通信情報保護學會誌
第6卷 第3號, 1996. 9

ECC를 위한 요소 이론들에 대한 조사 연구

이 인 수*, 진 원 일*, 김 철**

제 1 절 소 개

타원 곡선을 이용한 공개키 암호시스템 즉, 유한체위에서 정의된 타원 곡선군에서의 이산 대수 문제에 기초한 이산 대수 암호시스템의 한 종류인 ECC(Elliptic Curve Cryptosystems)는 1985년 N. Koblitz[1]와 V. Miller[2]에 의해 처음으로 제안된 이후 활발히 연구되고 있다.

유한체 K위에서 정의된 타원 곡선 E위의 점들은 가환군의 형태를 이룬다. 이 가환군의 더하기 연산은 기초체 K에서의 산술 연산 몇개를 포함하며, 하드웨어와 소프트웨어로 구현하기가 쉽다. 또한 이 가환군에서 이산 대수를 사용하는 암호시스템은 유한체의 곱셈군에 기초한 시스템에 비해 다음 두가지 장점을 가지고 있다. 첫째, 이 군에서의 이산 대수 문제는 매우 어렵고 (즉, 이 군에서는 subexponential time algorithm으로 이산 대수 문제를 풀 수 없다), 특히 같은 크기인 K 유한체에서의 이산 대수 문제보다 더 어렵다. 다시말하면, ECC는 작은 키 길이를 가지고도 현존하는 공개키 시스템의 안전도를 보장받을 수 있다. 짧은 키 길이는 몇몇의 응용에서의 중요 요소인 작은 대역폭과 적은 메모리로 ECC를 사용할 수 있음을 의미한다(예: 메모리와 처리 능력이 제한된 Smart Card 시스템의 설계). 둘째, 타원 곡선을 사용함에 따른 또 다른 이점은 비록 모든 사용자들이 같은 기초체 K를 사용하더라도 각 사용자가 다른 곡선 E를 선택할 수 있다(즉, 주어진 군에서 다양한 타원곡선을 사용할 수 있다). 결과적으로 모든 사용자들은 같은 하드웨어로 체 연산을 실행하고, 요구되는 안전도를 위해 주기적으로 곡선 E를 변화시킬 수 있다.

1990년에 괄목할 만한 성과 중의 하나가 Menezes, Okamoto와 Vanstone[3]에 의해 연구되었다. 그들은 이 연구에서 소위 초특이 타원 곡선이라 불리우는 타원 곡선의 이산 대수 문제가 유한체에서의 이산 대수 문제로 바뀔 수 있음을 보였다. 그러므로 만약 현존하는 최고의 지식에 의하여 완전 지수 복잡도로 이 암호시스템이 안전하기를 원한다면(상대적으로 작은) 초특이 타원 곡선을 피해야 한다.

본 논문에서는 ECC를 설계, 구현하는 데 필요한 수학적인 요소 이론들을 체계적으로 정리하고(2절), ECC의 형태를 분류하여 ECC가 공통적으로 가지고 있는 구조를 파악해 본다(3절).

* 연세대학교 수학과
** 광운대학교 수학과

제 2 절 ECC를 위한 요소 이론들

2.1 기본적인 용어들

본 절에서는 ECC를 정의하기 위하여 쓰이는 기본적인 용어들을 우선 정의한다. 여타 정의들은 각 요소 이론의 전개에서 필요에 따라 정의한다.

이산 대수 문제(Discrete Logarithm Problem)란 군 G의 기저를 $g(\in G)$라 할 때, 주어진 $y(\in G)$에 대하여 $g^x = y$를 만족하는 정수 x를 찾는 문제이다.

타원 곡선 이산 대수 문제(ECLP, Elliptic Curve Logarithm Problem)란 P가 위수 n인 $E(F_q)$의 원소라 할 때, 주어진 P와 R에서 $R = mP$를 만족하는 정수 $m(0 \le m \le n-1)$을 찾는 문제이다.

타원 곡선 암호시스템(ECC, Elliptic Curve Cryptosystems)이란 유한체위에서 정의된 타원 곡선 군에서의 이산 대수 문제에 기초한 이산 대수 암호시스템의 한 종류이다.

2.2 타원 곡선의 정의와 연산

이제 타원 곡선을 구체적으로 정의하고, 타원 곡선상의 여러 연산에 대하여 살펴보자.

2.2.1 정의와 표기

$\bar{K}$는 체(field) K의 대수적 폐포(algebraic closure)를 나타내며, F_q는 q 원소를 가지는 유한체(q는 소수의 멱)를 나타낸다. 특히 $K = F_q$라 하면 F_q의 대수적 폐포 $\bar{F}_q$는 $\cup_{m=1} F_{q^m}$이다. K 위에서 아핀 n-공간 $A^n(\bar{K})$란 $\{(x_1, x_2, \cdots, x_n) \mid x_i \in K\}$의 집합을 말하고, 사영 n-공간 $P^n(\bar{K})$이란 모든 i에 대하여 $x_i = \lambda y_i$를 만족하는 $\lambda \in \bar{K}^*$가 존재할 때, 즉, $(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n)$에 의해 주어진 모듈러 동치 관계이고, 적어도 하나의 x_i가 0이 아닌 $(x_0, \cdots, x_n) \in \bar{A}^{n+1}(K)$의 동치류 집합을 말한다.

■ **정의 3.1** (Weierstrass 방정식) $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 (a_i \in \bar{K}, i = 1, 2, 3, 4, 6)$ 형태의 3차 제차 방정식 또는 $Z \neq 0$일 때 비균질화에 의해 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 (a_i \in \bar{K})$으로 볼 수도 있다.

[예 2.1] $F(X,Y,Z) = Y^2Z - X^3 - XZ^2 - 6Z^3 = 0$, $a_i \in \bar{F}_{13}$.

$F(X,Y,Z) = Y^2 + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$을 만족하는 모든 사영점 $P = (X:Y:Z) (\in P^2(\bar{K}))$들에 대하여, 다음 3개의 편도함수들 $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$, $\frac{\partial F}{\partial Z}$ 중에서 적어도 하나가 점 P에서 0이 아닐 때, Weierstrass 방정식이 매끄럽다(smooth) 또는 비특이(non-singular)라 말한다.

Weierstrass 방정식에는 다음의 특별한 두 점이 있다.

가) 특이점 P(singular point)란 편도함수 3개 모두가 점 P에서 0일 때의 점 P를 말한다.

[예 2.2] Weierstrass 방정식이 $y^2 = x^3 + x^2$으로 주어졌을 때, $(0:0:1)$은 특이점이다.

나) 무한원점($\mathcal{O}$)이란 E에서 Z-좌표가 0인 점, 즉 $(0:1:0)$을 말한다.

■ **정의 2.2** (타원 곡선 (E)) 비특이 3차 곡선, $P^2(\bar{K})$에서 매끄러운 Weierstrass 방정식의 해 집합, $A^2(\bar{K})$에서 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a^6$의 해 집합과 무한원점($\mathcal{O}$), 또는 지너스 1의 대수 곡선을 일컫는다.

타원 곡선 E에서 $a_i \in K(i = 1,2,3,4,6)$일 때, 즉, K 위에서 정의된 타원 곡선 E는 E/K로 표기하고, 타원 곡선 E에서 K-유리점들의 집합, 즉, 집합 $\{(x,y) \in K \times K \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$은 $E(K)$로 표기한다.

[예 2.3] $E/F_{11} : y^2 = x^3 + x + 6$

■ **정의 2.3**

판별식 (Δ) : $= -(a_1^2 + 4a_2)^2 (a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2) - 8(2a_4 + a_1a_3)^3 - 27(a_3^2 + 4a_6)^2 + 9(a_1^2 + 4a_2)(2a_4 + a_1a_3)(a_3^2 + 4a_6)$이고, 특히, $\Delta \neq 0$일 때, E는 타원곡선이다.

j-불변식 ($j(E)$) :

$$= \frac{((a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3))^3}{\Delta}$$

($\Delta \neq 0$일 때).

