An index calculus algorithm for non-singular plane curves of high genus

Claus Diem

University of Leipzig

Presented at the

10th Workshop on Elliptic Curve Cryptography (ECC)

Toronto, Sep. 18-20 2006

Motivation

Recall that for $\alpha \in (0,1)$ and $c > 0$, we have the subexponentiality function

$$L_n[\alpha, c] := e^{c \cdot \log(n)^{\alpha} \cdot \log(\log(n))^{1-\alpha}} .$$

There are $L[1/3, O(1)]$-algorithms for integer factorization as well as for the discrete logarithm problem in finite fields.

However, for the discrete logarithm problem in degree 0 class groups (Jacobian groups) of curves of high genus, there are only $L[1/2, O(1)]$-algorithms.

Motivation

Heuristic Result Let $d \geq 4$ be fixed, and let us consider curves over finite fields $\mathbb{F}_q$ represented by plane models of degree d. Then the DLP in the degree 0 class groups of these curves can be solved in an expected time of

$$\tilde{O}(q^{2-\frac{2}{d-2}}) \ .$$

The result

Heuristic Result Let us consider a family of non-singular plane curves over finite fields $\mathbb{F}_q$ with $g \in \Omega(\log(q)^2)$, where g is the genus. Then one can solve the DLP in the degree 0 class groups of these curves in an expected time of

$$O(L_{q^g}[1/3, (\frac{64}{9})^{1/3} + \epsilon])$$

The result

Heuristic Result Let us consider a family of non-singular plane curves over finite fields $\mathbb{F}_q$ with $g \in \Omega(\log(q)^2)$, where g is the genus. Then one can solve the DLP in the degree 0 class groups of these curves in an expected time of

$$O(L_{q^g}[1/3, (\frac{64}{9})^{1/3} + \epsilon]) \qquad ((\frac{64}{9})^{1/3} \leq 1.923) .$$

(Compare with the running time of $L_{q^g}[1/3, (\frac{64}{9})^{1/3} + o(1)]$ for the number field sieves for factoring and DLP in prime fields.)

Idea of index calculus

Let $\mathcal{C}/\mathbb{F}_q$ be a curve of genus g, and let $a, b \in \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_q)$ with $b \in \langle a \rangle$.

The goal is to find an $x \in \mathbb{N}$ such that $x \cdot a = b$.

We fix a *smoothness bound* s, and let the *factor base* $\mathcal{F}$ be the set of all prime divisors of degree $\leq s$.

The goal is the generate relations between factor base elements and the inputs a, b for the DLP and to solve the DLP via linear algebra.

The group order

Idea by F. Heß:

By p-adic point counting algorithms, one can determine the L-polynomial of $\mathcal{C}/\mathbb{F}_q$ in polynomial time in $\log(q)$. We do this computation at the beginning. Then we can perform all linear algebra computations modulo the group order $\#\operatorname{Cl}^0(\mathcal{C}/\mathbb{F}_q)$. We thereby use sparse linear algebra.

Generating relations fast

Let $\mathcal{C}/\mathbb{F}_q$ be a non-singular plane curve, given by

$$F(X, Z, Z) = 0 \ .$$

Let $d := \deg(F)$. Note that

$$g = \frac{(d-1)(d-2)}{2}$$

Let $D_\infty := \operatorname{div}_{\mathcal{C}}(Z)$ be the intersection of $\mathcal{C}$ with the line $Z = 0$; this is an effective divisor of degree d.

Generating relations fast

Idea of the previous algorithm for plane curves of small degree over large finite fields:

Let D be the intersection of $\mathcal{C}$ with any line. Then

$$D \sim D_\infty$$

that is,

$$[D] - [D_\infty] = 0 \ .$$

We now want that D splits over the factor base.

Generating relations fast

What about high genus?

Idea: Intersect the curve with lines, quadrics, cubics, quartics etc.

Let $t \in \mathbb{N}$ and let us consider the linear system

$$\mathfrak{d}_t := \{\mathrm{div}_{\mathcal{C}}(G) \mid G \in \mathbb{F}_q[X,Y,Z]_t\} \ .$$

This is a subsystem of the complete linear system

$$\begin{aligned} |tD_\infty| &= \{D \geq 0 \mid D \sim tD_\infty\} \\ &= \{tD_\infty + (f) \mid (f) \geq -tD_\infty\} \end{aligned}$$

In particular it is a projective space. What can be said about its dimension?

