Elliptic Curve Discrete Logarithms and the Index Calculus

Joseph H. Silverman (Brown University)
joint work with Joe Suzuki (Osaka University)
University of Waterloo, September 1998

Notation.

$\mathbb{F}_p$	a field with p elements (p prime).
E	an elliptic curve over $\mathbb{F}_p$, say given by a Weierstrass equation $$E : y^2 = x^3 + ax + b.$$
N_p	$= \#E(\mathbb{F}_p)$, the number of points on E.
S, T	two points in $E(\mathbb{F}_p)$.
m	$= m(S,T)$, an integer so that $S = mT$. We write $m = \log_T(S)$.

The *Elliptic Curve Discrete Logarithm Problem* (ECDLP) is the determination of the multiplier m from the data (p, E, S, T).

In the first part of this talk, I will discuss the possibility of an Index Calculus attack on the ECDLP.

$\boxed{\textbf{The Index Calculus for } \mathbb{F}_p^*}$

Let

$$\alpha \text{ and } \beta \text{ be non-zero elements of } \mathbb{F}_p.$$

The *Discrete Logarithm Problem* (DLP) for the multiplicative group $\mathbb{F}_p^*$ is to determine, from the data (p, α, β), the “multiplier” $m = m(\alpha, \beta)$ so that

$$\alpha = \beta^m \quad \text{in } \mathbb{F}_p^*.$$

We write $m = \log_\beta(\alpha)$.

The *Index Calculus* is a sub-exponential method for solving the DLP.

$\boxed{\textbf{The Index Calculus for } \mathbb{F}_p^*}$

Step 1. Choose a set of multiplicatively independent integers (usually the first r primes)

$$\Gamma = \{\pi_1, \pi_2, \ldots, \pi_r\}.$$

The set Γ is called the *factor basis*.

Step 2. Randomly choose exponents $e < p$, compute $\beta^e \bmod p$, and attempt to factor it as a product

$$\beta^e \bmod p = \pi_1^{m_1(e)} \pi_2^{m_2(e)} \cdots \pi_r^{m_r(e)}. \qquad (*)$$

Step 3. Repeat Step 2 to find r independent factorizations $(*)$, then solve the system of congruences

$$e_i \equiv m_1(e_i) \log_\beta(\pi_1) + \cdots + m_r(e_i) \log_\beta(\pi_r) \pmod{p-1}$$

for the quantities $\log_\beta(\pi_j)$.

Step 4. Randomly choose exponents $e < p$, compute $\alpha\beta^e \bmod p$, and attempt to factor it as a product

$$\alpha\beta^e \bmod p = \pi_1^{k_1} \pi_2^{k_2} \cdots \pi_r^{k_r}. \qquad (**)$$

When this is successful, the relation

$$\log_\beta(\alpha) + e \equiv k_1 \log_\beta(\pi_1) + \cdots + k_r \log_\beta(\pi_r) \pmod{p-1}$$

gives the value of $\log_\beta(\alpha)$.

Requirement: There are "a lot of" r-smooth numbers between 1 and p.

$\boxed{\textbf{The Index Calculus for the ECDLP}}$

Step 1. Lift $E/\mathbb{F}_p$ to an elliptic curve $\mathcal{E}/\mathbb{Q}$ and fix a set of independent points

$$\Gamma = \{P_1, P_2, \dots, P_r\} \in \mathcal{E}(\mathbb{Q}).$$

Step 2. Randomly choose integers $e < N_p$, compute $eT \in E(\mathbb{F}_p)$, lift eT to a point in $\mathcal{E}(\mathbb{Q})$, and attempt to write the lift as a linear combination

$$\operatorname{Lift}(eT) = m_1(e)P_1 + \cdots + m_r(e)P_r. \qquad (*)$$

Step 3. Repeat Step 2 to find r independent expressions $(*)$, then solve the system of congruences

$$e_i \equiv m_1(e_i)\log_T(P_1) + \cdots + m_r(e_i)\log_T(P_r) \pmod{N_p}$$

for the quantities $\log_T(P_j)$.

