ELLIPTIC CURVE DISCRETE LOGARITHMS AND WIEFERICH PRIMES

JUNG HEE CHEON, DONG HOON LEE, SANG GEUN HAHN, AND SEONGTAEK CHEE

Abstract. Recently, a new method, called by Xedni calculus, to solve ECDLP was proposed by Silverman and Kim *et. al.* [11, 5]. The Xedni addresses a novel idea, but has two difficulties. One is to find good liftings and the other is to compute the dependence relation among lifted rational points. In this paper, we propose a fast algorithm to compute the dependence relation modulo the order, $n_{\tilde{P}}$, of $\tilde{P}$ for given two dependent rational points of elliptic curve over $\mathbb{Q}$. Using this, if we could find liftings P, Q and E with rank 1 of $\tilde{P}, \tilde{Q}, \tilde{E}$, then we can solve the ECDLP very fast. Moreover, by this algorithm, we can easily check whether two lifted points are linearly independent or not. Also we investigate the possibility to get such liftings for elliptic curves with a non-trivial 2-torsion, and generate lots of liftings of rank ≤ 2.

1. Introduction

Since Diffie and Hellman have invented a concept of public key cryptosystem in 1977, the Discrete Logarithm Problem(DLP) has become a very interesting problem to many mathematicians. In particular, the DLP is considered to be more difficult on the group of points of an elliptic curve defined over a finite field, say the Elliptic Curve Discrete Logarithm Problem(ECDLP). Let $\tilde{E}$ be an elliptic curve over $\mathbb{F}_p$ and $\tilde{P}, \tilde{Q} \in \tilde{E}(\mathbb{F}_p)$. Then the ECDLP is to compute m satisfying $m\tilde{P} = \tilde{Q}$. In fact, no subexponential time algorithm is known for the ECDLP except several special cases including the smooth cases where $N_p = |\tilde{E}(\mathbb{F}_p)|$ is divisible by only small primes, the supersingular cases where $N_p = p + 1$, and the anomalous cases where $N_p = p$ [6, 7, 8, 12]. Recently, a new method,called by Xedni calculus, to solve ECDLP was proposed by Silverman and Kim *et. al.* independently [11, 5]. The Xedni addresses a novel idea, but has two difficulties.

At first, it seems not to find good liftings as remarked in [4] and [5]. Secondly, although we get good liftings, it is still difficult to compute the dependence relation among the lifted points because the lifted points of a good lifting should have significantly large height.

In this paper, we propose a very fast algorithm to compute the dependence relation modulo the order, $n_{\tilde{P}}$, of $\tilde{P}$ between two lifted rational points. Using this, when we find a good lifting for 2 points, we can solve the ECDLP very fast. Also, we can easily check whether two lifted points are linearly independent or not(that is, whether a lifting is good or not). More precisely, let $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$ and $\tilde{Q} = \tilde{m}\tilde{P}$. Assume that P and $Q \in \langle P_0 \rangle \subset E(\mathbb{Q})$ are liftings of $\tilde{P}$ and $\tilde{Q} \in \tilde{E}(\mathbb{F}_p)$. Then if q is a prime factor of $n_{\tilde{P}}$ satisfying $N_p P_0 \not\equiv O \mod q^2$ - such prime is called Wieferich prime, we have

$$\tilde{m} \equiv \left(\frac{\psi_q(N_q Q)}{\psi_q(N_q P)} \right) \mod q$$

where ψ_q is the q-adic elliptic logarithm. Hence if $n_{\tilde{P}}$ is almost prime and $q^2 \nmid N_p$ for the largest prime factor q of $n_{\tilde{P}}$, then we can compute $\tilde{m}$ in $O(\log(N_q))$ group operation on $E \mod q^2$. No one knows how many primes satisfy the Wieferich criterion for given point of an elliptic curve, but one would certainly expect that the set of Wieferich primes should have density 1 [9].

Key words and phrases. Elliptic Curve, Discrete Logarithm, Wieferich Prime, Rank.

In section 2, we state and prove the main result. In section 3, we present an example to explain the procedure to compute dependence relation for given two dependent rational points by our result. In section 4, we investigate the possibility to find a lifting of rank 1 satisfying some condition. That is, we can generate lots of liftings with rank ≤ 2 if an elliptic curve defined over a finite field $\mathbb{F}_p$ has a non-trivial 2-torsion and $p \equiv 3 \mod 4$. If $p \equiv 1 \mod 4$, we should add the condition that each x-coordinate of $\tilde{P}$ and $\tilde{Q}$ is a quadratic residue in the finite field.

