International Journal of Pure and Applied Mathematics
Volume 71 No. 2 2011, 193-205

THE LIFTING PROBLEM FOR THE ECDLP AND THE SELMER RANK

Masaya Yasuda
[1]Fujitsu Laboratories Ltd.
1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki
211-8588, Japan

Abstract: The hardness of the elliptic curve discrete logarithm problem (ECDLP) on a finite field is essential for the security of all elliptic curve cryptographic schemes. A number of ways of approaching the solution to the ECDLP on a finite field is known, for example, the MOV attack [7], and the anomalous attack (see [9], [13]). In their paper [2], Cheon et al. proposed an algorithm to solve the ECDLP on prime fields, which is very efficient if we could lift two points to an elliptic curve over $\mathbb{Q}$ with rank one. In this paper, we investigate the success probability of their method by estimating the Selmer rank of lifted elliptic curves. We note that the Selmer rank means the upper bound of the rank given by the Selmer group (see [11]).

AMS Subject Classification: 11G05, 14H52
Key Words: ECDLP, formal groups, the Selmer rank

1. Introduction

In 1985, Neal Koblitz and Victor Miller independently proposed using elliptic curves to design public-key cryptographic systems (see [5], [6], [8]). The hardness of the elliptic curve discrete logarithm problem (ECDLP) on a finite field is essential for the security of all elliptic curve cryptographic schemes, for example, elliptic curve-based signature, public-key encryption, and key establishment schemes. The ECDLP on a field K is as follows: given an elliptic curve E defined over K, a point $S \in E(K)$, and a point $T \in E(K)$ with $T \in \langle S \rangle$, find the integer d such that $T = dS$. A number of ways of approaching the solution to the ECDLP on a finite field is known. However, no efficient algorithm is

Received: April 8, 2011

known for the ECDLP on a finite field except several special cased including the supersingular cases and the anomalous cases (see [1], [7], [9], [10], [13]).

For an elliptic curve E over $\mathbb{Q}$, the *rank* of E is the non-negative integer r satisfying

$$E(\mathbb{Q}) \simeq E_{\mathrm{tors}}(\mathbb{Q}) \times \mathbb{Z}^r,$$

where $E_{\mathrm{tors}}(\mathbb{Q})$ is the torsion subgroup (see [11] for details). In their paper [2], Cheon et al. proposed an algorithm to solve the ECDLP on prime fields, which is very efficient if we could lift two points to an elliptic curve over $\mathbb{Q}$ with rank one. We here call their method the *rank one attack*. Moreover, they investigated the success possibility that lifted elliptic curves have rank one. In general, it is very difficult to calculate the rank of an elliptic curve over $\mathbb{Q}$. Their method to check whether lifted elliptic curve E has rank one is to estimate the rank of E by calculating the upper bound of rank of E given by the number of primes divisors of the discriminant of E. However, the upper bound of rank of E given by them becomes significantly larger than the rank of E. Therefore it is not accurate to investigate the success probability of the rank one attack by their method. In this paper, we estimate the rank of E by calculating the upper bound of the rank of E given by the *Selmer rank*. The Selmer rank means the upper bound of the rank given by the Selmer group (see [11] for details). We note that the Selmer rank of an elliptic curve E is smaller than the upper bound of the rank of E given by them.

The outline of this paper is as follows: In Section 2, we review on the method of the rank one attack. In Section 3, we define the Selmer rank of an elliptic curve over $\mathbb{Q}$ and investigate the success probability of the rank one attack by calculating the Selmer rank of lifted elliptic curves. In Section 4, we conclude our study.

2. Review of the Rank One Attack

Cheon et al. in [2] proposed an algorithm to solve the ECDLP on prime fields, which is very efficient if we could lift two points to an elliptic curve over $\mathbb{Q}$ with rank one. We note that the rank of an elliptic curve E over $\mathbb{Q}$ is the non-negative integer r satisfying

$$E(\mathbb{Q}) \simeq E_{\mathrm{tors}}(\mathbb{Q}) \times \mathbb{Z}^r,$$

where $E_{\mathrm{tors}}(\mathbb{Q})$ is the torsion subgroup (see [11]). We here call their method the *rank one attack*. In this section, we shall review on the rank one attack.