$E_1/K \cong E_2/K \Rightarrow j(E_1) = j(E_2)$. 단, 역은 K가 대수적 폐포체일 때 성립한다.

또한, 유한체 K 위에서 정의된 타원 곡선이 $\mathrm{char}(K) \neq 2, 3$일 때(즉, $E/K : y^2 = x^3 + ax + b$, $a,b \in K$), 판별식 $\Delta = -16(4a^3 + 27b^2)$이고, j-불변식은 $-1728(4a)^3/\Delta$이다. $\mathrm{char}(K) = 2$일 때, 유한체 K 위에서 정의된 타원 곡선은 j-불변식의 값에 따라 두 가지 형태로 나타난다.

j-불변식의 값이 0이 아닐 때, 곡선 E_1/K는 $y^2 + xy = x^3 + ax^2 + a_6$로 표현되고, $\Delta = a_6$, $j(E_1) = 1/a_6$이다.

j-불변식의 값이 0일 때, 곡선 E_2/K는 $y^2 + a_3y = x^3 + a_4x + a_6$로 표현되고, $\Delta = a_3^4$, $j(E_2) = 0$이다.

[예 2.4] $E/F_{11} : y^2 = x^3 + x + 6$일 때, $\Delta = -16(4 \times 1^3 + 27 \times 6^2) \equiv -40 \equiv 4 \pmod{11}$이고, $j(E/F_{11}) = -1728(4)^3/4 \equiv 6 \pmod{11}$이다.

■ **정의 2.4**

초특이 타원 곡선(Supersingular Elliptic Curve)이란 $q = p^m$(p: 소수)이고, $\mathrm{char}(F_q) = p$, $\#E(F_q) = q + 1 - t$일 때, p가 t를 나누는 곡선을 말한다. 만일 $\#E(F_q) = p + 1$이면, F_p에서 정의된 타원 곡선 E는 초특이 타원 곡선이다. 특히, $p = 2$ 또는 $p = 3$인 경우 $j(E) = 0$과 동치이다.

비 초특이 타원 곡선(Non-supersingular Elliptic Curve)이란 초특이 타원 곡선이 아닐 때를 일컫는다.

2.2.2 K 위에서의 곡선

타원 곡선위의 점들이 어떤 더하기 연산 아래에서 가환군을 이룬다는 것은 이미 잘 알려진 사실이다. 더하기 규칙은 다음과 같다.

〈성질〉

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$에 의해 타원 곡선 E가 주어졌을 때, 모든 점 P, $Q \in E$에 대하여,

가) $\mathcal{O} + P = P + \mathcal{O} = P$. (즉, $\mathcal{O}$는 항등원 역할을 한다.)

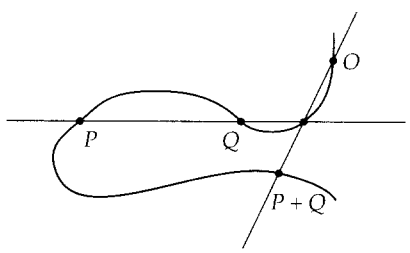
나) $-\mathcal{O} = \mathcal{O}$.

다) $P = (x_1,y_1) \neq \mathcal{O} \Rightarrow -P = (x_1, y_1 - a_1x_1 - a_3)$.

라) $Q = -P \Rightarrow P + Q = O$.

마) $P \neq O$, $Q \neq O$ 그리고 $Q \neq -P$이면 $P + Q = -R$이다.

단, R = { 곡선 E와 직선 $\overline{PQ}$의 세번째 교점 ($P \neq Q$일 때); 곡선 E에서 점 P의 접선과의 교점 ($P = Q$일 때). }



〈더하기 연산〉

$P = (x_1,y_1)$, $Q = (x_2,y_2)$, $P + Q = (x_3,y_3)$라 하고, 직선 l을 $P \neq Q$일 때 P와 Q를 지나는 직선 또는 $P = Q$일 때 점 P에서 곡선 E의 접선이라 하자. 직선 l을 $y = \lambda x + \beta$라 할 때,

$$\text{기울기 } \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & (P \neq Q\text{일 때}) \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & (P = Q\text{일 때}) \end{cases}$$

이고, (2.1)

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \beta - a_3$$

이다. 그러므로, 유한체 K에서 $P + Q$는 다항식 시간안에서 계산이 가능하다.

❖ 정리 2.5 $E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $E_2 : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$로 주어진 두 타원 곡선 E_1/K와 E_2/K가 '유한체 K 위에서 동형이다'와 동치조건은 'E_1의 방정식에서 변수 (x,y)를 $(u^2x + r, u^3y + u^2sx + t)$로 변화시켜 E_2의 방정식으로 변화시킬 수 있는 u,r,s,t $(\in K)$ $(u \neq 0)$가 존재한다'이다.

표수가 2, 3이 아닌 유한체 K 위에서 정의된 타원 곡선의 Weierstrass 방정식은 허용 변수 변화(admissible change of variables)에 의해 아래 식으로 상당히 단순화 시킬 수 있고, 각각 표수가 2 또는 3일 때에도 단순화 시킬 수 있으나, 표수가 3일 때의 단순화는 본 논문에서 생략하기로 한다.

2.2.2.1 char(K) $\neq$ 2,3

Weierstrass 방정식이 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$으로 주어졌을 때, 표수가 2가 아니면 허용 변수 변화 $(x,y) \rightarrow (x, y - \frac{a_1}{2}x - \frac{a_3}{2})$에 의해 $E'/K : y^2 = x^3 + b_2x^2 + b_4x + b_6$로 변화될 수 있고, 표수가 2, 3이 아니면, 허용 변수 변화 $(x,y) \rightarrow (\frac{x - 3b_2}{36}, \frac{y}{216})$에 의해 $E''/K : y^2 = x^3 + ax + b$, a,b $\in K$로 변화될 수 있다(즉, $E \cong E' \cong E''$).

〈더하기 연산〉

가) $P = (x_1,y_1) \in E \Rightarrow -P = (x_1,-y_1)$.

나) $Q = (x_2,y_2) \in E$, $Q \neq -P$

$\Rightarrow P + Q = (x_3,y_3)$.

단, $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$,

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & (P \neq Q\text{일 때}) \\ \dfrac{3x_1^2 + a}{2y_1} & (P = Q\text{일 때}). \end{cases} \quad (2.2)$$

2.2.2.2 $\mathrm{char}(K) = 2$

E/K를 Weierstrass 방정식 $E : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$에 의해 주어진 타원곡선이라 하고, 표수가 2이면, $j(E) = (\bar{a}_1^{12})/\Delta$으로 구할 수 있다. $j(E) \neq 0$, 즉 $\bar{a}_1 \neq 0$이면, E는 허용 변수 변화 $(x, y) \rightarrow (\bar{a}_1^2x + \frac{\bar{a}_3}{\bar{a}_1}, \bar{a}_1^3y + \frac{\bar{a}_1^2\bar{a}_4 + \bar{a}_3^2}{\bar{a}_1^3})$에 의해 $E_1/K : y^2 + xy = x^3 + a_2x^2 + a_6$ $(j(E_1) \neq 0)$로 변화될 수 있다. $j(E) = 0$, 즉, $\bar{a}_1 = 0$이면, E는 허용 변수 변화 $(x, y) \rightarrow (x + \bar{a}_2, y)$에 의해 $E_2/K : y^2 + a_3y = x^3 + a_4x + a_6$로 변화될 수 있다.

〈더하기 연산, $E_1/K : y^2 + xy = x^3 + a_2x^2 + a_6$ $(j(E_1) \neq 0)$〉

가) $P = (x_1, y_1) \in E_1 \Rightarrow -P = (x_1, y_1 + x_1)$.