2. Statement and Proof of Main Result

Definition 1 ([9])**.** Let $E/\mathbb{Q}$ be an elliptic curve, and let $P_0 \in E(\mathbb{Q})$ be a point of infinite order. A set of Wieferich primes for E and P_0 is a set of the form

$$W_{E,P_0} = \left\{p \mid N_p P_0 \not\equiv O \mod p^2\right\}$$

where $N_p = |\tilde{E}(\mathbb{F}_p)|$.

Silverman proved in [9] that when j-invariant of $E/\mathbb{Q}$ is 0 or 1728, assuming abc-conjecture,

$$|\{p \in W_{E,P_0} \mid p \leq X\}| \gg_{E,P} \sqrt{\log(X)} \quad \text{as} \quad X \to \infty.$$

However, it is likely that the estimate given above is far from the truth. In fact, one would certainly expect that W_{E,P_0} should have density 1 [9]. Therefore we may assume that the prime q is an element in W_{E,P_0}.

Suppose that $p, q > 16$. If Φ is a torsion group then $|\Phi| \leq 16$ by the well-known Mazur's theorem [10], hence Φ is a subgroup of $\tilde{E}(\mathbb{F}_p)$ and $\tilde{E}(\mathbb{F}_q)$.

Lemma 1. *Assume $M \in \langle P_0 \rangle \times \Phi$ with a torsion group Φ, $q \in W_{E,P_0}$ and $q > 16$.*

$$N_q M \equiv O \mod q^2 \text{ if and only if } M = qR + T \text{ for some } R \in E(\mathbb{Q}) \text{ and } T \in \Phi.$$

Proof. ($\Longleftarrow$)

Since $|\Phi|$ is prime to q, Φ is also a subgroup of $\tilde{E}(\mathbb{F}_q)$, hence $N_q T = O$. The following sequence is exact [10].

$$0 \longrightarrow E_1(\mathbb{Q}_q) \longrightarrow E(\mathbb{Q}_q) \longrightarrow \tilde{E}(\mathbb{F}_q) \longrightarrow 0$$

where $\mathbb{Q}_q$ is the q-adic completion field. Hence

$$E(\mathbb{Q}_q)/E_1(\mathbb{Q}_q) \simeq \tilde{E}(\mathbb{F}_q), \quad E_1(\mathbb{Q}_q)/E_2(\mathbb{Q}_q) \simeq \mathbb{F}_q^+$$

where $E_n(\mathbb{Q}_q) = \{P \in E(\mathbb{Q}_q) \mid P \equiv O \mod q^n\}$, and

$$\begin{aligned} & R \in E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_q) \\ \Rightarrow \quad & N_q R \in E_1(\mathbb{Q}_q) \\ \Rightarrow \quad & q(N_q R) \in E_2(\mathbb{Q}_q) \cap E(\mathbb{Q}) = E_2(\mathbb{Q}). \end{aligned}$$

Therefore $N_q M = N_q(qR) + N_q T = q(N_q R) \in E_2(\mathbb{Q})$

($\Longrightarrow$) Since $E(\mathbb{Q}) \simeq \langle P_0 \rangle \times \Phi$, we can write $M = nP_0 + T$ for some $n \in \mathbb{Z}$ and $T \in \Phi$. By the assumption, $N_q M = N_q n P_0 + N_q T = N_q n P_0 \in E_2(\mathbb{Q}_q)$. If $q|n$, then the lemma is proved for $R = (n/q)P_0$. Otherwise, $N_q P_0 \in E_2(\mathbb{Q}_q)$, that is, $q \notin W_{E,P_0}$ since $N_q P_0 \in E_1(\mathbb{Q}_q)$ and $|E_1/E_2| = q$. This is a contradiction. □

Let $\mathcal{E}$ be the formal group associated to E. Then we have a following isomorphism called the q-adic elliptic logarithm ψ_q [10, 12].