2.1. Mathematical Foundations

Let E be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

By making a change of variables

$$z = -\frac{x}{y} \text{ and } w = -\frac{1}{y} \left(\Leftrightarrow x = \frac{z}{w} \text{ and } y = -\frac{1}{w}\right),$$

we see that the Weierstrass equation becomes

$$w = z^3 + a_1zw + a_2z^2w + a_4zw^2 + a_6w^3. \tag{1}$$

We note that z is an uniformizier at $(z, w) = (0, 0)$. By substituting the equation (1) into itself recursively, we can express w as a power series in z. Using the power series w in z, we find *Laurent series* for x and y as follows:

$$\begin{aligned} x(z) &= \frac{z}{w} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3z - (a_4 + a_1a_3)z^2 + \cdots \\ y(z) &= -\frac{1}{w} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1a_3)z + \cdots . \end{aligned}$$

The pair $(x(z), y(z))$ provides a "formal solution" to the Weierstrass equation (1). Similarly, the invariant differential $\omega \in H^0(E, \Omega_E)$ has the Laurent series

$$\begin{aligned} \omega(z) &= \frac{dx}{2y + a_1x + a_3} \\ &= (1 + a_1z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + 2a_3)z^3 \\ &\quad + (a_1^4 + 3a_1^2a_2 + 6a_1a_3 + a_2^2 + 2a_4)z^4 + \cdots)dz. \end{aligned} \tag{2}$$

Let q be a prime number and let E be an elliptic curve defined over the q-adic field $\mathbb{Q}_q$ given by a Weierstrass equation (1) with coefficients in $\mathbb{Z}_q$. The *q-adic elliptic logarithm* of E is given by

$$\begin{aligned} \log_E(z) &= \int \omega(z)dz \\ &= z + \frac{a_1}{2}z^2 + \frac{a_1^2 + a_2}{3}z^3 + \cdots \in \mathbb{Q}_q[[z]]. \end{aligned}$$

Reducing the coefficients of E modulo q, we obtain a curve $\widetilde{E}$ over $\mathbb{F}_q$. For simplicity, we assume that $\widetilde{E}$ is an elliptic curve. Let $\pi : E(\mathbb{Q}_q) \to \widetilde{E}(\mathbb{F}_q)$ be

the reduction map (see [11, Chapter VII] for its definition). Let $E_1(\mathbb{Q}_q)$ be the subgroup of $E(\mathbb{Q}_p)$ defined by $\ker \pi$. The map

$$\log_E : E_1(\mathbb{Q}_q) \to q\mathbb{Z}_q, \quad (x, y) \mapsto \log_E(z)$$

is a group homomorphism, where $q\mathbb{Z}_q$ is the subgroup of the additive group $\mathbb{Z}_q$ and $z = -\frac{x}{y}$.

2.2. The Rank One Attack

We consider the ECDLP on prime fields as follows: Given an elliptic curve $\widetilde{E}$ over $\mathbb{F}_p$ for a prime number p, a point $\widetilde{S} \in \widetilde{E}(\mathbb{F}_p)$, and a point $\widetilde{T} \in \widetilde{E}(\mathbb{F}_p)$ with $\widetilde{T} \in \langle \widetilde{S} \rangle$, find the integer d such that $\widetilde{T} = d\widetilde{S}$. For simplicity, we assume that the point $\widetilde{S}$ has a large prime order q and $\widetilde{E}(\mathbb{F}_p) = \langle \widetilde{S} \rangle$. We note that $d \bmod q$ is uniformly determined.

Fix a lifted elliptic curve E over $\mathbb{Q}$ of $\widetilde{E}$. Let h_q denote the map $h_q : E(\mathbb{Q}_q) \to E_1(\mathbb{Q}_q)$ given by the multiplication by q. For any lifting map $u : \widetilde{E}(\mathbb{F}_p) \to E(\mathbb{Q})$, we consider a composition of the following maps:

$$\begin{aligned} \lambda_{E,q} : \widetilde{E}(\mathbb{F}_p) \quad &\xrightarrow{u} \quad E(\mathbb{Q}) \xrightarrow{[N_{\mathrm{tors}}]} E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_q) \xrightarrow{h_q} E_1(\mathbb{Q}_q) \\ &\xrightarrow{\log_E} \quad q\mathbb{Z}_q \xrightarrow{\bmod q^2} q\mathbb{Z}_q/q^2\mathbb{Z}_q \simeq \mathbb{F}_q^+, \end{aligned}$$

where $[N_{\mathrm{tors}}]$ denotes the multiplication by the order N_{tors} of the torsion subgroup of $E(\mathbb{Q})$ and $\mathbb{F}_q^+$ denotes the additive group of $\mathbb{F}_q$. We show the following result (cf. [2, Theorem 2]):

