通信情報保護學會論文誌
第 8 卷 第 3 號. 1998. 9

새로운 타원곡선 이산로그 공격

천정희*, 김환준**, 한상근**, 박춘식*

On the Discrete Logarithm of an Elliptic Curve

Jung Hee Cheon*, Hwanjoon Kim**, Sang Geun Hahn**, Choonsik Park*

요 약

타원곡선 이산로그는 특별한 경우에는 다항식 시간 혹은 준지수 시간안에 푸는방법이 알려져 있으나, 일반적인 경우에는 지수 시간이 걸려야 풀 수 있는문제로 알려져 있다. 본 고에서는 타원곡선 이산로그를 푸는 새로운 방법을 제시한다. 본 방법에 의하면 유한체 위에서 정의된 타원곡선을 rank가 3 이하인 유리수위의 타원곡선으로 lifting할 수 있으면 다항식 시간안에타원곡선 이산로그 문제를 풀 수 있다.

Abstract

In general, there are no algorithm of subexponential running time for solving the elliptic discrete logarithm problem. In this paper, we propose new method of solving the elliptic discrete logarithm of elliptic curves by using the lifting over Q and the canonical height.

Ⅰ. 서 론

$\tilde{E}$ 가 F_p위에서 정의된 타원곡선으로 임의의 두점 $\tilde{P},\tilde{Q} \in \tilde{E}(F_p)$가 $m\tilde{P}=\tilde{Q}$의 관계에 있을 때, $log_{\tilde{P}}\tilde{Q}$을 m으로 정의하자. 이 경우, $log_{\tilde{P}}\tilde{Q}$ 을 구하는 문제를 타원곡선 위에서의 이산대수 문제(discrete logarithm problem on an elliptic curve) 혹은 타원로그문제(elliptic logarithm problem)라 한다[2]. 임의의 군 위의 이산로그를 푸는 방법으로는 baby-step giant-step, Pollard rho, Pohlig-Hellman, index calculus 방법 등이 있으며,[3] 타원곡선 군의 특수한 성질을 이용하여 타원로그를 푸는 방법은 singular, supersingular, anomalous 타원곡선의 경우에 알려져 있다.

* 한국전자통신연구원
** 한국과학기술원 수학과

1.1 일반적인 경우 (General case)

- Baby-step giant-step과 Pollard rho방법은 군의 위수가 n일 때 $O(\sqrt{n})$의 계산량을 가지는 방법으로 n이 2^{120}이상이면 이산로그를 풀 수 없다.
- Pohlig-Hellman의 방법은 군의 위수가 작은 소수의 곱으로 인수분해 될 때 각각의 prime subgroup 상에서 이산로그를 구한 후 중국인의 나머지 정리를 이용하여 전체 군에서의 이산로그를 푸는 방법이다. 이 방법에서 시간이 걸리는 부분은 각 부분군에서 이산대수를 푸는 과정이므로 이 방법에 견디기 위해서는 주어진 군의 위수가 큰 소수 인수(적어도 2^{120}이상)를 포함하여야 한다.
- Index calculus방법은 위 방법 중에 유일하게 subexponential time 알고리즘이다. 그러나 이 방법은 주어진 군의 구조에 의존하며 타원곡선 위의 이산로그에 대해서는 아직까지 불가능하다고 알려져 있다. 실제 Miller가 처음 타원곡선 암호를 제안할 때 index calculus 방법에 대해언급한 바 있는데, 그는 factor base의 가능성이 있는 후보는 유한체 위에 정의된 타원곡선을 유리수 위로 lifting하여 그 중 height가 작은 점들이나, 이 점들의 개수가 너무 적고, 많은 점들을 lifting하기가 어려워 index calculus 방법을 적용하는 것이 불가능하다고 주장하였다[5].

