On Partial Lifting and the Elliptic Curve Discrete Logarithm Problem

Qi Cheng[1] * and Ming-Deh Huang[2] **

[1] School of Computer Science
The University of Oklahoma
Norman, OK 73019, USA.
Email: qcheng@cs.ou.edu.
[2] Computer Science Department
University of Southern California
Los Angeles, CA 90089
Email: huang@cs.usc.edu.

Abstract. It has been suggested that a major obstacle in finding an index calculus attack on the elliptic curve discrete logarithm problem lies in the difficulty of lifting points from elliptic curves over finite fields to global fields. We explore the possibility of circumventing the problem of explicitly lifting points by investigating whether partial information about the lifting would be sufficient for solving the elliptic curve discrete logarithm problem. Along this line, we show that the elliptic curve discrete logarithm problem can be reduced to three partial lifting problems. Our reductions run in random polynomial time assuming certain conjectures, which are based on some well-known and widely accepted conjectures concerning the expected ranks of elliptic curves over the rationals. Should the elliptic curve discrete logarithm problem admit no subexponential time attack, then our results suggest that gaining partial information about lifting would be at least as hard.
Keyword: Elliptic curve cryptosystem, discrete logarithm, partial lifting.

1 Introduction

The discrete logarithm problem over elliptic curves is a natural analog of the discrete logarithm problem over finite fields. It is the basis of elliptic curve cryptosystems proposed independently by Koblitz and Miller [11, 17]. Steady progress has been made in constructing better and more sophisticated, albeit subexponential time algorithms for the discrete logarithm problem over finite fields. In contrast, no subexponential attacks have been found for the elliptic curve discrete logarithm problem except in very special cases [14, 27, 18, 20]. See also [4, 5, 15, 16]. Consequently elliptic curve cryptosystems have attracted considerable

* This research is supported in part by NSF career award CCR-0237845.
** This research is supported in part by NSF grant CCR-0306393

attention, especially in cryptographic applications where key length needs to be kept to the minimal.

Most subexponential algorithms for discrete logarithms over finite fields have been based on the *index calculus* method (see [19] for a survey). This method involves lifting elements from a finite field to a global field to take advantage of the arithmetic structures in the global field. The lifting of elements is simple and straightforward. For example in the case of a finite prime field $\mathbf{F}_p$, an element $a \bmod p \in \mathbf{F}_p$ with $0 < a < p$ is simply lifted to $a \in \mathbf{Z}$. However extending this method to the elliptic curve discrete logarithm problem seems to be difficult. It has been suggested [17] that a major obstacle in finding an index calculus attack on the elliptic curve discrete logarithm problem lies in the difficulty of lifting points from elliptic curves over finite fields to global fields. The reason behind such difficulty is that elliptic curves over $\mathbf{Q}$ usually have very small rank – at least heuristically and practically speaking. As a result rational points with reasonably bounded heights are severely limited in number, rendering the lifting problem difficult. (See the next section for an illustration, and [8, 9, 25] for more in-depth discussion).

In this paper we explore the possibility of circumventing the problem of explicitly lifting points by investigating whether partial information about the lifting would be sufficient for solving the elliptic curve discrete logarithm problem. We show that the elliptic curve discrete logarithm problem can be reduced to three partial lifting problems. These partial lifting problems have the same basic setup as the explicit lifting problem, namely, an elliptic curve $E/\mathbf{F}_p$, a nonzero point $S \in E(\mathbf{F}_p)$, an elliptic curve $\mathcal{E}/\mathbf{Q}$ having E as its good reduction modulo p, and $X \in \mathcal{E}(\mathbf{Q})$ which reduces to S modulo p. Moreover we assume that $E(\mathbf{F}_p)$ is cyclic of prime order, so that every point in $E(\mathbf{F}_p)$ is liftable to $\mathcal{E}(\mathbf{Q})$. For the first partial lifting problem, we are given $T \in E(\mathbf{F}_p)$, a height bound $h \in \mathbf{Q}$, and the goal is to decide whether T can be lifted to a point in $\mathcal{E}(\mathbf{Q})$ of height bounded by h. We call this problem the *height decision problem.* Note that if the height bound h is around p, it may take exponential time just to write down a lift of T. However in the height decision problem all that we ask is whether such a lift exists or not. For the second partial lifting problem, we are given $T \in E(\mathbf{F}_p)$ and a prime r, and the goal is to find the reduction modulo r of any lift of T to $\mathcal{E}(\mathbf{Q})$. We call this problem the *shifting prime problem.* Note that a lift of T can again be large, but its reduction modulo r has length $O(\log r)$. For the third partial lifting problem, we are given $T \in E(\mathbf{F}_p)$, and the goal is to construct a straight-line program of any lift of T to $\mathcal{E}(\mathbf{Q})$. We call this problem the *straight-line description problem.* (As will be observed in the next section that a small straight-line description of a lift of T usually does exist.)

