ELLIPTIC CURVE LIFTING PROBLEM AND ITS APPLICATIONS

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

1. Introduction

In this paper, we introduce a new method to solve the elliptic curve discrete logarithm probelm (ECDLP) over a finite field by using the elliptic curve lifting problem.[1] Moreover, we propose 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 discrete logarithm problem (DLP) and the integer factorization problem (IFP). Finally, we find that the minimum of canonical height of a point in $E_1(\mathbb{Q})$ is almost $O(|\tilde{E}(\mathbb{F}_p)|)$, which means that it is too large to be found by the brute force search.

2. ECDLP on $\mathbb{Z}/n\mathbb{Z}$ and IFP

Throughout this section, we assume that n is a square free integer. 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 $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$. The elliptic curve E over $\mathbb{Q}$ is called by the lifted elliptic curve of $\tilde{E}$ if $E \equiv \tilde{E} \bmod n$. Similarly, if the points $P_1, \cdots, P_r$ of $E(\mathbb{Q})$ are congruent to $\tilde{P}_1, \cdots, \tilde{P}_r$ modulo n respectively, then they are called by the lifted points of $\tilde{P}_i$'s. We define $(E, P_1, \cdots, P_r)$ to be the lifting of $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$ if E and P_i's are as above. Furthermore, if $P_1, \cdots, P_r$ are linearly dependent, then we call $(E, P_1, \cdots, P_r)$ by the "good" lifting.*

Finally, we define that the elliptic curve lifting problem (shortly, the lifting problem) is to find an good lifting $(E, P_1, \cdots, P_r)$ for a given $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$.

Suppose $\tilde{E}$ is an elliptic curve defined over $\mathbb{Z}/n\mathbb{Z}$ with $\tilde{P}$, $\tilde{Q}$ in $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$. Then the ECDLP on $\mathbb{Z}/n\mathbb{Z}$ is to find

$$\log_{\tilde{P}} \tilde{Q} := \min\{m \in \mathbb{N} | \tilde{Q} = m\tilde{P}\}.$$

We show how to solve the ECDLP on $\mathbb{Z}/n\mathbb{Z}$ assuming the lifting problem is solved.

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, y_i we take

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

Step 2 Solve a lifting problem for $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_r)$. Then we get a lifted 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

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

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

[1]Silverman proposed a similar method named by "Xedni calculus" independently [7].

by the descent method which will be explained in section 2.1.
Step 4 By reduction modulo n, we have

$$\log_{\tilde{P}} \tilde{Q} \equiv -\frac{\sum \alpha_i x_i}{\sum \alpha_i y_i} \mod \mathrm{ord}\tilde{Q}.$$

2.1. **Descent method.** By descent method, we can compute the coefficients of the dependence equation for the linearly dependent points P_i's of $E(\mathbb{Q})$.

There are some variations of the descent method with respect to computation of the canonical heights. One may use the non-degenerate bilinear quadratic form induced by the canonical heights. But he also has difficulty in computing the exact value of the canonical heights. On the other hand, one may not use the canonical heights at all but use only the absolute heights as [7]. But, he can not estimate the number of required steps. Our method need not to compute the exact value of the canonical heights and can estimate the number of required steps.
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 [5, 12].
Step 2 For $k = 2, \cdots, r$, determine the sign of ϵ_k satisfying

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

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

And then we 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 not easy to compute the exact values of $\hat{h}(P)$ for the rational points P in general. However, considering that what we need is only the comparison of the canonical heights, we can easily determine the signs of ϵ_i's [6, 11]. Also, it is easy to compute the halving point R of P satisfying $2R = P$ for $P \in 2E(\mathbb{Q})$ because it is equivalent to finding the rational roots of the polynomial of degree 4 with rational coefficients. Moreover, when E has rational 2-torsion points, there is exact formula to compute the halving point R [5, 12].
Step 3 Repeat this procedure with new P_i's where only P_j is replaced by R for the largest index j with $\epsilon_j \neq 0$ until R is a torsion point. 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.

The running-time of this algorithm is as following.

Theorem 2.2. *Suppose $r = 3$ and we have $P_i^{(n)}$'s after repeating n-times the above procedure, then*

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

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. Suppose that R and ϵ_i's are defined as Step 2, then

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

which proves the theorem. □

Even in the case $r > 3$, the probability that $\hat{h}(R)$ is increasing is smaller. For example, when $r = 4$, we probably expect this algorithm terminates within $15n(E, P_r)/14$-times repeating.

2.2. **The order of a point $\tilde{P}$.** Let $\tilde{E}$ be an elliptic curve defined over $\mathbb{Z}/n\mathbb{Z}$ and let $\tilde{P}_i = n_i\tilde{P}$ for a random point $\tilde{P}$ of $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$ and integers $n_1, \cdots, n_r$.

Note that for $n = p_1 \cdots p_s$ 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 $\phi(P) = (P \mod p_1, \cdots, P \mod p_s)$. 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 in $\tilde{E}'(\mathbb{Z}/n\mathbb{Z})$.

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

$$\alpha_1 P_1 + \cdots + \alpha_r P_r = O, \tag{2}$$

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 $\tilde{P}$.