나) $Q = (x_2, y_2) \in E_1$, $Q \neq -P$

$\Rightarrow P + Q = (x_3, y_3)$.

$$\text{단, } x_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 \\ \quad + x_2 + a_2 \quad (P \neq Q\text{일 때}), \\ x_1^2 + \frac{a_6}{x_1^2} \quad (P = Q\text{일 때}) \end{cases}$$

$$y_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) \\ \quad + x_3 + y_1 \quad (P \neq Q\text{일 때}) \\ x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3 \\ \quad (P = Q\text{일 때}). \end{cases}$$

〈더하기 연산, $E_2/K : y^2 + a_3y = x^3 + a_4x + a_6$ $(j(E_2) = 0)$〉

가) $P = (x_1, y_1) \in E_2 \Rightarrow -P = (x_1, y_1 + a_3)$.

나) $Q = (x_2, y_2) \in E_2$, $Q \neq P$

$\Rightarrow P + Q = (x_3, y_3)$.

$$\text{단, } x_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2 \\ \quad (P \neq Q\text{일 때}) \\ \frac{x_1^4 + a_3^2}{a_3^2} \quad (P = Q\text{일 때}), \end{cases}$$

$$y_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) \\ \quad + y_1 + a_3 \quad (P \neq Q\text{일 때}) \\ \left(\frac{x_1^2 + a_4}{a_3}\right)(x_1 + x_3) \\ \quad + y_1 + a_3 \quad (P = Q\text{일 때}). \end{cases}$$

2.2.3 인자 정리(Divisor Theory)

인자(divisor)는 유리함수의 극점과 영점의 진로를 보여주는 유용한 장치이다. 또한 1990년에 Menezes, Okamoto와 Vanstone[4]은 타원곡선에서의 이산 대수 문제를 어떤 유한체위에서의 이산 대수 문제로 바꾸는 과정에서 인자 정리를 사용하여 Weil 쌍을 계산하였다.

■ **정의 2.6** 가) 인자 D는 E_q점들의 형식적인 합이다. $D = \sum_{P \in E} n_P(P)$ $(n_P \in Z$, 유한개의 $P \in E$를 제외하면 $n_P = 0)$.

나) 인자 D의 대(supp(D))란 $\{P \in E \mid n_P \neq 0\}$을 말한다.

다) 인자 D의 차수(deg(D))란 $\sum n_P$ $(\in Z)$을 말한다.

라) 차수가 0인 모든 D의 집합은 D^0로 표기한다.

마) K 위에서 E의 좌표환은 $K[E]$로 표기한다. 즉, $K[E]$란 $r(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ $(\in K[x,y])$일 때, $K[E] = K[x,y]/(r)$이다. $((r) : K[x,y]$에서 r에 의해 생성되는 이디얼).

바) $K[E]$의 체분수 또는 K 위에서 E의 체함수는 $K(E)$로 표기한다.

사) 유리함수란 $\bar{K}(E)$의 원소를 말한다.
$f \in \bar{K}(E)^*$는 0이 아닌 유리함수이고, $P \in E\backslash\{O\}$라 하자.

아) f가 $f = g/h$, $(g, h \in \bar{K}[E], h(P) \neq 0)$로 표현될 수 있을 때, f는 P에서 정의되었다고 하고, f가 P에서 정의되었을 때, $f(P) = \frac{g(P)}{h(P)}$로 정의한다. 만일 $f(P) = 0$이면, f는 P에서 영점을 갖는다고 하고, f가 P에서 정의되지 않으면 f는 극점을 갖는다고 하며 $f(P) = \infty$로 표기한다.

자) P에 대한 일의화 매개변수 u란 모든 점 $P \in E$에 대하여, $f \in K(E)^*$이면, $f = u^d s$로 쓸 수 있는 유리함수 $u \in \bar{K}(E)$, $(u(P) \neq 0)$가 존재할 때 그 u를 말한다 $(s \in \bar{K}(E), s(P) \neq 0, \infty)$.

❖ **정리 2.7** $P \in E$, P에서 E의 접선이 아닌 P를 지나는 직선을 $l : ax + by + c = 0$이라 하면, l은 P에 대한 일의화 매개변수이다.

[예 2.5] 타원 곡선을 $E/F_q : y^2 = x^3 + ax + b$라 놓자 $(\mathrm{char}(F_q) \neq 2,3)$.

가) $P = (c,d) \notin E[2]$라 하면, P에서의 E에 대한 접선 방정식은 $(-3c^2 - a)(x - c) + 2d(y - d) = 0$이고, $d \neq 0$이므로 P에 대한 일의화 매개변수는 $u = x - c$이다.

나) $P = (c,0) \in E$를 위수 2인 점이라 하면, P에서의 E에 대한 접선 방정식은 $(-3c^2 - a)(x - c) = 0$이므로 P에 대한 일의화 매개변수는 $u = y$이다. $f \in K(E)$, $P \in E$라 하고, $f = u^d s$로 쓰자 (u : P에 대한 일의화 매개변수, $s \in \bar{K}(E)$, $s(P) \neq 0, \infty$). P에서 f의 위수를 d로 정의하고, $ord_P(f) = d$라고 표기한다. 함수 f는 E 위에서 단지 유한개의 영점과 극점을 가지므로 f의 인자($\mathrm{div}(f)$)를 $\mathrm{div}(f) = \sum_{P \in E} ord(f)(P)$와 같이 정의할 수 있다.

[예 2.6] 타원 곡선을 $E/F_q : y^2 = x^3 + ax + b$라 놓자 $(\mathrm{char}(F_q) \neq 2,3)$.

가) $P = (c,d) \notin E[2]$라 하면, $\mathrm{div}(f) = (P) + (-P) - 2(O)$이다.

나) P_1, P_2, P_3를 위수 2인 점들이라 하면, $\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(O)$이다.

다) $b \neq 0$이라 가정하고, $P_1 = (0, \sqrt{b})$, $P_2 = (0, -\sqrt{b})$라 하면, $\mathrm{div}(x/y) = (P_1) + (P_2) + (O) - (P_1) - (P_2) - (P_3)$이다.

어떤 $f \in K(E)^*$가 $D = \mathrm{div}(f)$를 만족하면, '인자 $D(\in D^0)$는 주요하다' 라고 한다.

❖ **정리 2.8** 인자 D를 $\sum n_P(P)$라 할 때, '인자 $D(\in D^0)$는 주요하다'와 동치 조건은 $\deg(D) = 0$이고, $\sum n_P P = O$이다.

D_f을 모든 주 인자들의 집합이라 하자. $f_1, f_2 \in K(E)$이면 $\mathrm{div}(f_1 f_2) = \mathrm{div}(f_1) + \mathrm{div}(f_2)$이다. 즉, D_f은 D^0의 부분군의 형태를 띤다. $D_1 - D_2 \in D^0$, 즉, 어떤 $f \in \bar{K}(E)$에 대하여 $D_1 = D_2 + \mathrm{div}(f)$이면 '두 인자 $D_1, D_2(\in D^0)$가 동형이다' 라고 말하고, $D_1 \sim D_2$로 표기한다.

2.2.4 Z_n 위에서의 타원 곡선

Z_n 위에서의 타원 곡선은 Lenstra's integer factoring algorithm[11]과 Goldwasser-Kilian primality proving algorithm[10]에서 사용되었다.

n을 6과 서로소라 하자. Z_n 위에서의 타원 곡선은 다음과 같이 주어진다.

$$E_{a,b} : y^2 = x^3 + ax + b,$$
$$(a,b \in Z,\ \gcd(4a^3 + 27b^2,\ n) = 1).$$
$$E_{a,b}(Z_n) = \{(x,y) \in Z_n \times Z_n \mid$$
$$y^2 = x^3 + ax + b\} \cup \{O\}.$$

앞에서 정의한 덧셈과 같은 방법으로 의덧셈을 정의할 수 있으나, 이 의덧셈 아래에서는 덧셈이 정의되지 않을 수도 있기 때문에 $E_{a,b}(Z_n)$는 군이 되지를 못한다. 왜냐하면,

$$(x_2 - x_1,\ n) > 1 \qquad (P \neq Q\text{일 때})$$
$$(2y_1,\ n) > 1 \qquad (P = Q\text{일 때})$$

인 경우, Z_n에서 역원이 존재하지 않는 원이 있기 때문에 λ를 구할 수 없다.