Step 4. Randomly choose exponents $e < N_p$, compute $S + eT \in E(\mathbb{F}_p)$, lift it to a point in $\mathcal{E}(\mathbb{Q})$, and attempt to write it as

$$\operatorname{Lift}(S + eT) = k_1P_1 + k_2P_2 + \cdots + k_rP_r. \qquad (**)$$

When this is successful, the relation

$$\log_T(S) + e \equiv k_1\log_T(P_1) + \cdots + k_r\log_T(P_r) \pmod{N_p}$$

gives the value of $\log_\beta(\alpha)$.

Requirement: There are "a lot of" linear combinations $m_1P_1 + \cdots + m_rP_r$.

The Index Calculus for the ECDLP

In his influential 1986 paper, Victor Miller gives two reasons why “it is extremely unlikely that an ‘index calculus’ attack on elliptic curves will ever be able to work.” Miller’s reasons may be summarized as follows:

(A) It is difficult to lift $E/\mathbb{F}_p$ to an elliptic curve $\mathcal{E}/\mathbb{Q}$ so that $\mathcal{E}(\mathbb{Q})$ has high rank and is generated by points of small height.

(B) Given an elliptic curve $\mathcal{E}/\mathbb{Q}$, a large prime p, and the reduction modulo p map,

$$\mathcal{E}(\mathbb{Q}) \to E(\mathbb{F}_p),$$

it is difficult to lift a point $Q \in E(\mathbb{F}_p)$ to a point of $\mathcal{E}(\mathbb{Q})$.

In his paper, Miller briefly gives some heuristic arguments supporting these contentions. Suzuki and I have made a more detailed analysis of the difficulties inherent in an index calculus approach to the ECDLP.

Summary of Our Results.

- Using a method of Mestre, it is possible to lift $E/\mathbb{F}_p$ to an elliptic curve $\mathcal{E}/\mathbb{Q}$ of (at least) moderately high rank possessing generators of moderately low height.
- Based on both theoretical and numerical evidence, if $P_1, \ldots, P_r$ are independent points in $\mathcal{E}(\mathbb{Q})$, then their (logarithmic) height will satisfy

$$\max h(P_i) \gg \max\{\log p, r \log r\}.$$

- By way of contrast, the generators (factor basis) $\pi_1, \ldots, \pi_r$ used for the DLP on $\mathbb{F}_p^*$ have (logarithmic) height

$$\max h(\pi_i) = \log r + O(\log\log r).$$

- The fact that a factor basis for the ECDLP is exponentially larger than a factor basis for the DLP makes the lifting problem for the ECDLP intractable.

Conclusion.

Index Calculus Methods cannot be used to efficiently solve the ECDLP.

$\boxed{\textbf{Mestre's Method for "High" Ranks}}$

Mestre (1986) gave the following method to produce curves of high rank:

(1) For each small prime $\ell \le L$, choose an elliptic curve
$$E_\ell : y^2 = x^3 + a_\ell x + b_\ell$$
so $\#E_\ell(\mathbb{F}_\ell) = \ell+1+\lfloor 2\sqrt{\ell}\rfloor$ is as large as possible.

(2) Use the Chinese Remainder Theorem to simultaneously lift the E_ℓ's to a curve $\mathcal{E}/\mathbb{Q}$ while (more-or-less) minimizing the discriminant $\Delta(\mathcal{E})$.

(3) Search for points $(x, y) \in \mathbb{Z}^2$ in $\mathcal{E}(\mathbb{Q})$ close to the 2-torsion point(s) of $\mathcal{E}$, and check how many of them are independent.

