The Four Faces of Lifting for the Elliptic Curve Discrete Logarithm Problem

Joseph H. Silverman

Brown University

11th Workshop on Elliptic Curve Cryptography
Shannon Institute, Dublin, Ireland

September 5–7, 2007

The Elliptic Curve Discrete Logarithm Problem

Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$ and let $S, T \in E(\mathbb{F}_p)$. The (in)famous

Elliptic Curve Discrete Logarithm Problem

(ECDLP) is the problem of finding an integer m satisfying

$$T = mS.$$

There have been many methods proposed for solving the ECDLP, and in some special cases there are fast (subexponential) algorithms, but for general curves and points, the best known algorithms are slow (exponential), and indeed have running time $O(\sqrt{p}\,)$.

The Discrete Logarithm Problem Over $\mathbb{F}_p^*$

Before the introduction of elliptic curves into cryptography, Diffie and Hellman suggested using the discrete logarithm problem in $\mathbb{F}_p^*$ as an underlying had problem.

The **Index Calculus** is a fast algorithm to solve the DLP in $\mathbb{F}_p^*$. The simple idea underlying the Index Calculus is to lift the problem from $\mathbb{F}_p^*$ to $\mathbb{Z}$, solve the problem in $\mathbb{Z}$, and then reduce the solution modulo p.

Of course, there's more to the Index Calculus than that. In particular, a crucial property of $\mathbb{Q}$ that makes it work is the fact that $\mathbb{Q}^*$ has a comparatively large number of small generators (primes).

Thus in order to solve $\beta = \alpha^m$ in $\mathbb{F}_p$, one lifts many choices of α^i and $\beta\alpha^j$ modulo p to $\mathbb{Z}$, finds instances where the lifts are smooth (products of small primes), eliminates the primes to get a relation among the lifts, and then reduces modulo p.

The Four Faces of Lifting ECDLP

It is tempting to try a similar lifting procedure to solve the ECDLP, and many people have tried to do this in various ways. None have been successful, but it seems worthwhile to take stock of the methods that have been tried and to fit them into a general framework.

Further, I feel that it is quite instructive to compare not only the different methods, but also to study the reasons why each one seems to fail to work.

It turns out that there are four quite distinct ways to try to lift the ECDLP. None of them succeeds, but each appears to fail for a different reason. My aim in this talk is to survey these

Four Faces of Lifting ECDLP,

explain their similarities and differences, and describe the distinct roadblocks that arise.

The Elliptic Curve Lifting Problem

Let $E/\mathbb{F}_p$ and $S, T \in E(\mathbb{F}_p)$ be an ECDLP. The

Lifting Problem for $(\mathbb{F}_p, E, S, T)$

is the problem of finding the following quantities:

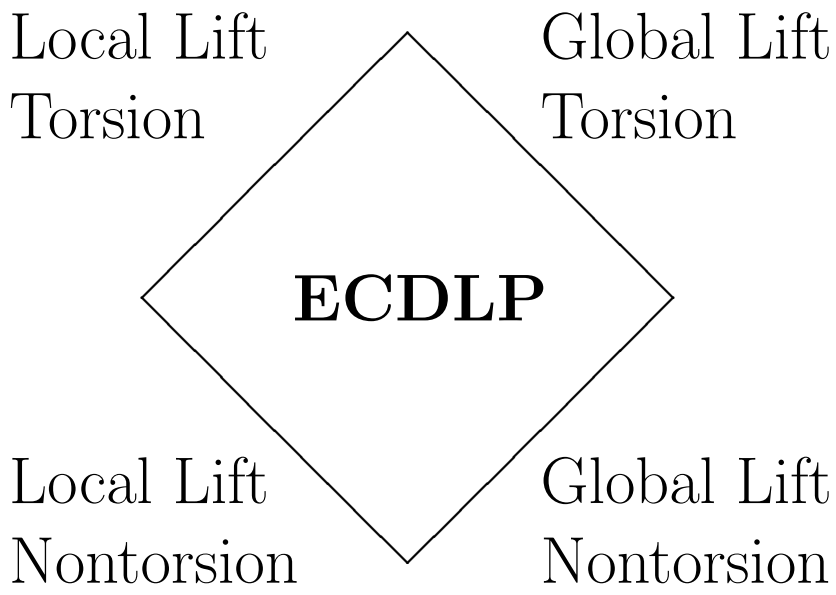
- A ring $\hat{R}$ contained in a field $\hat{K}$.
- An ideal $\mathfrak{p}$ of $\hat{R}$ with $\hat{R}/\mathfrak{p} = \mathbb{F}_p$.
- An elliptic curve $\hat{E}/\hat{K}$ satisfying $\hat{E} \equiv E \pmod{\mathfrak{p}}$.
- Points $\hat{S}, \hat{T} \in \hat{E}(\hat{K})$ satisfying