〈의덧셈의 성질〉

가) $P, Q \in E_{a,b}(Z_n)$와 $P + Q$가 정의되지 않는다면, 덧셈 규칙의 적용에서 n의 자명하지 않는 인수를 발생시켜야 한다.

나) $P, Q \in E_{a,b}(Z_n)$와 $P + Q$가 의덧셈에 의해 정의된다면, n의 모든 소인자 p에 대하여 $(P+Q)_p = P_p + Q_p$를 만족한다.

다) $P \in E_{a,b}(Z_n)$, $k \in Z$라 하자. kP가 의덧셈의 반복 적용에 의해 정의된다면, n의 모든 소인자 p에 대하여 $(kP)_p = kP_p$를 만족한다.

$n = pq$라 가정하고 $\tilde{E}_{a,b}(Z_n) = E_{a,b}(F_p) \times E_{a,b}(F_q)$이라 하면, $\tilde{E}_{a,b}(Z_n)$은 두 군의 직합이며 군이 된다. 각 점 $P \in E_{a,b}(Z_n)$는 $\tilde{E}_{a,b}(Z_n)$의 원소(즉, (P_p, P_q))에 유일하게 대응된다. 이 대응은 점 (P, Q)가 $P = (O)_p$ 또는 $Q = (O)_q$인 경우를 제외하면 ($P = (O)_p$이고, $Q = (O)_q$인 경우는 제외), $\tilde{E}_{a,b}(Z_n)$의 모든 원소에 대해 성립한다. 의덧셈의 성질 나)에 의하여, $E_{a,b}(Z_n)$에서의 덧셈 연산과 $\tilde{E}_{a,b}(Z_n)$에서의 군 연산이 일치하기 때문에, p와 q를 모르더라도 군 $\tilde{E}_{a,b}(Z_n)$에서 계산을 할 수 있다. 또한 p, q가 크다면(각각 100자리 이상), n의 소인수분해는 풀 수 없다.

2.3 유한체 위에서 타원 곡선의 동형류

■ **정의 2.9** (동형) V_1과 V_2가 사영 다양체로서 동형일 때, 즉, $\phi : V_1 \to V_2$, $\psi : V_2 \to V_1$일 때 $\phi \circ \psi$와 $\psi \circ \phi$들이 각각 V_1, V_2에서 항등함수이면 'V_1과 V_2가 동형이다' 라고 말한다.

2.3.1 F_q 위에서 타원 곡선의 동형류, $\mathrm{char}(F_q) \neq 2,3$

$$E_1/F_q : y^2 = x^3 + ax + b,$$
$$a, b \in F_q \qquad (2.3)$$
$$E_2/F_q : y^2 = x^3 + ax + b,$$
$$a, b \in F_q \qquad (2.4)$$

를 F_q 위에서 동형이라 하자.

다음 3가지 경우를 살펴보자.

가) $a \neq 0$, $b \neq 0$ (즉, $j(E) \neq 0, 1728$)이면 $u^6 = \frac{ab}{ab}$이므로 해는 $u \in \{u', -u'\}$이다.

나) $a = 0$, $b \neq 0$ (즉, $j(E) = 0$)이면 $u^6 = \frac{b}{b}$이므로 F_q^*가 위수 3의 원소 α를 갖는다면 6개의 해가 있다 ($u \in \{u', \alpha u', \alpha^2 u', -u', -\alpha u', -\alpha^2 u'\}$). 그렇지않다면, 해는 $u \in \{u', -u'\}$이다.

다) $a \neq 0$, $b = 0$ (즉, $j(E) = 1728$)이면 $u^4 = \frac{a}{a}$이므로 F_q^*가 위수 4의 원소 β를 갖는다면 $u \in \{u', \beta u', \beta^2 u', \beta^3 u'\}$이다. 그렇지않다면 해는 $u \in \{u', -u'\}$이다.

❖ **정리 2.10** 유한체 F_q 위에서 $\mathrm{char}(F_q) > 3$일 때, 정의된 타원 곡선의 동형류 수는 $q \equiv 1, 5, 7, 11 \pmod{12}$일 때 각각 $2q+6$, $2q+2$, $2q+4$, $2q$이다.

2.3.2 F_q 위에서 타원 곡선의 동형류, $\mathrm{char}(F_q) = 2$

2.3.2.1 F_{2^m} 위에서 비초특이 타원 곡선의 동형류

❖ **정리 2.11** F_{2^m} 위에서의 비초특이 타원 곡선의 동형류는 $2(2^m - 1)$개가 있으며, $\{y^2 + xy = x^3 + a_2x^2 + a_6 \mid a_6 \in F_{2^m}^*, a_2 \in \{0, \gamma\}\}$의 형태를 가진다. ($\gamma$는 $\mathrm{Tr}(\gamma) = 1$인 F_{2^m}의 원소, 특히 m이 홀수이면 $\gamma = 1$으로 놓을 수 있다.) ($\mathrm{Tr} : F_{2^m} \to F_2$, $\mathrm{Tr}(\alpha) = \alpha + \alpha^{2^1} + \alpha^{2^2} + \cdots + \alpha^{2^{m-1}}$)

2.3.2.2 F_{2^m} 위에서 초특이 타원 곡선의 동형류, m : 홀수

3개의 F_{2^m} 위에서 초특이 타원 곡선의 동형류 (m : 홀수)가 있으며, 각 동형류의 형태는 다음과 같다.

가) $y^2 + y = x^3$
나) $y^2 + y = x^3 + x$
다) $y^2 + y = x^3 + x + 1$

2.3.2.3 F_{2^m} 위에서 초특이 타원 곡선의 동형류, m : 짝수

다음 3가지 곡선의 형태로 나누어 생각해 보자.

형태 Ⅰ : a_3가 입방체가 아닐 때.
형태 Ⅱ : a_3가 입방체이고, $Te(a_4) \neq 0$일 때.
형태 Ⅲ : a_3가 입방체이고, $Te(a_4) = 0$일 때.
($\mathrm{Te} : F_{2^m} \to F_4$, $\mathrm{Te}(\alpha) = \alpha + \alpha^{2^2} + \alpha^{2^4} + \cdots + \alpha^{2^{m-2}}$)

❖ **정리 2.12** 7개의 F_{2^m} 위에서 초특이 타원 곡선의 동형류 (m : 짝수)가 있으며, 각 동형류의 형태는 다음과 같다.

가) $E_1 : y^2 + \gamma y = x^3$ (형태 Ⅰ)
나) $E_2 : y^2 + \gamma y = x^3 + \alpha$ (형태 Ⅰ)
다) $E_3 : y^2 + \gamma^2 y = x^3$ (형태 Ⅰ)
라) $E_4 : y^2 + \gamma^2 y = x^3 + \beta$ (형태 Ⅰ)
마) $E_5 : y^2 + y = x^3 + \delta x$ (형태 Ⅱ)
바) $E_6 : y^2 + y = x^3$ (형태 Ⅲ)
사) $E_7 : y^2 + y = x^3 + \omega$ (형태 Ⅲ)

단, $\gamma (\in F_{2^m})$는 입방체가 아니고, α, β, γ, ω는 $Tr(\gamma^2\alpha) = 1$, $Tr(\gamma^4\beta) = 1$, $Te(\delta) \neq 0$, 그리고 $Tr(\omega) = 1$를 만족하는 F_{2^m}의 원소들이다.

