ON REMARKS OF LIFTING PROBLEMS FOR ELLIPTIC CURVES

HWAN JOON KIM, JUNG HEE CHEON, AND SANG GEUN HAHN

Abstract. No subexponential time algorithm is known yet for the Elliptic Curve Discrete Logarithm Problem(ECDLP) except some special cases. In this paper, we introduce the lifting problem and show that it implies the ECDLP and integer factorization problem(IFP) and we note that finding a point in $E_1(\mathbb{Q})$, the kernel of the reduction map, also implies the ECDLP and the IFP since it solves the lifting problem. Moreover, we analyze the difficulty of the lifting problem by estimating the minimum of the canonical heights on $E_1(\mathbb{Q})$.

1. Introduction

Since Diffie and Hellman have invented a concept of public key cryptosystem in 1977, the Discrete Logarithm Problem(DLP) has become one of the most important problems 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 than on the multiplicative group of a finite field. This is the Elliptic Curve Discrete Logarithm Problem(ECDLP).

Let $\tilde{E}$ be an elliptic curve over $\mathbb{F}_q$ ($q = p^n$ for a prime p) and $\tilde{P}, \tilde{Q} \in \tilde{E}(\mathbb{F}_q)$. Then the ECDLP is to compute $\tilde{m}$ satisfying $\tilde{m}\tilde{P} = \tilde{Q}$.

The DLP on a finite field can be solved in subexponential time by the index calculus method, but Silverman showed that the natural generalization of the index calculus method to the ECDLP yields an algorithm which is less efficient than the brute-force search algorithm [14]. Therefore, the Pollard ρ method is the most efficient algorithm to solve the ECDLP in the general cases until now. Since it needs $O(\sqrt{n})$ elliptic curve operations for an elliptic curve with order n, it has exponential running time. That is, any subexponential time algorithm is not known yet for the general ECDLP. The ECDLP is solved in only some special cases which include the singular cases, the supersingular cases where $q + 1 - N_q$ is divided by a characteristic of $\mathbb{F}_q$ [7] and the anomalous cases where $N_q = q$ [8][9][15].

In this paper, by using the lifting problem, we propose a new method to solve the ECDLP which can be applied to the general cases. For a given elliptic curve $\tilde{E}$ over $\mathbb{F}_p$ and the points $\tilde{P}_i$ ($i = 1, \cdots, r$) of $\tilde{E}(\mathbb{F}_p)$, we define "the lifting problem" to find an "lifted" elliptic curve $E/\mathbb{Q}$ and linearly dependent "lifted" points P_i ($i = 1, \cdots, r$) in $E(\mathbb{Q})$ which are reduced to $\tilde{E}$ and $\tilde{P}_i$'s modulo p respectively, that is,

$$E \equiv \tilde{E} \mod p \quad \text{and} \quad P_i \equiv \tilde{P}_i \mod p \quad \text{for all } i\ .$$

Key words and phrases. Elliptic Curve Discrete Logarithm, Discrete Logarithm, Integer Factorization, Canonical Height, Descent, Elliptic Curve.

We will show that it is easy to compute the coefficients of the dependence equation among linearly dependent rational points by the 2-descent method. This means that if we can solve the lifting problem, we can solve the ECDLP by reducing the dependence equation to a finite field.[1]

For the case of the ECDLP over $\mathbb{F}_{2^m}$, we propose the lifting problem to a function field $\mathbb{F}_2(t)$. In this paper, we show that the 2-descent method can be applied to the case of a function field similarly to the case of the rational field. That is, we show that the lifting problem implies the ECDLP not only over a prime field $\mathbb{F}_p$, but also over a extension field $\mathbb{F}_{2^m}$.[2]

Moreover, we show that the lifting problem for an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ can be used in computing the order of a given point of an elliptic curve defined over $\mathbb{Z}/n\mathbb{Z}$ and this solves the Integer Factorization Problem (IFP). It is a generalization of the Koblitz's comment in [13]. He also noted that the lifting problem implies the discrete logarithm problem (DLP) on a finite field because a finite field is explicitly isomorphic to a singular reduction of an elliptic curve over $\mathbb{Q}$ to the finite field. It is very surprising and remarkable that the important problems (ECDLP, IFP, DLP) in cryptography are implied by one problem because it means that the cryptosystems based on these problems may be cracked by one method.

Unfortunately, the lifting problem may or may not be harder than the original problem. In fact, Silverman showed that the rank of the lifted elliptic curve tends to be the same as the number of the lifted points and that even when the rank is smaller than the number of lifted points, the size of the coefficients of the linearly dependence relation among the lifted points are very small, which means that the given ECDLP is trivial [4].

In this paper, we note that if we can find a non-trivial point of the kernel of the reduction map from a lifted elliptic curve to the elliptic curve given by ECDLP, then we can solve the lifting problem. Moreover, we find the relation between the size of the coefficients of the linearly dependence relation among the lifted points and the minimum of the canonical heights of the points in the kernel of the reduction map. Unfortunately, the minimum of the canonical heights of the points in the kernel of the reduction map is $O(|\tilde{E}(\mathbb{F}_p)|)$, which implies that a non-trivial point in the kernel is too large to be found by brute force search so that some additional technique is required to solve the lifting problem.

2. Lifting Problem and ECDLP

¿From now on, we assume that n is a square free integer and that $\tilde{E}$ is an elliptic curve defined over $\mathbb{Z}/n\mathbb{Z}$ [7].[3] In particular, if n is a prime p, then $\tilde{E}$ is an elliptic curve defined over a finite field $\mathbb{F}_p$.

In this section, we first define the lifting problem for $\tilde{E}$ and we show that it implies the elliptic curve discrete logarithm problem (ECDLP) on $\mathbb{Z}/n\mathbb{Z}$. Secondly, we introduce the 2-descent method to check the linearly dependence between rational points of an elliptic curve defined over $\mathbb{Q}$ and to compute its coefficients, which is necessary to connect between the lifting problem and the ECDLP. Finally, we show that the 2-decent method can be applied to the case of function field so that the

[1]Silverman proposed a similar method named by 'Xedni calculus' independently [13].

[2]We consider it can be generalized to small characteristic p.