Our reductions run in random polynomial time assuming a conjecture which in turn is based on some widely accepted conjectures concerning the expected ranks of elliptic curves over the rationals. They are stated explicitly in the next section. Our results lead to the following open question: can partial information on lifting as described above be extracted in subexponential time? An affirmative answer will lead to a subexponential algorithm for the the elliptic curve discrete

logarithm problem. On the other hand, should the elliptic curve discrete logarithm problem admit no subexponential time attack, then our results suggest that gaining partial information about lifting would be at least as hard.

2 Statements of results

An elliptic curve is a smooth cubic algebraic curve. Let k be a field. An elliptic curve over k can be given as an equation of the form:

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

where $a_i \in k$, $1 \leq i \leq 6$. Denote by $E(k)$ the set of points $(x, y) \in k^2$ that satisfy this equation, along with a point O at infinity. If the characteristic of k is neither 2 nor 3, we may assume that the elliptic curve is given by an equation of the form

$$y^2 = x^3 + ax + b, \qquad a, b \in k$$

The discriminant of this curve is defined as the discriminant of polynomial $x^3 + ax + b$, which is $-4a^3 - 27b^2$. The curve is smooth iff its discriminant is not zero.

The set $E(k)$ forms an additive group. It is isomorphic to $T \times \mathbf{Z}^r$, where T is the finite torsion group, and r is the rank of the group. A lot of theoretical and experimental evidence shows that most elliptic curves would have as small a rank as allowed by the sign of their functional equations [1, 2, 21]. In particular most elliptic curves over the rationals with a rational point of infinite order are expected to be either of rank 1 or 2. Parts of our proofs are based on such a heuristic assumption. An explicit statement of the assumption sufficient for our purposes is given below.

Conjecture 1. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbf{Z}/(n)$. Let P be a point on the E all of whose coordinates are in $(\mathbf{Z}/(n))^*$ and let $X = (x_0, y_0)$ be the natural lift of P to $\mathbf{Z}$. Consider the family of curves over $\mathbf{Z}$

$$\mathcal{F}(E, X) = \{\mathcal{E}(\alpha, \beta) || \alpha |, |\beta| \leq 3n^3, \mathcal{E} \text{ passes } X \text{ and } \mathcal{E} \text{ reduces to } \ E \text{ modulo } n\}$$

where $\mathcal{E}(\alpha, \beta)$ is defined by the equation $y^2 = x^3 + \alpha x + \beta$. Then for sufficiently large n, a random curve in the family has rank 1 with probability greater than some constant.

In light of the general heuristic assumption [1, 2, 21], it would be actually reasonable to expect that a random curve in $\mathcal{F}(E, X)$ has rank 1 with probability around 1/2, and rank 2 with probability around 1/2.

How do we sample a random curve in the family? To do this, we choose a random integer $i < n$ and set $\alpha = a + in$, then set $\beta = y_0^2 - x_0^3 - \alpha x_0$. It is easy to see that $\mathcal{E}$ passes through X. Moreover one can show that a substantial fraction of integers i satisfies $\gcd(\alpha, y_0^2 - x_0^3) = 1$ and $\gcd(\alpha, \beta) = 1$ if $a, b \in (\mathbf{Z}/(n))^*$.