2.4 타원 곡선의 이산 대수 문제

2.4.1 Weil 쌍

E를 유한체 F_q($\mathrm{char}\, F_q = p$)에서 정의된 타원 곡선이라 하자. $f \in \bar{F}_q(E)^*$를 D와 $\mathrm{div}(f)$가 서로대(disjoint supports)를 이루는 유리함수라 할 때, D에서 함수 f의 값을 $f(D) = \prod_{P \in supp(D)} f(P)^{n_P}$으로 정의할 수 있다.

$D = \sum n_P(P)$는 인자, $\gcd(m, p) = 1$, $\mu_m (\subset \bar{F}_q^*)$는 단위원의 m제곱근의 군, $P, Q \in E[m] (= \{P \in E(\bar{F}_q) \mid mP = \mathcal{O}\})$, A와 B는 $A \sim (P) - (\mathcal{O})$, $B \sim (Q) - (\mathcal{O})$를 만족하는 차수 0인 인자로 서로대를 갖는다고 하고 f_A, $f_B \in \bar{K}(E)$는 $\mathrm{div}(f_A) = mA$, $\mathrm{div}(f_B) = mB$를 만족하는 함수라 하자.

■ **정의 2.13** Weil 쌍, e_m은 다음과 같이 정의된 함수이다.

$$e_m : E[m] \times E[m] \rightarrow \mu_m,$$
$$\text{즉, } e_m(P, Q) = \frac{f_A(B)}{f_B(A)}.$$

이 때, $e_m(P, Q)$의 값은 A, B, f_A와 f_B의 선택과 독립적이다.

〈성질〉

가) 모든 $P \in E[m]$에 대하여, $e_m(P, P) = 1$.

나) 모든 $P, Q \in E[m]$에 대하여, $e_m(P, Q) = e_m(Q, P)^{-1}$.

다) 모든 $P, Q, R \in E[m]$에 대하여, $e_m(P+Q, R) = e_m(P, R)e_m(Q, R)$이고, $e_m(P, Q+R) = e_m(P, Q)e_m(P, R)$이다.

라) $P \in E[m]$이면 $e_m(P, \mathcal{O}) = 1$이고, 더우기 모든 $Q \in E[m]$에 대하여, $e_m(P, Q) = 1$이면 $P = \mathcal{O}$이다.

마) $E[m] \subset E(K)$이면, 모든 $P, Q \in E[m]$에 대하여 $e_m(P, Q) \in K$이다.(즉, $\mu_m \subset K^*$).

바) $P \in E[m]$, $Q \in E[mm']$이면 $e_{mm'}(P, Q) = e_m(P, m'Q)$이다.

2.4.2 Weil 쌍의 계산

$\gcd(m, p) = 1$이고, $P, Q \in E[m]$이라 할 때 Weil 쌍 $e_m(P, Q)$을 계산해 보자. $P+T \neq U$, $Q+U$이고 $T \neq U$, $Q+U$인 점 T, $U(\in E)$를 선택한다. $A = (P+T) - (T)$이라 하면, $A \sim (P) - (\mathcal{O})$이다. 마찬가지로 $B = (Q+U) - (U)$이라 하면, $B \sim (Q) - (\mathcal{O})$이다. f_A, $f_B \in \bar{K}(E)$를 $\mathrm{div}(f_A) = m(P+T) - m(T)$, $\mathrm{div}(f_B) = m(Q+U) - m(U)$를 만족하는 함수는 함수라 하자. 그러면, $e_m(P, Q) = \frac{f_A(B)}{f_B(A)} = \frac{f_A((Q+U) - (U))}{f_B((P+T) - (T))} = \frac{f_A(Q+U)f_B(T)}{f_A(U)f_B(P+T)}$ 이다.

[예 2.7] $E/F_{13} : y^2 = x^3 + 7x$라 할 때, $E(F_{13})$의 점들과 위수는 다음 표와 같다.

점	위수	점	위수
$P_0 = \mathcal{O}$	1	$P_9 = (5,11)$	6
$P_1 = (0,0)$	2	$P_{10} = (8,3)$	6
$P_2 = (2,3)$	6	$P_{11} = (8,10)$	6
$P_3 = (2,10)$	6	$P_{12} = (9,5)$	3
$P_4 = (3,3)$	3	$P_{13} = (9,8)$	3
$P_5 = (3,10)$	3	$P_{14} = (10,2)$	3
$P_6 = (4,1)$	3	$P_{15} = (10,11)$	3
$P_7 = (4,12)$	3	$P_{16} = (11,2)$	6
$P_8 = (5,2)$	6	$P_{17} = (11,11)$	6

위 표로부터 $\#E(F_{13}) = 18$, $E(F_{13}) \cong Z_6 \oplus Z_3$임을 알 수 있다. $P = P_4 = (3,3)$, $Q = P_6 = (4,1)$이라 하자. 이제 $e_3(P, Q)$를 구해보자. 임의로 점 $T = (8,3)$, $U = (5,2)$를 잡고, $P+T = (2,10)$, $Q+U = (5,11)$을 계산한다. 표준적인 인자의 형태는 다음과 같다.

$$3(P+T) - 3(\mathcal{O}) = (P_1) - (\mathcal{O}) + \mathrm{div}\left(\frac{(8x+y)(x+y+1)}{x(x+3)}\right). \quad (2.5)$$

$$3(T) - 3(\mathcal{O}) = (P_1) - (\mathcal{O}) + \mathrm{div}\left(\frac{(11x+y)(8x+y+11)}{x(x+4)}\right). \quad (2.6)$$

$$3(Q+U) - 3(\mathcal{O}) = (P_1) - (\mathcal{O}) + \mathrm{div}\left(\frac{(3x+y)(x+y+10)}{x(x+9)}\right). \quad (2.7)$$

$$3(U) - 3(\mathcal{O}) = (P_1) - (\mathcal{O}) + \mathrm{div}\left(\frac{(10x+y)(12x+y+3)}{x(x+9)}\right). \quad (2.8)$$

$\mathrm{div}(f_A) = 3(P+T) - 3(T)$, $\mathrm{div}(f_B) = 3(Q+U) - 3(U)$임을 앞에서 알았다. 그러므로

$$f_A = \frac{(8x+y)(x+y+1)(x+4)}{x(x+3)(11x+y)(8x+y+11)}$$

$$f_B = \frac{(3x+y)(x+y+10)}{(10x+y)(12x+y+3)}$$

이다. 결론적으로,

$$e_3(P,Q) = \frac{f_A(Q+U)}{f_A(U)}\frac{f_B(T)}{f_B(P+T)} = 9$$이다.

2.5 타원 곡선의 이산 대수문제를 유한체의 이산 대수문제로의 축소

$P \in E(F_q)$이고 P의 위수가 n일 때, 만약 주어진 P와 R에서 $R = mP$를 만족하는 정수 $m(0 \le m \le n-1)$이 존재한다면, 그 m을 찾는 타원 곡선 이산 대수 문제를 살펴보자.

〈알고리즘 1〉 m에 대한 부분적 정보

입 력 : 최대 위수가 n_1인 $P \in E(F_q)$, $R = mP$.
출 력 : $m' \equiv m \pmod{n'}$, $n' : n_2$의 약수.
단계 1 : 임의로 점 $T \in E(F_q)$를 선택한다.
단계 2 : $\alpha = e_{n_1}(P,T)$와 $\beta = e_{n_1}(R,T)$를 계산한다.
단계 3 : m'을 계산한다.

〈알고리즘 2〉

타원 곡선의 이산 대수 문제를 유한체의 이산 대수 문제로 축소하는 방법.

입 력 : 위수 n인 $P \in E(F_q)$, $R \in \langle P \rangle$.
출 력 : $R = mP$를 만족하는 정수 m.
단계 1 : $E[n] \subseteq E(F_{q^k})$를 만족하는 가장 작은 정수 k를 선택한다.
단계 2 : $\alpha = e_n(P,Q)$ (위수 n)을 만족하는 $Q \in E[n]$를 찾는다.
단계 3 : $\beta = e_n(R,Q)$를 계산한다.
단계 4 : m을 계산한다.