$$\hat{S} \equiv S \pmod{\mathfrak{p}} \qquad \text{and} \qquad \hat{T} \equiv T \pmod{\mathfrak{p}}.$$

The lifting problem has many variants. For example, the ring R may be a local ring (e.g., $\mathbb{Z}_p$, the ring of p-adic integers) or a global ring (e.g., $\mathbb{Z}$) and the lifted points $\hat{S}, \hat{T}$ may be torsion points or nontorsion points.

The Four Faces

Thus we may picture the ECDLP as a castle with four walls, under each of which is camped a "Lifting Army" having its own unique weaponary to use for an assault.



The remainder of this talk will be devoted to considering in turn each of these lifting scenarios.

Local Nontorsion Lifts

Local Nontorsion Lifts

We start by fixing a Weierstrass equation for $\hat{E}$ with integer coefficients whose reduction modulo p is the original curve.

The goal now is to lift a point $Q \in E(\mathbb{F}_p)$ to a p-adic point $\hat{Q} \in \hat{E}(\mathbb{Q}_p)$. This is accomplished via Hensel's Lemma.

The idea is to start with the point $Q = Q_1$ and first lift it to a point

$$Q_2 \text{ modulo } p^2,$$

and then lift that to a point

$$Q_3 \text{ modulo } p^3,$$

and so on.

We illustrate the procedure with an example.

Local Nontorsion Lifts — An Example

We take $p = 257$ and look at the curve and point

$$E : Y^2 = X^3 + 23X + 11 \pmod{p}, \qquad Q = (7, 1) \in E(\mathbb{F}_p).$$

In order to lift Q, we set

$$Q' = (7 + pu, 1 + pv),$$

substitute into the equation for E,

$$(1 + pv)^2 \equiv (7 + pu)^3 + 23(7 + pu) + 11 \pmod{p^2},$$

and solve for u and v. We find that u and v satisfy

$$v \equiv 85u + 1 \pmod{p}.$$

Hence for every $u \in \mathbb{Z}/p\mathbb{Z}$ we have lifted Q to

$$Q' = (7 + 257u, 258 + 21845u) \in E(\mathbb{Z}/p^2\mathbb{Z}).$$

The same process gives lifts modulo p^3, p^4, etc., and at each step we have p choices for the lift.

Solving the ECDLP Using Local Nontorsion Lifts

Let's try to solve the ECDLP for $S, T \in E(\mathbb{F}_p)$ using nontorsion lifts, where

$$T = mS \quad \text{in } E(\mathbb{F}_p).$$

Suppose that we can lift S and T to nontorsion points $\hat{S}, \hat{T} \in \hat{E}(\mathbb{Q}_p)$ while maintaining the relation

$$\hat{T} = m\hat{S}.$$

Multiplying by $N = \#E(\mathbb{F}_p)$, the points $N\hat{T}$ and $N\hat{S}$ are in the so-called *formal group of* $E(\mathbb{Q}_p)$, and the formal group has an easily computable logarithm function $\log_{\mathcal{F}}$.