1.2 특수한 타원곡선의 경우 (Special case)

- **Singular case**

  타원곡선을 정의하는 다항식이 특이점(singular point)를 가질 경우, 이 곡선은 singular 하다고 한다. 이 경우 대응되는 타원곡선 군은 유한체와 동형이며 그 동형사상을 구체적으로 찾을 수 있다. 실제 E/F_q가 cusp을가질 경우 다음이 성립한다[9].

$$E_{ns}(F_q) \cong F_q.$$

- **Supersingular Case**

  유한체 F_q위에 정의된 타원곡선의 위수는 $q+1-t$꼴로 쓰여질 수 있는데, q의 표수가 t를 나누는 경우 이 타원곡선은 supersin-gular 하다고 한다. Menezes, Okamoto, Vanstone은 1992년 Weil pairing을 사용하여 유한체 위의 타원곡선군과 유한체 사이의 explicit isomorphism을 찾아내었다[4]. 즉 타원곡선에 의존하는 정수 r에 대하여 다음이 성립한다.

$$E(F_q) \rightarrow F_{q^r}$$

  이때 타원곡선 E가 supersingular가 아닐 경우에는 r이 매우 큰 값을 갖게 되나, E가 supersingular일 경우에는 r이 6 이하의 값을 갖게 된다. 따라서 이 경우에 타원곡선 이산로그 문제는 유한체 위의 이산로그와 마찬가지로 subexponential time 알고리즘이 된다. 특히, $E(F_q) = q+1$일 경우 다음이 성립한다.

$$E(F_q) \rightarrow F_{q^2}$$

- **Anomalous Case**

  유한체 F_q위에 정의된 타원곡선의 위수가 p가 될 때 이 타원곡선을 anomalous 타원곡선이라 하며 그 위의 타원로그는 $O(\log p)$의 시간안에 풀리게 된다. 이

방법은 1995년 Semaev에 의해 처음 발견되었고[7], 1997년 Smart[11]와 Satoh[6]에 의해 독립적으로 다시 제안되었다. Semaev의 방법은 Ruck에 의해 임의의 Abelian Variety위의 이산로그를 푸는 방법으로 일반화되었다. Semaev의 방법은 divisor 이론을 사용하였으며 $O(\log p)$의 계산량이 필요하고, Smart와 Satoh의 방법은 완비체(Complete field) 위의 logarithm function을 사용하였고 $O(\log^4 p)$의 계산량이 필요하다. Smart와 Satoh는 완비체상에 정의된 타원곡선위의 이산로그는 $O(\log p)$의 계산량으로 쉽게 풀 수 있음에 착안하여, $E(F_q)$위의 점들을 $E(Q_p)$위의 점들로 lifting 시켜 타원로그 문제를 풀었다. 이 방법은 위수의 법 p에 대한 나머지 값을 찾는 것이므로 $E(F_q)\cong F_q$인 경우에만 의미가 있다. 또한 이 방법은 p가 소수의 멱수일 경우로도 확장할 수 있으나, Pohlig-Hellman의 방법과 F_p위에서의 Smart-Satoh의 방법을 반복 사용하는 것과 큰 차이가 없다.

2. 제안된 방법

타원로그문제를 준지수시간안에 푸는 방법은 특별한 경우의 타원곡선의 경우에만 알려져 있고, 일반적인 경우에는 알려져 있지 않다. 특히, 앞서 말한바와 같이 준지수시간 알고리즘인 Index calculus 방법은 아직 타원로그 문제에 적용하는 것이 불가능하다고 알려져 있다.

우리는 유한체 위에서 정의된 타원곡선을 유리수위에서 정의된 타원곡선으로 올림(lifting)으로서 타원로그문제를 준지수시간안에 푸는 방법을 제시한다. 이 방법은 일반적인 방법이며, 유리수위로 올린 타원곡선의 rank가 작을 경우에는 준지수시간안에 계산을 할수 있다. 다만, 유한체위에 정의된 타원곡선을 항상 유리수위의 rank가 작은 타원곡선으로 올릴 수 있는지의 여부는 미해결 문제이다.

우선, 다음 성질을 만족하는 타원곡선 E/Q가 존재한다고 가정하자.