[3]For ECDLP, we consider only the case n is a prime. The case of a composite number n is considered for IFP in the below.

lifting problem implies the ECDLP not only on $\mathbb{Z}/n\mathbb{Z}$ but also on the general finite fields $\mathbb{F}_{p^m}$.

2.1. **Lifting Problem.** To begin with, we define the lifting problem.

Definition 2.1. *Let $\tilde{E}$ be an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ and $\tilde{P}_1, \tilde{P}_2, \cdots, \tilde{P}_r$ be the points of $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$. We call the elliptic curve E over $\mathbb{Q}$ by the lifted elliptic curve of $\tilde{E}$ if $\tilde{E}$ is isomorphic to the reduction of E modulo n, namely $E \equiv \tilde{E} \mod n$. In this case, a point P of $E(\mathbb{Q})$ is a lifted point of $\tilde{P}$ of $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$, if it is congruent to $\tilde{P}$ modulo n.*

We define the lifting for $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$ to be the pair $(E, P_1, \cdots, P_r)$ of its lifted elliptic curve E and lifted points P_i's of $\tilde{P}_i$'s respectively.

Furthermore, if the lifted points P_i's are linearly dependent, then we call it by the "good" lifting. The lifting problem means to find an good lifting for given $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$.

In general, if we omit the condition of the linearly dependent lifted points, we can easily construct the lifting as follows. Let $\tilde{E}$ be an elliptic curve defined on $\mathbb{Z}/n\mathbb{Z}$ given by the following Weierstrass equation

$$\tilde{E}: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

Then, for any rational numbers t_j $(j = 1, \cdots, 7)$ of which the numerators are prime to n, the following elliptic curve E becomes the lifted elliptic curve of $\tilde{E}$;

$$\begin{aligned} E &: (1+nt_1)y^2 + (a_1+nt_2)xy + (a_3+nt_3)y \\ &= (1+nt_4)x^3 + (a_2+nt_5)x^2 + (a_4+nt_6)x + (a_6+nt_7). \end{aligned}$$

Now, suppose $\tilde{P}_1, \cdots, \tilde{P}_r$ are the points of $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$ where $\tilde{P}_i = (x_i, y_i)$. By linear algebra, we can choose some rational numbers t_j's so that each of (x_i, y_i)'s becomes an integral point of E, that is, each of (x_i, y_i)'s becomes a lifted point by itself. Since the number of indeterminants t_j's is 7, we can make 6 points $\tilde{P}_i$'s the lifted points by themselves.[4] Therefore, we can easily construct infinitely many liftings for a given $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$ if $r < 7$. Unfortunately, the lifted points constructed in such way are usually inclined to be linearly independent. We will consider more on the good lifting in the section 4.

Now, we show how to solve the ECDLP on $\mathbb{Z}/n\mathbb{Z}$ assuming the lifting problem is solved. Suppose $\tilde{E}$ is an elliptic curve defined over $\mathbb{Z}/n\mathbb{Z}$ with $\tilde{P}$, $\tilde{Q}$ in $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$.
Step 1 Take r distinct points $\tilde{P}_i$ in $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$ which are linear combinations of $\tilde{P}$ and $\tilde{Q}$. That is, for small integers x_i's and y_i's we take

$$\tilde{P}_i = x_i\tilde{P} + y_i\tilde{Q}, \quad i = 1, \cdots, r.$$

For example, we can take $\tilde{P}_i = (i-1)\tilde{P} + \tilde{Q}$.
Step 2 Solve a lifting problem for $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$. Then we get a lifting elliptic curve $E/\mathbb{Q}$ and linearly dependent lifted points P_i's on $E(\mathbb{Q})$.
Step 3 Compute the coefficients α_i's of the dependence equation

$$\alpha_1P_1 + \cdots + \alpha_rP_r = O$$

by the 2-descent method which will be explained in the next subsection.

[4]If we use the homogeneous cubic equation instead of the Weierstrass equation which has 10 coefficients, we can construct a lifting with 9 lifted points [13].

Step 4 By reduction modulo n, we have

$$\sum \alpha_i x_i \tilde{P} + \sum \alpha_i y_i \tilde{Q} = O.$$

Therefore

$$m \equiv -\sum \alpha_i x_i / \sum \alpha_i y_i \mod \mathrm{ord}\tilde{Q}.$$

Note that the 2-descent procedure has the polynomial running-time that will be proved in the next subsection. Therefore, the running-time of the above algorithm depends only on the lifting problem.

Example Let $p = 113$ and

$$\tilde{E}/\mathbb{F}_p : y^2 = x^3 + 30x + 30, \quad \tilde{P} = (2, 18), \tilde{Q} = (10, 58).$$

Then, the lifting (E, P, Q) of $(\tilde{E}, \tilde{P}, \tilde{Q})$ is as follows.

$$E/\mathbb{Q} : y^2 - 113y = x^3 - 309x - 1100, \quad P = (2, 18), Q = (10, 58).$$

Then, by descent method, we can get the dependence equation

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

Finally, we have

$$\log_{\tilde{P}} \tilde{Q} = 17.$$

2.2. **Descent method.** In this subsection, we introduce the 2-descent method to compute the coefficients of the dependence equation for given linearly dependent points P_i's of $E(\mathbb{Q})$ and we show that it has the polynomial running-time.

Suppose that P_i's $(i = 1, \cdots, r)$ are given rational points of $E(\mathbb{Q})$.

Step 1 Rearrange the given linearly dependent points P_i's according to their canonical heights in an increasing order. and find $\epsilon_1, \cdots, \epsilon_r \in \{-1, 0, 1\}$ which are not all zero and satisfy

$$\epsilon_1 P_1 + \cdots + \epsilon_r P_r \in 2E(\mathbb{Q}). \tag{1}$$

Note that if $P_1, \cdots, P_r$ are linearly dependent with

$$\alpha_1 P_1 + \cdots + \alpha_r P_r = O,$$

then (1) is satisfied for each $\epsilon_i = (\alpha_i \mod 2)$. Moreover, it is also easy to check whether a given rational point is contained in $2E(\mathbb{Q})$ or not [1][5].

Step 2 For $2 \le k \le r$, determine the sign of ϵ_k to satisfy

$$\hat{h}(\sum_{i=1}^{k-1} \epsilon_i P_i + \epsilon_k P_k) \le \hat{h}(\sum_{i=1}^{k-1} \epsilon_i P_i - \epsilon_k P_k),$$

where $\hat{h}$ is the canonical height on $E/\mathbb{Q}$ [10].