Since we know $\hat{S}$ and $\hat{T}$ and N, we can compute

$$m = \frac{\log_{\mathcal{F}}(N\hat{T})}{\log_{\mathcal{F}}(N\hat{S})} \in \mathbb{Q}_p.$$

The Obstacle To Using Local Nontorsion Lifts

So what's the problem? As we have seen, it is easy to lift $S = S_1$ and $T = T_1$ to points S_2 and T_2 modulo p^2, and then to points S_3 and T_3 modulo p^3, and so on.

Indeed, it's so easy, we can actually compute p different choices for each of S_2 and T_2.

However, once we choose a particular S_2, then only one of the p possible choices for T_2 preserves the relation

$$T_2 = mS_2.$$

And as we continue making choices to compute lifts $\hat{S}$ and $\hat{T}$ in $\hat{E}(\mathbb{Q}_p)$, we only preserve the relation

$$\hat{T} = m\hat{S}$$

if, at each step, the lifts are chosen consistantly.

Unfortunately (or maybe I should say fortunately), there is no way known to make such consistant choices without already knowing the value of m.

Local Torsion Lifts

Local Torsion Lifts

Let $Q \in E(\mathbb{F}_p)$ be a point of order n (with $n \neq p$). We have seen that Q can be lifted to a p-adic point $\hat{Q} \in E(\mathbb{Q}_p)$ in many different ways.

However, one can show that there is a *unique* way to lift Q to a *point of order* n in $E(\mathbb{Q}_p)$. In other words, there is a unique point $\hat{Q} \in E(\mathbb{Q}_p)$ satisfying

$$n\hat{Q} = \hat{\mathcal{O}} \qquad \text{and} \qquad \hat{Q} \equiv Q \pmod{p}.$$

It is quite easy in practice to compute $\hat{Q}$. More precisely, we can calculate the lift Q_k mod p^k as long as we can work with integers of size p^k. We again illustrate with an example

Local Torsion Lifts — An Example

We continue with the prime $p = 257$, curve, and point

$$E : Y^2 = X^3 + 23X + 11 \qquad Q = (7, 1) \in E(\mathbb{F}_p).$$

The point Q has order $n = 83$, i.e., $83Q = \mathcal{O}$.

Recall that for every $u \in \mathbb{Z}/257\mathbb{Z}$, we found a lift

$$Q' = (7 + 257u, 258 + 85 \cdot 257u) \in E(\mathbb{Z}/257^2\mathbb{Z}).$$

We now impose the additional condition

$$83Q' \equiv \mathcal{O} \pmod{257^2}.$$

Treating u as an indeterminate, we can compute $83Q'$ modulo 257^2 using linear polynomials. We find that

$$83Q' \equiv \mathcal{O} \pmod{257^2} \iff u \equiv 18 \pmod{257}.$$

Hence $Q' = (4633, 63223) \in E(\mathbb{Z}/257^2\mathbb{Z})$ satisfies

$$Q' \equiv Q \pmod{257} \quad \text{and} \quad 83Q' \equiv \mathcal{O} \pmod{257^2}.$$

Solving ECDLP with Local Torsion Lifts

Let's make another attempt to solve the ECDLP for $S, T \in E(\mathbb{F}_p)$, this time using torsion lifts.

We lift S and T to points $\hat{S}$ and $\hat{T}$ of order n in $E(\mathbb{Q}_p)$ and observe that

$$\hat{T} - m\hat{S} \equiv T - mS \equiv \mathcal{O} \pmod{p}, \quad \text{and}$$
$$n(\hat{T} - m\hat{S}) = n\hat{T} - mn\hat{S} = \hat{\mathcal{O}}.$$

The uniqueness of the torsion lifts tells us that we still have the relation

$$\hat{T} = m\hat{S}.$$

Thus we are reduced to solving the ECDLP in $E(\mathbb{Q}_p)$.