$$\psi_q : E_1(\mathbb{Q}_q) \xrightarrow{\phi} q\mathbb{Z}_q \xrightarrow{\log_{\mathcal{E}}} q\mathbb{Z}_q$$

where

$$\phi(R) = -\frac{x(R)}{y(R)},$$
$$\log_{\mathcal{E}}(z) = z + \frac{a_1}{2}z^2 + \frac{a_1^2 + a_2}{3}z^3 + \frac{a_1^3 + 2a_1a_2 + 2a_3}{4}z^4 + \cdots \in \mathbb{Q}_q[[z]].$$

($\log_{\mathcal{E}}(z)$ is the formal logarithm of $\mathcal{E}$ [10]). Moreover $\psi_q : E_n(\mathbb{Q}_q) \simeq q^n\mathbb{Z}_q$ holds for any positive integer n and ψ_q has a homomorphic property:

$$\psi_q(P+Q) = \psi_q(P) + \psi_q(Q) \quad \text{for any} \quad P, Q \in E_1(\mathbb{Q}_q)$$

where the first addition is the operation of $E(\mathbb{Q}_q)$ and the second one is the addition of $\mathbb{Z}_q$.

Theorem 2. *Suppose that P and Q are linearly dependent rational points of E such that*

$$aP - bQ = O, \qquad \gcd(a, b) = 1$$

and $\tilde{P}$ and $\tilde{Q} \in \tilde{E}(\mathbb{F}_p)$ are the restriction of P and Q modulo p. Let q be a prime factor of the order, $n_{\tilde{P}}$, of $\tilde{P}$ modulo p such that

$$q \in W_{E,P_0}, \quad \textit{and} \quad q^2 \nmid N_p$$

where P_0 is a generator of P and Q. If we take

$$m_q = \left(\frac{\psi_q(N_qQ)}{\psi_q(N_qP)}\right) \mod q = \left(\frac{x(N_qQ)\cdot y(N_qP)}{y(N_qQ)\cdot x(N_qP)}\right) \mod q,$$

then $a/b \equiv m_q \mod q$. Consequently if $\tilde{Q} = \tilde{m}\tilde{P}$ then $\tilde{m} \equiv m_q \mod q$.

Proof. At first, we will show that m_q is well-defined. Since $N_qP,\ N_qQ \in E_1(\mathbb{Q}_q)$, we have $\psi_q(N_qP) \equiv \psi_q(N_qQ) \equiv 0 \mod q$. Hence for the well-definedness of m_q, it is enough to show that q^2 does not divide $\psi_q(N_qP)$. Suppose on the contrary, that is $N_qP \in E_2(\mathbb{Q}_q)$. Then $P = qR + T$ for some R and T by the previous lemma. Since $\gcd(|\Phi|, q) = 1$, $|\Phi| \mid (N_p/q)$ and $(N_p/q)P = N_pR + (N_p/q)T = N_pR$, which reduces to $\tilde{O}$ in $\tilde{E}(\mathbb{F}_p)$ so that $n_{\tilde{P}} \mid (N_p/q)$. Since $q \mid n_{\tilde{P}}$, we have $q^2 \mid N_p$, which contradicts with the assumption. Hence m_q is well-defined.

Let $m_q = \left(\frac{\psi_q(N_qQ)}{\psi_q(N_qP)}\right) \mod q$. Since $\psi_q(N_qP) \equiv 0 \mod q$, $\psi_q(m_qN_qP - N_qQ) \equiv 0 \mod q^2$. Hence

$$N_q(m_qP - Q) \in E_2(\mathbb{Q}).$$

By the previous lemma,

$$m_qP - Q = qR + T \quad \text{for some } R \in E(\mathbb{Q}) \text{ and } T \in \Phi.$$

Multiplying N_p/q to both sides and reducing to $\mathbb{F}_p$, $(N_p/q)m_q\tilde{P} = (N_p/q)\tilde{Q}$ since $|\Phi| \mid (N_p/q)$, so that $a/b \equiv m_q \mod q$.