2.5.1 초특이 곡선

〈알고리즘 3〉 초특이 곡선의 축소

입 력 : 위수 n인 특이 곡선위의 점 $P \in E(F_q)$, $R \in \langle P \rangle$.
입 력 : $R = mP$를 만족하는 정수 m.
단계 1 : 위 표를 참고하여, k와 c를 결정한다.
단계 2 : 임의로 점 $Q' \in E(F_{q^k})$를 선택하고, Q를 $(\frac{cn_1}{n})Q'$로 놓는다.

곡선류	t	군구조	$E(F_{q^k})$의 형태	k	n_1	c
I	0	cyclic	$(q+1, q+1)$	2	$q+1$	1
II	0	$Z_{q+1+\sqrt{2q}} \oplus Z_2$	$(q+1, q+1)$	2	$(q+1)/2$	2
III	$\pm\sqrt{q}$	cyclic	$(\sqrt{q^3} \pm 1, \sqrt{q^3} \pm 1)$	3	$q+1 \mp \sqrt{q}$	$\sqrt{q} \pm 1$
IV	$\pm\sqrt{2q}$	cyclic	(q^2+1, q^2+1)	4	$q+1 \mp \sqrt{2q}$	$q \pm \sqrt{2q}+1$
V	$\pm\sqrt{3q}$	cyclic	(q^3+1, q^3+1)	6	$q+1 \mp \sqrt{3q}$	$(q+1)(q \pm \sqrt{3q}+1)$
VI	$\pm 2\sqrt{q}$	$Z_{\sqrt{q}\mp 1} \oplus Z_{\sqrt{q}\mp 1}$	$(\sqrt{q} \mp 1, \sqrt{q} \mp 1)$	1	$\sqrt{q} \mp 1$	1

〈표 : 초특이 곡선에 대한 정보〉

단계 3 : $\alpha = e_n(P, Q)$와 $\beta = e_n(R, Q)$를 계산한다.

단계 4 : m'을 계산한다.

단계 5 : $m'P = R$이 성립하는지 조사한다. 만일 성립하면 $m = m'$이다. 성립하지 않으면 단계 2로 되돌아간다.

2.5.2 비초특이 곡선

대부분의 비초특이 곡선에서 알고리즘 2(즉, 타원 곡선의 이산 대수 문제)는 완전 지수 복잡도를 갖는다.

2.5.3 F_{2^m}에서 체 연산

유한체 F_{2^m}에서 정의된 타원 곡선은 하드웨어적으로 구현하기 쉬워 가장 관심이 많다. 여기에서는 이 체위에서 산술 연산을 행하는 효율적인 방법에 대해 살펴보기로 하자. 체 F_{2^m}은 F_2 위의 차수 m인 벡터 공간으로 생각할 수 있다. 즉, 모든 F_{2^m}의 원소 α를 $\alpha = \sum_{i=0}^{m-1} a_i\alpha_i$, $(a_i \in \{0,1\})$로 유일하게 표현할 수 있는 m개의 원소 $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$가 F_{2^m}에 존재한다. 그러면 α를 0-1 벡터 $(a_0, a_1, \cdots, a_{m-1})$로 표현할 수 있으므로, 하드웨어에서 각 체 원소는 길이 m의 자리이동 레지스터안에 저장된다.

〈덧셈〉

체 연산의 더하기는 벡터 표현의 각 비트별로 배타적 논리합을 실행하고, 시간은 한번의 시계 회전만큼 걸린다.

〈제곱〉

일반적으로, F_2 위의 F_{2^m}에는 많은 다른 종류의 기저가 있다. F_2 위의 F_{2^m}에서 정규 기저는 $\{\beta, \beta^2, \beta^{2^2}, \cdots, \beta^{2^{m-1}}\}(\beta \in F_{2^m})$의 형태이고, 그러한 기저는 항상 존재한다고 알려져 있다[6]. 임의의 원소 $\alpha(\in F_{2^m})$가 주어지면, $\alpha = \sum_{i=0}^{m-1} a_i \beta^{2^i}, (a_i \in \{0,1\})$로 쓸 수 있다. 제곱승은 F_{2^m}에서 선형 연산자이므로, $\alpha^2 = \sum_{i=0}^{m-1} a_i\beta^{2^{i+1}} = \sum_{i=0}^{m-1} a_{i-1}\beta^{2^i} = (a_{m-1}, a_0, \cdots, a_{m-2})$ (첨자는 모듈러 m으로 축소 됨)으로 계산된다. 즉, F_{2^m}의 원소를 정규기저로 표현하면 체 원소의 제곱이 벡터 표현의 단순한 회전으로 나타나고, 하드웨어적으로 구현하기가 쉽다는 장점을 지닌다. 원소의 제곱을 하는데 걸리는 시간 또한 한번의 시계 회전이다.

〈곱셈〉

정규 기저의 표현에서 곱셈은 훨씬 더 복잡하다. $A = (a_0, a_1, \cdots, a_{m-1})$, $B = (b_0, b_1, \cdots, b_{m-1}) \in F_{2^m}$이라 하고, $C = A \cdot B = (c_0, c_1, \cdots, c_{m-1})$라 놓자. 그러면, $C = \sum_{k=0}^{m-1} c_k\beta^{2^k} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i a_j \beta^{2^i}\beta^{2^j}$이다. $\beta^{2^i}\beta^{2^j} = \sum_{k=0}^{m-1} \lambda_{i,j}^{(k)} \beta^{2^k}$, $\lambda_{i,j}^{(k)} \in \{0, 1\}$이라 놓으면, β^{2^k}의 계수 비교에 의해 $c_k = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i a_j \lambda_{i,j}^{(k)}$, $0 \le k \le m-1$이다. 다시말하면, $c_k = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j \lambda_{i-k, j-k}^{(0)} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_{i+k} b_{j+k} \lambda_{i,j}^{(0)}$로 쓸 수 있다. 그러므로 입력 A, B를 갖는 논리회로가 곱 디지트 c_0를 계산할 수 있다면, 입력 A^{2^k}, B^{2^k}를 갖는 같은 회로로 곱 디지트 c_k를 생성할 수 있다. 이와같은 방법으로 C는 m번의 시계 회전으로 구할 수 있다. Massey와 Omura[7]는 정규 기저들의 이 특이한 성질을 조사하기 위해 serial-in serial-out multiplier를 설계했다. 그러한 회로의 복잡도는 0이 아닌 $\lambda_{i,j}^{(0)}$의 갯수 C_N에 의해 결정된다 $(2m-1 \le C_N \le m^2)$. 특히, $C_N = 2m-1$이 성립하면, 그 정규 기저는 '최적이다'라고 말한다. 최적 정규 기저에 대해서는 Mullin, Onyszchuk, Vanstone과 Wilson[8]들에 의해 소개되고 연구되었다.

〈역원의 계산〉

곱셈의 수를 줄이는 관점에서 최선의 방법을 Itoh, Teechai와 Tsujii[9]들이 제안하였다. $\alpha \in F_{2^m}$, $\alpha \neq 0$이면, $\alpha^{-1} = \alpha^{2^m-2} = \alpha^{(2^{m-1}-1)^2}$이다. 이제 m 값의 각 경우에 따른 계산을 살펴보자.

가) m : 홀수

$2^{m-1} - 1 = (2^{(m-1)/2} - 1)(2^{(m-1)/2} + 1)$이므로, $\alpha^{2^{m-1}-1} = (\alpha^{2^{(m-1)/2}-1})^{2^{(m-1)/2}+1}$이다. 그러므로 일단 $\alpha^{2^{(m-1)/2}-1}$이 계산되어져 있다면(제곱에 드는 시간은 무시), $\alpha^{2^{m-1}-1}$를 계산하는 데 단지 한번의 곱셈이 필요하다.