Let $S, T \in E(k)$ be two points on the curve. The discrete logarithm of T with base S is an integer m such that $T = mS$, if such an m exists. Now to

illustrate the difficulty of lifting points, let us consider an elliptic curve $E/\mathbf{F}_p$ with a nonzero point $S \in E(\mathbf{F}_p)$ which generates a cyclic group $< S >$ of large prime order r. It is not difficult to construct an elliptic curve $\mathcal{E}/\mathbf{Q}$ with E as its reduction at p, and $X \in \mathcal{E}(\mathbf{Q})$ which reduces to S modulo p. In practical terms $\mathcal{E}(\mathbf{Q})$ would most likely be of rank one or two. For simplicity suppose it is of rank one. Now suppose we want to lift a point T in the group $< S >$ to a point in $\mathcal{E}(\mathbf{Q})$. Suppose $\mathcal{E}(\mathbf{Q})$ has trivial torsion part and, to our advantage, X is a generator of $\mathcal{E}(\mathbf{Q})$. Then for $m < r$, mX is the lift of $T = mS$ of minimum possible canonical height. However $\hat{h}(mX) = m^2\hat{h}(X)$, which is $\Omega(p^2)$ in the worst case. Here $\hat{h}$ denotes the canonical height function. Therefore it is infeasible even to write down the coordinates of the lifting points of T.

$$\begin{array}{ccc} Y = m\ X & \in \mathcal{E}(\mathbf{Q}) \\ \Uparrow & \Uparrow \\ T = m\ S & \in E(\mathbf{F}_p) \end{array}$$

On the other hand, though the coordinates of Y are huge they actually have very short straight-line program (see definition in Section 5) essentially because multiplication of a point by m can be performed in $O(\log m)$ additions of points. So instead of trying to lift points explicitly we consider three partial lifting problems whose formal definitions are given below together with theorems concerning their relation to the elliptic curve discrete logarithm problem.

The height decision problem:

Input: p, E, $\mathcal{E}$, T and h where p is a prime, $E/\mathbf{F}_p$ is an elliptic curve such that $E(\mathbf{F}_p)$ is cyclic of prime order, $\mathcal{E}/\mathbf{Q}$ is an elliptic curve having E as its good reduction modulo p, $T \in E(\mathbf{F}_p)$ and $h \in \mathbf{Q}$ (a height bound).

Output: "Yes" if T can be lifted to a point in $\mathcal{E}(\mathbf{Q})$ of (naive) height bounded by h, and "no" otherwise.

Theorem 1. *Assuming Conjecture 1, then there is a random polynomial time reduction from the elliptic curve discrete logarithm problem to the height decision problem.*

A result similar to Theorem 1 was obtained by Gjosteen [6] where the naive height was replaced by the canonical height, and the height decisional problem was replaced by the problem of computing the minimal canonical height for the lifting. Gjosteen's result dose not depend on any conjecture on ranks of elliptic curves. However it requires that a set of generators be given explicitly for the group of rational points of the target elliptic curve.

The shifting prime problem:

Input: p, r, $\mathcal{E}$ and T where p and r are prime numbers, $\mathcal{E}/\mathbf{Q}$ is an elliptic curve, T is a point on E_1 where E_1 is the reduction of $\mathcal{E}$ modulo p.

Output: A point $R \in \mathbf{P}^2(\mathbf{F}_r)$ which is the reduction of $Y \in \mathcal{E}(\mathbf{Q})$ modulo r, where Y is any lift of P to $\mathbf{Q}$. Here we use $\mathbf{P}^2$ to denote the 2-dimensional projective space.

Theorem 2. *Assuming Conjecture 1, then there is a random polynomial time reduction from the elliptic curve discrete logarithm problem to the shifting prime problem.*

The straight-line description problem:

Input: p, r, $\mathcal{E}$ and T where p is a prime number, $\mathcal{E}/\mathbf{Q}$ is an elliptic curve, T is a point on E_1 where E_1 is the reduction of $\mathcal{E}$ modulo p.

Output: Straight-line programs of length polynomial in the size of input for the projective coordinates of any lift of T on $\mathcal{E}$.

Theorem 3. *Assuming Conjecture 1, then there is a random polynomial time reduction from the elliptic curve discrete logarithm problem to the straight-line description problem.*

It is easy to see that if we can solve the discrete logarithm problem on elliptic curves, we can solve the shifting prime problem and the straight-line description problem. Hence the shifting prime problem and the straight-line description problem are equivalent to the discrete logarithm problem on elliptic curves. However, it is unclear whether the height decision problem is equivalent to the discrete logarithm problem on elliptic curves.