It is not easy to compute the exact values of $\hat{h}(P)$ for the rational points P in general. However, we are enough to compare of the canonical heights, so we can easily determine the signs of ϵ_i's [11][12].

Step 3 Compute a point $R = R(P_1, \cdots, P_r)$ of $E(\mathbb{Q})$ with

$$2R = \epsilon_1 P_1 + \cdots + \epsilon_r P_r.$$

It is easy to compute the "halving" point R of P satisfying $2R = P$ for a given P of $2E(\mathbb{Q})$ because it is equivalent to finding the rational roots of the polynomial

of degree 4 with rational coefficients. Moreover, if E has rational 2-torsion points, there are exact formulas to compute R [5][1].

Step 4 If R is a non-torsion point, then record R and ϵ_i's, replace P_j by R for the largest index j with $\epsilon_j \neq 0$, and go to **Step 1**. If R is a torsion point, then we can construct the dependence equation for the original $P_1, \cdots, P_r$ from the records of R's and ϵ_i's.

In order to see whether this procedure will stop, we need the following lemma.

Lemma 2.2. *Suppose that R and ϵ_i's are defined as* **Step 3**. *Then*

$$4\hat{h}(R) \leq \hat{h}(\epsilon_1 P_1) + \cdots + \hat{h}(\epsilon_r P_r).$$

Proof. Since the canonical height satisfies the parallelogram law, we have

$$\begin{aligned} & 2\hat{h}(\epsilon_1 P_1 + \cdots + \epsilon_{r-1} P_{r-1}) + 2\hat{h}(\epsilon_r P_r) \\ = \quad & \hat{h}(\epsilon_1 P_1 + \epsilon_2 P_2 + \cdots + \epsilon_r P_r) + \hat{h}(\epsilon_1 P_1 + \cdots + \epsilon_{r-1} P_{r-1} - \epsilon_r P_r). \end{aligned}$$

By the choice of ϵ_i's,

$$\hat{h}(\epsilon_1 P_1 + \cdots + \epsilon_{r-1} P_{r-1} + \epsilon_r P_r) \leq \hat{h}(\epsilon_1 P_1 + \cdots + \epsilon_{r-1} P_{r-1} - \epsilon_r P_r).$$

Therefore, we get

$$\hat{h}(\epsilon_1 P_1 + \cdots + \epsilon_{r-1} P_{r-1} + \epsilon_r P_r) \leq \hat{h}(\epsilon_1 P_1 + \cdots + \epsilon_{r-1} P_{r-1}) + \hat{h}(\epsilon_r P_r).$$

Inductively, we can show that

$$\hat{h}(\epsilon_1 P_1 + \cdots + \epsilon_r P_r) \leq \hat{h}(\epsilon_1 P_1) + \cdots + \hat{h}(\epsilon_r P_r).$$

Since

$$4\hat{h}(R) = \hat{h}(2R) = \hat{h}(\epsilon_1 P_1 + \cdots + \epsilon_r P_r),$$

we have

$$4\hat{h}(R) \leq \hat{h}(\epsilon_1 P_1) + \cdots + \hat{h}(\epsilon_r P_r).$$

□

Theorem 2.3. *Suppose $r = 3$ and we have $P_i^{(n)}$'s after repeating n-times the above procedure, then*

$$\min_i(\hat{h}(P_i^{(n)})) \leq (3/4)^{\lfloor n/3 \rfloor} \max_i(\hat{h}(P_i)). \tag{2}$$

Therefore, if we let $\hat{h}_E$ be the minimum of $\hat{h}(P)$ for all non-torsion points P, then this algorithm terminate within $n(E, P_1, \cdots, P_r)$-times repeating where

$$n(E, P_1, \cdots, P_r) = \lceil 3\frac{\log \max_i(\hat{h}(P_i)) - \log \hat{h}_E}{\log 4 - \log 3} \rceil,$$

that is, it terminates in polynomial time of $\max_i(\hat{h}(P_i))$.

Proof. As we assume in the procedure, we suppose that $\hat{h}(P_i^{(n)}) < \hat{h}(P_j^{(n)})$ for all n if $i < j$. In particular, $P_i^{(0)} = P_i$ $(i = 1, 2, 3)$. By the above lemma, we get that

$$4\hat{h}(R) \leq \hat{h}(\epsilon_1 P_1) + \hat{h}(\epsilon_2 P_2) + \hat{h}(\epsilon_3 P_3)$$

where R is given in **Step 3**. Then, it is easy to see that

(1) If $\epsilon_3 \neq 0$, then $\hat{h}(R) < 3\hat{h}(P_3)/4$.
(2) If $\epsilon_3 = 0$ and $\epsilon_2 \neq 0$, then $\hat{h}(R) < \hat{h}(P_2)/2$.
(3) IF $\epsilon_2 = \epsilon_3 = 0$ and $\epsilon_1 \neq 0$, then $\hat{h}(R) < \hat{h}(P_1)/4$.

In the above three cases, the possible maximum of $\hat{h}(R)$ is smaller than $3\hat{h}(P_3)/4$, so we have proved the inequality (2).

Moreover, if

$$(3/4)^{\lfloor n/3 \rfloor} \max_i(\hat{h}(P_i)) < \hat{h}_E,$$

then (2) means that $P_1^{(n)}$ is a torsion-point. By solving this inequality for n, we have proved the theorem. □

Remark 2.4. *As we have seen in the proof, $n(E, P_1, \cdots, P_3)$ is very rough upper bound for the running-time of Descent method. In fact, the heights of R's decrease more rapidly.*

Remark 2.5. *Even in the case of $r \geq 4$, this algorithm can be applied. First, we consider the case of $r = 4$. In* **Step 3**, *we get*

$$2R = \epsilon_1 P_1 + \epsilon_2 P_2 + \epsilon_3 P_3 + \epsilon_4 P_4.$$

If one of ϵ_i's are 0, then it is satisfied that

$$\hat{h}(R) < (3/4) \max_i(\hat{h}(P_i)).$$

Moreover, even in the case that all ϵ_i's are non-zero,

$$\hat{h}(R) = \text{ average of } \hat{h}(P_i) < \max_i(\hat{h}(P_i)).$$

This means that the heights of R's decrease, so the algorithm terminates successfully.