Generating relations fast

Lemma For $t < d$, $\dim(\mathfrak{d}_t) = \binom{t+2}{2} - 1$.

Generating relations fast

Lemma For $t < d$, $\dim(\mathfrak{d}_t) = \binom{t+2}{2} - 1$.

Proof.
Let $\iota : \mathcal{C} \hookrightarrow \mathbb{P}^2_{\mathbb{F}_q} = \mathrm{Proj}(\mathbb{F}_q[X, Y, Z])$ be the immersion. Let $I = (F) \subseteq \mathbb{F}_q[X, Y, Z]$ be the defining ideal of $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{F}_q}$. We have an exact sequence

$$0 \longrightarrow I_t \longrightarrow \mathbb{F}_q[X, Y, Z]_t = \Gamma(\mathbb{P}^2_{\mathbb{F}_q}, \mathcal{O}(t)) \xrightarrow{\iota^*} \Gamma(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(t)) \ ,$$

and for $t < d$, $I_t = 0$, i.e.

$$\iota^* : \mathbb{F}_q[X, Y, Z]_t \hookrightarrow \Gamma(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(t)) \ .$$

$$|tD_\infty| \simeq \mathbb{P}(\Gamma(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(t)) \qquad \mathfrak{d}_t \simeq \mathbb{P}(\iota^* \mathbb{F}_q[X, Y, Z]_t) \ .$$

Some notation

For $\alpha \in (0,1)$ and $c > 0$, we have the subexponentiality function $L[\alpha, c]$ with

$$L_n[\alpha, c] = e^{c \cdot (\log n)^{\alpha} \cdot \log(\log(n))^{1-\alpha}}$$

Let $\ell[\alpha, c]$ be the function in two variables (q, g)

$$\ell_{q,g}[\alpha, c] = c \cdot g^{\alpha} \cdot (\frac{\log(g \log(q))}{\log(q)})^{1-\alpha} \ .$$

Note that

$$L_{q^g}[\alpha, c] = q^{\ell[\alpha, c]} \ .$$

Smoothness

Theorem (Heß) Let $0 < \beta < \alpha < 1$ and $c, d > 0$ be fixed, $\delta > \frac{1-\alpha}{\alpha-\beta}$.

For some curve over a finite field, let $\psi(n, m)$ be the number of effective divisors of degree n which are m-smooth.

Let us consider curves over finite fields $\mathbb{F}_q$ with $g \geq (\log(q))^\delta$.

Let

$$n = \lfloor \ell[\alpha, c] \rfloor \,, \; m = \lceil \ell[\beta, d] \rceil \,.$$

Then

$$\frac{\psi(n, m)}{q^n} \geq L_{q^g}[\alpha - \beta, -\frac{c}{d}(\alpha - \beta) - o(1)] \,.$$

Generating the relation lattice

Let us consider non-singular plane curves with $g \in \Omega(\log(q)^2)$.

Heuristic Result 1 Let $c := \left(\frac{8}{9}\right)^{1/3}$, and let $\epsilon > 0$ be fixed. Let the smoothness bound be $s := \ell[1/3, c]$. Let $t := \lfloor \ell[1/3, 4(c+\epsilon)]^{1/2} \rfloor$. Then for $q^g \gg 0$, the s-smooth divisors in $\mathfrak{d}_t$ generate the relation lattice of $\mathcal{F} \cup \{D_\infty\}$.

Generating the relation lattice

Let us consider non-singular plane curves with $g \in \Omega(\log(q)^2)$.

Heuristic Result 1 Let $c := \left(\frac{8}{9}\right)^{1/3}$, and let $\epsilon > 0$ be fixed. Let the smoothness bound be $s := \ell[1/3, c]$. Let $t := \lfloor \ell[1/3, 4(c+\epsilon)]^{1/2} \rfloor$. Then for $q^g \gg 0$, the s-smooth divisors in $\mathfrak{d}_t$ generate the relation lattice of $\mathcal{F} \cup \{D_\infty\}$.

Note The dimension of $\mathfrak{d}_t$ is $\sim t^2/2 \sim \ell[1/3, 2(c+\epsilon)]$.
$\Longrightarrow$ The relation collection and the linear algebra can be performed in a time of

$$L[1/3, 2(c+\epsilon) + o(1)] = L[1/3, \left(\frac{64}{9}\right)^{1/3} + 2\epsilon) + o(1)] \, .$$

Arguments for Heuristic Result 1

Heuristic Assumption Up to logarithmic factors, the probability that a uniformly chosen divisor in $\mathfrak{d}_t$ is s-smooth is equal to the probability that a uniformly chosen divisor of degree $\deg(tD_\infty) = td$ is s-smooth.

