ECC 암호화

- 타원곡선 이론에 기반한 공개키 암호 방식.

대수적 구조

- 군, 환, 체로 분류
- 군 : 집합 내에서 결합법칙과 항등원, 역원이 정의된다.
- 환 : 집합 내에서 결합법칙과 교환법칙, 분배법칙이 성립하고 항등원과 역원이 정의된다.

체

- 대수적 구조 중 하나로 집합 내에서 덧셈. 뺄셈, 곱셈, 나눗셈의 사칙연산을 소화할 수 있는 집합이다.
- 체의 조건
    1. 집합의 원소로 연산하며 연산을 통해 나온 값 역시 집합의 원소이다.
    2. 덧셈과 곱셈에 대하여 결합법칙과 교환법칙이 성립한다.
    3. 임의의 원소에 또 다른 임의의 원소를 더했을 때 임의의 원소가 그대로 나오는 항등원과 임의의 원소에 또 다른 임의의 원소를 더했을 때 0이 나오는 역원이 존재한다.

        예) 2+a=2를 만족시키는 항등원 0이 존재한다.

        2+a=0을 만족시키는 역원 -2가 존재한다.
    4. 임의의 원소에 또 다른 임의의 원소를 곱했을 때 임의의 원소가 그대로 나오는 항등원이 존재하고 임의의 원소에 또 다른 임의의 원소를 곱했을 때 1이 나오는 역원이 존재한다.

        예) 3×a=3을 만족시키는 항등원 1이 존재한다.

        3×a=1을 만족시키는 역원 $\frac{1}{3}$이 존재한다.

유한체(Z_p)

- 유한개의 원소를 가지는 체이다. 정수 집합 내에서 체의 조건이 적용 되므로 원소의 개수는 유한하다. 유한체의 원소의 개수를 나타내는 표수는 반드시 소수이어야 한다.

- 표수가 소수이어야 하는 이유
    1. 표수가 소수가 아닌 정수일 경우 항등원의 조건이 성립하지 않는다.

       예) 표수가 6인 유한체에서 2의 역원인 1/2은 집합에 존재하지 않으므로 성립하지 않는다.
- 유한체 상에서의 음수 모듈러 연산
    1. a가 음수이고 b가 소수일 때 $a\,mod\,b$는 $a\,mod\,b + b$로 연산한다.

       예) $-3mod11 =-3 + 11 = 8$

표수

- 유한체의 원소의 개수를 나타내는 수이다.

난수

- 정의된 범위 내에서 무작위로 만들어진 수를 말한다.

무한원점

- 직선이나 평면의 ‘끝’에 추가하는 가상의 점이다.