1. E의 reduction modulo p는 $\tilde{E}$이고, 어떤 유리점 $P_1, P_2, \cdots, P_r \in E(Q)$이 존재하여, $\tilde{P}_1 = \tilde{P}$, $\tilde{P}_2 = \tilde{Q}$, $\tilde{P}_i = (i-2)\tilde{P} + \tilde{Q}$, $(i=3, 4, \cdots, r)$ 이다.
2. $P_1, \cdots, P_r$이 Z-linearly dependent하고 dependency equation을 찾을 수 있다. 이때 우리는 discrete logarithm problem을 풀 수 있다. 실제로,

$$a_1P_1 + \cdots + a_rP_r = O$$

이라 가정하면, reduction modulo p에 의하여

$$a_1\tilde{P} + a_2\tilde{Q} + a_3(\tilde{P}+\tilde{Q}) + \cdots + a_r((r-2)\tilde{P}+\tilde{Q}) = O$$

즉,

$$(a_2 + a_3 + \cdots + a_r)\tilde{Q} = -(a_1 + a_3 + 2a_4 + \cdots + (r-2)a_r)\tilde{P}$$

이 때, $a_1 + a_3 + 2a_4 + \cdots + (r-2)a_r$의 역수를 modulo $\mathrm{ord}(\tilde{P})$로 구하면, 우리는 m을 정확히 구할 수 있다. 대부분의 discrete logarithm problem 에서 $\mathrm{ord}(\tilde{P})$는 큰 소수이므로 어떤 정수가 $\mathrm{ord}(\tilde{P})$와 서로 소일 확률은 매우 크다 가정할 수 있다. 우리는 3절에서 최대 6개의 점까지 lifting되는 타원곡선이 존재함, 즉 조건 1이 $r \le 6$인 모든 r에 대하여 성립함을 보인다. 또한 4절에서는 3절에서 구한 타원곡선이 3 이하의 rank를 가질 경우에는 조건 2를 만족시킴을 보인다. 결론적으로 3절과 4절에서 보이는 내용들은 다음 두 정리로 요약될 수 있다.

Theorem 2.1 Reduction modulo p가 $\tilde{E}$이고, $\tilde{P}_1 = \tilde{P}$, $\tilde{P}_2 = \tilde{Q}$, $\tilde{P}_i = (i-2)\tilde{P} + \tilde{Q}$, $(i = 3, 4, \cdots, r)$

을 만족하는 $P_1, P_2, \cdots, P_r$을 포함하는 타원곡선 $E_r(Q)$를 $O(r^3)$번의 기본연산으로 찾을 수 있다. 이때 E_r의 계수는 $O(p^{3r})$을 넘지 않는다.

Theorem 2.2 정리 2.1에서 얻어진 타원곡선 E_r의 rank가 3 이하일 경우 다항식 시간 안에 타원로그 문제를 풀 수 있다. 실제, 주어진 세 점 P_i들의 canonical height가 최대 m일 때, 타원로그를 푸는데 드는 계산량은 $O(log\ M)$이다.

실제 임의의 타원곡선을 잡았을 경우 이 타원곡선이 1 이하의 rank를 가질 확률은 매우 높다고 알려져 있으나, 정리 2.1에서와 같은 방법으로 생성된 타원곡선, 즉 임의의 r개의 유리점을 갖는 타원곡선의 rank에 대하여는 알려진바가 없다. 그러나, 큰 rank(대략 10 이상)를 갖는 타원곡선을 생성하는 것은 대단히 어려운 일이라고 알려져 있으며 현재까지 알려져 있는 타원곡선 중에 rank가 가장 큰 것은 23 정도이다[1].

3. 유리수 위로의 올림 (Lifting over Q)

본 절에서는 최대 6개의 점을 E(Q)로 올리는(lift) 방법을 제시한다. 우선, $\tilde{E}$를 F_p위에서 정의된 타원곡선으로 다음과 같은 Weierstrass equation으로 주어 졌다고 가정하자.

$$\tilde{E}: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6.$$

이때, 다항식 $f(x,y,t_1,t_2,\cdots,t_7)$을 다음과 같이 정의하자.

$$\begin{aligned} f(x,y,t_1,t_2,\cdots,t_7) = &(1+pt_1)y^2+(a_1+pt_2)xy+(a_3+\\ &pt_3)y-(1+pt_4)x^3-(a_2+pt_5)x^2\\ &-(a_4+pt_6)x-(a_6+pt_7). \end{aligned}$$

$P_1,\cdots, P_6 \in \tilde{E}(F_p)$, $P_i=(x_i,y_i)$라 한다면, $\{f(x_i, y_i, t_1,t_2,\cdots, t_7)=0 | i=1, 2,\cdots, 6\}$은 t_i들에 대한 7 원 1차 연립방정식을 주게 된다. 따라서, 이 연립방정식의 근은 직선을 이루며, 이중 적당한 근 s_i들을 선택하여

$$E: f(x,y,s_1,s_2,\cdots,s_7)=0$$

라 정의하면 $\tilde{E}$의 유리체 위로의 lifting이 되며, P_i들은 모두 E의 유리점이된다.