Since $\psi_q(N_qP) \in q\mathbb{Z}_q \backslash q^2\mathbb{Z}_q$ and $\psi_q(N_qQ) \in q\mathbb{Z}_q$,

$$m_q = \left(\frac{\psi_q(N_qQ)}{\psi_q(N_qP)}\right) \mod q = \left(\frac{\psi_q(N_qQ) \mod q^2}{\psi_q(N_qP) \mod q^2}\right) \mod q.$$

And

$$\begin{aligned}\psi_q(N_qQ) \mod q^2 &= \log_{\mathcal{E}}(\phi(N_qQ)) \mod q^2 \\ &= \phi(N_qQ) \mod q^2 \\ &= -\frac{x(N_qQ)}{y(N_qQ)} \mod q^2.\end{aligned}$$

Therefore

$$m_q = \left(\frac{x(N_qQ)\cdot y(N_qP)}{y(N_qQ)\cdot x(N_qP)}\right) \mod q$$

□

In general, it takes very long time to compute the exact values of N_qQ and N_qP. However in order to determine m_q, we don't have to compute their exact values. Since $x(N_qQ) \in \frac{1}{q^2}\mathbb{Z}_q$ and $y(N_qQ) \in \frac{1}{q^3}\mathbb{Z}_q$, it is sufficient to compute only the first terms of them in q-adic expansions. However $N_qQ \mod q^2$ is not well-defined. So we had better replace the affine coordinate $(x, y, 1)$ by the projective coordinate $(xq^3, yq^3, q^3) \mod q^5$ in order to compute $-\frac{x(N_qQ)}{y(N_qQ)} \mod q^2$. In this way we can compute $\psi_q(N_qP)$ and $\psi_q(N_qQ)$ very fast.

Remark 1. With the assumption of the main theorem, it needs to compute $N_qP \mod q^5$ and $N_qQ \mod q^5$, both of which take $\log(N_q)$ group operations on $E \mod q^5$ to compute m_q. So the running time is $O(\log(N_q))$ for each $q \mid n_{\tilde{P}}$. Hence when $n_{\tilde{P}} = c\prod_{i=1}^{n} q_i$ for distinct primes q_i's and small c, the running time is $O(\sqrt{c} + \sum_{i=1}^{n} \log N_{q_i})$.

Remark 2. For the anomalous case, the groups $\tilde{E}(\mathbb{F}_p)$ and $\mathbb{F}_p^+$ have the same order, namely p. So if we find a lifting P', Q' of $\tilde{P}, \tilde{Q}$ to $E(\mathbb{Q}_p)$, which is easily computed by the Hensel's lemma, we have $Q' - mP' = R \in E_1(\mathbb{Q}_p)$ so that $pQ' - pmP' = pR \in E_2(\mathbb{Q}_p)$. Hence we have

$$m \equiv \frac{\psi_p(pQ')}{\psi_p(pP')} \mod p.$$

However, for non-anomalous cases, $(\tilde{m}P - Q) = R \in E_1(\mathbb{Q}_p)$, does not give $N_pR \in E_2(\mathbb{Q}_p)$. So we need the previous lemma and must find liftings of $\tilde{P}, \tilde{Q}$ to $E(\mathbb{Q})$ (not $E(\mathbb{Q}_p)$). Unfortunately, it may be a very difficult problem.

Remark 3. By the theorem 2, we can easily check whether a lifting is a good lifting or not. If two lifted rational points are linearly dependent, it must satisfy $Q \equiv m_qP \mod q$ for $m_q \equiv \frac{\psi_q(N_qQ)}{\psi_q(N_qP)} \mod q$. Hence if two points do not satisfy the above equation, they must be linearly independent. Conversely, two linearly independent points may satisfy the equation with probability $1/q$ roughly. Moreover, since the equation must hold for any other prime q' different from q, we can test easily the linearly independence using primes smaller than q.

3. Example

Suppose $p = 541$, $\tilde{E} : y^2 = x^3 - 4x + 4$ and $\tilde{P} = (8, 22)$, $\tilde{Q} = (30, 404)$. We present a procedure to find the value $\tilde{m}$ such that $\tilde{Q} = \tilde{m}\tilde{P}$, using Theorem 2. Observe that the order of $\tilde{P}$, $n_{\tilde{P}} = 265 = 5 \cdot 53$ is not prime. Since $E(\mathbb{Q}) : y^2 = x^3 - 4x + 4$ has rank 1 and $P = (8, 22) \in E(\mathbb{Q})$, it is enough to find $Q \in E(\mathbb{Q})$ lifting of $\tilde{Q}$. Assume that we found such point Q as follows.

$$\begin{aligned}x(Q) &= \frac{309734042118015336313584 40}{98114403796666269768880 1}, \\ y(Q) &= -\frac{146853049988006230585801866823345828438}{307325894064611311737566941578832919 51}.\end{aligned}$$

As remarked in the previous section, it is very difficult to find such Q for given P and E. While in Xedni method, we have to compute the dependence relation between P and Q as rational points, in our method we don't need to compute it. In our algorithm, we directly compute the dependence relation modulo $n_{\tilde{P}}$, so that it is more efficient and faster.