This degree is

$$td \sim \ell[1/3, 4(c+\epsilon)]^{1/2} \cdot (2g)^{1/2} =$$

$$2(c+\epsilon)^{1/2} \cdot g^{1/6} \cdot (\frac{\log(g\log(q))}{\log(q)})^{1/3} \cdot (2g)^{1/2} =$$

$$8^{1/2} \cdot (c+\epsilon)^{1/2} \cdot g^{2/3} \cdot (\frac{\log(g\log(q))}{\log(q)})^{1/3} = \ell[2/3,\, 8^{1/2}(c+\epsilon)^{1/2}]$$

Arguments for Heuristic Result 1

The probability in question is then (heuristically)

$$P \in L[1/3, -\frac{8^{1/2}(c+\epsilon)^{1/2}}{c} \cdot \frac{1}{3} - o(1)] \,.$$

$\Longrightarrow$ We have

$$\sim P \cdot q^{\dim(\mathfrak{d}_t)} \in L[1/3, -\frac{8^{1/2}(c+\epsilon)^{1/2}}{c} \cdot \frac{1}{3} - o(1) + 2(c+\epsilon)]$$

relations over the factor base (and D_∞).

Arguments for Heuristic Result 1

The probability in question is then (heuristically)

$$P \in L[1/3, -\frac{8^{1/2}(c+\epsilon)^{1/2}}{c} \cdot \frac{1}{3} - o(1)] \; .$$

$\Longrightarrow$ We have

$$\sim P \cdot q^{\dim(\mathfrak{d}_t)} \in L[1/3, -\frac{8^{1/2}(c+\epsilon)^{1/2}}{c} \cdot \frac{1}{3} - o(1) + 2(c+\epsilon)]$$

relations over the factor base (and D_∞).

Claim. For $c = \left(\frac{8}{9}\right)^{1/3}$ this is $\geq L[1/3, c]$.

Arguments for Heuristic Result 1

That is,

$$-\frac{8^{1/2}(c+\epsilon)^{1/2}}{c}\cdot\frac{1}{3}-o(1)+2(c+\epsilon)\geq c\,.$$

$$(\frac{8^{1/2}}{3c^{1/2}}\leq c\Longleftrightarrow\frac{8}{9}\leq c^3\Longleftrightarrow c\geq(\frac{8}{9})^{1/3})$$

Input elements and factor base

Let $a, b \in \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_q)$ be the input elements. We want to find two relations of the form

$$\sum_j r_j[F_j] + r[D_\infty] = \alpha a + \beta b$$

Input elements and factor base

Let $a, b \in \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_q)$ be the input elements. We want to find two relations of the form

$$\sum_j r_j[F_j] + r[D_\infty] = \alpha a + \beta b$$

1. Step: Let D_0 be some divisor of degree g which splits over the factor base. Choose uniformly randomly α, β and compute an effective divisor D with

$$[D] - [D_0] = \alpha a + \beta b\ .$$

Repeat until D is $L[2/3, c - \epsilon]$-smooth.

Time needed: $L[1/3, \frac{1}{c-\epsilon} \cdot \frac{1}{3} + o(1)]$.

This is negligible.

The smoothing procedure

Input: A divisor D of degree $\ell[\alpha, c-\epsilon]$ $(\alpha \in [1/3, 2/3])$.

Output: A relation $[D] + \sum_i [D_i] + r[D_\infty] = 0$ with $D_i \geq 0$, $\deg(D_i) \leq \ell[\alpha/2 + 1/6, c-\epsilon]$.

Heuristic expected running time: $L[1/3, c+\epsilon']$

The smoothing procedure

Input: A divisor D of degree $\ell[\alpha, c-\epsilon]$ $(\alpha \in [1/3, 2/3])$.

Output: A relation $[D] + \sum_i [D_i] + r[D_\infty] = 0$ with $D_i \geq 0$, $\deg(D_i) \leq \ell[\alpha/2 + 1/6, c-\epsilon]$.

Heuristic expected running time: $L[1/3, c+\epsilon']$

E.g.: After an application to a divisor of degree $\ell[2/3, c-\epsilon]$, we have a relation with $\deg(D_i) \leq \ell[1/2, c-\epsilon]$.

