October 6, 2000

ECC 2000, Essen, Germany

MIRACLES OF THE HEIGHT FUNCTION —
A GOLDEN SHIELD PROTECTING ECC

Neal Koblitz

University of Washington

Outline of talk:

Definition & properties of height function

Index calculus attack on ECC

Why index calculus won't work

Xedni calculus attack on ECC

Why xedni calculus won't work

References:

1. J. Silverman & J. Suzuki, Asiacrypt '98

2. V. Miller, Crypto '85

3. Jacobson-Koblitz-Silverman-Stein-Teske, Designs, Codes & Cryptography, April 2000

Let

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

be an elliptic curve $\widetilde{E}$ over the field $\mathbb{Q}$ of rational numbers. Let $\widetilde{P} = (x(\widetilde{P}), y(\widetilde{P}))$ be a rational point of the curve that is not the point at infinity $\widetilde{O}$.

DEFINITION OF THE HEIGHT

First, for a nonzero rational number $x = a/b$ written in lowest terms, the height $H(x)$ is defined to be max$(|a|, |b|)$, and the logarithmic height $h(x)$ is defined to be $\ln(H(x))$.

Note that $h(x)$ is essentially (up to a constant factor) equal to the input length of x in the computer-science sense, i.e., the number of bits needed to write x.

The logarithmic height of a point $\widetilde{P}$ is now defined to be

$$h(\widetilde{P}) = \frac{1}{2}h(x(\widetilde{P})).$$

NOTE: The factor of $\frac{1}{2}$ comes from the fact that $x(\widetilde{P})$ is a function "of degree 2." It would be almost the same to define $h(\widetilde{P})$ to be $\frac{1}{3}h(y(\widetilde{P}))$ (since $y(\widetilde{P})$ is a function of degree 3) or $\frac{1}{d}h(f(\widetilde{P}))$ for any function $f(\widetilde{P})$ of degree d.

The logarithmic height function does not quite have nice properties, although it does have nice properties "up to a constant." For example, up to a constant it does not matter which function f was used in the definition $\frac{1}{\deg f} h(f(\widetilde{P}))$. For instance,

$$\left| \frac{1}{2} h(x(\widetilde{P})) - \frac{1}{3} h(y(\widetilde{P})) \right| < C.$$

Néron and Tate showed that a slight modification can be made in $h(\widetilde{P})$ so that the resulting function of $\widetilde{P}$ has the nice properties exactly, rather than only up to a constant. Their function $\widehat{h}(\widetilde{P})$ is called the "Néron–Tate canonical logarithmic height."

Before defining $\widehat{h}(\widetilde{P})$, we note a very important fact about the group law on the curve. If we keep adding a point to itself, the number of bits occupied by the numerators and denominators of the coordinates of $k\widetilde{P}$ grows quadratically in k. That is,

$$h(k\widetilde{P}) \approx \mathbf{const} \cdot k^2.$$

We now define

$$\widehat{h}(\widetilde{P}) = \lim_{j \longrightarrow \infty} \frac{1}{j^2} h(j\widetilde{P}).$$

(For the point at infinity $\widetilde{O}$ we define $\widehat{h}(\widetilde{O}) = 0$.)

This definition is independent of which function $f(\widetilde{P})$ was used to define $h(\widetilde{P})$. It is also obvious that $\widehat{h}(k\widetilde{P})$ grows exactly quadratically in k:

$$\widehat{h}(k\widetilde{P}) = k^2 \, \widehat{h}(\widetilde{P}).$$

Other properties of $\widehat{h}(\widetilde{P})$:

• $\widehat{h}(\widetilde{P}) = 0$ **iff** $\widetilde{P}$ **has finite order.**

• **On** $\widetilde{E}(\mathbb{Q})$**/(torsion subgroup),** $\widehat{h}(\widetilde{P})$ **gives a positive definite inner product defined by**

$$\langle \widetilde{P}, \widetilde{Q} \rangle = \frac{1}{2}\Big(\widehat{h}(\widetilde{P}+\widetilde{Q}) - \widehat{h}(\widetilde{P}) - \widehat{h}(\widetilde{Q})\Big).$$