Algorithm 1 (Lifting)

Input, for $0 \le a_i \le p-1$

$$\begin{aligned} \tilde{E}/Fp: f(x,y) = &a_1y^2+a_2xy+a_3y-\\ &(a_4x^3+a_5x^2+a_6x+a_7)=0. \end{aligned}$$

Input $P_1, P_2,\cdots, P_6 \in \tilde{E}(F_p)$ where $P_i=(x_i, y_i)$ for $0 \le x_i, y_i \le p-1$.

1. Set $v_{i1} \leftarrow y_i^2$, $v_{i2} \leftarrow x_iy_i$, $v_{i3} \leftarrow y_i$, $v_{i4} \leftarrow x_i^3$, $v_{i5} \leftarrow x_i^2$, $v_{i6} \leftarrow -x_i$, $v_{i7} \leftarrow -1$ and $\alpha_i \leftarrow f(x_i, y_i)/p$ for $i=1,\cdots,6$.
2. Using Gaussian elimination, solve the following for s_i.

$$\begin{bmatrix} v_{11} & v_{12} & \cdots & v_{17} \\ v_{21} & v_{22} & \cdots & v_{27} \\ \vdots & \vdots & \ddots & \vdots \\ v_{61} & v_{62} & \cdots & v_{67} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_7 \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_7 \end{bmatrix}$$

3. Output the lifting E/Q of $\tilde{E}/F_p$

$$E: g(x,y)=b_1y^2+b_2xy+b_3y-(b_4x^3+b_5x^2+b_6x+\ b_7)=0$$

where $b_i = a_i+ps_i$.

위의 알고리즘으로 구한 lifting E의 계수들을 생각해 보자. E위에서의 연산에 대한 어려움은 계수들의 크기, 즉, s_i들의 크기에 영향을 받는다. 이때, s_i는 행렬 $V=[v_{ij}]$의 cofactor들의 합을 행렬식으로 나눈 값이므로, $s_i=(k+ls)/m$, $(k,l,m \in Z, s$는 임의의 수)라 표현할 때,

$\max(|k|, |l|, |m|) = O(p^{10})$

이다. 또한, s를 잘 선택 하였을 때(예를 들어 $s=0$), 실험적으로 그 크기는 $O(p^8)$을 넘지 않는다.

Example 1

$p=163$, $\tilde{E}/F_p: y^2=x^3+2$라 하면, $|\tilde{E}(F_p)|=139$로 소수이다. $\tilde{P}=(8,5)$일 때, $\tilde{Q}=30\tilde{P}=(29,58)$, $\tilde{P}+\tilde{Q}=(132,140)$, $2\tilde{P}+\tilde{Q}=(116,93)$, $3\tilde{P}+\tilde{Q}=(22,50)$, $4\tilde{P}+\tilde{Q}=(61,139)$이다. 이 경우, 알고리즘 1에 의하여 다음의 결과를 얻을 수 있다.

$$\left(-\frac{46687457710614}{1062183146747}-\frac{7610055606830082}{1062183146747}s\right)y^2$$
$$+163\left(\frac{634004594136}{1062183146747}+\frac{103342748844168}{1062183146747}s\right)xy$$
$$+163\left(\frac{14539692959970}{1062183146747}+\frac{2369969952475110}{1062183146747}s\right)y$$
$$-(1+163\ s)x^3$$
$$+163\left(-\frac{866628702801}{1062183146747}-\frac{141260478556563}{1062183146747}s\right)x^2$$
$$+163\left(\frac{65382829281664}{1062183146747}+\frac{10657401172911232}{1062183146747}s\right)x$$
$$+\frac{61946003253427368}{1062183146747}+\frac{10097198530308660984}{1062183146747}s$$