Remark 2.6. *Although the heights of R's may not decrease in the case that r is larger, the heights of them are willing to be bounded since we choose the points R's with small heights. Therefore, we can expect that some point appears twice in this procedure. When this happens, it is not hard to construct the dependence equation as long as we keep track of the points R's and ϵ_i's* [13].

2.3. **ECDLP on $\mathbb{F}_{2^m}$.** In general, we cannot lift an elliptic curve $\tilde{E}$ over $\mathbb{F}_{p^m}$ to an elliptic curve over $\mathbb{Q}$ for $n > 1$, so we should lift it to an elliptic curve over a number field or an elliptic curve over a function field $\mathbb{F}_p(T)$. Here, we show that the 2-descent method can be applied not only to the case of the rational field but also to the case of the function field, so that the lifting problem generalized to the function fields means the ECDLP on $\mathbb{F}_{p^m}$ for $m > 1$. For simplicity, we consider only the case of $p = 2$.[5]

It is easy to generalize the definition 2.1 to the function fields and to see that each step of the algorithm to solve the ECDLP in the section 2 holds even in the case of the function field except the 2-descent procedure because there is no known algorithm to compute the canonical heights on the function fields.[6] However, the following theorem show that if the difference between the absolute heights of two points are sufficiently large, it is easy to compare between the canonical heights of them. Hence we can easily make the sequence of the points whose canonical heights are decreasing because the absolute heights are easily computable.

[5]Our algorithm may be applied to any finite fields with small characteristic p.

[6]For the definitions of absolute heights and canonical heights over the function fields, see [10].

Theorem 2.7. *Suppose E is an elliptic curve over $\mathbb{F}_2[T]$ defined by*

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad a_2 \text{ and } a_6 \in \mathbb{F}_2[T]$$

and the points R, R' of $E(\mathbb{F}_2(T))$ satisfy that

$$|h(R) - h(R')| > \frac{5}{6}\deg a_6.$$

Then

$$\hat{h}(R) > \hat{h}(R') \quad \text{if and only if} \quad h(R) > h(R').$$

Proof. First, we need the following lemma.

Lemma 2.8. *Suppose E is an elliptic curve over $\mathbb{F}_2[T]$ defined by*

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad a_2, a_6 \in \mathbb{F}_2[T].$$

Then

$$-\frac{1}{4}\deg a_6 \le \hat{h}(P) - \frac{1}{2}h(P) \le \frac{1}{6}\deg a_6.$$

Proof. First, we write $x(P) = f/g$ where f and g are relative prime polynomials of $\mathbb{F}_2[T]$. Then

$$x(2P) = \frac{f^4 + a_6g^4}{f^2g^2}.$$

Let $k = \gcd(f^4 + a_6g^4, f^2g^2) = \gcd(a_6, f^2)$, then

$$\begin{aligned} h(2P) &= \max\{\deg(f^4 + a_6g^4), \deg(f^2g^2)\} - \deg k \\ &\le \max\{4\deg f, 4\deg g + \deg a_6, 2\deg f + 2\deg g\} \\ &\le 4h(P) + \deg a_6 \end{aligned} \tag{3}$$

since $\deg k \le \deg a_6$.

If $4\deg f \ne 4\deg g + \deg a_6$, then

$$\deg(f^4 + a_6g^4) = \max\{4\deg f, 4\deg g + \deg a_6\}.$$

Hence,

$$h(2P) \ge 4h(P) - \deg a_6. \tag{4}$$

Now, suppose that $4\deg f = 4\deg g + \deg a_6$. Then

$$\begin{aligned} h(2P) &\ge 2\deg f + 2\deg g - \deg k \\ &\ge 4\deg f - \frac{3}{2}\deg a_6 \ge 4h(P) - \frac{3}{2}\deg a_6. \end{aligned} \tag{5}$$

With (3),(4) and (5), we have

$$-\frac{3}{2}\deg a_6 \le h(2P) - 4h(P) \le \deg a_6.$$

By applying 2^nP instead of P in the above,

$$-(1 + \cdots + 4^{n-1})\frac{3}{2}\deg a_6 \le h(2^nP) - 4^nh(P) \le (1 + \cdots + 4^{n-1})\deg a_6.$$

Since

$$\lim_{n\to\infty}\sum_{i=1}^{n}\frac{1}{4^n} = \frac{1}{3} \text{ and } \hat{h}(P) = \frac{1}{2}\lim_{n\to\infty}\frac{1}{4^n}h(2^nP) \text{ for any point } P,$$

we have

$$-\frac{1}{4}\deg a_6 \leq \hat{h}(P) - \frac{1}{2}h(P) \leq \frac{1}{6}\deg a_6.$$

□

By the above lemma, we get

$$h(R) - h(R') + \frac{5}{6}\deg a_6 \geq 2\hat{h}(R) - 2\hat{h}(R') \geq h(R) - h(R') - \frac{5}{6}\deg a_6$$

for any points R, R' of $E(\mathbb{F}_2(T))$. Therefore, if R and R' satisfy

$$|h(R) - h(R')| > \frac{5}{6}\deg a_6,$$

then $h(R) - h(R')$ and $\hat{h}(R) - \hat{h}(R')$ are both positive or negative. It proves the theorem. □

Hence we can compare the canonical heights of two points by comparing their absolute heights if the difference of their absolute heights is smaller than $5\deg a_6/6$. Therefore, when we make the sequence of the points R's in the 2-descent procedure, we choose ϵ_i's so that the absolute heights of R's are as small as possible. Then, even though we can not guarantee that the sequence of the points R's converges to O, we can expect that some point appearing twice in the sequence of R's with a reasonable probability because the heights of the points R's are bounded. Therefore, we can construct the dependence equation similarly to the case of the rational field.

Finally, we conclude that the lifting problem to function fields implies the ECDLP over $\mathbb{F}_{2^m}$.

3. Lifting Problem and Integer Factorization

In this section, we propose a method to factorize a square-free integer n by using the lifting problem. First, we compute the order of a given point $\tilde{P}$ of an elliptic curve $\tilde{E}$ defined over $\mathbb{Z}/n\mathbb{Z}$. Then, by using factors of the order, we can factorize n.

This method is an extended version of "Elliptic Curve Method" by Lenstra [6].