2.3. **Integer factorization problem.** Suppose that n is an integer that we want to factor. Take a random elliptic curve $\tilde{E}$ over $\mathbb{Z}/n\mathbb{Z}$ and a random point $\tilde{P}$ in $\tilde{E}(\mathbb{Z}/n\mathbb{Z})$. Assume that we get a non-zero α with $\alpha\tilde{P} = O$ by the above procedure. Then, for some divisor d of α and some prime factor p of n, it may occur that $(\alpha/d)\tilde{P}$ is O modulo p and not O modulo n. This means that $(\alpha/d)\tilde{P}$ gives a non-trivial factor p of n.

Actually, such 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.

Note that α may be difficult to factor even if we repeat it with another random points. This means that the order of $\tilde{E}(\mathbb{Z}/p\mathbb{Z})$ 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.

Remark 2.3. *The idea to relate the lifting problem to IFP was suggested first by Koblitz (See Appendix K in* [7]*). However, his method is to use the explicit isomorphism between $\mathbb{Z}/n\mathbb{Z}$ and a singular cubic curve defined over $\mathbb{Z}/n\mathbb{Z}$, our method can be applied not only to a singular cubic curve but also to general elliptic curves. Hence, our method is more natural.*

3. Analysis 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 $\tilde{E}(\mathbb{F}_p)$ $(r \leq 4)$[2]. By linear algebra, we can take appropriate rational numbers t_i's in the following equation

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

to make E to contain rational points P_i's whose reduction to $\mathbb{F}_p$ is $\tilde{P}_i$ respectively. However, an elliptic curve E constructed as above is inclined to have rank r because it contains large r integral points P_i's. Hence, without loss of generality, we can assume that the lifted points are the generators of $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$.

In this case, suppose that 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_pP_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, it 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. We first estimate the minimum of the canonical heights of points on $E_1(\mathbb{Q})$. To make this precise, we begin with the definition of "ϵ-difficult" ECDLP.

Definition 3.1. *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 $\epsilon < 1/2$, the number of $\tilde{Q}$'s which satisfy ϵ-difficult ECDLP is greater than $(1 - 4\epsilon^2)q$ by pigeon-hole principle. That is, for given $\epsilon < 1/2$, two randomly chosen points $\tilde{P}$ and $\tilde{Q}$ satisfy ϵ-difficult ECDLP with probability greater than $1 - 4\epsilon^2$. In general,

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

Theorem 3.2. *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 $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$ 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 $N = \max(|x_i|, |y_i|)$.

[2]It can be extended to the case $r \leq 9$ as in [7].

Proof of Theorem. Since we assume that 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

$$\epsilon\sqrt{q} < \max(\left|\sum x_i\alpha_i\right|, \left|\sum y_i\alpha_i\right|) < r \max_i(|x_i|, |y_i|) \max_i(|\alpha_i|). \tag{3}$$

The following lemma proves the theorem.

Lemma 3.3. *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

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

where $\vec{a}_k = (a_{k1}, \cdots, a_{kk-1}, a_{kk+1}, \cdots, a_{kr})$ 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 $E(K)/E(K)_{tor}$. Furthermore, it can be extended to $E(K)/E(K)_{tor} \otimes \mathbb{R}$ [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

$$\begin{aligned}
&\langle n_1P_1 + \cdots + n_rP_r, n_1P_1 + \cdots + n_rP_r\rangle \\
&= n_1^2(a_{11} + 2\sum_{i\ge 2} a_{1i}x_i + \sum_{i,j\ge 2} a_{ij}x_ix_j) \\
&\ge n_1^2(a_{11} - (a_{12}, \cdots, a_{1r})A_1^{-1}(a_{12}, \cdots, a_{1r})^T)
\end{aligned}$$

since $\langle , \rangle$ is the positive-definite symmetric bilinear form.

Especially, when $r = 2$, we get

$$c_i = 2\hat{h}(P_i) - \frac{(\hat{h}(P_1 + P_2) - \hat{h}(P_1) - \hat{h}(P_2))^2}{2\hat{h}(P_{3-i})} \quad (i = 1, 2).$$

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 (3) gives

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

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 lifted elliptic curve with r lifted points, then R must satisfies $\hat{h}(R) \geq c\epsilon^2 q/(r^2N^2)$ with probability $(1 - 4\epsilon^2)$, that is too large to be found by brute force search.

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 or the numerator of $x[R]$ is $O(\exp(2^{140}))$.

References

[1] 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.

[2] T. Satoh and K. Araki, **Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves**, 1997, to appear in Commentarii Math. Univ. St. Pauli.

[3] 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** (1998), 353–356.

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

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

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

[7] J. H. Silverman, **The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem**, 1998, to appear in Code, Design and Cryptography.

[8] J. Jacobson, N. Koblitz, J. H. Silverman, A. Stein and E. Teske, **Analysis of the Xedni calculus attack**, 1999, preprint, available at http://www.cacr.math.uwaterloo.ca.

[9] J. H. Silverman and J. Suzuki, **Elliptic curve discrete logarithms and the index calculus**, proc. of Asiacrypt'98 (1988), 110–125.

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

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

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

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

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

Electronics and Telecommunications Research Institute, 161 Kajong-Dong, Yusong-Gu, Taejon, 305-350, Republic of Korea

E-mail address: jhcheon@etri.re.kr

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

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