Theorem 1. *Let d be the integer with $\widetilde{T} = d\widetilde{S}$. Suppose that the rank of E is equal to one and the number N_{tors} is not divided by the prime q. Assume that $\lambda_{E,q}(\widetilde{S}) \not\equiv 0 \bmod q$. Then we have*

$$d \equiv \lambda_{E,q}(\widetilde{T}) \cdot \lambda_{E,q}(\widetilde{S})^{-1} \bmod q.$$

Proof. Since the rank of E is equal to one, we can fix a generator $P \in E(\mathbb{Q})$ for the free part of the group $E(\mathbb{Q})$. Set $S = u(\widetilde{S}), T = u(\widetilde{T}) \in E(\mathbb{Q})$. There exist an integer a and $R \in E_{\mathrm{tors}}(\mathbb{Q})$ such that $S = aP + R$. Since $\lambda_{E,q}(\widetilde{S}) \not\equiv 0 \bmod q$, we have $a \not\equiv 0 \bmod q$. Then we have

$$aT = bS + R'$$

for some $b \in \mathbb{Z}$ and $R' \in E_{\mathrm{tors}}(\mathbb{Q})$. Since the map $[N_{\mathrm{tors}}]$ satisfies that $[N_{\mathrm{tors}}](R'') = 0 \in E(\mathbb{Q})$ for any $R'' \in E_{\mathrm{tors}}(\mathbb{Q})$, we have

$$[N_{\mathrm{tors}}](aT) = [N_{\mathrm{tors}}](bS).$$

Therefore we have

$$a \cdot \lambda_{E,q}(\widetilde{T}) \equiv b \cdot \lambda_{E,q}(\widetilde{S}) \bmod q$$

Since the reduction map π is a group homomorphism, we have $N_{\mathrm{tors}}(a\widetilde{S} - b\widetilde{T}) = 0$ in the group $\widetilde{E}(\mathbb{F}_p)$. By the assumption, we have $a\widetilde{T} = b\widetilde{S} \in \widetilde{E}(\mathbb{F}_p)$. Therefore we have

$$d \equiv b \cdot a^{-1} \equiv \lambda_{E,q}(\widetilde{T}) \cdot \lambda_{E,q}(\widetilde{S})^{-1} \bmod q.$$

This completes the proof. □

If the rank of the lifted elliptic curve E is equal to one, we can reduce the ECDLP on $\mathbb{F}_p$ to the discrete logarithm problem (DLP) for the group $\mathbb{F}_q^+$ by Theorem 1. This is the method of the rank one attack.

Remark. Mazur's well-known result [11, Chapter VIII, Theorem 7.5] says that $N_{\mathrm{tors}} \leq 16$. Therefore it follows that the number N_{tors} is not divided by the primes $q \geq 17$.

Remark. We shall review here on the anomalous attack (see [9] for details). Let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_p$. Fix an elliptic curve E which is a lifting of $\widetilde{E}$ to $\mathbb{Q}_p$. For any lifting map $u : \widetilde{E}(\mathbb{F}_p) \to E(\mathbb{Q}_p)$, let λ_E be a composition of the following maps

$$\lambda_E : \widetilde{E}(\mathbb{F}_p) \overset{u}{\to} E(\mathbb{Q}_p) \overset{[N_p]}{\to} E_1(\mathbb{Q}_p) \overset{\log_E}{\to} p\mathbb{Z}_p \overset{\bmod p^2}{\to} p\mathbb{Z}_p/p^2\mathbb{Z}_p \simeq \mathbb{F}_p^+,$$

where $[N_p]$ denotes the multiplication by $N_p = \sharp\widetilde{E}(\mathbb{F}_p)$. Satoh and Araki showed that λ_E is a group homomorphism independent of the choice of u if $\widetilde{E}$ is anomalous (i.e. $N_p = p$) [9, Theorem 3.2]. Then we can reduce the ECDLP on $\mathbb{F}_p$ to the DLP on $\mathbb{F}_p^+$ if $\widetilde{E}$ is anomalous. Therefore we see that the rank one attack is very similar to the anomalous attack.