At first, let $q = 53$, then $N_q = 52$ and $Q \mod q^2 = (50 + 8q, 25 + 41q)$. By computing $52P$, $52Q \mod q^5$ by using the projective coordinates (with z-coordinate is q^3), we have

$$\begin{aligned} 52P \mod q^5 &= (q + 16q^3 + 45q^4, \\ &\qquad 1 + 24q^2 + 41q^3 + 9q^4, q^3), \\ 52Q \mod q^5 &= (15q + 4q^2 + 7q^3 + 27q^4, \\ &\qquad 47 + 47q + 51q^2 + 15q^3 + 22q^4, q^3). \end{aligned}$$

Since

$$\psi_q(52P) \mod q^2 = 52q, \quad \psi_q(52Q) \mod q^2 = 29q,$$

we have

$$m_{53} = \left(\frac{29}{52} \mod q\right) = 24.$$

In order to solve the discrete logarithm completely, what we need is only to compute $\tilde{m} \mod 5$. But $q = 5$ is too small ($q \leq 16$), so we may not be able to apply the above method. However we can compute $\tilde{m} \mod 5$ directly because q is small. $\frac{n_{\tilde{P}}}{q}\tilde{P}$ is a generator of order q and

$$\tilde{Q} = \tilde{m}\tilde{P} \Rightarrow \frac{n_{\tilde{P}}}{q}\tilde{Q} = \tilde{m}(\frac{n_{\tilde{P}}}{q}\tilde{P})$$

If we solve the discrete logarithm with $\frac{n_{\tilde{P}}}{q}\tilde{P}$ and $\frac{n_{\tilde{P}}}{q}\tilde{Q}$, then this is the value of $\tilde{m} \mod q$.

So compute $\frac{n_{\tilde{P}}}{q}\tilde{P}$ and $\frac{n_{\tilde{P}}}{q}\tilde{Q}$,

$$53\tilde{P} = (535, 322), \quad 53\tilde{Q} = (412, 77).$$

By computing $i(53\tilde{P})$ in turn for $i = 2, 3, \cdots, q-1$,

$$2(53\tilde{P}) = (412, 464), \quad 3(53\tilde{P}) = (412, 77), \cdots,$$

we have ($\tilde{m} \mod 5) = 3$, and so $\tilde{m} = 183$ by Chinese Remainder Theorem. It is easy to check that $\tilde{Q} = 183\tilde{P} \mod p$.

4. Lifting to an elliptic curve over $\mathbb{Z}$ with integral points

As the previous section, if we could lift two points of $\tilde{E}(\mathbb{F}_p)$ to a rational elliptic curve with rank 1, then we could solve the ECDLP. So in this section, we investigate the possibility to get such liftings for elliptic curves with a non-trivial 2-torsion.

A. Brumer analyzed the rank distribution of $\left\{E \mid |\Delta| \leq 10^8, |a_6| \leq 2^{31} - 1\right\}$ with $|\Delta|$ prime and got the following table [2],

Rank	0	1	2	3	4	5
$\Delta > 0$	31748	51871	24706	5267	377	0
$\Delta < 0$	61589	91321	36811	6594	427	5
percents	30.04	46.08	19.80	3.82	0.26	

and he also showed in [3] that the average rank is at most 2.3. When one takes an arbitrary elliptic curve over $\mathbb{Q}$, he may expect that its rank is 1 with high probability. Unfortunately, in our cases, we consider only an elliptic curve with two large rational points. So, it's rank would

be larger than general cases. Nothing is known about the rank distribution of elliptic curves with two rational points.

To begin with, we introduce the well-known fact on an upper bound of a rank of an elliptic curve with a non-trivial 2-torsion.