$s=0$을 대입하여 잘 정리하면,

$$b_1 = -46687457710614,$$
$$b_2 = 634004594136p,$$
$$b_3 = 14539692959970p,$$
$$b_4 = 1062183146747,$$
$$b_5 = -866628702801p,$$
$$b_6 = 65382829281664p,$$
$$b_7 = 61946003253427368.$$

앞서 살펴본 바와 같이, 가장 큰 계수도 p^8을 넘지 않는다. lifting할 점의 수가 적어진다면, 계수들의 크기 또한 줄어들 것이다. 또한, 만일 타원곡선의 식에 x^4 항도 추가한다면 7점의 lifting도 가능하다. (다만, 계수의 크기는 증가한다.)

4. 내림 방법 (Descent Method)

유리수 위에서 정의된 타원곡선 E에 대하여 P_1, P_2, P_3를 E의 유리점으로, 최대 공약수가 1인 정수 a_1, a_2, a_3에 대하여

$$a_1P_1+a_2P_2+a_3P_3=O \qquad (1)$$

을 만족한다고 가정하자. 이때, $\tilde{a}_i\in\{-1,0,1\}$를 다음과 같이 정의하자. 여기서 $h(P)$는 점 P의 canonical height를 의미한다[9].

- $a_i\equiv\tilde{a}_i \bmod 2$.
- $h(\tilde{a}_1P_1+\tilde{a}_2P_2)\le h(\tilde{a}_1P_1-\tilde{a}_2P_2)$
- $h(\tilde{a}_1P_1+\tilde{a}_2P_2+\tilde{a}_3P_3)\le h(\tilde{a}_1P_1+\tilde{a}_2P_2-\tilde{a}_3P_3)$

그러면, 어떤 유리점 R이 존재하여,

$$\tilde{a}_1P_1+\tilde{a}_2P_2+\tilde{a}_3P_3=(\tilde{a}_1-a_1)P_1+(\tilde{a}_2-a_2)P_2+(\tilde{a}_3-a_3)P_3=2R \qquad (2)$$

이며, 다음과 같은 성질을 만족한다.

Lemma 4.1

$h(R)<(h(P_1)+h(P_2)+h(P_3))/4$.

proof

$$h(2R)=h(\tilde{a}_1P_1+\tilde{a}_2P_2+\tilde{a}_3P_3)=2h(\tilde{a}_1P_1+\tilde{a}_2P_2)+2h(\tilde{a}_3P_3)-h(\tilde{a}_1P_1+\tilde{a}_2P_2-\tilde{a}_3P_3).$$

이때, $\tilde{a}_i$의 선택에 의하여,

$$h(\tilde{a}_1P_1+\tilde{a}_2P_2+\tilde{a}_3P_3)\le h(\tilde{a}_1P_1+\tilde{a}_2P_2-\tilde{a}_3P_3).$$

따라서,

$$h(\tilde{a}_1P_1+\tilde{a}_2P_2+\tilde{a}_3P_3) \le h(\tilde{a}_1P_1+\tilde{a}_2P_2)+ h(\tilde{a}_3P_3)$$
$$\le h(\tilde{a}_1P_1)+h(\tilde{a}_2P_2)+h(\tilde{a}_3P_3)$$

즉,

$$4h(R) \le h(\tilde{a}_1P_1)+h(\tilde{a}_2P_2)+h(\tilde{a}_3P_3)$$

이 성립한다.

편의상, $\tilde{a}_3 \neq 0$, $h(P_1) \le h(P_2) \le h(P_3)$라 가정하자. 이때, 식 (1)에 의하여 적당한 $a_{11}, a_{12}, a_{13} \in Z$에 대하여 다음 식이 성립한다.

$$a_{11}P_1+a_{12}P_2+a_{13}R=0,\ h(R) < \frac{3}{4}h(P_3). \qquad (3)$$

이때, height 크기순으로 P_1, P_2, R을 나열하여, 이를 $P_1^{(1)}$, $P_2^{(1)}$, $P_3^{(1)}$이라 하자. 이 과정을 n번 반복하여, $P_1^{(n)}$, $P_2^{(n)}$, $P_3^{(n)}$을 얻었다면, 이 점들은 다음을 만족한다.