3.1. **The order of a point of $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$.** Let $n = p_1 \cdots p_s$ with $\gcd(n, 6) = 1$. An elliptic curve $\tilde{E}$ defined over $\mathbb{Z}/n\mathbb{Z}$ is given by the following Weierstrass equation

$$\tilde{E} : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}/n\mathbb{Z}$ and $\gcd(4a^3 + 26b^2, n) = 1$. The points on $\tilde{E}$, denoted by $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$, are the set of solutions in $\mathbb{Z}/n\mathbb{Z}$ to the Weierstrass equation together with a point at infinity, denoted O.

We define a "pseudo-addition" on the points of $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$ by using the same addition rules as that of elliptic curves defined on fields. This is evident since the addition is not always defined: if

$$\gcd(x(\tilde{P}) - x(\tilde{Q}), n) > 1 \quad (\text{resp. } \gcd(2y(\tilde{P}), n) > 1),$$

then the addition (resp. multiplication by 2) involves division by a non-invertible element in $\mathbb{Z}/n\mathbb{Z}$. Note that we can get a non-trivial divisor of n when pseudo-addition is not defined. Therefore, because our final object is to get a non-trivial divisor of n, we may consider only the case that the pseudo-addition is defined. In

practice, since n has only large prime factors, it is very rare that the pseudo-addition is not defined.

Moreover, we have an inclusion

$$\phi : \tilde{E}(\mathbb{Z}/n\mathbb{Z}) \hookrightarrow \tilde{E}'(\mathbb{Z}/n\mathbb{Z}) = \tilde{E}(\mathbb{Z}/p_1\mathbb{Z}) \times \cdots \times \tilde{E}(\mathbb{Z}/p_s\mathbb{Z})$$

which is defined as $\phi(P) = (P \mod p_1, \cdots, P \mod p_s)$. Therefore, even though $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$ is not a group, we can define the order of $\tilde{P}$ in $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$ to be the order of $\phi(\tilde{P})$ in $\tilde{E}'(\mathbb{Z}/n\mathbb{Z})$.

Now, we compute the order of a point $\tilde{P}$ of an elliptic curve $\tilde{E}$ defined over $\mathbb{Z}/n\mathbb{Z}$. First, let $\tilde{P}_i = n_i\tilde{P}$ for some integers $n_1, \cdots, n_r$. Assuming that we find a good lifting $(E, P_1, \cdots, P_r)$ for $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$, then we can use the descent method so as to get

$$\alpha_1 P_1 + \cdots + \alpha_r P_r = O, \tag{6}$$

for some integers $\alpha_1, \cdots, \alpha_r$. By reduction modulo n, we get

$$\sum \alpha_i \tilde{P}_i = (\sum \alpha_i n_i)\tilde{P} = O.$$

That is, we get $\alpha = \sum \alpha_i n_i$ as a multiple of the order of $\tilde{P}$. So, by factorizing α, we can compute the exact order of $\tilde{P}$.[7]

Note that α may be 0. But, $\alpha = 0$ implies $(\alpha_1, \cdots, \alpha_r)$ is the solution of

$$\alpha_1 n_1 + \cdots + \alpha_r n_r = 0.$$

So, if $n_1, \cdots, n_r$ are chosen to be relatively prime, the possibility of $\alpha_1 n_1 + \cdots + \alpha_r n_r = 0$ is not so high even though α_i's satisfy (6). Moreover, even in the case of $\alpha = 0$, we can repeat the same procedure for different n_i's until we have non-zero α.

3.2. **Integer Factorization.** Suppose that n is a square-free integer that we want to factorize.

Step 1 Take a random elliptic curve $\tilde{E}$ over $\mathbb{Z}/n\mathbb{Z}$ and a random point $\tilde{P}$ in $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$ and compute a non-zero integer α with $\alpha\tilde{P} = O$ by the above procedure.

Step 2 Factorize α and find a divisor d of α such that

$$(\alpha/d)P = (x : y : t) \text{ with } 1 < \gcd(t, n) < n.$$

Then we can get a non-trivial divisor $\gcd(t, n)$ of n. Go to **Step 1** with $n \leftarrow \gcd(t, n)$ (or $n/\gcd(t, n)$).

Step 3 If we get a prime divisor d of α such that

$$(\alpha/d)P = (x : y : t) \text{ with } \gcd(t, n) = 1 \text{ and}$$
$$d > (\sqrt[4]{n} + 1)^2,$$

then n is a prime.

Note that if $n = p_1 p_2 \cdots p_r$, then the order of $\tilde{P}$ in $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$ is the least common multiplier (LCM) of $\mathrm{ord}(\tilde{P} \mod p_i)$ in $\tilde{E}(\mathbb{Z}/p_i\mathbb{Z})$ $(i = 1, \cdots, r)$.

Therefore, if $\mathrm{ord}(\tilde{P} \mod p_i)$ divide α/d and if $\mathrm{ord}(\tilde{P} \mod p_j)$ does not divide α/d, then

$$(\alpha/d)P \equiv O \text{ in } \tilde{E}(\mathbb{Z}/p_i\mathbb{Z}) \text{ and}$$

[7]Also, if we can compute the order $N_n$of $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$, by computing the GCD of N_n and α, we can compute the order of $\tilde{P}$ more easily.

$$(\alpha/d)P \equiv O \text{ in } \tilde{E}(\mathbb{Z}/p_j\mathbb{Z}).$$

That is, **Step 2** gives a non-trivial divisor of n.

Step 3 is the "Goldwasswer-Kilian test". In **Step 3**, d divides the order of $\tilde{P}$ mod p in $\tilde{E}(\mathbb{Z}/p\mathbb{Z})$ for any prime divisor p of n. By Hasse's theorem, we have

$$d < (\sqrt[4]{p} + 1)^2$$

which is smaller then $(\sqrt[4]{n}+1)^2$ if n is a composite number. But, since $d > (\sqrt[4]{n}+1)^2$, this means that n is a prime.