Theorem ([1])**.**

$$E : y^2 = x(x^2 + ax + b), \quad a, b \in \mathbb{Z}.$$

Let $w(x)$ denote the number of distinct primes dividing x. Then

$$\mathrm{Rank}(E/\mathbb{Q}) \leq w(b) + w(a^2 - 4b) - 1.$$

If we could choose a and b such that b and $a^2 - 4b$ become primes, then $\mathrm{Rank}(E/\mathbb{Q}) \leq 1$. So we wish to choose a and b such that b and $a^2 - 4b$ have distinct prime factors as few as possible.

Let $\tilde{E} : y^2 = x(x^2 + ax + b) = f(x)$ be an elliptic curve with a non-trivial 2-torsion point over $\mathbb{F}_p$, $\tilde{P} = (\tilde{x}_1, \tilde{y}_1)$ and $\tilde{Q} = (\tilde{x}_2, \tilde{y}_2)$ be points in $\tilde{E}(\mathbb{F}_p)$ with $\tilde{x}_1 \neq \tilde{x}_2$. Choose a lifting E of $\tilde{E}$ such that

$$E : y^2 = x(x^2 + (a + Ap)x + (b + Bp))$$

where $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E$ and $x_i \equiv \tilde{x}_i$, $y_i \equiv \tilde{y}_i \mod p$. Then

$$A = \frac{G - H}{x_1 - x_2}, \quad B = -\frac{Gx_2 - Hx_1}{x_1 - x_2}$$

where $px_1G = y_1^2 - f(x_1)$, $px_2H = y_2^2 - f(x_2)$. We shall take G and H integers such that $G \equiv H \mod (x_1 - x_2)$ to make A and B integers. Also, we shall take x_i and y_i such that $x_i \mid y_i^2$ because $G, H \in \mathbb{Z}$ if and only if $x_i \mid y_i^2$.

If $|x_i|$ is not a square, then there is a prime r such that $v_r(x_i) = e$ is odd where v_r is r-adic valuation. So $v_r(y_i) \geq \frac{e+1}{2}$ and $r \mid (b + Bp)$. Unless $b + Bp = \pm r$, $b + Bp$ cannot be a prime. This is not the case we want, so we assume that $|x_i|$ is a square and $x_i \mid y_i^2$.

Let $x_1 = t_1^2$, $x_2 = -t_2^2$, $y_i = t_i b_i$ and

$$\begin{aligned} \gamma_i &= (t_i p)^{-1} \mod (x_1 - x_2), \\ (1 - \gamma_i t_i p) &= \delta_i (x_1 - x_2), \\ y_i' &= y_i \delta_i (x_1 - x_2) + t_i^2 pn. \end{aligned}$$

Then ${y_1'}^2 \equiv {y_2'}^2 \mod (x_1 - x_2)$, hence A' and B' become integers. Denote $s_i = b_i \delta_i$ and compute $a + A'p$ and $b + B'p$,

$$\begin{aligned} a + A'p &= p^2 n^2 + 2(s_1 t_1 + s_2 t_2)pn + (s_1^2 + s_2^2)(x_1 - x_2) - (x_1 + x_2), \\ b + B'p &= 2(s_1 t_2 - s_2 t_1) t_1 t_2 pn + (s_1^2 t_2^2 - s_2^2 t_1^2)(t_1^2 + t_2^2) - t_1^2 t_2^2. \end{aligned}$$

Hence

$$\begin{aligned} &(a + A'p)^2 - 4(b + B'p) \\ =&(p^2 n^2 + 2(s_1 t_1 + s_2 t_2 + t_1)pn + (s_1^2 + s_2^2 + 1 + 2s_1)(t_1^2 + t_2^2)) \\ &\times (p^2 n^2 + 2(s_1 t_1 + s_2 t_2 - t_1)pn + (s_1^2 + s_2^2 + 1 - 2s_1)(t_1^2 + t_2^2)). \end{aligned}$$

Furthermore, each factor of the above is always higher than 1, hence it cannot be a unit. It needs to assume that t_1 and t_2 are relatively prime odd numbers in order that coefficients of $b + B'p$ are relatively prime. Since $b + B'p$ and each factor of the above are irreducible, we may find n

such that all become primes. Then for such integer n, $\mathrm{Rank}(E/\mathbb{Q}) \leq 2$. For example, consider the following elliptic curve over $\mathbb{F}_{353}$.