(Un)fortunately, if we multiply the relation $\hat{T} = m\hat{S}$ by n to move it into the formal group, then we get $\hat{\mathcal{O}} = m\hat{\mathcal{O}}$. And no one knows an efficient way to solve the ECLDP in $E(\mathbb{Q}_p)$ without moving into the formal group.

Global Torsion Lifts

Global Torsion Lifts Over $\mathbb{Q}$

Suppose instead that we lift $S, T \in E(\mathbb{F}_p)$ to global torsion points

$$\hat{S}, \hat{T} \in \hat{E}(\mathbb{Q})_{\text{tors}}.$$

Then the relation $\hat{T} = m\hat{S}$ is maintained, and it is very easy to find m. For example, we could look at

$$\hat{T} \equiv m\hat{S} \pmod{q} \quad \text{for small primes } Q = 3, 5, 7, \ldots,$$

and use the Chinese Remainder Theorem to reconstruct m.

(Un)fortunately, this won't work, since $\hat{E}(\mathbb{Q})_{\text{tors}}$ tends to be small, and in general we have:

Theorem. (Mazur) For all elliptic curves $\hat{E}/\mathbb{Q}$,

$$\#\hat{E}(\mathbb{Q})_{\text{tors}} \leq 16.$$

Global Torsion Lifts Over Number Fields

There is no reason to restrict our attention to $\mathbb{Q}$. If we take a sufficiently large number field $K/\mathbb{Q}$, then we can always find points

$$\hat{S}, \hat{T} \in E(K)_{\text{tors}}$$

and a prime ideal $\mathfrak{p}$ of the ring of integers R_K so that

$$\hat{S} \equiv S \pmod{\mathfrak{p}} \quad \text{and} \quad \hat{T} \equiv T \pmod{\mathfrak{p}}.$$

Then solving $\hat{T} = m\hat{S}$ in $E(K)$ solves the ECLDP. To do this, we need to work in the field K. If $K/\mathbb{Q}$ has small degree, this is feasible. (Un)fortunately, we have:

Theorem. (Serre) Let $\hat{E}/\mathbb{Q}$ and let $T \in E(K)$ be a point of order n. Then generally one has

$$[K : \mathbb{Q}] \geq c\#\,\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \approx cn^4.$$

Global Nontorsion Lifts

Global Nontorsion Lifts

Continuing with our besieged castle imagery, the "Global Nontorsion Army" has two different pieces of artillary in its armory.

These two methods are:

- The **Easy Lifting Method**.
- The **Hard Lifting Method**.

In the *Easy Lifting Method*, we choose the lifted curve $\hat{E}$ and lifted points $\hat{Q}_1, \ldots, \hat{Q}_r \in \hat{E}(\mathbb{Q})$ simultaneously using some elementary method such as linear algebra.

In the *Hard Lifting Method*, we use an elementary method to lift the curve (and possibly one or more points). Then we attempt to lift one or more additional points that were not considered when constructing the original lift.

The Easy Lifting Method

Global Nontorsion Lifts — The Easy Lifting Method

If we treat the coefficients of the Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

as indeterminates, then we can substitute up to 5 points $(x_1, y_1), (x_2, y_2), \ldots$ and solve for the coefficients.

More generally, we can use linear algebra to force a cubic form $F(X, Y, Z)$ to go through 9 specified points.

For example, given a curve $E/\mathbb{F}_p$ and points $S, T \in E(\mathbb{F}_p)$, it is easy to find $\hat{E}/\mathbb{Q}$ and $\hat{S}, \hat{T} \in \hat{E}(\mathbb{Q})$ satisfying

$$\hat{E} \equiv E \pmod{p}, \quad \hat{S} \equiv S \pmod{p}, \quad \hat{T} \equiv T \pmod{p}.$$

If $\operatorname{rank} \hat{E}(\mathbb{Q}) = 1$, or more generally if $\hat{S}$ and $\hat{T}$ are dependent, then it is easy (using descent or canonical heights) to write $\hat{T} = m\hat{S}$. Reducing modulo p solves the ECDLP.