$$h(P_3^{(n)}) \le (3/4)^{[n/3]}h(P_3).$$

이때, 임의의 상수 C에 대하여 $h(P) < C$인 유리점 $P \in E(Q)$의 개수는 유한하므로, 적당한 n에 대하여 $h(P_3^{(n+1)})=0$이 된다. 이때,

$$\tilde{a}_{n1}P_1^{(n)}+\tilde{a}_{n2}P_2^{(n)}+\tilde{a}_{n3}P_3^{(n)}=2P_3^{(n+1)},\ h(P_3^{(n+1)})=0$$

이고 height가 0인 점은 torsion point뿐이므로 위 식에 적당한 상수배를 취하면 $P_1^{(n)}, P_2^{(n)}, P_2^{(n)}$에 대한 dependency equation을 찾을 수 있다. 이 점들은 모두 P_1, P_2, P_3에서 생성되었으므로 그 과정을 거슬러 올라가면 P_1, P_2, P_3에 대한 dependency equation을 얻을 수 있다. 이를 알고리즘으로 나타내면 다음과 같다.

Algorithm 2 (Descent)

Input P_1, P_2, $P_3 \in E(Q)$. Set $\alpha \leftarrow 0$ and $\beta \leftarrow 0$.

1. Find a_1, a_2, $a_3 \in \{0, 1\}$ and compute $R \in E(Q)$ such that $a_1P_1+a_2P_2+a_3P_3=2R$. If there are no such a_i's, output "P_i's are linearly independent" and terminate the algorithm.
2. Set $a_2 \leftarrow -a_2$, $\alpha \leftarrow 1$ If $h(a_1P_1+a_2P_2) > h(a_1P_1-a_2P_2)$.
3. Set $a_3 \leftarrow -a_3$, $\beta \leftarrow 1$ If $h(a_1P_1+a_2P_2+a_3P_3) > h(a_1P_1+a_2P_2-a_3P_3)$.
4. Set $R \leftarrow R-\alpha P_2-\beta P_3$
5. If $h(R)=0$, output a, b, c such that $aP_1+bP_2+cP_3=O$ for original P_i's and terminate the algorithm. Otherwise, set $\alpha \leftarrow 0$, $\beta \leftarrow 0$ and $P_j \leftarrow R$ where P_j has the maximum height among P_i's. Go to step 1.

주어진 타원곡선 E/Q에 대하여 m_E를 non-torsion 점들에 대한 canonical height의 최소값이라 하면, 이 값은 0보다 큰 실수값이 된다.

$$m_E = \min\{h(P) | P \neq O,\ P \in E(Q)/E(Q)_{tor}.$$

이때, Algorithm 2에서 세 점의 height의 최대값을 m이라 할때,

$$n(M) = \left\lceil 3\frac{\log M - \log m_E}{\log 4 - \log 3} \right\rceil$$

이라 하면, $h(P_3^{(n(M))}) < m_E$이므로, m_E의 정의에 의해 $h(P_3^{(n(M))})=0$이다. 따라서, Algorithm 2는 $O(\log M)$ step 이내에 결과를 출력한다.

각 step은 3번의 height 비교 연산과 한번의 square root연산이 필요하므로 전체적으로 $3n(M)$번의 height 비교 연산과 $n(M)$번의 타원곡선 square root 연산이 필요하다. 예를 들어 160 비트 타원곡선을 사용할 경우 n은 8이하가 되어 16번의 $E(Q)$위의 square root 연산과 48번의 height 비교 연산으로 타원로그를 풀 수 있다. 여기서 height 비교 연산이란 타

원곡선위의 두 점이 주어졌을 때, 두 점의 canonical height를 비교하여 두 점 중 canonical height가 큰 점을 찾아 내는 것이다. 이 연산은 타원곡선의 minimal discriminant의 소인수 분해를 알 때 local height를 이용하여 계산할 수 있다[10].

