b)mod(p-1)도 a의 조건을 만족해야 함

  → a의 범위 {0, …, p-2} , Z_{p-1} = {0, …, p-2}

  $E(x) = g^x$: $E(x+y) \rightarrow g^x \cdot g^y = g^{(x+y) \bmod p-1} = E(x+y) = E(x) \cdot E(y)$

➢ x와 y를 몰라도 E(x+y)를 구할 수 있게 되고 그 때의 x, y값을 찾기 어려워짐

동형암호 함수

❖ 덧셈지원 동형암호 함수

- $E(x) = g^x \ (x \in Z_{p-1})$

  1. $x \neq y$ 라면 g^x 와 g^y의 값은 서로 다름
  2. $E(x) = g^x$ 에 대해 x값을 찾기 어려움
  3. $E(x+y) = g^{x+y \bmod p-1} = g^x \cdot g^y = E(x) \cdot E(y)$

     → x, y 몰라도 E(x+y) 구할 수 있음

➢ g^x 사용하여 동형암호 함수의 세가지 조건 모두 만족

동형암호 함수

❖ Blind Evaluation of polynomial

- 다항식의 결과값을 다항식 없이 or 변수 없이 구하는 방법
- A는 다항식을 구성하는 계수를 알고 있고 B는 다항식 없이 본인만 아는 값을 넣었을 때의 결과 값 원함

  A는 B의 비밀값 s를 모르는 상태로 은닉정보(E(s))만 가지고 결과값을 만들어주어야 하는 상황

❖ 유한체 F_p

- $F_p = \{0, \ldots, p-1\}$, 덧셈 및 곱셈은 나머지 연산
- 덧셈군, 곱셈군 有 : 덧셈, 곱셈에 대해 닫혀있음

❖ 유한체 F_p에 대한 d차 다항식 P

- $P(x)=a_0+a_1 \cdot x+a_2 \cdot x^2+\ldots+a_d \cdot x^d$, $a_0, \ldots, a_d \in F_p$

동형암호 함수

❖ 다항식과 선형 결합

- 어떤 점 s가 F_p에 속할 때의 d차 다항식 P(s) : (s, P(s))

  $P(s) = a_0 \cdot s^0 + a_1 \cdot s^1 + a_2 \cdot s^2 + \dots + a_d \cdot s^d, \quad a_0, \dots, a_d \in F_p$

- 점 s를 벡터로 생각하면 $s^0 = v_0, \dots, s^d = v_d$

  다항식의 각 계수를 가중치로 사용하는 가중합 → 벡터의 선형결합 형태로 나타낼 수 있음

  $P(s) = a_0 \cdot V_0 + a_1 \cdot V_1 + \dots + a_d \cdot V_d$

  * 벡터의 선형결합 : 벡터에 스칼라값을 곱한 후 더한 것 : 상수배 후 덧셈

    → 선형결합으로 얻은 벡터 또한 동일한 벡터공간 내에 존재

동형암호 함수

❖ 동형암호함수와 선형 결합

- 동형암호 함수도 선형결합 지원
- a, b가 주어지고 E(x), E(y)를 알고 있다면 E(ax+by)를 구할 수 있음
- $E(ax+by) = g^{(ax+by)} = g^{ax} \cdot g^{by} = (g^x)^a \cdot (g^y)^b = E(x)^a \cdot E(y)^b$

- A가 아는 정보 : $P(s) = a_0 \cdot s^0 + a_1 \cdot s^1 + a_2 \cdot s^2 + \ldots + a_d \cdot s^d$

  B가 제공하는 은닉정보 : $E(x) = g^x$

  A가 구해야 하는 것 : $E(a_0 \cdot s^0 + a_1 \cdot s^1 + a_2 \cdot s^2 + \ldots + a_d \cdot s^d) = E(P(s))$

  $g^{(a_0 \cdot s^0 + a_1 \cdot s^1 \ldots + a_d \cdot s^d)} = g^{(a_0 \cdot s^0)} \cdot g^{(a_1 \cdot s^1)} \cdot g^{(a_d \cdot s^d)} = E(s^0)^{a_0} \cdot E(s^1)^{a_1} \ldots \cdot E(s^d)^{a_d}$

➢ Blind Evaluation에서 A는 자신이 알고 있는 다항식의 계수와 은닉 정보(E(s))만 알고 있으면 S를 모르고도 다항식의 결과 값을 구할 수 있음

KC 테스트

❖ Knowledge of Coefficient Test

- 올바른 다항식(P(x))을 사용해 은닉값을 만들었음을 증명하기 위한 테스트

❖ 곱셈을 위한 유한체 F^*_p

- $F^*_p = \{1,\ldots, p-1\}$: F_p에서 0을 제외

❖ p개의 원소를 가지는 순환군 G

- $\alpha \in F^*_p$ 인 α 를 사용하여 생성자 g 를 가지는 순환군 G 에 대해 덧셈순환 진행
  → g^a 대신 $\alpha \cdot g$