나) m : 짝수

$\alpha^{2^{m-1}-1} = (\alpha^{2(2^{(m-2)/2}-1)})^{(2^{(m-2)/2}+1)+1}$이므로, 일단 $\alpha^{2^{(m-2)/2}-1}$이 계산되어져 있다면(제곱에 드는 시간은 무시), $\alpha^{2^{m-1}-1}$를 계산하는 데 두번의 곱셈이 필요하다. 위 과정을 귀납적으로 반복한다.

2.6 곡선과 체 K의 선택

두 점을 더할 때의 체 연산의 수를 최소화하는 곡선과 체 K를 선택해야 한다. $K = F_{2^m}$ 위에서의 곡선은 다음 4가지 이유에 의해 선호된다.

가) F_{2^m}에서의 산술은 표수가 2보다 큰 유한체에서의 산술보다 하드웨어적으로 구현하기가 쉽다.

나) 정규 기저를 사용하여 F_{2^m}의 원소를 나타내면, 체 원소의 제곱은 단순한 벡터 표현의 회전 이동으로 구할 수 있으므로 두 점을 더할 때 곱셈의 수를 줄일 수 있다.

다) F_{2^m} 위의 곡선은 점의 x 좌표와 한 비트(여분의 정보)가 주어진다면, 점의 y 좌표를 복구하기 쉽다. (이것은 ElGamal 암호시스템에서 메세지 확장을 줄일 때 유용하다.)

라) F_{2^m} 위의 초특이 타원 곡선에서 $a_3 = 1$으로 놓을 수 있기 때문에 점을 배로 더할 때 역원을 구하는 연산을 제거할 수 있다. 즉, 연산의 횟수를 더 줄일 수 있다.

이와같은 이유에 의해 먼저 비초특이 타원 곡선을 살펴보자. 알고리즘 2의 공격이 쉽지 않다면, 비초특이 타원 곡선에서 이산 대수 문제를 풀기 위한 알려진 최상의 알고리즘은 baby-step giant-step 알고리즘이다. 그러므로 비초특이 타원 곡선이 암호학적으로 적용하기에 적당하려면 곡선의 위수가 큰 소수(즉, 적어도 40자리 이상의 소인자)에 의해 나누어져야만 한다. 결론적으로 기반 체의 크기는 적어도 2^{130} 이상 이어야 하고, 또한 효율적인 체 연산을 위하여 최적 정규 기저를 가져야 한다. 더우기 곡선 군이 순회적이면 더 좋다. (예를 들면, $\#E(F_q)$가 중복 소인자를 가지지 않을 때, 즉, $\#E(F_q)$가 서로 다른 소수의 곱이면 $E(F_q)$는 순회적이다.). 곡선을 선택하는 한가지 방법은 $\#E(F_q)$를 직접 계산할 수 있도록 q가 충분히 작은 F_q 위에서 정의된 타원 곡선을 선택하고, 그 다음 적당한 n에 대하여 군 $E(F_{q^n})$을 사용한다($\#E(F_{q^n})$은 Weil 정리에 의해 쉽게 계산될 수 있다.). 또한 n을 선택할 때, n이 소수이거나 작은 소인자와 큰 소인자의 곱이어야 한다. 왜냐하면, l이 n을 나누면 $\#E(F_q)$이 $\#E(F_{q^n})$을 나누기 때문이다.

❖ **정리 2.14** (Weil 정리) E를 F_q 위에서 정의된 타원 곡선이라 하고, $t = q + 1 - \#E(F_q)$라 하면, $1 - tT + qT^2 = (1 - \alpha T)(1 - \beta T)$를 만족하는 복소수 α, β에 대하여 $\#E(F_{q^k}) = q^k + 1 - \alpha^k - \beta^k$이다.

2.7 그 밖의 타원 곡선의 활용

2.7.1 소인수 분해

타원 곡선 방법(ECM, Elliptic Curve Method)은 곱셈 군을 무작위 타원 곡선위의 점의 군으로 바꾸어 Pollard의 $(p-1)$ 방법을 사용하는 것이다.

〈정수 $n(>1)$의 자명하지 않는 약수를 찾는 방법〉

가) Z_n 위에서 정의된 타원 곡선과 $P \in E$, k를 선택한다. (k : 양의 정수, 많은 작은 소수들의 제곱승에 의해 나누어 진다.)

나) 곡선의 더하기 연산을 사용하여, kP를 계산한다.

다) $kP \equiv O \pmod p$인 n의 소인수 p를 찾는다 (즉, 만약 E가 동형 Weierstrass 방정식 $(y^2z = x^3 + axz^2 + bz^4)$과 $O = (0:1:0)$으로 주어졌다면, 'kP의 z 좌표가 p에 의해 나누어진다'와 동형이다.)

라) gcd(z 좌표, n)을 계산하여, n의 자명하지 않는 인수를 찾는다. 만일 하나의 곡선 E를 이용한다면, 위 알고리즘의 성질은 Z_p^*의 위수 $p-1$을 Z_p에서 좌표를 갖는 E 위의 점들의 군 $E(Z_p)$의 위수로 바꾼 Pollard의 $(p-1)$ 방법의 성질과 정확히 일치한다. Hasse의 정리에 의해 E의 점들의 군 $E(Z_p)$의 위수는 $p+1-t$의 형태를 띤다 (t : E와 p에 의존하는 정수, $|t| \le 2\sqrt{p}$). 만약 어떤 n의 소인수 $p(<n)$에 대하여 $p+1-t$가 작은 소수로부터 만들어진다면, 위의 알고리즘으로 n의 자명하지 않는 약수를 찾는 것은 쉽다. 그렇지않다면 n의 자명하지 않는 약수를 찾는 것은 쉽지 않다. 그러나 위 알고리즘으로 n의 자명하지 않는 약수를 찾지 못하면 다른 타원 곡선으로 알고리즘을 반복한다. 소인수가 다소 큰 것을 가질 수 있으면, 곡선 $E_{a,b}$를 사용할 수 있다.[10, 11]

2.7.2 소수성 판정

소수성 판정은 정수론에서 가장 관심있는 분야중의 하나이다. 1985년에 H. W. Lenstra[4]는 타원 곡선을 사용한 소인수 분해를 소개하였고, 소수성 판정을 위해 비슷한 방법을 찾기 원하였다. Goldwasser와 Kilian은 Schoof에 기인한 이론적 알고리즘과 함께 DOWNRUN 알고리즘의 구조를 사용하여 처음으로 그 방법을 찾았다. 그들은 이 알고리즘이 기대되는 임의의 다항식 시간안에 소수를 인식할 수 있음을 알았다. 거의 동시에 A. O. L. Atkin은 같은 아이디어에 기초한 유한체위에서 정의된 타원 곡선의 이론을 사용하여 실제적 알고리즘을 디자인하였다.

❖ **정리 2.15** $\gcd(N,6) = 1$, E/Z_N, $P \in E$, $s \mid m$($s,m \in Z$), 각 s의 소인수 q에 대하여 $(m/q)P = (x_q : y_q : z_q)$라 놓자. 모든 q에 대하여 $mP = O$이고, $\gcd(z_q, N) = 1$이라 가정하면, p가 N의 소인수일 때, $\#E(Z/pZ) \equiv 0 \pmod s$를 만족한다.

보조정리 2.16 위와 같은 조건하에서, $s > (\sqrt[4]{N}+1)^2$이면, N은 소수이다.

〈Goldwasser-Kilian 알고리즘〉

가) 소수일 것 같은 q에 대해, $m = 2q$를 만족하는 m개의 점을 갖는 타원 곡선 $E(Z_N)$을 선택한다.

나) $s = m$일 때, 위 정리의 조건을 (E,m)이 만족하면, N은 소수이고, 그렇지 않으면 N은 합성수이다.