Using this method, Mestre produced many curves of elevated rank ($r = 8$, 9, 10) and one curve of rank 14. He also gave theoretical reasons, based on the Birch-Swinnerton-Dyer conjecture and an "explicit formula" (in the sense of Weil) for the success of his method. Assuming standard conjectures, he proved (for any $\mathcal{E}$) that
$$\operatorname{rank} \mathcal{E}(\mathbb{Q}) \ll \frac{\log|\Delta(\mathcal{E})|}{\log\log|\Delta(\mathcal{E})|}.$$

Thus the discriminant must grow faster than exponentially in the rank.

Mestre's Examples of Curves of "High" Rank

The following table lists the curves of given rank and smallest discriminant found by Mestre.

Table 1. Data for Mestre's High Rank Curves

r	$\dfrac{(\mathrm{Reg}\,E)^{1/r}}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\min\limits_i \dfrac{\hat{h}(P_i)}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\max\limits_i \dfrac{\hat{h}(P_i)}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\dfrac{\log\lvert\Delta\rvert}{r\log r}$
4	0.612	0.772	0.844	2.382
5	0.627	0.840	0.941	2.362
6	0.600	0.937	0.994	2.295
7	0.696	1.032	1.063	2.116
8	0.776	1.103	1.128	2.111
9	0.543	1.051	1.073	2.311
10	0.756	1.091	1.106	2.271
12	0.674	0.916	0.923	2.273
14	0.585	1.018	1.025	2.341

The points $P_1, \ldots, P_r$ are generators for $\mathcal{E}(\mathbb{Q})$. The conclusion to be drawn from this table is if $P_1, \ldots, P_r$ are independent points in $\mathcal{E}(\mathbb{Q})$, then it is very likely that

$$\max \hat{h}(P_i) \geq \frac{1}{12}\log\lvert\Delta\rvert \geq \frac{1}{6} r \log r.$$

A Small Numerical Example

We chose to use $p = 173$ and more-or-less randomly took the curve

$$E : y^2 = x^3 + 42x + 86.$$

We then used Mestre's method to lift E. Among 269280 curves tested, there were three examples of rank 6 and three examples of rank 7.

Table 2. Lifting From Mod 173 To "High" Rank

r	$\dfrac{(\mathrm{Reg}\,\mathcal{E})^{1/r}}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\min\limits_i \dfrac{\hat{h}(P_i)}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\max\limits_i \dfrac{\hat{h}(P_i)}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\dfrac{\log\lvert\Delta\rvert}{r\log r}$
6	0.702	0.849	0.948	5.823
6	0.722	0.890	0.965	5.859
6	0.673	0.854	0.942	6.252
7	0.670	0.908	0.937	4.651
7	0.686	0.891	0.952	4.712
7	0.672	0.861	0.971	4.956

The relationship between $\max \hat{h}(P_i)$ and $\log\lvert\Delta\rvert$ is essentially the same in Tables 1 and 2; but the relationship between $\log\lvert\Delta\rvert$ and r has changed, due to the fact that the Table 2 curves satisfy an added "mod p" congruence condition. Based on this (and other) examples, it appears that applying Mestre's method in an Index Calculus setting yields curves that satisfy

$$\max \hat{h}(P_i) \geq c_1 \log p + c_2 r \log r.$$

For the data in Table 2, we get approximately

$$\max \hat{h}(P_i) \approx \frac{1}{12} \log |\Delta| \approx \log p + \frac{1}{50} r \log r.$$

Difficulty of Lifting Points

Lift $E/\mathbb{F}_p$ to a curve $\mathcal{E}/\mathbb{Q}$ of (large) rank r. Choose B so that the points in $\mathcal{E}(\mathbb{Q})$ with height $\le B$ cover most of $E(\mathbb{F}_p)$.

For the DLP, we can take $B \approx \sqrt{p}$, because the factor basis has height $\ll \log r$. But for the ECDLP, the factor basis has height $\gg r \log r$, which is exponentially larger. A tremendously optimistic view of the experimental data, for reasonable cryptographic values of p (say $2^{80} < p < 2^{240}$) gives

$$B \approx p^{3 \log_2 p} \qquad \text{and} \qquad r \approx \log_2 p.$$

The first problem is that this requires curves of rank on the order of 80 to 240, while the largest rank known is 22. However, there is a bigger problem, as pointed out by Miller.