❖ α쌍

- $a,b \in G$, $\alpha \in F^*_p$일 때, $a,b \neq 0, b = \alpha \cdot a$ 를 만족하는 두 원소들의 쌍 (a,b)

α 쌍

- p = 7, α·g ≡ 1 mod 7 일 때,
- g의 위수 = α → g = 1, α = 1 / g = 2, α = 4 / g = 3, α = 5 / g = 4, α = 2 / g = 5, α = 3 / g = 6, α = 6
- Generator g = 6

  α·g → 1*6 2*6 3*6 4*6 5*6 6*6 → mod 7 → 6 5 4 3 2 1 : G의 모든 원소 표현 가능
- α쌍 : b = α · a

1	2	3	4	5	6
(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)
(2,2)	(2,4)	(2,6)	(2,1)	(2,3)	(2,5)
(3,3)	(3,6)	(3,2)	(3,5)	(3,1)	(3,4)
(4,4)	(4,1)	(4,5)	(4,2)	(4,6)	(4,3)
(5,5)	(5,3)	(5,1)	(5,6)	(5,4)	(5,2)
(6,6)	(6,5)	(6,4)	(6,3)	(6,2)	(6,1)

- B가 A에게 α쌍 (4,5) 전송 → A는 γ=2 선택 → (a′,b′) = (2·4,2·5) = (8,10) = (1,3)

  (4,5)와 (1,3)은 α쌍 (γ 를 곱한 값이 α쌍이 됨)

KC 테스트

❖ KC Assumption (KCA)

- A가 B의 (a,b) 에 대해 올바른 α 쌍 (a′,b′) 을 응답했다면 A는 a′=γ·a 를 만족하는 γ 를 알고 있다고 가정

  이 때, A의 추출기는 a′=γ·a를 만족하는 γ를 내어놓음

  → A의 추출기가 내어놓는 γ는 모두 α쌍을 만족 : 올바른 값을 사용

❖ Verifiable Blind Evaluation

- Blindness

  A는 s 값을 모르고, B는 P(x) 를 모름

- Verifiability

  A가 d차수의 특정 다항식 P(x)를 사용하지 않고 E(P(S)) 를 만들어 보냈을 때(다른 다항식 사용),

  B가 수용하는 상황은 매우 드물다

  → 서로 다른 다항식은 거의 모든 점이 겹치지 않음 → 제출하는 증명도 다를 것

Extended KCA

ex) mod 7의 경우 : α쌍 (1,3), (5,4), (2,4), (3,2) 받고 γ = 1,2,5,6 선택했을 때,

(a',b') = (39,43) → mod 7 → (4,1)

→ α쌍 만족 (α = 2)

→ B는 α를 통해 A가 올바른 값을 사용하여 결과 값을 만들 수 있다고 생각하게 됨

ex) mod 11의 경우 : α쌍 (1,3), (5,4), (2,4), (3,2) 받고 γ = 1,2,8,9 선택했을 때,

(a',b') = (54,61) → mod 11 → (10,6)

→ α쌍 불만족

→ α쌍이어야 C_i를 알고있음을 증명 가능

- **α쌍이 나오는 경우도 있지만 p가 커질수록 d차 다항식 P(x)에 대해 α쌍을 만족하기는 어려워짐**

d-급수에 대한 KCA : Verifiable Blind Evaluation Protocol

❖생성자 g에 대한 동형암호함수 $E(x) = x \cdot g$

- B는 $\alpha \in F^*_p$ 와 $s \in F_p$ 를 선택하여 α쌍 생성 후 A에게 전송

  S값 그대로 주지 않고 은닉값 E(s)과 α쌍 전송 : $(s^0 \cdot g, \alpha s^0 \cdot g), (s^1 \cdot g, \alpha s^1 \cdot g), \ldots, (s^d \cdot g, \alpha s^d \cdot g)$: α쌍

- A는 B에게 새로운 α쌍 전송 with 선형결합

  $C_0 \cdot s^0 \cdot g + C_1 \cdot s^1 \cdot g + .. + C_d \cdot s^d \cdot g = a' \in F^*_p$

  $b' = C_0 \cdot \alpha \cdot s^0 \cdot g + C_1 \cdot \alpha \cdot s^1 \cdot g + .. + C_d \cdot \alpha \cdot s^d \cdot g = \alpha(C_0 \cdot s^0 \cdot g + C_1 \cdot s^1 \cdot g + C_d \cdot s^d \cdot g) = \alpha \cdot a'$

  → $\alpha \cdot g(C_0 \cdot s^0 + C_1 \cdot s^1 + C_d \cdot s^d) = \alpha \cdot g \cdot P(s)$: A가 고른 C_i는 다항식 P의 각 항의 계수가 됨

- B는 $b' = \alpha \cdot a'$ 인지 확인

  α쌍이라면 A가 다항식 P의 모든 계수(C_i)를 알고 있고 올바른 다항식을 사용했음을 검증

➢ **S에 대한 정보를 주지 않고도 E(P(s))를 얻을 수 있으며, 은닉 값 E(s)에 대해 옳은 결과 값임을 검증**

Q & A