Now, consider the possibilities that the above algorithm fails. First, about the existence of d, such divisor d always exists except in the case that the orders of $\tilde{P}$ in $\tilde{E}(\mathbb{Z}/p\mathbb{Z})$ are the same for all divisors p of n, which is not probable. Secondly, α may be difficult to factor even if we repeat it with another random points. This means that the order $\#\tilde{E}(\mathbb{Z}/p\mathbb{Z})$ contains only large prime factors for each prime factors p of n, which is also rare. In this case, however, we can avoid it by trying with another elliptic curve $\tilde{E}$. Consequently this algorithm is successful with high probability under the assumption of the lifting problem.

In summary, we present the relations among hard problems as follows:

- The lifting problem implies the ECDLP on a prime field $\mathbb{F}_p$.
- The lifting problem implies the order problem in an elliptic curve on $\mathbb{Z}/n\mathbb{Z}$.
- The order problem in an elliptic curve on $\mathbb{Z}/n\mathbb{Z}$ implies the integer factorization problem(IFP).

Remark 3.1. *The idea to relate the lifting problem to IFP was suggested first by Koblitz*[8]*. His method is to use the explicit isomorphism between $\mathbb{Z}/n\mathbb{Z}$ and a singular cubic curve defined over the ring. If one assume the lifting problem, he can solve DLP on a singular cubic curve over $\mathbb{Z}/n\mathbb{Z}$ and also DLP on $\mathbb{Z}/n\mathbb{Z}$, which implies the IFP. However, our method can be applied not only for a singular cubic curve but also for elliptic curves. Our method seems to be more natural.*

Remark 3.2. *Our method for the IFP is similar to Lenstra's ECM in that both methods try to find the order of a random point to solve the IFP. The difference is that ECM uses brute force depending on the distribution of smooth number to find the order and our method uses the lifting method to get a dependence equation which gives directly a multiple of the order, though the difficulty of the lifting problem should be analyzed and looks more difficult.*

4. Analysis of Lifting Problem

The lifting problem is the most important part of our method, but it seems to be very difficult. In this section, we look over the basic method for the construction of lifting elliptic curve with given points and analyze the possibility to solve the lifting problem and we note that if we can find a point of $E_1(\mathbb{Q})$ which is the kernel of the reduction, then we can solve the lifting problem even when the lifting points are linearly independent. Moreover, we show that the points of $E_1(\mathbb{Q})$ has large canonical heights so that it is difficult to find a point of $E_1(\mathbb{Q})$ by brute force search.

[8]See Appendix K in [13].

4.1. **Basic Method of Lifting Problem.** Let $\tilde{E}$ be an elliptic curve defined on $\mathbb{F}_p$ given by the following Weierstrass equation

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

and $\tilde{P}_1, \cdots, \tilde{P}_r$ the points of $\tilde{E}(\mathbb{F}_p)$ $(r < 7)$. Since $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, we can consider the coefficients a_i's of the Weierstrass equation and the coordinates of $\tilde{P}_i$'s as integers less than p. We define the integral points P_i's by the point $\tilde{P}_i$'s respectively which are determined as above. Then, by linear algebra, we can determine $t_1, \cdots, t_7 \in \mathbb{Q}$ such that

$$\begin{aligned} E &: (1+pt_1)y^2 + (a_1+pt_2)xy + (a_3+pt_3)y \\ &= (1+pt_4)x^3 + (a_2+pt_5)x^2 + (a_4+pt_6)x + (a_6+pt_7) \end{aligned}$$

has the points P_i's as the rational points of $E(\mathbb{Q})$. Note that there are infinitely many choices of t_i's since $r < 7$ and since the plane cubic curve is given by an equation with 10-terms we can lift 9 points generally.

At first, the authors expected that it is possible to find the lifting elliptic curve E with rank $< r$ for a given $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$ by brute force search. More precisely, A. Brumer analyzed the rank distribution of $\{E \mid |\Delta| \leq 10^8, |a_6| \leq 2^{31} - 1\}$ with prime $|\Delta|$ and got the following table,

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

and he also showed that the average rank is at most 2.3 [2]. That is, the rank of an elliptic curve tends to be small. Moreover, the rank of an elliptic curve is bounded by the number of prime factors of the discriminant.

Theorem 4.1. [1] *Suppose that the elliptic curve E is defined by the following Weierstrass equation*

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

and that $w(x)$ is the number of distinct primes dividing x. Then

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

So, at first, we had expected that the good lifting could be constructed by making the discriminant of the lifting elliptic curve have a few prime factors.

However, since the above lifting method gives only elliptic curves with several large rational points, their ranks would be larger than general cases. Moreover, when $r = 2$, the discriminant of the lifting elliptic curve constructed by the basic method has at least 3 prime factors [3]. That is, we can construct only the lifting of which the rank of $E(\mathbb{Q})$ is same as the number of the lifted points. (Of course, the lifted points are linearly independent.) Also, even when its rank is smaller than the number of lifting points, the linearly dependence relation is satisfied with small coefficients, which implies that the basic method solves the lifting problem only if the ECDLP is trivial.

Remark 4.2. *Silverman suggested another method to reduce the rank of lifting elliptic curves is to use the reverse of Mestre's method* [13]. *Mestre applied Birch and Swinnerton-Dyer Conjecture to get high rank elliptic curves. The conjecture says that an elliptic curve over $\mathbb{Q}$ whose reduction to finite fields has large order*

may have large rank. Silverman applied Mestre's method reversely to get elliptic curves with lower rank.

But, he found that asymptotically his algorithm is virtually certain to fail, because of an absolute bound on the size of the coefficients of the linearly dependence relation satisfied by the lifting points [4].

4.2. $E_1(\mathbb{Q})$ **and Lifting Problem.** Suppose that the lifted elliptic curve E of $\tilde{E}$ with r linearly independent lifted points P_i's of $\tilde{P}_i$'s has the rank r. If we can find a point R of $E_1(\mathbb{Q})$ where

$$E_1(\mathbb{Q}) = \{P \in E(\mathbb{Q}) | P \equiv O \mod p\},$$

then $(E, P_1, \cdots, P_r, R)$ becomes a good lifting of $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r, \tilde{O})$. Moreover, if R is not contained in the group generated by $N_p P_i$'s where $N_p = |\tilde{E}(\mathbb{F}_p)|$, then the dependence relation of $\{P_1, \cdots, P_r, R\}$ gives a non-trivial dependence relation of $\{\tilde{P}_1, \cdots, \tilde{P}_r\}$. That is, To find a non-trivial point of $E_1(\mathbb{Q})$ solves the ECDLP.