이 알고리즘은 height 비교 연산에 대부분의 계산시간이 소요되는데, 왜냐하면, 소인수 분해가 필요하기 때문에, 타원곡선의 계수들이 크기가 큰 분모 (혹은 분자)를 갖는 유리수이면 계산이 어렵게 된다. 이에 관하여, 최근 Silverman은 discriminant의 소인수 분해를 모르고도 비교적 쉽게 height를 계산할 수 있는 방법을 제시하였다. 그러나, 이 경우에도 타원곡선의 계수들에 의하여 결정되는 어떤 수의 소인수 분해가 필요하므로, 빠른 연산을 위해 타원곡선의 계수를 작게 하는것이필요하다[8].

Example 2.

$p=97$, $\tilde{E}/F_p: y^2+y=x^3+x^2+25x+16$ 라 하면, $|E(F_p)|=103$으로 소수이고, supersingular도 anomalous도 아니다. 따라서, 이산로그 문제가 안전한 타원곡선이다. 이때, $\tilde{P}=(6,5)$, $\tilde{Q}=(31,24)$에 대하여 $log_{\tilde{P}}\tilde{Q}$를 계산한다.

우선, 다양한 m에 대하여 $\tilde{P}$, $\tilde{Q}$, $m\tilde{P}+\tilde{Q}$가 lifting 되는 타원곡선을 구한다. 이 중 $m=11$, $\tilde{R}=11\tilde{P}+\tilde{Q}=(61,47)$인 경우에 다음과 같은 좋은 lifting이 존재한다.

$$E:\ y^2+y=x^3+x^2-72x+210,$$
$$P=(6,5),\ Q=(31,-170),\ R=(198991/22201,$$
$$61572365/3307949).$$

이때, P, Q, R의 dependence equation 을 구하면 다음과 같다.

$$3P+2Q+R=O.$$

이 식을 F_p 위로 reduction 을 취하여 정리하면,

$$3\tilde{P}+2\tilde{Q}+\tilde{R}=3\tilde{P}+2\tilde{Q}+11\tilde{P}+\tilde{Q}=O.$$
$$\therefore 3\tilde{Q}=-14\tilde{P}.$$

따라서 $\log_{\tilde{P}}\tilde{Q}=-14/3\ mod\ 103=64.$

Example 3.

$p=233$, $\tilde{E}/F_p$는 다음과 같이 정의된 타원곡선이다.

$$\tilde{E}: y^2+y=x^3+154x+109.$$

이때, $\#\ \tilde{E}(F_p)=229$는 소수로, Example 2와 같이 같이 supersingular도 anomalous도 아니다. 이 타원곡선에서 $\tilde{P}=(-6,-25)$, $\tilde{Q}=(3,-12)$에 대한 $log_{\tilde{P}}\tilde{Q}$를 계산한다. $\tilde{E}$의 유리수 위로의 lifting E/Q는 다음과 같다.

$$E: y^2+y=x^3-79x+342.$$

위의 타원곡선은 많은 정수점을 갖는 타원곡선으로 실제로 $|x|<100$인 정수 x에 대하여 34개의 정수점을 갖는다 ($x<1000$ 인 경우, 38개). 뿐만 아니라, $(-6,-25)$, $(3,-12)\in E(Q)$ 으로, $\tilde{P}$, $\tilde{Q}$는 그 자신이 $E(Q)$의 lifting 점이 된다. 각 경우를 구분하기 위하여 $E(Q)$의 정수점은 각각 $P=(-6,-25)$, $Q=(3,-12)$라 하자. 또한, $E(Q)$의 정수점들을 $\tilde{E}$로 reduction 하여 $m\tilde{P}+n\tilde{Q}$형태로 나타나는 정수점을 찾아, 이 점을 $m\tilde{P}+n\tilde{Q}$의 lifting 점으로 취할 수 있다. 실제로, $-10\tilde{P}+4\tilde{Q}=(19,157)$이며, 이 점의 lifting $R=(19,-76)$은 다음의 식을 만족한다.

$$P-Q-R=O.$$

Reduction modulo p로 우리는 다음의 식을 얻을 수 있다.