For simplicity, suppose that $\widetilde{E}(\mathbb{Q})$ **has trivial torsion. Then** $\widetilde{E}(\mathbb{Q}) \approx \mathbb{Z}^r$**, where** r **is the** *rank***; and the canonical logarithmic height makes** $\widetilde{E}(\mathbb{Q})$ **into a full lattice in** $\mathbb{R}^r$**.**

The volume of a fundamental parallelepiped for the lattice is the squareroot of

$$\mathrm{Reg}(\widetilde{E}) = \det(\langle \widetilde{P}_i, \widetilde{P}_j \rangle)_{1 \le i,j \le r},$$

where $\widetilde{P}_1, \ldots, \widetilde{P}_r$ are a set of generators of $\widetilde{E}(\mathbf{Q})$. This determinant is called the *regulator* of the curve.

Theoretical use of the height function: to prove the Mordell–Weil theorem, which says that the group of points is finitely generated.

FIRST PHASE OF INDEX CALCULUS

Suppose that we want to solve the ECDLP on a curve E defined over $\mathbb{F}_p$. That is, given $P, Q \in E(\mathbb{F}_p)$, we want to find an integer m such that $Q = mP$. (In practice, P and Q usually belong to a subgroup of $E(\mathbb{F}_p)$ of large prime order n, where n is almost as large as p.)

The first idea of an index calculus approach is to lift the curve to a curve $\widetilde{E}(\mathbb{Q})$ — that is, to a curve whose equation reduces modulo p to that of the original curve E over $\mathbb{F}_p$ — and then lift the two points P, Q in the ECDLP to two points $\widetilde{P}, \widetilde{Q} \in \widetilde{E}(\mathbb{Q})$ — that is, to two points whose coordinates reduce modulo p to those of $P, Q \in E(\mathbb{F}_p)$.

Since the most likely value of r for a random elliptic curve over $\mathbb{Q}$ is either 0 or 1, let us first consider those possibilities.

Case 1. The lifted curve has zero rank, i.e., $\widetilde{E}(\mathbb{Q})$ is a finite group. According to a deep theorem of Barry Mazur, there are at most 16 points on $\widetilde{E}(\mathbb{Q})$; and the largest prime number that can be the order of a point is 7. Since ECC is going to be taking place in a group of prime order $n >> 7$, you simply cannot lift your points to $\widetilde{E}(\mathbb{Q})$.

Case 2. The lifted curve has rank 1. For simplicity, let's suppose that $\widetilde{E}(\mathbb{Q})$ has trivial torsion, i.e., $\widetilde{E}(\mathbb{Q}) \approx \mathbb{Z}$. Let $\widetilde{P}_1$ be a generator of $\widetilde{E}(\mathbb{Q})$.

Suppose that there exist integers s, t with

$$|s|, |t| < B$$

such that $\widetilde{P} = s\widetilde{P}_1$ and $\widetilde{Q} = t\widetilde{P}_1$ lift P and Q.

Then

$$\widehat{h}(\widetilde{P}),\ \widehat{h}(\widetilde{Q}) \approx B^2\,\widehat{h}(\widetilde{P}_1),$$

and so the lifted points require about

$$k \approx B^2 \widehat{h}(\widetilde{P}_1)$$

symbols to write down.

Now if m is the discrete log that we're looking for, then $\widetilde{Q} - m\widetilde{P} = (t - ms)\widetilde{P}_1$ must reduce mod p to the point at infinity on E, i.e.,

$$t - ms \equiv 0 \pmod{n},$$

where n is the order of the group of points of the cryptosystem. (Presumably n is a prime of roughly the same size as p.)

But for random m, the probability that $|s|,\ |t| < B$ exist with $t - ms \equiv 0 \pmod{n}$ is less than

$$\frac{2B^2}{n} \approx \frac{k}{p\,\widehat{h}(\widetilde{P}_1)}.$$

Thus, there is only a probability $O\left(\frac{k}{p}\right)$ that P and Q can be lifted to points that can be expressed in k symbols.