Unfortunately, any algorithm to find a non-trivial point of $E_1(\mathbb{Q})$ is not known yet except the brute force search. Therefore, we first estimate the minimum of the canonical heights of points on $E_1(\mathbb{Q})$. To make this precise, we define ϵ-difficult ECDLP.

Definition 4.3. *Let $\tilde{E}$ be an elliptic curve defined over $\mathbb{F}_p$ where $q = |\tilde{E}(\mathbb{F}_p)|$ is a prime. Then, for given $\tilde{P}, \tilde{Q} \in \tilde{E}(\mathbb{F}_p)$, we say that $\tilde{P}$, $\tilde{Q}$ satisfy ϵ-difficult ECDLP $(0 < \epsilon \leq 1)$ if and only if $a_1\tilde{P} + a_2\tilde{Q} \neq O$ for all $0 < |a_i| < \epsilon\sqrt{q}$.*

Note that for a fixed $\tilde{P}$, each solution (a_1, a_2) of

$$a_1\tilde{P} + a_2\tilde{Q} = O$$

is unique for the choice of $\tilde{Q}$. Hence for a fixed $\tilde{P}$ and a fixed $\epsilon < 1/2$, the number of $\tilde{Q}$'s which satisfy ϵ-difficult ECDLP is greater than $(1 - 4\epsilon^2)q$. That is, two randomly chosen points $\tilde{P}$ and $\tilde{Q}$ satisfy ϵ-difficult ECDLP with probability greater than $1 - 4\epsilon^2$.

The following theorem gives the lower bound of the canonical heights of the points $E_1(\mathbb{Q})$ where E is the lifting elliptic curve associated to the points $\tilde{P}$ and $\tilde{Q}$ which satisfy ϵ-difficult ECDLP.

Theorem 4.4. *Suppose that $\tilde{P}, \tilde{Q}$ in $\tilde{E}(\mathbb{F}_p)$ satisfy ϵ-difficult ECDLP and that $(E, P_1, \cdots, P_r)$ is a lifting of $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$ where P_i's are the generators of the Mordell-Weil group $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$ and $\tilde{P}_i = x_i\tilde{P} + y_i\tilde{Q}$ for some integers x_i, y_i respectively.*

Then, there exists a constant c which is uniquely determined by $(E, P_1, \cdots, P_r)$ such that

$$\hat{h}(R) > \frac{c\epsilon^2 q}{r^2 N^2}.$$

for any point R of $E_1(\mathbb{Q})$ where $N = \max(|x_i|, |y_i|)$.

Proof of Theorem. Since P_i's are the generators of $E(\mathbb{Q})$ / $E(\mathbb{Q})_{tor}$, for any point R of $E_1(\mathbb{Q})$, there exist integers $\alpha_1, \cdots, \alpha_r$ such that

$$R = \alpha_1 P_1 + \cdots + \alpha_r P_r.$$

By taking reduction modulo p with the above equation, we get

$$\left(\sum x_i\alpha_i\right)\tilde{P} + \left(\sum y_i\alpha_i\right)\tilde{Q} = O.$$

Since $\tilde{P}, \tilde{Q}$ satisfy the ϵ-difficult ECDLP, we get

$$\begin{aligned} \epsilon\sqrt{q} &< \max(\Big|\sum x_i\alpha_i\Big|, \Big|\sum y_i\alpha_i\Big|) \\ &< r \max_i(|x_i|, |y_i|) \max_i(|\alpha_i|). \end{aligned} \tag{7}$$

The following lemma proves the theorem.

Lemma 4.5. *Let E be an elliptic curve defined over K and the points $P_1, \cdots, P_r$ of $E(K)$ are linearly independent. Define the matrix*

$$A = (a_{ij})_{1 \le i,j \le r}$$

where

$$a_{ij} = \hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j), \quad (i, j = 1, \cdots, r).$$

If we define

$$c_k = a_{kk} - \mathbf{a}_k A_k^{-1} \mathbf{a}_k^T \quad (k = 1, \cdots, r)$$

where $\mathbf{a}_k = (a_{k1}, \cdots, a_{kk-1}, a_{kk+1}, \cdots, a_{kr})$ and A_k is the matrix obtained by removing kth-row and kth-column in A, then, for any integers $n_1, \cdots, n_r$,

$$\hat{h}(n_1P_1 + \cdots + n_rP_r) \ge c \max(n_1^2, \cdots, n_r^2)$$

where

$$c = c(E, P_1, \cdots, P_r) = \frac{1}{2}\min(c_1, \cdots, c_r) > 0.$$

Especially, in the case of $r = 2$,

$$c = \min(\hat{h}(P_1), \hat{h}(P_2)) - \frac{(\hat{h}(P_1 + P_2) - \hat{h}(P_1) - \hat{h}(P_2))^2}{4\max(\hat{h}(P_1), \hat{h}(P_2))}.$$

Proof. Note that

$$\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$$

is the positive-definite symmetric bilinear form on $E(K)/E(K)_{tor}$. Moreover, it can be extended to

$$\langle\ ,\ \rangle : (E(K)/E(K)_{tor} \otimes \mathbb{R})^2 \to \mathbb{R}$$

with taking tensor product on $(E(K)/E(K)_{tor}$ by $\mathbb{R}$ [10].

For simplicity, we may assume that $|n_1| = \max_i(|n_i|)$. Then if we define $a_{ij} = \langle P_i, P_j \rangle$ and $x_i = n_i/n_1$ $(i = 1, \cdots, r)$, then

$$\langle n_1P_1 + \cdots + n_rP_r, n_1P_1 + \cdots + n_rP_r \rangle = n_1^2(a_{11} + 2\sum_{i \ge 2} a_{1i}x_i + \sum_{i,j \ge 2} a_{ij}x_ix_j).$$

Since $\langle , \rangle$ is the positive-definite symmetric bilinear form, it is easy to show that

$$f(x_2, \cdots, x_r) = a_{11} + 2\sum_{i \ge 2} a_{1i}x_i + \sum_{i,j \ge 2} a_{ij}x_ix_j$$

has the minimum

$$a_{11} - (a_{12}, \cdots, a_{1r})A_1^{-1}(a_{12}, \cdots, a_{1r})^T$$

when

$$(x_2, \cdots, x_r)^T = -A_1^{-1}(a_{12}, \cdots, a_{1r})^T.$$

That is,

$$2\hat{h}(n_1P_1 + \cdots + n_rP_r) = \langle n_1P_1 + \cdots + n_rP_r, n_1P_1 + \cdots + n_rP_r \rangle \ge c_1n_1^2.$$