3. Lifting Problem and the Selmer Rank

Let p be a prime number and let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_p$. Let $\widetilde{S} \in \widetilde{E}(\mathbb{F}_p)$ be a point of prime order q and let $\widetilde{T} \in \langle \widetilde{S} \rangle$. We consider the lifting problem $(\widetilde{E}, \widetilde{S}, \widetilde{T})$ to (E, S, T), where E is a lifted elliptic curve over $\mathbb{Q}$ of $\widetilde{E}$ and $S, T \in E(\mathbb{Q})$ are lifting points of $\widetilde{S}, \widetilde{T}$. If the rank of E is equal to one, we can solve the ECDLP on $\mathbb{F}_p$ by the rank one attack. To investigate the success probability of the rank one attack, we need to estimate the rank of lifted elliptic curves. However, in general, computing the rank of an elliptic

curve is very difficult. In this section, we define the Selmer rank of an elliptic curve and estimate the Selmer rank of lifted elliptic curves. We note that the Selmer rank means the upper bound of the rank given by the Selmer group (see [11] for details).

3.1. Upper Bounds of the Rank and the Selmer Rank

Cheon et al. in [2] used the following result on estimating the upper bound of an elliptic curve:

Theorem 2. *Let E be an elliptic curve given by a Weierstrass equation*

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

Let $w(x)$ denote the number of disinct primes dividing $x \in \mathbb{Z}$. Then we have

$$\operatorname{rank}(E) \leq w(b) + w(a^2 - 4b) - 1, \tag{3}$$

where $\operatorname{rank}(E)$ *denotes the rank of E.*

Here we introduce the *Selmer rank* on an upper bound of the rank of an elliptic curve. For $D \in \mathbb{Q}$, let E_D be an elliptic curve defined over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 + Dx.$$

Without loss of generality, we suppose that D is a fourth-power free integer and not divided by 4 (if necessary, we consider the dual curve E_{-4D}). Let $\varphi : E_D \to E_{-4D}$ be the isogeny of degree 2 defined by

$$(x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(D - x^2)}{x^2}\right)$$

and φ' the dual isogeny of φ. Let

$$S = M_{\mathbb{Q}}^{\infty} \cup \{\text{primes dividing } 2D\}$$

and let $\mathbb{Q}(S, 2)$ be the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ given by

$$\{b \in \mathbb{Q}^*/\mathbb{Q}^{*2} \mid \operatorname{ord}_v(b) \equiv 0 \pmod 2 \text{ for all } v \notin S\},$$

where ord_v is the normalized valuation at v. Consider the following commutative diagram:

$$\begin{array}{ccc} E_{-4D}(\mathbb{Q})/\varphi(E_D(\mathbb{Q})) & \xrightarrow{\delta} & \mathbb{Q}(S,2) \\ \downarrow & & \downarrow{\scriptstyle \prod_{p\in S} \mathrm{res}_p} \\ \prod_{p\in S} E_{-4D}(\mathbb{Q}_p)/\varphi(E_D(\mathbb{Q}_p)) & \xrightarrow[\prod_{p\in S}\delta_p]{} & \prod_{p\in S} \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}, \end{array}$$

where δ and δ_p are connecting homomorphisms (see [11] for details). Similarly, we denote by δ'_p the connecting homomorphism $E_D(\mathbb{Q}_p)/\varphi'(E_{-4D}(\mathbb{Q}_p)) \to \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. From the definition of the Selmer group, we have the following definition:

$$\begin{cases} S^{(\varphi)}(E_D) = \cap_{p\in S}\mathrm{res}_p^{-1}(\mathrm{Im}(\delta_p)), \\ S^{(\varphi')}(E_D) = \cap_{p\in S}\mathrm{res}_p^{-1}(\mathrm{Im}(\delta'_p)). \end{cases}$$

Then we have the formula

$$\mathrm{rank}(E_D) \leq \dim_{\mathbb{F}_2} S^{(\varphi)}(E_D) + \dim_{\mathbb{F}_2} S^{(\varphi')}(E_D) - 2.$$

We call the value of the right hand side the *Selmer rank*. It is well-known that we have the following:

$$\mathrm{rank}(E) \leq (\text{the Selmer rank of } E) \leq (\text{the right hand side of (3)}).$$