Application of the smoothing procedure

Say we have

$$[D]-[D_0] = \alpha a+\beta b \quad \text{with } D = \sum_i D_i \ , \ \deg(D_i) \leq \ell[2/3, c-\epsilon] \ .$$

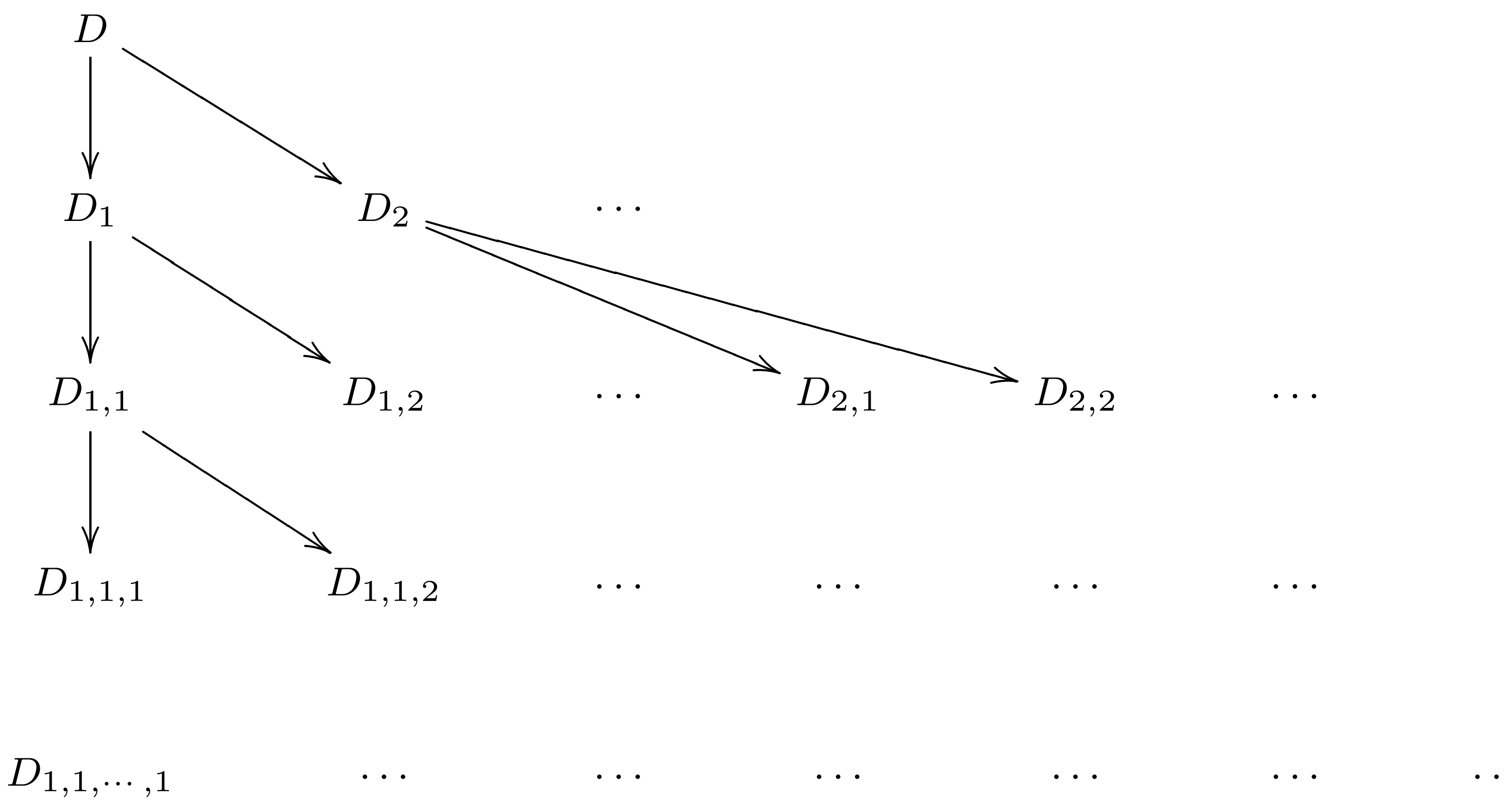
Then to each D_i we apply the smoothing procedure. We obtain

$$D_i \sim -\sum_j D_{i,j} + r_i D_\infty \qquad \text{with } D_{i,j} \geq 0 \ ,$$

$\deg(D_{i,j}) \leq \ell[1/3+1/6, c-\epsilon] = \ell[1/2, c-\epsilon]$ and $r_i \in \mathbb{N}$.
Then we apply the smoothing procedure again to each $D_{i,j}$, then again ... (until we have a representation as a sum of effective divisors of degree $\leq \ell[1/3, c]$).