The Easy Lifting Method — An Example

We work with the curve and points

$$E : Y^2 = X^3 + 23X + 11 \quad \text{modulo } 257$$
$$S = (7, 1) \in E(\mathbb{F}_{257}) \quad \text{and} \quad T = (110, 15) \in E(\mathbb{F}_{257}).$$

We write a lift $\hat{E}$ as

$$\hat{E} : Y^2 = X^3 + (23 + 257\alpha)X + (11 + 257\beta).$$

Substituting in $S = (7, 1)$ and $T = (110, 15)$ yields two equations for α and β. Solving gives

$$\hat{E} : Y^2 = X^3 - \frac{1330433}{103}X + \frac{9277805}{103}$$
$$\hat{S} = (7, 1) \in \hat{E}(\mathbb{Q}) \quad \text{and} \quad \hat{T} = (110, 15) \in \hat{E}(\mathbb{Q}).$$

(Un)fortunately, the points $\hat{S}$ and $\hat{T}$ are linearly independent in $\hat{E}(\mathbb{Q})$, so we cannot use them to solve the ECDLP for S and T.

The Easy Lifting Method in General

In general, we can lift many random linear combinations

$$Q_i = a_i S - b_i T \quad \text{for } i = 1, 2, \ldots, r.$$

Note that if we can find any linear relationship

$$n_1 Q_1 + n_2 Q_2 + \cdots + n_r Q_r = \mathcal{O},$$

then we can probably solve the ECDLP using

$$(n_1 a_1 + \cdots + n_r a_r) S = (n_1 b_1 + \cdots + n_r b_r) T.$$

A general cubic form $F(X, Y, Z) = 0$ has 10 coefficients, so we can use linear algebra lift E and up to 9 points,

$$\hat{Q}_1, \hat{Q}_2, \ldots, \hat{Q}_9 \in \hat{E}(\mathbb{Q}).$$

If $\operatorname{rank} \hat{E}(\mathbb{Q}) \leq 8$, then we can use descent or height methods to find a linear relation among the Q_i and solve the ECDLP.

The Obstacle to the Easy Lifting Method

Theorem. (Masser) Let $\mathcal{E}_U$ be a parameterized family of elliptic curves, where $U = (U_1, \ldots, U_n)$, and let $Q_{1,U}, \ldots, Q_{r,U}$ be parameterized families of points that are linearly independent. Then

$$\{u \in \mathbb{Q}^n : Q_{1,u}, \ldots, Q_{r,u} \text{ are dependent in } \mathcal{E}_u(\mathbb{Q})\}$$

is a small set (set of density 0).

If we view the coefficients of the elliptic curve as being the parameters, then the precise statement of Masser's theorem suggests that the probability that lifted points are linearly dependent is less than $1/p$.

We might try choosing the lifted curve carefully to "encourage" it to have small rank (e.g., using a heuristic suggested by the Birch–Swinnerton-Dyer conjecture), but one can show that the lifted points still tend to be independent.

The Hard Lifting Method

Global Nontorsion Lifts — The Hard Lifting Method

In the Hard Lifting Method, we lift the curve E and (say) one point S to get a curve $\hat{E}/\mathbb{Q}$ and a point $\hat{S} \in \hat{E}(\mathbb{Q})$. There is a reasonably good chance that

$$\operatorname{rank} \hat{E}(\mathbb{Q}) = 1 \qquad \text{and} \qquad \hat{E}(\mathbb{Q}) \bmod p = E(\mathbb{F}_p).$$

In particular, there is a point $\hat{T} \in \hat{E}(\mathbb{Q})$ that is a lift of T, and $\hat{S}$ and $\hat{T}$ are linearly dependent. Note that if we can find $\hat{T}$, then it is easy (using descent or heights) to compute a relation

$$a\hat{T} = b\hat{S}.$$

Reducing modulo p gives a relation

$$aT = bS$$

in $E(\mathbb{F}_p)$ that generally solves the ECDLP for S and T.