The Selmer group is defined as the intersection of all images of connecting homomorphisms. In the case $p = \infty$, it holds that

$$\begin{cases} D > 0 & \Rightarrow \mathrm{Im}(\delta'_\infty) = \{1\}, \mathrm{Im}(\delta_\infty) = \{\pm 1\}. \\ D < 0 & \Rightarrow \mathrm{Im}(\delta'_\infty) = \{\pm 1\}, \mathrm{Im}(\delta_\infty) = \{1\}. \end{cases}$$

The following results give the images of the connecting homomorphisms δ'_p and δ_p for the bad primes of E_D (see [4] for details). We denote by $\langle c_1, \cdots, c_n\rangle$ the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ or $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ for some $p \in S$ generated by $c_1, \cdots, c_n \in \mathbb{Q}$, and u represents a non-square element modulo p. Note that $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, u, p, pu\}$ for an odd prime p, and $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \{\pm 1, \pm 5, \pm 2, \pm 10\}$.

Proposition 3. *Let p be an odd prime dividing D, and $\mathrm{ord}_p(D) = a$, $D = p^a D'$. Then the images $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$ are obtained as follows:*

1. *If $a = 1$ or 3, then $\mathrm{Im}(\delta'_p) = \langle D\rangle$, $\mathrm{Im}(\delta_p) = \langle -D\rangle$.*
2. *Suppose that $a = 2$ and $p \equiv 1 \pmod 4$.*
   - (a) *If S is a p-adic square, then*
     - i. $(-D')^{(p-1)/4} \equiv 1 \pmod p \Rightarrow \mathrm{Im}(\delta'_p) = \langle p\rangle$, $\mathrm{Im}(\delta_p) = \langle p\rangle$,
     - ii. $(-D')^{(p-1)/4} \equiv -1 \pmod p \Rightarrow \delta'_{\mathrm{p}} = \langle pu\rangle$, $\mathrm{Im}(\delta_p) = \langle pu\rangle$.
   - (b) *If D is a p-adic non-square, then $\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^*\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, $\mathrm{Im}(\delta_p) = \mathbb{Z}_p^*\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.*
3. *Suppose that $a = 2$ and $p \equiv 3 \pmod 4$.*

(a) *If D is a p-adic square, then* $\mathrm{Im}(\delta'_p) = \{1\}$, $\mathrm{Im}(\delta_p) = \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.
(b) *If D is a p-adic non-square, then* $\mathrm{Im}(\delta'_p) = \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, $\mathrm{Im}(\delta_p) = \{1\}$.

Note that $(-D')^{(p-1)/4} \equiv 1 \pmod{p}$ if and only if $-D'$ is a quadratic residue modulo p.

Proposition 4. *The images of* $\mathrm{Im}(\delta'_2)$ *and* $\mathrm{Im}(\delta_2)$ *are obtained as follows:*

1. *If* $D \equiv 1 \pmod 8$, *then* $\mathrm{Im}(\delta'_2) = \{1\}, \mathrm{Im}(\delta_2) = \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$.
2. *If* $D \equiv 5 \pmod 8$, *then* $\mathrm{Im}(\delta'_2) = \langle 5\rangle, \mathrm{Im}(\delta_2) = \mathbb{Z}_2^*\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$.
3. *If* $D \equiv 3 \pmod{16}$, *then* $\mathrm{Im}(\delta'_2) = \langle -5\rangle, \mathrm{Im}(\delta_2) = \langle -2, 5\rangle$.
4. *If* $D \equiv 7, 11 \pmod{16}$, *then* $\mathrm{Im}(\delta'_2) = \mathbb{Z}_2^*\mathbb{Q}_2^{*2}/\mathbb{Q}_2^{*2}, \mathrm{Im}(\delta_2) = \langle 5\rangle$.
5. *If* $D \equiv 15 \pmod{16}$, *then* $\mathrm{Im}(\delta'_2) = \langle -1\rangle, \mathrm{Im}(\delta_2) = \langle 2, 5\rangle$.
6. *If D is even, then* $\mathrm{Im}(\delta_2) = \langle -D\rangle$ *and* $\mathrm{Im}(\delta'_2)$ *is given by the following theorem.*

Theorem 5. *Let $p \in S$ and $(,)_p$ be the Hilbert symbol. For a subgroup $V \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, we define $V^\perp = \{x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \mid (x, y)_p = 1$ for all $y \in V\}$. Then it holds that* $\mathrm{Im}(\delta_p) = \mathrm{Im}(\delta'_p)^\perp$.