Application of the smoothing procedure

Let $e_1 := 1, e_{i+1} := \frac{e_i}{2} + \frac{1}{6}$ (such that $e_i = \frac{1}{3} + \frac{2}{3} \cdot \frac{1}{2^{n-1}}$). Then we obtain a tree where the degrees of the divisors in row i are bounded by $\ell[e_i, c]$.



Application of the smoothing procedure

We repeat this until $i \approx \log_2(g)$. Then $e_i \approx \frac{1}{3} + \frac{2}{3} \cdot \frac{1}{g}$.

Then the degrees are

$$\leq \ell[e_i, c - \epsilon] \in \ell[1/3, (c - \epsilon)(1 + o(1))] \leq \ell[1/3, c] \ .$$

We have to apply the smoothing procedure only $L[1/3, o(1)]$ times, and the matrix has only $L[1/3, o(1)]$ non-zero entries per row.

The smoothing procedure

Let an effective divisor D of degree $\ell[\alpha, c-\epsilon]$ be given. Let $t_\alpha := \lfloor \ell[\alpha, 4(c+\epsilon)]^{1/2} \rfloor$ and consider the linear system

$$|t_\alpha D_\infty - D| \cap \mathfrak{d}_{t_\alpha} \ .$$

Any divisor D' in this linear system satisfies

$$D' + D \sim t_\alpha D_\infty \ .$$

We want to find some D' which is $\ell[\alpha/2 + 1/6, c-\epsilon]$-smooth.

The smoothing procedure

Let an effective divisor D of degree $\ell[\alpha, c-\epsilon]$ be given. Let $t_\alpha := \lfloor \ell[\alpha, 4(c+\epsilon)]^{1/2} \rfloor$ and consider the linear system

$$|t_\alpha D_\infty - D| \cap \mathfrak{d}_{t_\alpha} \; .$$

This linear system has dimension

$$\geq \binom{t_\alpha + 2}{2} - \deg(D) \sim \ell[\alpha, 2(c+\epsilon)] - \ell[\alpha, c-\epsilon] = \ell[\alpha, c+3\epsilon]$$

and degree

$$\sim \ell[\alpha, 4(c+\epsilon)]^{1/2} \cdot (2g)^{1/2} = \ell[\alpha/2 + 1/2, \; 8^{1/2}(c+\epsilon)^{1/2}] \; .$$

The smoothing procedure

Let an effective divisor D of degree $\ell[\alpha, c-\epsilon]$ be given. Let $t_\alpha := \lfloor \ell[\alpha, 4(c+\epsilon)]^{1/2} \rfloor$ and consider the linear system

$$|t_\alpha D_\infty - D| \cap \mathfrak{d}_{t_\alpha} \ .$$

Heuristic Result 2 There exists a universal constant C such that for $\epsilon < C$, the linear system $|t_\alpha D_\infty - D| \cap \mathfrak{d}_{t_\alpha}$ contains $L[1/3, \Omega(1)]$ s-smooth divisors.

The algorithm

Given: A non-singular plane curve $\mathcal{C}/\mathbb{F}_q$ and $a, b \in \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_q)$ of high genus with $b \in \langle a \rangle$.

1. Compute $\#\,\mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_q)$ using a p-adic point counting algorithm.

2. Let $s := \ell[1/3, \left(\frac{8}{9}\right)^{1/3}]$, and let the factor base $\mathcal{F}$ consist of all prime divisors of degree $\leq s$.

3. Generate relations by considering divisors of the form $\mathrm{div}_{\mathcal{C}}(G)$ for polynomials G of degree $\leq (\ell[1/3, 4\left(\frac{8}{9}\right)^{1/3} + \epsilon])^{1/2}$.

4. Relate the input elements to the factor base, using the "smoothing procedure".

5. Linear algebra

Curves of higher degree

Heuristic Result Let $\frac{1}{2} \leq \beta \leq \frac{3}{4}$. Let us consider curves represented by plane models of degree $d \leq g^{\beta}$ (and $g \in \Omega(\log(q)^2)$).

Then the DLP in the degree 0 class groups of these curves can be solved in an expected time of $L[\frac{2}{3} \cdot \beta + \epsilon, O(1)]$.