3 Reduction to the height decision problem

In this section, we prove Theorem 1 by demonstrating a random polynomial time reduction from the elliptic curve discrete logarithm problem to the height decision problem.

Suppose for the rest of this section that p is a prime larger than 3 and E is an elliptic curve defined over $\mathbf{F}_p$ given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{F}_p$, $E(\mathbf{F}_p)$ is cyclic of prime order r, and $S, T \in E(\mathbf{F}_p)$. In the discrete logarithm problem we are to find m so that $T = mS$ on $E(\mathbf{F}_p)$.

First we observe that if p is sufficiently large, then any lift $\mathcal{E}$ of E with good reduction cannot have any nontrivial rational torsion point. Indeed by a result of Mazur [12, 13], we know that $\mathcal{E}(\mathbf{Q})$ has at most 16 torsion points. Since the torsion subgroup injects into $E(\mathbf{F}_p)$ and since the order of $E(\mathbf{F}_p)$ is prime, it follows that the torsion part of $\mathcal{E}(\mathbf{Q})$ must be trivial. From now on we assume that p is large enough.

Let $X = (x_0, y_0)$ be the natural lift of S to $\mathbf{Z}$.

In the first step of our reduction we construct a lift of E to some $\mathcal{E}/\mathbf{Q}$ passing through X, given by $y^2 = x^3 + \alpha x + \beta$ with $\alpha, \beta \in \mathbf{Z}$, and $(\alpha, \beta) = 1$. It follows from the results in [22–24] that one can compute $h_0 \in \mathbf{Q}$ in time polynomial in $\log p$ so that $|\hat{h}(X) - h_0| < \frac{1}{r^2}$.

Since $X \in \mathcal{E}(\mathbf{Q})$ is non-torsion, $\mathcal{E}(\mathbf{Q})$ is of rank at least one. Moreover the reduction map from $\mathcal{E}(\mathbf{Q})$ to $E(\mathbf{F}_p)$ is surjective, since $S = X \bmod p$ and $E(\mathbf{F}_p)$ is cyclic of prime order. Therefore every point in $E(\mathbf{F}_p)$ has a lift to $\mathcal{E}(\mathbf{Q})$. In particular, T has a lift of the form mX.

Suppose $\mathcal{E}(\mathbf{Q})$ is of rank one and G is a generator of $\mathcal{E}(\mathbf{Q})$. (We will not actually compute the rank nor a generator.) Then $X = lG$ for some $l \in \mathbf{Z}$, and if $nG \bmod p = T$ $(n < r)$, lT has a lift nX. From l and n, the discrete logarithm problem is solved, since upon reduction we get $lT = nS$.

Since $X = lG$, $\hat{h}(X) = l^2\hat{h}(G)$. Now by construction, $\hat{h}(X) = (\log p)^{O(1)}$. On the other hand, by [7, 3], $\hat{h}(G) > c(\log \Delta)^{-O(1)}$ where c is an absolute constant and Δ is the minimum discriminant of $\mathcal{E}$. It follows that $l = (\log p)^{O(1)}$.

Again by the result in [22–24], we have $|h(Y) - 2\hat{h}(Y)| < c$ for $Y \in \mathcal{E}(\mathbf{Q})$, where c is a constant independent of Y and $\mathcal{E}$. In particular for positive integers $i < r$,

$$|h(iX) - 2i^2h_0| \leq |h(iX) - 2\hat{h}(iX)| + |2\hat{h}(iX) - 2i^2h_0| < c + 2.$$

Set $c' = c+2$.Then it follows that if $h(nX) < 2i^2h_0$, then $n \leq i+c'$. This implies that using a binary search technique beginning with the query asking if lT is liftable to a point of height no greater than $2r^2h_0$, we can determine n within $O(1)$ in $O(\log p)$ queries.

Consequently, for the constructed lift $\mathcal{E}$ and each value of l up to $(\log p)^{O(1)}$, we will attempt to find an $n < r$ so that lT has a lift to $\mathcal{E}(\mathbf{Q})$ of the form nX. When we succeed to find such n for an l, we then verify if $lT = nS$ and if so, the discrete logarithm is solved. If we fail for all possible values of l, then it must be the case that the rank of $\mathcal{E}(\mathbf{Q})$ is greater than one. In that case we construct another random lift and apply the same procedure all over again. By our heuristic assumption, a randomly constructed $\mathcal{E}(\mathbf{Q})$ has rank one with probability about $1/2$, thus we expect to succeed in several trials with probability arbitrarily close to 1. Hence Theorem 1 follows.