3.2. Analysis of the Rank One Attack

Let p be a prime number and let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_p$. Let $\widetilde{S} \in \widetilde{E}(\mathbb{F}_p)$ be a point of prime order q and let $\widetilde{T} \in \langle \widetilde{S}\rangle$. Here we construct a lifting (E, S, T) of $(\widetilde{E}, \widetilde{S}, \widetilde{T})$ and estimate the Selmer rank of E, where E is a lifted elliptic curve over $\mathbb{Q}$ and $S, T \in E(\mathbb{Q})$ are lifting points of $\widetilde{S}, \widetilde{T}$.

3.2.1. A Construction of Lifted Elliptic Curves

If E is given by an equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$, then the *quadratic twist* of E by a non-zero rational number D is the elliptic curve $E^{(D)}$ given by the equation

$$E^{(D)} : Dy^2 = x^3 + ax + b.$$

To make the change of the variables $(x, y) \mapsto (Dx, D^2y)$, we can rewrite this curve in the form

$$E^{(D)} : y^2 = x^3 + aD^2x + bD^3.$$

Algorithm 1 Lifting to a quadratic twist elliptic curve

Input: $(\widetilde{E}, \widetilde{S}, \widetilde{T})$, where $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$ given by the equation $y^2 = x^3 + ax \bmod p$ and $\widetilde{S} = (x_1, y_1), \widetilde{T} = (x_2, y_2)$ are points of $\widetilde{E}$.

Output: (E, S, T), a lifting of $(\widetilde{E}, \widetilde{S}, \widetilde{T})$ such that E is a quadratic twist elliptic curve.

1: Choose $X_i, Y_i \in \mathbb{Z}$ $(i = 1, 2)$ such that $X_i \equiv x_i, Y_i \equiv y_i \pmod p$ and $|\det C|$ is small, where $C = \begin{pmatrix} Y_1^2 & X_1 \\ Y_2^2 & X_2 \end{pmatrix}$. Set $B = \begin{pmatrix} Y_1^2 & X_1^3 & X_1 \\ Y_2^2 & X_2^3 & X_2 \end{pmatrix}$.

2: For $s \in \mathbb{Z}$ with $s \equiv a \pmod p$, let $\mathbf{u}_s = \begin{pmatrix} -1 \\ 1 \\ s \end{pmatrix}$. Choose an integer s with $s \equiv a \pmod p$ such that the equation

$$C \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \mathbf{v}_s \tag{4}$$

has integral solutions, where $\mathbf{v}_s$ is the vector satisfying $B\mathbf{u}_s = p\mathbf{v}_s$. If it has no integral solutions, return to step 1.

3: Let $(u_1, u_2) = (B_1, B_2)$ be an integral solution to the equation (4). Let $D = 1 + pB_1, A = s - pB_2$. Set $S = (X_1, Y_1), T = (X_2, Y_2)$ and let E be a quadratic twist elliptic curve given by the equation

$$Dy^2 = x^3 + Ax.$$

Then (E, S, T) is a lifting of $(\widetilde{E}, \widetilde{S}, \widetilde{T})$ such that E is a quadratic twist elliptic curve.

For any $(\widetilde{E}, \widetilde{S}, \widetilde{T})$ with $\widetilde{E} : y^2 = x^3 + ax$, we can lift $(\widetilde{E}, \widetilde{S}, \widetilde{T})$ to (E, S, T) such that E is a quadratic twist elliptic curve, using the method of Xedni-calculus [12]. We give an algorithm in Algorithm 1.

Remark. In step 1 of the Algorithm 1, we choose $X_i, Y_i \in \mathbb{Z}$ $(i = 1, 2)$ such that $|\det(C)|$ is small so that the equation (4) has integral solutions.