$$\tilde{E} : y^2 = x(x^2 - x + 16).$$

Let $\tilde{P} = (9, 63) = (703^2, 703 \cdot (-21))$ and $\tilde{Q} = (17, 183) = (-439^2, 439 \cdot 154)$ in $\tilde{E}(\mathbb{F}_{353})$. As stated in the above paragraph, we can compute the followings.

$$b + B'p = 635728705996536026n - 1792587436107314570824479$$

and

$$\begin{aligned}&(a + A'p)^2 - 4(b + B'p)\\ =&(124609n^2 + 303443264744n + 8697969664620875680)\\ &\times (124609n^2 + 303442272108n + 8697963332447929000).\end{aligned}$$

So we could find $n = -1793$ and 181 for $-2000 \leq n \leq 2000$ such that all 3 factors are prime numbers. Therefore we obtain two curves for $t_1 = 703, t_2 = 439$ which have at most rank 2. If we would take different t_i's then we could find different curves with rank ≤ 2.

Observe that one can test very easily whether an integer is prime or not. Hence, one may expect to find an integer n in polynomial time such that a polynomial of n becomes a prime. Consequently, we can generate lots of liftings with rank ≤ 2 if an elliptic curve over $\mathbb{F}_p$ has a non-trivial 2-torsion and $p \equiv 3 \mod 4$. If $p \equiv 1 \mod 4$, we should add the condition that each x-coordinate of $\tilde{P}$ and $\tilde{Q}$ is a quadratic residue in the finite field.

5. Conclusion

Xedni method is not practical because it has two difficulties. We remove one of them by proposing an algorithm to directly compute the dependence relation modulo $n_{\tilde{P}}$ for given two dependent points in $E/\mathbb{Q}$. Hence if we could lift two points in $\tilde{E}/\mathbb{F}_p$ to $E/\mathbb{Q}$ with rank 1, then we can solve ECDLP by our result. But as remarked in [4] and [5], the lifting problem seems to be very difficult. However we investigate the possibility that lifted curves have rank 1 with a certain condition. Actually we could generate many elliptic curves over $\mathbb{Q}$ with rank ≤ 2.

References

[1] "Elliptic Curve Handbook", ftp://math.mcgill.ca/pub/ECH1.

[2] A. Brumer and O. McGuinness, The behavior of the Mordell-Weil group of elliptic curves, *Bull.(New Series) of the Amer. Math. Soc.* **23(2)** (1990), 375–382.

[3] A. Brumer, The average rank of elliptic curves. I., *Invent. Math.* **109(3)** (1992), 445–472.

[4] J. Jacobson, N. Koblitz, J. H. Silverman, A. Stein and E. Teske, Analysis of the Xedni caculus attack, *preprint*, (1999).

[5] H. Kim, J. Cheon and S. Hahn, Elliptic curve discrete logarithm and lifting problem, *preprint*, (1999).

[6] A. Menezes, "Elliptic Curve Public Key Cryptosystems", Kluwer Academic publishers, 1993.

[7] T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *preprint* (1997).

[8] I. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, *Math. of Comp.* **67** (1998), 353–356.

[9] J. H. Silverman, Wieferich's criterion and the *abc*-conjecture, *Journal of number theory* **30** (1988), 226–237.

[10] J. H. Silverman, "The Arithmetic of Elliptic Curves", Springer-Verlag, 1992.

[11] J. H. Silverman, The Xedni calculus and the elliptic curve discrete logarithm problem, to appear *Design,Code and Cryptography.*

[12] N. P. Smart, The discrete logarithm problem on elliptic curves of trace one, *Journal of Cryptology* **12** (1999), 193–196.

Electronics and Telecommunications Research Institute, 161Kajong-Dong, Yusong-Gu, Taejon, 305-350, South Korea
E-mail address: jhcheon@etri.re.kr

Department of Mathematics, KAIST, 373-1 Kusong-Dong,Yusong-Gu,Taejon, 305-701, South Korea
E-mail address: dhlee@math.kaist.ac.kr

Department of Mathematics, KAIST, 373-1 Kusong-Dong,Yusong-Gu,Taejon, 305-701, South Korea
E-mail address: sghahn@math.kaist.ac.kr

Electronics and Telecommunications Research Institute, 161Kajong-Dong, Yusong-Gu, Taejon, 305-350, South Korea
E-mail address: chee@etri.re.kr