4 The shifting prime problem.

In this section, we show that the shifting prime problem is equivalent to the discrete logarithm problem on elliptic curves. The main idea in the proof is to lift an elliptic curve $E/\mathbf{F}_p$ to an elliptic curve $\mathcal{E}/\mathbf{Q}$ of rank one with additive reduction modulo r, where r is the prime order of $E(\mathbf{F}_p)$. We demonstrate that, with the help of an oracle for the shifting prime problem, the discrete logarithm problem on $E(\mathbf{F}_p)$ can be shifted over to the group of nonsingular $\mathbf{F}_r$-points on $\mathcal{E} \bmod r$, which is isomorphic to the addition group of $\mathbf{F}_r$, and the corresponding discrete logarithm problem is easy to solve.

First we review some facts about additive reduction. Let $\mathcal{E}(\mathbf{Q}) : y^2 = x^3 + ax + b$, $a, b \in \mathbf{Z}$, be an elliptic curve over $\mathbf{Q}$. It is possible that when modulo some prime r, the reduction curve $E/\mathbf{F}_r$ is not smooth anymore. If E has a cusp, we say that E is an additive reduction of $\mathcal{E}$ at r.

Let $E^{(ns)}$ be the set of non-singular points on E, we can define "addition" on $E^{(ns)}$ in very much the same way as in the smooth case [26]. Moreover,

$$E^{(ns)}(\mathbf{F}_r) \cong \mathbf{F}_r$$

by sending (x, y) to $\frac{x}{y}$ and the infinity point to 0. (Note that since (x, y) is not a singular point, $y \neq 0$.) Hence the discrete logarithm problem on $E^{(ns)}(\mathbf{F}_r)$ is easy to solve.

For example, if $\mathcal{E}$ is defined by

$$y^2 = x^3 + ax + b$$

where $a, b \in \mathbf{Z}$. $r \neq 2, 3$. $\mathcal{E}$ has additive reduction at p if and only if $r|a$ and $r|b$.

Let $\mathcal{E}(\mathbf{Q})$ be an elliptic curve with rank 1 and with no rational torsion point other than O, and let G be the generator for $\mathcal{E}(\mathbf{Q})$. Let $E_1/\mathbf{F}_p$ be the reduction of $\mathcal{E}$ modulo p. Suppose the order of $E_1(\mathbf{F}_p)$ is a prime r. Moreover suppose $\mathcal{E}$ has additive reduction modulo r, and let $E_2/\mathbf{F}_r$ be the resulting curve. Let G_1 and G_2 be the reduction of G on E_1 and E_2 respectively. Moreover suppose that G_1 and G_2 are neither points at infinity nor singular. It follows that all the points on $\mathcal{E}(\mathbf{Q})$ reduce to smooth points on E_1 and E_2. Let $E_2^{(ns)}$ denote the set of non-singular points on the curve E_2. Then $\mathcal{E}(\mathbf{Q}) \to E_1(\mathbf{F}_p)$ and $\mathcal{E}(\mathbf{Q}) \to E_2^{(ns)}(\mathbf{F}_r)$ are group homomorphisms.

$$\begin{array}{ccc} & \mathcal{E}(\mathbf{Q}) & \\ \swarrow & & \searrow \\ E_1(\mathbf{F}_p) & \xrightarrow{\psi} & E_2^{(ns)}(\mathbf{F}_r) \end{array}$$

Since $E_1(\mathbf{F}_p)$ and $E_2^{(ns)}(\mathbf{F}_r)$ have same order, there is a well-defined isomorphism ψ between $E_1(\mathbf{F}_p)$ and $E_2^{(ns)}(\mathbf{F}_r)$ determined by

$$\psi(iG_1) = iG_2.$$

Suppose $T, S \in E(\mathbf{F}_p)$, $T = mS$ and we want to find m. Certainly $\psi(T) = m\psi(S)$. If we can solve the shifting prime problem efficiently, we will get $\psi(T), \psi(S)$. Hence we have reduced the discrete logarithm problem in $E_1(\mathbf{F}_p)$ to the discrete logarithm problem in $E_2^{(ns)}(\mathbf{F}_r)$. Since E_2 is an additive reduction of $\mathcal{E}$, the discrete logarithm on E_2 is simply division in finite fields.