NOTE: The constant in the big-O contains $\frac{1}{\widehat{h}(\widetilde{P}_1)}$. So perhaps the situation wouldn't be totally hopeless if we could get $\widehat{h}(\widetilde{P}_1)$ to be extremely small. But that's not feasible. (More on this later.)

Now let's consider general r, and suppose that we are able to lift a significant proportion of points of $E(\mathbb{F}_p)$ to points of $\widetilde{E}(\mathbb{Q})$. Here "significant" means not hopelessly miniscule, e.g., $> 10^{-8}$.

Outline of how index calculus would work:

1. Choose a lifting $\widetilde{E}(\mathbb{Q})$ of $E(\mathbb{F}_p)$, and find a basis $\widetilde{P}_1, \widetilde{P}_2, \ldots, \widetilde{P}_r$ of linearly independent points on $\widetilde{E}(\mathbb{Q})$. (For simplicity, here and in what follows we'll assume that $\widetilde{E}(\mathbb{Q})$ has trivial torsion.)

2. Compute the multiples $2P$, $3P$, $4P$, etc. in $E(\mathbb{F}_p)$, and for each k try to lift kP to a point $\mathcal{P}_k \in \widetilde{E}(\mathbb{Q})$. Let $k_1, k_2, \ldots$ be a sequence of values for which this is possible. For each k_i express $\mathcal{P}_{k_i}$ as a linear combination

$$\mathcal{P}_{k_i} = \sum_{j=1}^{r} \alpha_{ij} \widetilde{P}_j.$$

3. Let $P_j \in E(\mathbb{F}_p)$ be the reduction mod p of $\widetilde{P}_j$, and let u_j denote the (at present unknown) discrete logarithm of P_j to the base P. After enough multiples $k_i P$ have been lifted, we can solve the system of linear congruences

$$k_i \equiv \sum_{j=1}^{r} \alpha_{ij} u_j \pmod{n}$$

for the unknowns u_j, where n is either the order of $E(\mathbb{F}_p)$, or else the order of the large subgroup of $E(\mathbb{F}_p)$ in which the cryptosystem was constructed.

4. Try to lift Q, $Q+P$, $Q+2P$, $Q+3P$, etc. to a point of $\widetilde{E}(\mathbb{Q})$, until you find a single such point $Q+kP$ that lifts to $\mathcal{Q} \in \widetilde{E}(\mathbb{Q})$. After expressing $\mathcal{Q}$ as a linear combination

$$\mathcal{Q} = \sum_{j=1}^{r} \beta_j \widetilde{P}_j,$$

you can find the desired discrete logarithm m from

$$m + k \equiv \sum_{j=1}^{r} \beta_j u_j \pmod{n}.$$

WHY THIS WON'T WORK

Let V_r denote the volume of the unit ball in $\mathbb{R}^r$. Then the volume of the ball of radius $\sqrt{B}$ is

$$V_r B^{r/2},$$

and the number of integer points in $\mathbb{R}^r$ whose square of distance from the origin is $\leq B$ is asymptotic to this value.

If we want an asymptotic expression for the number of points in some other lattice whose square of distance from the origin is $\leq B$, then it is intuitively clear that we must divide the above expression by the volume of a fundamental parallelepiped of this lattice. This gives the result:

$$\#\left\{\widetilde{P} \in \widetilde{E}(\mathbb{Q}) \;\middle|\; \widehat{h}(\widetilde{P}) \leq B\right\} \approx \frac{V_r}{\sqrt{\operatorname{Reg}(\widetilde{E})}}\, B^{r/2}.$$

Very little is known about how to lift points from $E(\mathbb{F}_p)$ to $\widetilde{E}(\mathbb{Q})$. But a necessary condition for lifting $P \in E(\mathbb{F}_p)$ is that there be a point $\widetilde{P} \in \widetilde{E}(\mathbb{Q})$ that reduces to P modulo p and that has reasonable height, i.e., that has coordinates that can be written out in a reasonable number of digits.

Thus, in order to be able to lift $> 10^{-8}p$ points, for reasonable B we want to have

$$\frac{V_r}{\sqrt{\mathrm{Reg}(\widetilde{E})}} B^{r/2} > 10^{-8}p.$$

We probably won't want B to be more than about 100, and we'll want p to be at least 10^{50}. Thus, we need either r to be large or $\mathrm{Reg}(\widetilde{E})$ to be very small, or preferably both.