타원 곡선

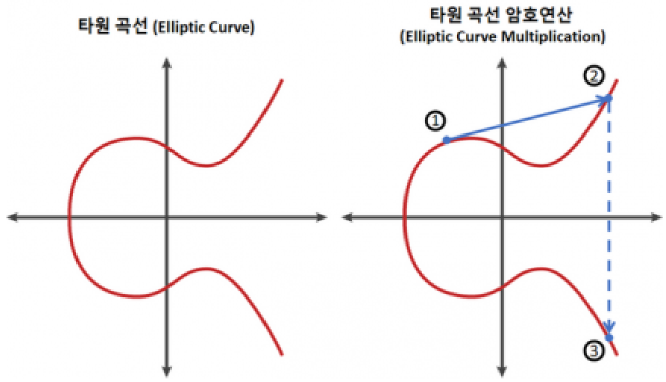
- 실수 위에서의 타원곡선은 a와 b가 고정된 실수일 경우 방정식

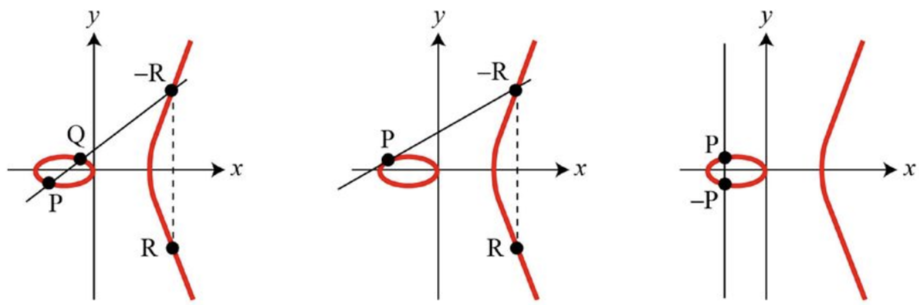
$$y^2 = x^3 + ax + b$$

만족하는 (x, y)점들의 집합을 의미한다. 우변인 $x^3 + ax + b$가 중근을 갖지 않으면 타원곡선은 군을 정의 할 수 있는 대수적 특성을 제공하는 것으로 알려져 있다.

타원 곡선 상에서의 연산

- 해당 타원곡선 위의 모든 점들과 무한원점이라고 명명된 특수 점으로 구성되고 여기에 덧셈이 정의된다.





a. (R = P + Q) b. (R = P + P) c. (O = P + (– P))

a. P와 Q를 지나는 직선이 타원과 만나는 교점R을 x축으로 대칭시킨 점을 P+Q=R로 정의한다.

b. 덧셈 연산과 같이 P의 접점을 타원 곡선으로 이은 교점R을 x축으로 대칭시킨 점을 2P=R로 정의한다.

c. P와 -P는 x축에 대칭되는 값이기 때문에 P+(-P)=0이다.

- 타원 곡선 상의 덧셈 연산의 수학적 표시 (λ는 기울기)

○ Addition $(P \neq Q)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = (x_1 - x_3)\lambda - y_1$$

○ Doubling $(P = Q)$

$$\lambda = \frac{3{x_1}^2 + a}{2y_1}$$
$$x_3 = \lambda^2 - 2x_1$$
$$y_3 = (x_1 - x_3)\lambda - y_1$$

타원 곡선 상 임의의 점 P(x_1, y_1)와 Q(x_2, y_2)를 지나는 직선의 방정식을 이용하여 그래프와 직선의 교점 R(x_3, y_3)을 구할 수 있다.

유한체 상에서의 타원 곡선

- Z_p로 표기하며 p는 소수를 나타낸다.
- 타원곡선의 연산 조건
    1. 덧셈과 곱셈이 정수 집합 내에서 이뤄지며, 연산 결과 또한 집합의 원소이다.
    2. 교환 법칙과 결합 법칙이 성립한다.
    3. 항등원과 역원이 존재한다.
    4. 분배 법칙이 성립한다.

타원곡선 암호화 방식

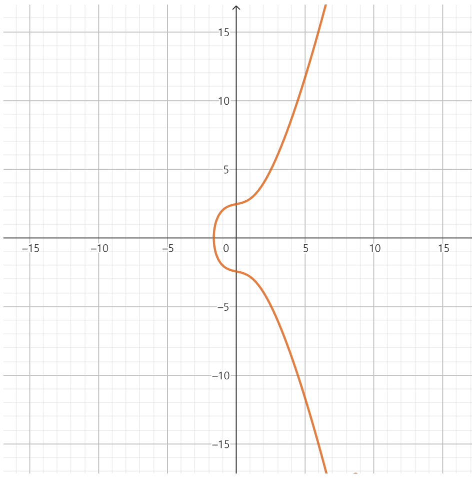
- 비공개키(k) : 타원곡선 상에 임의의 점 G를 더하여 새로운 점을 계산하는 횟수
- 공개키(kG) : G를 k번 더해서 생성되는 새로운 점에 해당되는 값
- 생성자(G) : 타원곡선 상의 임의의 점

1. G+Q+R=0이 되는 점 G, Q, R을 선택한다.
2. 시작점은 G와 Q가 중근을 갖는 점을 선택한다. (G=Q)
3. G+G+R=0, R=-2G, R을 x축 대칭시킨 점 2G+G+R=0, R=-3G…

- 이와 같은 작업을 무수히 반복하여 얻어진 점 kG를 공개키로 공개한다.
  공개키(kG)로 암호된 암호문을 비공개키 k를 사용하면 복호화가 되고, 반대로 사용하면 전자 서명이 된다.