Suppose $E_1 : y^2 = x^3 + ax + b$ is an elliptic curve over F_p with r points. S and T are the input points for the discrete logarithm. Assume that $r > 3$ is a prime. The reduction algorithm is as follows:

Algorithm 1 *1. Let $E_2 : y^2 = x^3$ over F_r.*

2. *Combine E_1 and E_2 to construct an elliptic curve E_3 over ring $\mathbf{Z}/(pr)$ using Chinese Remaindering.*
3. *Lift curve E_3 to a random curve $\mathcal{E}$ over $\mathbf{Q}$, passing a point X, where X is natural lift of S' on E_3, which reduces to S on E_1. (We may assume that S' does not reduce to O on E_2.)*
4. *Query the shifting prime problem for S and T with input prime r.*
5. *If the output points are S' and T', we solve the discrete logarithm of T' base S' on E_2. Let the result be m'.*
6. *Check whether $T = m'S$. If yes, output m' and terminate the algorithm. Otherwise, go back to step 3.*

Step 2 can be done very efficiently. By Conjecture 1 we expect the curve constructed in step 3 to be of rank one with reasonable probability. With the same probability, we will get the correct discrete logarithm of T, once the shifting prime problem is solved. Thus Algorithm 1 reduces the elliptic curve discrete logarithm problem to the shifting prime problem in random polynomial time, and Theorem 2 follows.

As in the previous reduction, we note that the reduction here is a Turing reduction. Since discrete logarithm is easily to check for correctness, there is no need to verify if the lifting curve is of rank one.

5 Straight-line program for the lifting points.

In this section, we will derive theorem 3 from theorem 2. Straight-line programs are widely used for representing integers and polynomials, see [10] for an example. We first give a formal definition of a straight-line program.

Definition 1. *A straight-line program for an integer m (integers $m_1, m_2, \cdots, m_n$) is a sequence of assignments*

$$z \leftarrow x \alpha y$$

where z is a symbol never appeared before. $\alpha \in \{*, +, -\}$ and x, y are two previously appeared symbols or 1, such that after we run the program, the last symbol (the last n symbols) stores the value m ($m_1, m_2, \cdots, m_n$).

In some cases, a straight-line program is a compact description of a integer. It can represent a huge number in small length. For example, m^n has a straight-line program of length $(\log mn)^{O(1)}$. It is an important open problem whether $n!$ has a short straight-line program.

It seems hard to compute with straight-line programs. For example, given straight-line programs for the integers x and y, it is not a trivial problem to decide whether $x = y$. However, from a straight-line program of integer i, we can read out the reduction of i modulo any prime p, by performing every step of the straight-line program modulo p. Similarly, if we have the straight-line program for the coordinates of a global point $P = (x : y : z) \in \mathbf{P}^2(\mathbf{Q})$, we usually can calculate the reduction of P at p for any given prime p.

However, there is some subtlety here. Let x, y, z be the integers output by a straight-line program. If $p \nmid \gcd(x, y, z)$, we can compute the reduction of $(x : y : z)$ at p efficiently. If x, y, z share a lot of p's, after executing the straight-line program modulo p(or p^i for i small), we get the point $(0 : 0 : 0)$, which is not well-defined in the projective space. This motivates us to define *properly reduced* coordinates. Without lose of generality, let $\mathcal{E}/\mathbf{Q}$ be an elliptic curve of rank one with no rational torsion point other than O.