다) q의 소수성도 같은 방법으로 증명된다.

그러나 $\#E(Z/pZ)$를 계산하는 Schoof의 알고리즘은 거의 구현하기 불가능하다. GK 알고리즘은 곡선을 찾는 것부터 시작하여, 곡선위의 점들의 갯수를 센다. 또한 GK 알고리즘과 정확히 반대 과정인 타원 곡선 소수성 판정(ECPP, Elliptic Curve Primality Proving) 알고리즘이 있다.

제 3 절 ECC의 분류와 구성

3.1 ECC의 분류

3.1.1 유한체위에서의 ECC

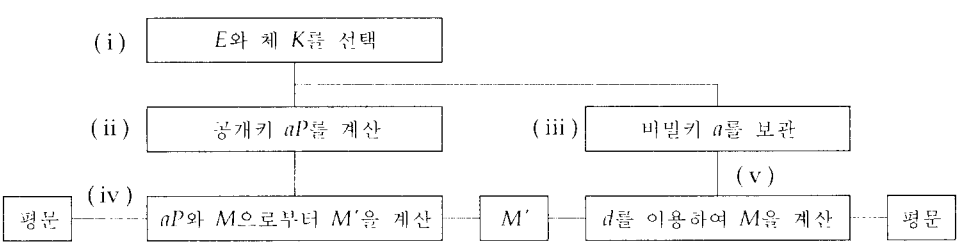
유한체위에서의 타원 곡선을 사용하는 ECC에서는 E의 크기를 반드시 알아야 한다. 만일 $K = F_q$가 유한체이면, E는 유한군이고, Hasse의 정리에 의해 E의 위수는 다음 부등식을 만족시킨다. $|\#E - (q+1)| \leq 2\sqrt{q}$. 즉, 그 군의 크기는 그 유한체의 크기와 거의 비슷하다. 모든 타원 곡선에 대해 $\#E$를 구하는 효율적인 알고리즘을 찾으려는 시도는 1985년 Schoof의 논문을 시작으로 많이 연구되어 왔다. N. Elkies, V. Miller, J. Buchmann과 그의 제자들, S. A. Vanstone과 그의 제자들의 연구와 특히 A. O. L. Atkin의 새로운 아이디어로 인하여 q가 200자리 이상인 유한체 F_q 위에서 정의된 타원 곡선의 크기 $\#E$는 실제적으로 계산 가능하게 되었다. 초특이 타원 곡선의 크기를 구하는 것은 쉬웠기 때문에 처음으로 제안되었다. 그러나 이 곡선들은 이산 대수 문제가 작은 차수의 확장체 K에서의 이산 대수 문제로 축소되는 치명적인 약점을 가진다. 비초특이 타원 곡선에서는 일반적으로 그러한 축소 알고리즘이 존재하지 않고, 단지 지수 복잡도를 갖는 Pollard의 알고리즘만이 알려져 있다.

3.1.2 환위에서의 ECC

각 사용자(A)는 2개의 큰 소수 p, q를 선택한다($p, q \equiv 2 \pmod 3$). $n = pq$를 계산한다. A는 $\gcd(e, (p-1)(q-1)) = 1$인 임의의 정수 e를 선택한다. $ed \equiv 1 \pmod{(p-1)(q-1)}$인 정수 d를 계산한다. A는 n과 e를 공개한다. 메세지 $m = (x,y) \in Z_n \times Z_n$을 A에게 보내기 위해 B는 $e\cdot(x,y) = (c_1, c_2) (\in \tilde{E}_{a,b}(Z_n) = E_{a,b}(F_p) \times E_{a,b}(F_q)$, $b \equiv y^2 - x^3 \pmod n$)를 계산한다.

3.1.3 3.1.1과 3.1.2의 차이점

3.1.1은 이산 대수 문제에 기초하여 시스템을 구축하지만, 3.1.2는 RSA 시스템과 같이 n의 소인수 분해의 어려움에 안전도를 기반 둔다. 그러나 그 시스템을 깨는 것이 n의 소인수 분해를 푸는 것과 동치인지는 아직 알려지지 않았다. 비록 RSA 시스템보다 비효율적이기는 하지만, RSA를 공격하는 지금까지 알려진 몇 개의 공격에 대해 안전하다. 또한, 곡선 위에서의 계산을 행하는 것이 메세지에 의존한다.



〈그림 : ECC의 일반적 구조도〉

3.2 ECC의 일반적 구조

$P \in E$, $a \in Z$, d는 a의 역원이고, M은 K의 원소이다.

(i)은 요구되는 안전도에 의해 곡선 E와 체 K를 선택한다(2.6절). (iv)에서 공개키 aP를 이용하여 M을 구하는 것은 타원 곡선의 이산 대수 문제이다. 또한, (iv)와 (v)에서의 연산 방법은 2.2.2절과 2.5.3절에서 언급되었다.

제 4 절 결 론

본 논문에서는 ECC의 구성에 필요한 수학적인 요소 이론들의 체계적으로 정리하고 이들이 ECC의 일반적인 구조에서 어떻게 활용되는 지를 나타내 보았다.

참 고 문 헌

[1] N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, 48(1987), 203-209.

[2] V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology - CRTYPTO '85, Lecture Notes in Computer Science, 218(1986), Springer-Verlag, 417-426.

[3] A.Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", IEEE Transactions on Information Theory, 39(1993), 1639-1646.

[4] H. W. Lenstra, "Factoring integers with elliptic curves", Annals of Mathematics, 126(1987), 649-673.

[5] S. Goldwasser and J. Kilian, "Almost all primes can be quickly cerified", Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing, 1986, 316-329.

[6] R. Lidl and H. Niederreiter, "Finite Fields", Cambridge University Press, 1987

[7] J. Omura and J. Massey, "Computational method and apparatus for finite field arithmetic", U.S.patent number 4, 587, 627, May 1986.

[8] R. Mullin, I. Onyszchuk, S. Vanstone and R. Wilson, "Optimal normal bases in GF(p^n)", Discrete Applied Mathematics, 22(1988/89), 149-161.

[9] T.Itoh, O. Teechai and S. Tsujii, "A fast algorithm for computing multiplicative inverses in GF(2^n) using normal bases" (in Japanese) J. Society for Electronic Communications(Japan), 44(1986), 31-36.

[10] R. P. Brent, "Some integer factorization algorithms using elliptic curves", Research report CMA-R32-85, The Australian National University, Canberra, 1985.

[11] D. V. Chudnovsky and G. V. Chudnovsky, "Sequences of numbers generated by addition in formal groups and new primality and factorization test", Advances in Applied Mathematics, 7(1986), 187-237.

[12] A. Menezes, "Elliptic Curve Public Key Cryptosystems", Kluwer Academic Publishers, 1993.

[13] J. H. Silverman, "The Arithmetic of Elliptic Curves", Springer-Verlag, 1986.

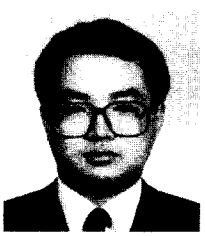
□ 著者紹介

이 인 수

연세대학교 이과대학 수학과 졸업(이학사)
현재 연세대학교 본 대학원 수학과 석사과정

진 원 일

연세대학교 이과대학 수학과 졸업(이학사)
한국과학기술원 수학과 졸업(이학석사)
(주)한국마이크로소프트
연세대학교 본 대학원 수학과 박사과정



김 철

연세대학교 이과대학 수학과 졸업(이학사)
미국 North Carolina 주립대 대학원 수학과 졸업(이학석사.박사)
미국 North Carolina 주립대 수학과 시간강사
미국 Shaw University 전임강사
미국 University of South Dakota 수학과 부교수
현재 광운대학교 이과대학 수학과 부교수

※ 관심 분야 : 추상 대수학의 응용, 암호학의 수학적 이론 및 응용 등임.