→서로 다른 타원곡선을 선택하여 사용할 수 있으며 추가 보안을 위해 주기적으로 타원곡선을 바꿀 수 있다.

예를 들어 $y^2 = x^3 + x + 6$이 표수(p)가 11인 유한체 위에 존재할 때



$$y^2 = x^3 + x + 6$$

$$E: y^2 = x^3 + x + 6 \; over \; Z_{11}$$

$$G(\alpha) = (2, 7)$$

$$2\alpha = (x_2, y_2)$$

α는 생성자(G), 주어진 값이 α 하나만 있으므로 Doubling을 이용한다.

2α를 구한다면,

$$\lambda = \frac{3{x_1}^2 + a}{2y_1} = \frac{3(2)^2 + 1}{2 \times 7} = \frac{13}{14} = 2 \times 3^{-1} = 2 \times 4 = 8 \mod 11$$

$$x_2 = \lambda^2 - 2x_1 = (8)^2 - 2 \times (2) = 5 \mod 11$$

$$y_2 = (x_1 - x_2)\lambda - y_1 = (2 - 5) \times 8 - 7 = 2 \mod 11$$

$$2\alpha = (5, 2)$$

$13 mod 11 = 2$, $14 mod 11 = \frac{1}{3} = 3^{-1}$이고 $3^{-1} mod 11 = 4$가 된다.

비밀키(k)×생성자(G)=공개키(kG)를 이용하여

$\alpha = (2, 7)$, $2\alpha = (5, 2)$, $3\alpha = (8, 3)$

$4\alpha = (10,\ 2)$, $5\alpha = (3,\ 6)$, $6\alpha = (7,\ 9)$

$7\alpha = (7,\ 2)$, $8\alpha = (3,\ 5)$, $9\alpha = (10,\ 9)$

$10\alpha = (8,\ 8)$, $11\alpha = (5,\ 9)$, $12\alpha = (2,\ 4)$

를 구할 수 있다.

유한체 상에서의 암호화와 복호화 과정을 알아보자.

$$\alpha = (2,\ 7)$$

$$k = 7 \text{ (비공개키)}$$

$$r = 3 \text{ (난수)}$$

$$x = (10,\ 9) \text{ (보내고자 하는 평문)}$$

- 위와 같이 유한체 상의 타원곡선이 존재하고 공개키 $\alpha(2,\ 7)$인 상태에서 어떤 사람 A가 B에게 $x(10,\ 9)$라는 평문을 보내고 싶어한다면 A가 선택한 비공개키 $k = 7$이라 가정하고 A가 선택한 난수 $r = 3$이라 가정한다.

ECC에서 암호화 공식은 다음과 같다.

$$\beta = k \times \alpha = 7a$$
$$y_1 = r \times a = 3(2,\ 7) = 3\alpha$$
$$y_2 = x + r \times \beta = (10,\ 9) + 3 \times 7\alpha$$
$$\therefore e_k(x,\ r) = (r\alpha,\ x + r\beta)$$

- $y(y_1,\ y_2)$는 암호화된 평문 x
- $\beta = k \times a$ (β는 공개키)
- $y_1 = r \times \alpha$
- $y_2 = x + r \times \beta$

위의 r, α, x 및 Addiction, Doubling을 우리는 알고 있으니 y_1, y_2를 구할 수 있다.

- $y(y_1,\ y_2)$를 B에게 보내면 B는 아래와 같은 복호화 과정을 거친다.

$$x = y_2 - (k \times y_1)$$
$$x = y_2 - 7y_1$$

$k = 7$ 이므로 $x = y_2 - 7 \cdot y_1$이다.

출처

[암호학] 비대칭키-ECC, Elliptic Curve Cryptosystem, 티스토리, 2023.08.23. 인출, [암호학] 비대칭키 - ECC, Elliptic Curve Cryptostystem (tistory.com)

체(대수학), 나무위키, 2023.08.22. 인출, 체(대수학) - 나무위키 (namu.wiki)