However, $\sqrt{\mathrm{Reg}(\widetilde{E})}$ can be bounded from below in terms of the r-th power of the length of the shortest vector, which is the square root of μ, where we define

$$\mu = \min_{\widetilde{P}\in\widetilde{E}(\mathbf{Q}),\ \widetilde{P}\neq\widetilde{O}} \widehat{h}(\widetilde{P}).$$

And, according to a conjecture of Serge Lang, μ is bounded from below by a constant multiple of $\log|\Delta|$, where Δ is the discriminant of $\widetilde{E}$.

Next, it is intuitively clear that $\log|\Delta|$ is at least of the order of $\log p$, i.e.,

$$\log|\Delta| \gg \log p$$

(since the coefficients of $\widetilde{E}$ are liftings modulo p of the coefficients of E). Also, it has been proved (under the assumption of certain standard conjectures) that

$$\log|\Delta| \gg r\log r.$$

Putting this all together, we see that there is no way to make $\sqrt{\mathrm{Reg}(\widetilde{E})}$ extremely small. And if we try to make r very large, we'll have to pay a price in terms of increasing $\sqrt{\mathrm{Reg}(\widetilde{E})}$.

In any case, no elliptic curve has been found with $r > 23$, even though concerted efforts have been made to produce curves of high rank. Moreover, in practice, one cannot get anywhere near $r = 23$ with a curve that must simultaneously be a lifting of a given mod-p curve E.

Thus, on any lifting $\widetilde{E}(\mathbb{Q})$ there are going to be too few points of reasonable height to provide liftings of a significant proportion of points of $E(\mathbb{F}_p)$.

That's why index calculus won't work.

Two remarks:

1. If the finite field is not a prime field, then it would be natural to lift to elliptic curves over a number field. But $\widehat{h}$ generalizes to number fields. See §5–6 of Ch. VIII of Silverman's *The Arithmetic of Elliptic Curves*.

2. Another approach would be to lift to elliptic curves over a function field (i.e., over a finite extension of $\mathbb{F}_q(T)$). But $\widehat{h}$ generalizes to function fields. See §4 of Ch. III of Silverman's *Advanced Topics in the Arithmetic of Elliptic Curves*.

J. SILVERMAN'S XEDNI ATTACK

We want to find an integer m such that $Q = mP$ in $E(\mathbb{F}_p)$.

We first randomly choose r different linear combinations $P_j = s_j P + t_j Q$ of the points P and Q in $E(\mathbb{F}_p)$. Here r is an integer between 2 and 9.

Next, we choose r points $\widetilde{P}_j$ in the plane with integer coordinates whose residues modulo p are our points $P_j \in E(\mathbb{F}_p)$.

We also choose an elliptic curve $\widetilde{E}(\mathbb{Q})$ that passes through all of the $\widetilde{P}_j$ and that reduces modulo p to the curve $E(\mathbb{F}_p)$. (For this r can be at most 9.)

Now if we're very lucky, the points $\widetilde{P}_j \in \widetilde{E}(\mathbb{Q})$ will be linearly dependent, in which case we find integer coefficients α_j such that

$$\sum_{j=1}^{r} \alpha_j \widetilde{P}_j = \widetilde{O} \in \widetilde{E}(\mathbb{Q}).$$

Reducing mod p, we find that

$$\sum_{j=1}^{r} \alpha_j (s_j P + t_j Q)$$

is the point at infinity in $E(\mathbb{F}_p)$, and so we have

$$\begin{aligned}\sum_{j=1}^{r} \alpha_j (s_j + t_j m) &= \left(\sum_{j=1}^{r} \alpha_j s_j\right) + \left(\sum_{j=1}^{r} \alpha_j t_j\right) m \\ &\equiv 0 \pmod{n},\end{aligned}$$

from which we can solve for the discrete logarithm m.

Silverman had various strategies to (at least conjecturally) increase the probability that the $\widetilde{P}_j$ are linearly dependent; these will not concern us here.