The Hard Lifting Method — An Example

We work with the curve and points

$$E : Y^2 = X^3 + 23X + 11 \quad \text{modulo } 257$$
$$S = (7, 1) \in E(\mathbb{F}_{257}) \quad \text{and} \quad T = (140, 71) \in E(\mathbb{F}_{257}).$$

We lift E and S so that $\hat{S} \in \hat{E}(\mathbb{Q})$,

$$\hat{E} : Y^2 = X^3 + 23X - 503, \qquad S = (7, 1) \in \hat{E}(\mathbb{Q}).$$

The problem is how to lift T to $\hat{E}(\mathbb{Q})$. Even if we know that a lift exists, there is no known algorithm to find $\hat{T}$.

Here is the answer, which is not so easy to find!

$$\hat{T} = \left(\frac{6239431086988004986355 9}{8736078981416085105625}, \frac{4130665692373765369756729240437877}{8165350423947492616771476241718 75}\right).$$

And we are *lucky* that $\hat{T}$ is so uncomplicated(!), since it turns out that $\hat{T} = 5\hat{S}$. If instead, say, $T = 53S$, then the coordinates of $\hat{T}$ would have thousands of digits.

The Obstacle to the Hard Lifting Method

Suppose that we lift $E/\mathbb{F}_p$ and $S \in E(\mathbb{F}_p)$ to $\hat{E}/\mathbb{Q}$ and $\hat{S} \in \hat{E}(\mathbb{Q})$, and suppose that we know that there does exist a lift of T to $\hat{T} \in \hat{E}(\mathbb{Q})$.
We are searching for m satisfying $T = mS$, where in general $m = O(p)$. The lift will satisfy $\hat{T} = m\hat{S}$, so the theory of canonical heights tells us

$$\hat{h}(\hat{T}) = \hat{h}(m\hat{S}) = m^2\hat{h}(\hat{S}).$$

It takes $O\big(\hat{h}(\hat{T})\big)$ bits to write down the coordinates of $\hat{T}$, so we find that it takes $O(p^2)$ bits to even write down the point $\hat{T}$. This is infeasible for cryptographic size primes $p \approx 2^{160}$.
And even if we could solve this storage problem, there is no known way to find $\hat{T}$ without knowing m. (But might we "describe" $\hat{T}$ without writing it down explicitly? No one knows how!)

Summary

We have outlined four lifting methods for ECDLP:

Local-Nontorsion: Lift to nontorsion points in $\hat{E}(\mathbb{Q}_p)$

Fails because lose the relationship $\hat{T} = m\hat{S}$.

Local-Torsion: Lift to torsion points in $\hat{E}(\mathbb{Q}_p)_{\text{tors}}$

$\hat{T} = m\hat{S}$ true. Fails because cannot determine m.

Global-Torsion: Lift to points in $\hat{E}(\mathbb{Q})_{\text{tors}}$ or $\hat{E}(K)_{\text{tors}}$

Fails since $E(\mathbb{Q})_{\text{tors}}$ is too small, $[K : \mathbb{Q}]$ is too large.

Global-Nontorsion: Lift to nontorsion points in $\hat{E}(\mathbb{Q})$

Easy Lift Method:

Fails because lifted points are independent.

Hard Lift Method:

Fails because no method known to lift points.

Addendum on Function Fields

Question asked at the conference: What happens if rather than lifting to $\mathbb{Q}$ or a number field, we instead lift to a function field such as $\mathbb{F}_p(T)$?

Answer: The field $\mathbb{F}_p(T)$ and its finite extensions are also global fields, and its completions are local fields. There are thus lifting methods for function fields analogous to those for $\mathbb{Q}$ and its extensions; and each of the four function field lifting scenarios fails for essentially the same reasons as does its number field counterpart.

The Four Faces of Lifting for the Elliptic Curve Discrete Logarithm Problem

Joseph H. Silverman

Brown University

11th Workshop on Elliptic Curve Cryptography
Shannon Institute, Dublin, Ireland

September 5–7, 2007