Suppose we know generators $P_1, \dots, P_r \in \mathcal{E}(\mathbb{Q})$, suppose we are given a point $Q \in E(\mathbb{F}_p)$, and suppose we know that there is probably a linear combination

$$n_1 P_1 + n_2 P_2 + \cdots + n_r P_r \in \mathcal{E}(\mathbb{Q}) \qquad (*)$$

of height at most $B \approx p^{3 \log_2 p}$ which lifts Q. How can we find the linear combination $(*)$? Searching through $n_1, \ldots, n_r \in \mathbb{Z}$ (with time-space tradeoff) is $O(p^{1/2})$, so is infeasible. If B were smaller, say $B \ll p^{1-\varepsilon}$, then maybe we could lift from mod p to mod p^k (this will certainly work if $B \ll p^{1/2-\varepsilon}$); but for $B \gg p$, there are too many ways to lift.

Conclusion. The Index Calculus will not work for solving the ECDLP because it is not possible to lift $E/\mathbb{F}_p$ to a curve $\mathcal{E}/\mathbb{Q}$ having many independent points of sufficiently small height.

This concludes the discussion of my joint work with Joe Suzuki on the Index Calculus for the Elliptic Curve Discrete Logarithm Problem.

The Xedni Calculus for the ECDLP

The *Xedni Calculus* is a new method which <u>might</u> be used to solve the ECDLP.

It has not yet been tested in practice.

As we have seen, the Index Calculus does not work because it is hard to find curves of large rank and it is hard to lift points onto such curves. The Xedni Calculus works in reverse (whence its name).

Index Calculus	**Xedni Calculus**
[**1**] Lift $E/\mathbb{F}_p$ to $\mathcal{E}/\mathbb{Q}$; use Mestre's method to make $\operatorname{rank}\mathcal{E}(\mathbb{Q})$ large.	[**1**] Choose points in $E(\mathbb{F}_p)$ and lift them to points in $\mathbb{Z}^2$.
[**2**] Choose points in $E(\mathbb{F}_p)$ and try to lift them to points in $\mathcal{E}(\mathbb{Q})$.	[**2**] Choose a curve $\mathcal{E}/\mathbb{Q}$ containing the lifted points; use Mestre's method (in reverse) to make $\operatorname{rank}\mathcal{E}(\mathbb{Q})$ small.

Acknowledgment

Jung Hee Cheon (ETRI), Sang Guen Hahn (KAIST) and Hwanjoon Kim (KAIST) have independently devised a version of the Xedni Calculus (although without the use of Mestre's method in reverse to induce lower rank), so I would like to acknowledge them as independent creators of the Xedni Calculus method for the ECDLP.

Outline of the Xedni Calculus (Naive Version)

Step 1. Fix $3 \le r \le 6$. Choose integers

$$1 \le s_1, t_1, \ldots, s_r, t_r < N_p,$$

compute the points

$$s_i S - t_i T \in E(\mathbb{F}_p) \quad \text{for } i = 1, \ldots, r,$$

and lift them to points

$$P_i = (x_i, y_i) \in \mathbb{Z}^2.$$

Step 2. Find a small solution (e.g., using LLL) to the r-by-7 system of linear equations

$$\begin{pmatrix} y_1^2 & x_1y_1 & y_1 & -x_1^3 & -x_1^2 & -x_1 & -1 \\ y_2^2 & x_2y_2 & y_2 & -x_2^3 & -x_2^2 & -x_2 & -1 \\ \vdots & & & \ddots & & & \vdots \\ y_r^2 & x_ry_r & y_r & -x_r^3 & -x_r^2 & -x_r & -1 \end{pmatrix} \begin{pmatrix} U_1 \\ U_2 \\ \vdots \\ U_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

satisfying

$$(u_1, u_2, u_3, u_4, u_5, u_6, u_7) \equiv (1, 0, 0, 1, 0, a, b) \pmod{p}.$$

[Recall $E : y^2 = x^3 + ax + b$.]