In general

$$2\hat{h}(n_1P_1 + \cdots + n_rP_r) \geq \min_i(c_i)\max_i(n_i^2).$$

Especially, when $r = 2$, we get

$$c_1 = 2\hat{h}(P_1) - \frac{(\hat{h}(P_1+P_2) - \hat{h}(P_1) - \hat{h}(P_2))^2}{2\hat{h}(P_2)}$$

$$c_2 = 2\hat{h}(P_2) - \frac{(\hat{h}(P_1+P_2) - \hat{h}(P_1) - \hat{h}(P_2))^2}{2\hat{h}(P_1)}.$$

Since

$$2^{-1}\min(c_1, c_2) = \min(\hat{h}(P_1), \hat{h}(P_2)) - \frac{(\hat{h}(P_1+P_2) - \hat{h}(P_1) - \hat{h}(P_2))^2}{4\max(\hat{h}(P_1), \hat{h}(P_2))},$$

the lemma is done. □

By the above lemma, the equation (7) gives

$$\epsilon^2 q < r^2N^2\hat{h}(R)/c(E, P_1, \cdots, P_r),$$

which proves the theorem. □

By the above theorem, if we try to solve the ECDLP by finding a point $R \in E_1(\mathbb{Q})$ where E is the lifting elliptic curve with r lifted points, then R must satisfies $\hat{h}(R) \geq c\epsilon^2 q/(r^2N^2)$ with probability $(1 - \epsilon^2)$, that is too large to be found by brute force search. That is, some additional technics should be developed to solve ECDLP by this method.

For example, let p be a 160-bit prime and $\epsilon = 2^{-10}$. Then the canonical height of R is $O(2^{140})$ and this means that the denominator of $x[R]$ (and numerator of $x[R]$) is $O(\exp(2^{140}))$.

Example Let E, P, Q be same as the above example and $p = 269$. Then $|\tilde{E}(\mathbb{F}_p)| = 277$ is a prime, and, for any a_1, a_2 with $|a_i| < 16$,

$$a_1P + a_2Q \not\equiv O \mod p.$$

So, P and Q satisfy ϵ-difficult ECDLP for $\epsilon = 16/\sqrt{277} \sim 0.961$.

By Theorem 4.4,

$$\hat{h}(R) > c\epsilon^2 q/rN > 97.16207922.^9$$

In fact, $(a_1, a_2) = (16, 7)$ is the minimal solution, so $R = a_1P + a_2Q$ is the point with minimal canonical height on $E_1(\mathbb{Q})$. Its x-coordinate is

$$\begin{array}{ll} - & 900275065185198172229382750515524917704507648 58 \\ & 668915853075764947366351876980052919747393617 83 \\ & 829121644478626123858905257307621747912328322 36 \\ / & 956978384789385309059539093098866093086297486 60 \\ & 413065870661609518142212332534747359237595341 91 \\ & 586241716502959236815332168000486776355009592 01 \end{array},$$

and $\hat{h}(R)$ is about 162.7319387. It is too large to be found by brute force search.

[9] As in the proof of theorem 4.2, we should apply $r = 1$ in case that we use the original point $\tilde{P}, \tilde{Q}$ as the lifted points.

5. Conclusion

In this paper, we introduced the "lifting problem", that is to lift an elliptic curve over a finite field to one over a global field with the rank smaller than the number of lifted points.

We showed that it solves many important problems in mathematics and cryptography such as the elliptic curve discrete logarithm problem and the integer factorization problem. This is the first attempt within our knowledge to use general properties of elliptic curves to attack the ECDLP, the DLP and the IFP.

In order to solve the lifting problem, we proposed to find a non-trivial point in $E_1(\mathbb{Q})$ in order to get a lifted elliptic curve with rank smaller than the number of lifted points. By this method, we conclude that finding a non-trivial point in $E_1(\mathbb{Q})$ implies solving the ECDLP, the DLP and the IFP.

Moreover, we proved that if we construct the lifted elliptic curve with the basic method, the minimum of canonical height of a point in $E_1(\mathbb{Q})$ is almost $O(|\tilde{E}(\mathbb{F}_p)|)$, which is too large to be found by the brute force search. That is, the proposed method is not practical yet.

References

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

[2] A. Brumer. The average rank of elliptic curves i. *Invent. math.*, 109:445–472, 1992.

[3] J. H. Cheon, D. H. Lee, and S. G. Hahn. Elliptic curve discrete logarithms and wieferich primes. preprint, 1998.

[4] J. Jacobson, N. Koblitz, J. H. Silverman, A. Stein, and E. Teske. Analysis of the xedni calculus attack. to appear in Designs, Codes and Cryptography.

[5] A. W. Knapp. *Elliptic curves*. Princeton University Press, 1992.

[6] H. W. Lenstra. Factoring integers with elliptic curves. *Ann. of Math.*, 126:649–673, 1987.

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

[8] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, 1999.

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

[10] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition, 1986.

[11] J. H. Silverman. *Advanced topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, 1994.

[12] J. H. Silverman. Computing canonical heights with little (or no) factorization. *Math. Comp.*, 66(218):787–805, 1997.

[13] J. H. Silverman. The xedni calculus and the elliptic curve discrete logarithm problem. to appear in Designs, Codes and Cryptography, 1998.

[14] J. H. Silverman and J. Suzuki. Elliptic curve discrete logarithms and the index calculus. *Advances in Cryptology - ASIACRYPT'98*, pages 110–125, 1988.

[15] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.

Initech Co. Ltd., Kwang-Sung B/D 8th Floor, 831-47 Youksam-Dong, Kangnam-Gu, Seoul 135-070, Republic of Korea

E-mail address: hwanjoon@initech.com

Math. Dept, Brown University/Box 1917, Providence, RI 02912, USA

E-mail address: jhcheon@math.brown.edu

Department of Mathematics, KAIST, 373-1 Kusong-Dong, Yusong-Gu, Taejon 305-701, Republic of Korea

E-mail address: sghahn@math.kaist.ac.kr