Definition 2. *Let x', y', z' be three integers, where $(x' : y' : z') = m(x : y : z) \in \mathcal{E}(\mathbf{Q})$ and $(x : y : z)$ is the generator of Mordell-Weil group of $\mathcal{E}(\mathbf{Q})$. If $p \nmid z'$, whenever the order of $(x : y : z)$ modulo p is greater than m, we call x', y', z' the* **properly reduced** *coordinates.*

Let E be the reduction of $\mathcal{E}$ at p. Assume that every point on E is liftable to $\mathcal{E}$. Let P, r be the remaining input of shifting prime problem. Given an algorithm which can solve the straight-line description problem with properly reduced output, we can lift P to X, which is represented by a straight-line program of length polynomial in the size of the input. Then making use of the fact that the output of the straight-line program is properly reduced, we can compute X modulo r for any prime r, hence provide answers to the shifting prime queries. This means that we have reduction from shifting prime problem to straight-line description problem. Thus Theorem 3 follows from theorem 2.

The proof of Theorem 3 raises the question of the existence of a "short" straight-line program for properly reduced coordinates of a point on the elliptic curve. We give an affirmative answer to this question.

Proposition 1. *Given $m, x, y, z, a, b \in \mathbf{Z}$ where $\gcd(x, y, z) = 1$ and $(x : y : z)$ is a point on the elliptic curve $\mathcal{E}$ defined by $y^2 = x^3 + ax + b$, we can write a straight-line program for properly reduced coordinates $x', y', z' \in \mathbf{Z}$ in length $\log^{O(1)}(|xyz| + |m| + |a| + |b|)$, where $(x' : y' : z') = m(x : y : z) \in \mathcal{E}(\mathbf{Q})$.*

Proof: First, we consider the explicit formulas for addition of two points and for doubling a point.

Let $(x_1 : y_1 : z_1)$ and $(x_2 : y_2 : z_2)$ be two points on an elliptic curve $\mathcal{E} : y^2 = x^3 + ax + b$, $x_1, y_2, z_1, x_2, y_2, z_2 \in \mathbf{Z}$. Assume that $\gcd(x_1, y_1, z_1) = \gcd(x_2, y_2, z_2) = 1$. If $x_1 z_2 \neq x_2 z_1$, then according to the addition law on elliptic curves, $(x_1 : y_1 : z_1) + (x_2 : y_2 : z_2) = (x_3 : y_3 : z_3)$, where

$$\begin{aligned} x_3 &= z_1 z_2 (y_2 z_1 - y_1 z_2)^2 (x_2 z_1 - x_1 z_2) - (x_1 z_2 + x_2 z_1)(x_2 z_1 - x_1 z_2)^3 \\ y_3 &= (y_2 z_1 - y_1 z_2)(z_1 z_2 (y_2 z_1 - y_1 z_2)^2 - (x_1 z_2 + x_2 z_1)(x_2 z_1 - x_1 z_2)^2) \\ &\quad - z_1 z_2 (y_1 x_2 - y_2 x_1)(x_2 z_1 - x_1 z_2)^2 \\ z_3 &= z_1 z_2 (x_2 z_1 - x_1 z_2)^3 \end{aligned}$$

From the formula we conclude

Lemma 1. *$p \neq 2, 3$. If $(x_1 : y_1 : z_1)$ and $(x_2 : y_2 : z_2)$ are not the infinite point and $(x_1 : y_1 : z_1) \not\equiv -(x_2 : y_2 : z_2) \bmod p$, then $p \nmid z_3$.*

If $(x_1 : y_1 : z_1) = (x_2 : y_2 : z_2)$ and $y_1 z_1 \neq 0$, then

$$\begin{aligned} x_3 &= 2y_1 z_1(3x_1^2 + az_1^2) - 16x_1 y_1^3 z_1^2 \\ y_3 &= -(3x_1^2 + az_1^2)((3x_1^2 + az_1^2) - 8x_1 y_1^2 z_1) - 4y_1^2 z_1(x_1^3 + ax_1 z_1^2 + 2bz_1^3) \\ z_3 &= 8y_1^3 z_1^3 \end{aligned}$$

From the formula we conclude

Lemma 2. *$p \neq 2, 3$. If (x_1, y_1, z_1) is not a torsion point of order 2 modulo p nor O modulo p, then $p \nmid z_3$.*

Write m in binary $\sum_{i=1}^{a} 2^{e_i}$, $0 \leq e_1 < e_2 < \cdots < e_a$, then

$$m(x : y : z) = \sum_{i=1}^{a} 2^{e_i}(x : y : z).$$

When we apply the squaring technique to write straight-line program for $m(x : y : z)$, we first use the doubling formula to compute $2^{e_1}(x : y : z)$, $2^{e_2}(x : y : z)$,$\cdots$, $2^{e_a}(x : y : z)$. Then we use formula for addition of two different points to sum them up. It is not possible that some of the intermediate points will be equal, as long as $(x : y : z)$ is not a torsion point. This concludes the proof of proposition 1.