$\tilde{P}-\tilde{Q}-(-10\tilde{P}+4\tilde{Q})=O.$

$$\therefore\ 11\tilde{P}=5\tilde{Q}$$

따라서, $log_{\tilde{P}}\ \tilde{Q}=\ 11/5\ mod\ 229\ =\ 48.$

5. 결론 및 문제점

앞서 우리는 3점의 dependence equation 을 구하는 알고리즘을 알아보았다. 실제로, 타원곡선의 rank는 그 평균값이 2.3[1]으로, 3점이 서로 Z-linearly dependent할 확률은 그리 작지 않다고 추측할 수 있다. 그러나, 일반적으로, lifting한 3점이 mathbb Z-linearly dependent 하지 않을 경우도 있다. 이런 경우, 좀더 많은 점을 lifting하여 이들의 dependence equation 을 구하여야 한다. 앞서 살펴 본 바와 같이, 일반적으로 6점의 lifting이 가능하므로, 우선, 확률적으로 4점까지 확장할 수 있다.

$$a_1P_1+a_2P_2+a_3P_3+a_4P_4=O$$

의 Z-linear dependence equation 이 주어졌을 때, 모든 $a_i \equiv 1\ mod\ 2$일 확률은 1/16이다. 따라서, 확률 15/16 으로 height는 그 최대값이 3/4 배로 줄어든다고 추측할 수 있다. 그러나, 점의 수가 많아지면, 그 합들의 height는 계속 커지기 때문에, 일반적으로 확장은 불가능하다. 5점 이상의 dependence equation은 height 에 의하여 정의되는 non-degenerate bilinear form으로 구할 수 있으나 그 속도나 효율성 등은 연구중에 있다.

참 고 문 헌

[1] Armand Brumer, The average rank of elliptic curves I, Invent. math. 109 (1992), 445--472.

[2] N. Koblitz, Elliptic curve cryptosystems, Math. of Comp. {\bf 48} (1987), 203--209.

[3] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1997.

[4] A. Menezes, T. Okamoto and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite fields, IEEE Trans. on Info. Thory, vol 39(5), Sep.(1993), 1639--1646.

[5] V. Miller, Uses of elliptic curves in cryptography, Advanced in Cryptology-CRYPTO' 85(1985), 417--426.

[6] T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves}, 1997, preprint.

[7] I. A. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, Math. of Comp. {\bf 67} (1998), 353--356.

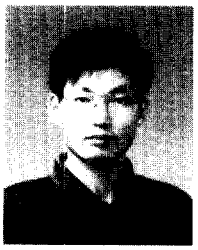
[8] J. H. Silverman, Computing canonical heights with little (or no) factorization, Math. Comp. {\bf 66} No. 218 (1997), 787--805.

[9] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1985.

[10] J. H. Silverman, Advanced topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1994.

[11] N. P, Smart, The discrete logarithm problem on elliptic curves of trace one, 1997, preprint.

□ 著者紹介

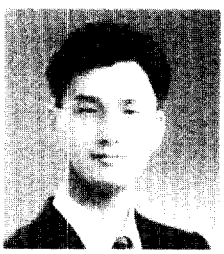


천 정 희

1991년 2월 한국과학기술원 한국과학기술대학 수학과(학사)
1993년 2월 한국과학기술원 수학과 (석사)
1997년 2월 한국과학기술원(박사)
1997년 2월 - 현재 한국전자통신연구원 선임연구원

※ 주관심 분야 : 정수론 및 그의 응용, 타원곡선 이론, 암호 이론

□ 著者紹介



김 환 준

1993년 2월 한국과학기술원 수학과 (학사)
1995년 2월 한국과학기술원(석사)
1995년 - 현재 한국과학기술원 수학과 박사과정

□ 著者紹介

한 상 근

1979년 2월 서울대학교 수학과 (학사)
1982년 5월 뉴멕시코 주립대학 수학과 (석사)
1987년 6월 오하이오 주립대학 수학과 (박사)
1987년 - 1988년 오하이오 주립대학 강사
1989년 - 1992년 한국과학 기술원 조교수
1993년 - 1994년 조지아 대학 방문교수
1992년 - 1998년 한국과학 기술원 부교수
1998년 - 현재 한국과학 기술원 정교수

박 춘 식

광운대학교 전자통신과 졸업 (학사)
한양대학교 대학원 전자통신과 졸업(석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원 연구원
1982년 - 현재 한국전자통신연구원 책임연구원
1997년 한국통신정보보호학회 편집이사, 종신회원
※ 주관심 분야 : 암호이론, 통신이론