Example. Set $p = 229$ and let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_p$ given by the equation $y^2 = x^3 + 73x \bmod p$. Set $\widetilde{S} = (56, 54), \widetilde{T} = (53, 71) = 29\widetilde{S} \in \widetilde{E}(\mathbb{F}_p)$. We see that the order of $\widetilde{S}$ is $q = 113$. In the notation of Algorithm 1, let $X_1 = 56 + pm, Y_1 = 54, X_2 = 53 + pn, Y_2 = 71$ for integers m, n. Then we have $\det(C) = (-5041m + 2916n)p - 127748$. Taking $m = -623286, n = -1077498$,

we have $\det(C) = 34$. For $s = 73$, the equation $C \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \mathbf{v}_s$ has an integral solution (u_1, u_2) with

$$\begin{cases} u_1 = & -183247799202102610928669093068, \\ u_2 = & -374372209953166563273 4732. \end{cases}$$

Therefore we have

$$\begin{cases} D = & -419637460172814979026652223 12571, \\ A = & 857312360792751429899050478. \end{cases}$$

Let E be an elliptic curve defined by the equation $Dy^2 = x^3 + Ax$. The elliptic curve E has rational points $S = (X_1, Y_1), T = (X_2, Y_2)$. Making the change of variables $(x, y) \mapsto (Dx, D^2y)$, we can rewrite this curve in the form

$$E : y^2 = x^3 + AD^2x \tag{5}$$

and we have $S = (DX_1, D^2Y_1), T = (DX_2, D^2Y_2) \in E(\mathbb{Q})$. Note that (E, S, T) is lifting of $(\widetilde{E}, \widetilde{S}, \widetilde{T})$. By [11, Chap. 7, Remark 1.1], the Weierstrass equation given by (5) is minimal at the prime q. Considering S, T as the elements of the group $E(\mathbb{Q}_q)$, we can write

$$\begin{aligned} S &= (5 + 66q + 42q^2 + O(q^3), 92 + 77q + 87q^2 + O(q^3)), \\ T &= (8 + 68q + 26q^2 + O(q^3), 54 + 83q + 102q^2 + O(q^3)). \end{aligned}$$

By [11, Chap. 10, Prop. 6.1], we see $\sharp E_{\mathrm{tors}}(\mathbb{Q}) = 2$. Therefore we can compute

$$\lambda_{E,q}(T) \cdot \lambda_{E,q}(S)^{-1} \equiv 96 \pmod{q}.$$

However we have $\widetilde{T} \neq 96\widetilde{S}$, which implies that the rank of E is not equal to 1 by Theorem 1.

3.2.2. The Selmer Rank of Lifted Elliptic Curves

We investigate the upper bound of the rank of lifted elliptic curves by computing the Selmer rank. Let p be a prime number and let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_p$. Fix a point $\widetilde{S} \in \widetilde{E}(\mathbb{F}_p)$ of prime oder q. For randomly chosen points $\widetilde{T} \in \langle \widetilde{S} \rangle$, we consider liftings (E, S, T) of $(\widetilde{E}, \widetilde{S}, \widetilde{T})$ by Algorithm 1 and compute the Selmer rank of E. In the following tables, we list the number of lifted elliptic curves E with given Selmer rank.

1. Let $p = 229, \widetilde{E} : y^2 = x^3 + 73x \bmod p$ and $\widetilde{S} = (56, 54)$ as in Example 1. We note that the order of $\widetilde{S}$ is $q = 113$. As shown in Table 1, we have that the average of the Selmer rank of lifted elliptic curves is equal to 5.8.

Selmer rank	1	2	3	4	5	6	7	8	9	10
$\sharp E$	0	0	1	2	8	2	3	4	0	0

Table 1: $p = 229,\ \widetilde{E} : y^2 = x^3 + 73x \bmod p,\ \widetilde{S} = (56, 54)$

2. Let $p = 233, \widetilde{E} : y^2 = x^3 + 43x \bmod p$ and $\widetilde{S} = (38, 179)$. We note that the order of $\widetilde{S}$ is $q = 109$. As shown in Table 2, we have that the average of the Selmer rank of lifted elliptic curves is equal to 5.9.

Selmer rank	1	2	3	4	5	6	7	8	9	10
$\sharp E$	0	0	2	2	3	8	2	1	2	0

Table 2: $p = 233,\ \widetilde{E} : y^2 = x^3 + 43x \bmod p, \widetilde{S} = (38, 179)$

3. Let $p = 557, \widetilde{E} : y^2 = x^3 + 228x \bmod p$ and $\widetilde{S} = (155, 499)$. We note that the order of $\widetilde{S}$ is $q = 293$. As shown in Table 3, we have that the average of the Selmer rank of lifted elliptic curves is equal to 6.2.