Let $\mathcal{E}/\mathbf{Q} : y^2 = x^3 + ax + b$, $a, b \in \mathbf{Z}$, be an elliptic curve with rank 1. Every liftable point on its reduction curve has a short straight-line program. More precisely, we have

Corollary 1. *let E be the reduction of $\mathcal{E}$ modulo prime p. If $Q \in E/\mathbf{F}_p$ is liftable to $\mathcal{E}(\mathbf{Q})$, then it can be lifted to some $X \in \mathcal{E}(\mathbf{Q})$ which has a properly reduced straight-line program of length $\log^{O(1)}(|a| + |b| + |p|)$.*

References

1. A. Brumer. The average rank of elliptic curves I. *Invent. Math.*, 109:445–472, 1992.
2. J.E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, 1992.
3. Sinnou David. Points de petite hauteur sur les courbes elliptiques. *J. Number Theory*, 64(1):104–129, 1997.
4. G. Frey. Applications of arithmetical geometry to cryptographic constructions. In *Proceedings of the Fifth International Conference on Finite Fields and Applications*. Springer-Verlag, 2001.
5. P. Gaudry, F. Hess, and N. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. of Cryptology*, 15:19–46, 2002.
6. Kristian Gjosteen. A minimal canonical height lifting algorithm. Preprint, 2003.
7. M. Hindry and J. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93:419–450, 1988.
8. Ming-Deh Huang, Ka Lam Kueh, and Ki-Seng Tan. Lifting elliptic curves and solving the elliptic curve discrete logarithm problem. In *ANTS*, volume 1838 of *Lecture Notes in Computer Science*. Springer-Verlag, 2000.

9. M.J. Jacobson, N. Koblitz, J.H. Silverman, A. Stein, and E. Teske. Analysis of the xedni calculus attack. *Design, Codes and Cryptography*, 20:41–64, 2000.
10. E. Kaltofen. Greatest common divisors of polynomials given by straight-line programs. *J. of ACM*, 35(1):231–264, 1988.
11. N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.
12. B. Mazur. Modular curves and the eisenstein ideal. *IHES publi. Math.*, 47, 1977.
13. B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44, 1978.
14. A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to a finite field. *IEEE Trans. Inform. Theory*, 39:1639–1646, 1993.
15. A. Menezes and M. Qu. Analysis of the Weil descent attack of Gaudry, Hess and Smart. In *CT-RSA*, volume 2020 of *Lecture Notes in Computer Science*, 2001.
16. A. Menezes, E. Teske, and A. Weng. Weak fields for ECC. In *CT-RSA*, volume 2964 of *Lecture Notes in Computer Science*, pages 366–386, 2004.
17. V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology: Proceedings of Crypto'85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer-Verlag, 1985.
18. T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comm. Math. Univ. Sancti. Pauli*, 47:81–92, 1998.
19. O. Schirokauer, D. Weber, and Th. Denny. Discrete logarithms: The effectiveness of the index calculus method. In *ANTS II*, volume 1122 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.
20. I. A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comp.*, 67:353–356, 1998.
21. Alice Silverberg. Open questions in arithmetic algebraic geometry. In *Arithmetic Algebraic Geometry(Park City, UT, 1999)*, volume 9 of *Institute for Advanced Study/Park City Mathematics Series*, pages 83–142. American Mathematical Society, 2001.
22. J.H. Silverman. Computing heights on elliptic curves. *Mathematics of Computation*, 51, 1988.
23. J.H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Mathematics of Computation*, 55, 1990.
24. J.H. Silverman. Computing canonical heights with little(or no) factorization. *Mathematics of Computation*, 66, 1997.
25. J.H. Silverman and J. Suzuki. Elliptic curve discrete logarithms and the index calculus. In *Advances in Cryptology-Asiacrypt'98*, pages 110–125. Springer-Verlag, 1998.
26. Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 1986.
27. N.P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. of cryptology*, 12:193–196, 1999.