ECC 암호화

- 타원곡선 이론에 기반한 공개키 암호 방식.

타원 곡선

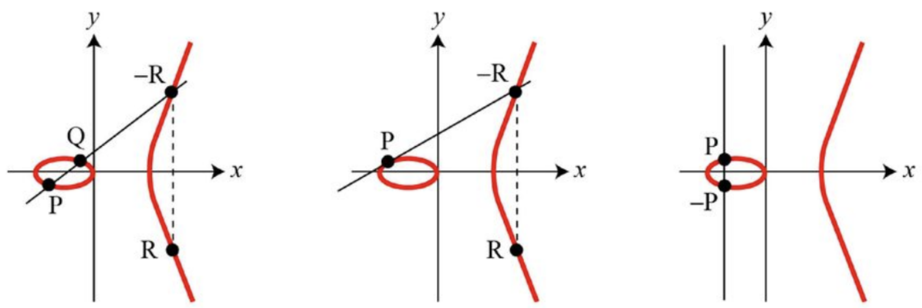
- 실수 위에서의 타원곡선은 a와 b가 고정된 실수일 경우 방정식

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

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 무한대 점이라고 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 $(P = Q)$

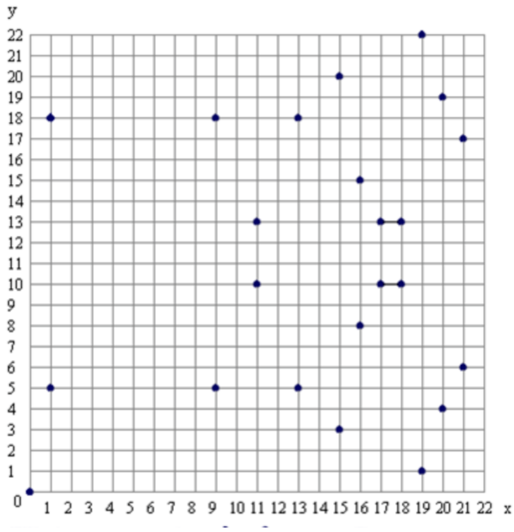
$$\lambda = \frac{3x_1^{\ 2} + a}{2y_1}$$
$$x_3 = \lambda^2 - 2x_1$$
$$y_3 = (x_1 - x_3)\lambda - y_1$$

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

- F_p로 표기하며 p는 소수를 나타낸다.
- 타원곡선의 연산 조건
  1. 덧셈과 곱셈이 닫혀 있어야 한다.
  2. 교환 법칙과 결합 법칙이 성립해야 한다.
  3. 항등원과 역원이 존재해야 한다.
  4. 분배 법칙이 성립해야 한다.

- 유한체 상에서의 타원 곡선의 연산의 예
  1. 덧셈 : (18+9) mod 23 = 4
  2. 뺄셈 : (7-14) mod 23 = 16
  3. 곱셈 : 4· 7 mod 23 = 5



$y^2 = (x^3 + x)\ over\ F_{23}(p = 23)$ → (소수가 23인 유한체 위 타원곡선)

예를 들어 x=11이면

$$y^2 mod23 = (1331 + 11)mod23 = 1342mod23 = 8$$

$y^2 mod23 = 9$ 이므로 식을 만족하는 y값은 10과 13이다.

- 유한체의 p가 커지면 y를 쉽게 찾을 수 없게 되는 것을 활용한다.

타원곡선 암호화 방식

- 개인키(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 개인키 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 소수(p)가 11인 유한체 위에 존재할 때

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

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

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

2α를 구한다면,

$$\lambda = \frac{3{x_1}^2 + a}{2y_1} = \frac{3(2)^2 + 1}{2\times 7} = \frac{13}{14} = 2\times 3^{-1} = 2\times 4 = 8 \mod 11$$
$$x_2 = \lambda^2 - 2x_1 = (8)^2 - 2\times(2) = 5 \mod 11$$
$$y_2 = (x_1 - x_2)\lambda - y_1 = (2-5)\times 8 - 7 = 2 \mod 11$$

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

$$\alpha = (2,7)$$
$$pk = 7 \ (Private \ Key)$$
$$k = 3 \ (Random \ value)$$
$$x = (10,9) \ (x \ is \ plaintext)$$

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

ECC에서 암호화 공식은 다음과 같다.

$$\beta = pk * \alpha = 7\alpha$$

$$y_1 = k * \alpha = 3(2,7) = 3\alpha$$
$$y_2 = x + k*\beta = (10,9) + 3*7\alpha$$

$$\therefore e_k(x,k) = (k\alpha, \ x + k\beta)$$

- $\beta = pk \cdot a$
- $y_1 = k \cdot \alpha$
- $y_2 = x + k \cdot \beta$

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

$$x = y_2 - (pk * y_1)$$

$$x = y_2 - 7y_1$$

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