Selmer rank	1	2	3	4	5	6	7	8	9	10
$\sharp E$	0	0	3	5	10	12	8	7	4	1

Table 3: $p = 557,\ \widetilde{E} : y^2 = x^3 + 228x \bmod p,\ \widetilde{S} = (155, 499)$

4. Let $p = 577, \widetilde{E} : y^2 = x^3 + 20x \bmod p$ and $\widetilde{S} = (155, 493)$. We note that the order of $\widetilde{S}$ is $q = 313$. As shown in Table 4, we have that the average of the Selmer rank of lifted elliptic curves is equal to 6.6.

5. Let $p = 1049, \widetilde{E} : y^2 = x^3 + 207x \bmod p$ and $\widetilde{S} = (312, 962)$. We note that the order of $\widetilde{S}$ is $q = 557$. As shown in Table 5, we have that the average of the Selmer rank of lifted elliptic curves is equal to 6.5.

6. Let $p = 1021, \widetilde{E} : y^2 = x^3 + 723x \bmod p$ and $\widetilde{S} = (156, 951)$. We note that the order of $\widetilde{S}$ is $q = 541$. As shown in Table 6, we have that the average of the Selmer rank of lifted elliptic curves is equal to 7.1.

REMARK. As shown in the above tables, we have that the average of the Selmer rank of lifted elliptic curves is about 6. Moreover, we can not construct

Selmer rank	1	2	3	4	5	6	7	8	9	10
$\sharp E$	0	1	3	2	7	10	11	7	8	1

Table 4: $p = 577,\ \widetilde{E} : y^2 = x^3 + 20x \bmod p, \widetilde{S} = (155, 493)$

Selmer rank	1	2	3	4	5	6	7	8	9	10
$\sharp E$	0	0	1	4	5	13	15	10	2	0

Table 5: $p = 1049,\ \widetilde{E} : y^2 = x^3 + 207x \bmod p,\ \widetilde{S} = (312, 962)$

lifted elliptic curves with rank one by our method even if the size of p is very small.

4. Conclusion

Cheon et al. in [2] proposed an algorithm to solve the ECDLP on prime fields, which is very efficient if we could lift two points to an elliptic curve defined over $\mathbb{Q}$ with rank one. We call their method the rank one attack. In this paper, we briefly explain the method of the rank one attack and show that the average of the Selmer rank of lifted elliptic curves by Xedni-calculus is about 6 when the size of p is very small. Thus we see that lifted elliptic curves E have $\mathrm{rank}(E) \approx 3$ if we assume that the Selmer rank is twice as the rank. The Selmer rank of lifted elliptic curves would become large when the size of p becomes large. Therefore we conclude that the rank one attack would be inefficient if we could not find a method of constructing a good lifting.

References

[1] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press (1999).

[2] J.H. Cheon, D.H. Lee, S.G. Hahn, S. Chee, Elliptic curve discrete logarithms and wieferich primes, *Technical report of IEICE*, ISEC, **99**, No. 584, 53-60.

[3] P. Gaudry, Some remarks on the elliptic curve discrete logarithm, available at http://www.loria.fr/ gaudry/publis/liftDL.ps.gz (2003).

Selmer rank	1	2	3	4	5	6	7	8	9	10	11
$\sharp E$	0	0	1	2	10	6	8	11	7	4	1

Table 6: $p = 1021,\ \widetilde{E} : y^2 = x^3 + 723x \bmod p,\ \widetilde{S} = (156, 951)$

[4] T. Goto, A note on the Selmer group of the elliptic curve $y^2 = x^3 + Dx$, *Proc. Japan Acad., Ser. A*, **77** (2001).

[5] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer Professional Computing (2004).

[6] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, **48** (1987), 203-209.

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

[8] V.S. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology CRYPTO '85, LNCS*, **218** (1986), 417-426.

[9] T. Satoh, K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *Comm. Math. Univ Sancti Pauli*, **47** (1998), 81-92.

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

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. Springer-Verlag, Berlin-Heidelberg-New York (1986).

[12] J. H. Silverman, The Xedni calculus and the elliptic discrete logarithm problem, *Designs, Codes and Cryptography*, **20** (2000), 5-40.

[13] N.P. Smart, The discrete logarithm problem on elliptic curves of trace one, *J. Crypto.*, **12** (1999), 110-125.

206