Let $\widetilde{E}(\mathbf{Q})$ be the lifted curve constructed in an iteration of the algorithm, and for simplicity suppose that it has trivial torsion.

Recall the canonical logarithmic height $\widehat{h}(\widetilde{P})$, whose properties make it unlikely that index calculus can be adapted for elliptic curves.

$\widetilde{E}(\mathbf{Q})$ may be regarded as a full lattice in a vector space V having $\sqrt{\widehat{h}}$ as metric.

Let $\widetilde{P}_1, \ldots, \widetilde{P}_r \in \widetilde{E}(\mathbf{Q})$ be the lifted points that we hope are dependent.

Consider the map from r-tuples of integers to $\widetilde{E}(\mathbf{Q}) \subset V$ given by

$$(\alpha_1, \ldots, \alpha_r) \mapsto \alpha_1 \widetilde{P}_1 + \cdots + \alpha_r \widetilde{P}_r,$$

and suppose that the $\widetilde{P}_j$ are dependent.

Let

$$\mathcal{M} = \max_{1 \leq i \leq r} \widehat{h}(\widetilde{P}_i),$$

and, as before, let

$$\mu = \min_{\widetilde{P} \in \widetilde{E}(\mathbf{Q}),\ \widetilde{P} \neq \widetilde{O}} \widehat{h}(\widetilde{P}).$$

If $\mathcal{M}/\mu$ is bounded from above by an absolute constant, then it follows from

$$\begin{cases} \textbf{geometry of numbers} \\ \textbf{pigeon – hole argument} \end{cases}$$

that the $\widetilde{P}_j$ satisfy a nontrivial dependency relation whose coefficients α_j are bounded from above by an absolute constant C.

The idea of the proof of this fact is that there are $O(C^r)$ possibilities for the r-tuple of coefficients, and only $O(C^{r-1})$ possible image-points $\sum \alpha_j \widetilde{P}_j$, where the constant in the second big-O depends on the bound for $\mathcal{M}/\mu$.

But then the original $P_j \in E(\mathbb{F}_p)$ must satisfy a dependency with $|\alpha_j| \leq C$, and there is only an exponentially small probability that this happens.

It remains only to justify the assumed absolute boundedness of $\mathcal{M}/\mu$. This follows from two very plausible assumptions (here Δ denotes the discriminant of $\widetilde{E}(\mathbb{Q})$):

(1) $\mu \geq C_1 \log|\Delta|$ **for an absolute constant** C_1**;**

(2) $\log|\Delta| \geq C_2\mathcal{M}$ **for an absolute constant** C_2**.**

These imply that

$$\frac{\mathcal{M}}{\mu} \leq \frac{1}{C_1 C_2}.$$

Assumption (1) is Lang's conjecture, which has been proved by J. Silverman in many cases.

What about (2)?

Roughly speaking, assumption (2) says that whenever we pass a curve $\widetilde{E}(\mathbf{Q})$ through r points $\widetilde{P}_j$, the size of (i.e., number of symbols needed to write) the curve's coefficients — and hence Δ, which is a polynomial function of these coefficients — is at least of the same magnitude as the size of the points $\widetilde{P}_j$.

NOTE: If you start with $\widetilde{E}(\mathbf{Q})$, and if $\widetilde{E}(\mathbf{Q})$ has nonzero rank, then it is easy to find points $\widetilde{P}_j$ of size much larger than $\log|\Delta|$. For example, just take multiples of a given point.

On the other hand, when you start with the points $\widetilde{P}_j$ and then obtain $\widetilde{E}(\mathbf{Q})$ by passing a curve through these points, then it is extremely unlikely that you'll be able to get a curve whose discriminant has small size compared to the points.

We conclude that asymptotically the Silverman algorithm has exponential expected running time $O(p)$ — worse than that of squareroot attacks.

Thus, the height function $\widehat{h}(\widetilde{P})$, by imbedding $\widetilde{E}(\mathbb{Q})$ as a lattice in $\mathbb{R}^r$, shows us that there are only polynomially many $O(B^r)$ points of reasonable input-length $\leq B$. This is what prevents both the index calculus attack and the xedni calculus attack from having any chance of success.