Step 3. Let $\mathcal{E}/\mathbb{Q}$ be the elliptic curve

$$\mathcal{E} : u_1 y^2 + u_2 xy + u_3 y = u_4 x^3 + u_5 x^2 + u_6 x + u_7.$$

Note that

$$P_1, \ldots, P_r \in \mathcal{E}(\mathbb{Q}) \qquad \text{and} \qquad \mathcal{E} \equiv E \pmod{p}$$

by construction.

Step 4. If $P_1, \ldots, P_r$ are independent, go back to Step 1. Otherwise find an equation of dependence

$$n_1 P_1 + n_2 P_2 + \cdots + n_r P_r = O \quad \text{in } \mathcal{E}(\mathbb{Q}). \qquad (*)$$

(Implementation note: There are two efficient ways to perform this step, via canonical heights and via 2-descents.)

Step 5. Reduce $(*)$ modulo p to get a relation

$$\left(\sum_{i=1}^{r} n_i s_i\right) S = \left(\sum_{i=1}^{r} n_i t_i\right) T \quad \text{in } E(\mathbb{F}_p).$$

Let $s = \sum n_i s_i$. If $\gcd(s, N_p) = 1$ (as is almost certainly the case), multiply by $s^{-1} \bmod N_p$ to find $S = mT$.

Outline of the Xedni Calculus (Improvements)

Problem: For "most" choices, the points $P_1, \ldots, P_r$ will be independent (Néron, Masser). This is analogous to the Index Calculus, where for most choices of a lift $\mathcal{E}/\mathbb{Q}$, the rank of $\mathcal{E}(\mathbb{Q})$ will be small.

Index Calculus	**Xedni Calculus**
[Problem] It is likely that a randomly chosen lift of E will have low rank.	[Problem] It is likely that randomly lifted points will be independent.
[Solution] Use Mestre's method (impose congruence conditions) to increase the likelihood of high rank.	[Solution] Use Mestre's method (congruence conditions) <u>in reverse</u> to increase the likelihood of low rank.

Note that we cannot unilaterally impose congruence conditions on the coefficients of $\mathcal{E}$. Instead, we impose additional congruence conditions on the points $P_1, \ldots, P_r$ in such a way that the curve $\mathcal{E}$ will be forced to have $\#\mathcal{E}(\mathbb{F}_\ell)$ small for many small primes ℓ.

Other Improvements Include:

- Use general cubic curves to make the coefficients of $\mathcal{E}$ smaller and/or allow more points to be lifted.
- Normalize the first 4 points to make the coefficients of $\mathcal{E}$ smaller.
- (Locally) minimize the discriminant to increase the likelihood that $\mathcal{E}$ has small rank.
- Compute Mestre-type sums $\sum a_\ell/\ell$ to eliminate unlikely cases.
- Precompute quadratic and cubic residues modulo small primes to speed check for dependence.

Final Note. Neal Koblitz has made two interesting observations:

(1) The Xedni Calculus can be applied to the DLP (i.e., to the multiplicative group $\mathbb{F}_p^*$) by lifting to an elliptic curve $\mathcal{E}/\mathbb{Q}$ having split multiplicative reduction at p.

(2) The Xedni Calculus can be applied to the factorization problem by choosing random powers of a modulo N and lifting to an elliptic curve with split multiplicative reduction at all primes dividing N (without knowing the factorization of N).

A copy of my article with Joe Suzuki, "Elliptic curve discrete logarithms and the index calculus" (ASIACRYPT '98) may be downloaded from my home page:

`www.math.brown.edu/~jhs`

For a more detailed description of the Xedni calculus, see "The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem," preliminary manuscript, August 3, 1998.