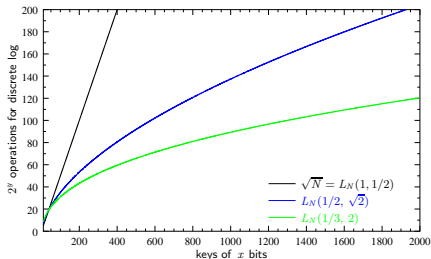


An $L(1/3)$ algorithm for the discrete logarithm problem in low degree curves

Andreas Enge
(joint work with Pierrick Gaudry)

INRIA Futurs & Laboratoire d'Informatique (LIX)
École polytechnique
France
enge@lix.polytechnique.fr
<http://www.lix.polytechnique.fr/Labo/Andreas.Eng>

The 10th Workshop on Elliptic Curve Cryptography — ECC 2006
September 19, 2006



The discrete logarithm problem (DLP)

Given $b = a^x$ in some group, find x .
Given $b = x \cdot a$ in some group, find x .

The subexponential function L

$$L_N(\alpha, c) = e^{(c+o(1))(\log N)^\alpha (\log \log N)^{1-\alpha}}, \alpha \in (0, 1), c > 0$$

- $\alpha = 0$: $(\log N)^c$
- $\alpha = 1$: N^c
- $L_N(\alpha, c_1) \cdot L_N(\alpha, c_2) = L_N(\alpha, c_1 + c_2)$
- $(\log N)^k \in L_N(\alpha, 0)$
- $L_{q^g}(\alpha, c) \approx q^{c g^\alpha} \approx q^{g^\alpha}$ **number of elements**
- $\log_q L_{q^g}(\alpha, \cdot) \approx g^\alpha$ **degree of elements**

1 Discrete logarithms in $L(1/2)$

- \mathbb{F}_{2^g}
- Algebraic curves

2 Finding relations in $L(1/3)$

- \mathbb{F}_{2^g}
- Algebraic curves

3 Computing discrete logarithms

- Optimally unbalanced curves
- More balanced curves

Problem: Given $b = a^x \in \mathbb{F}_{2^g}^\times$, find x ; $\mathbb{F}_{2^g} = \mathbb{F}_2[X]/(f(X))$

- elements
polynomials over \mathbb{F}_2 of degree $< g$
- prime elements
irreducible polynomials
- size function $\longrightarrow \mathbb{R}^+$, homomorphic
deg
- factor base of prime elements up to some smoothness bound B
 $\mathcal{F} = \{p_1, \dots, p_n\}$
- non-unique decomposition into prime elements

$$r(X) = \prod p_i^{e_i}$$

$$r(X) + (X^4 + 1)f(X) = \prod p_i^{f_i}$$

relation $\prod p_i^{e_i - f_i} = 1$

Subexponential algorithm for \mathbb{F}_{2^g}

- Take random $\alpha_j, \beta_j \in \mathbb{Z}$ and compute

$$a^{\alpha_j} b^{\beta_j} \bmod f, \text{ a polynomial over } \mathbb{F}_2 \text{ of degree } < g$$

- Sometimes, the result is \mathcal{F} -smooth (or B -smooth)

$$a^{\alpha_j} b^{\beta_j} = \prod_{i=1}^n p_i^{\alpha_{ij}}$$

$$\alpha_j + \beta_j x = \sum \alpha_{ij} \log_a p_i$$

- Linear algebra yields x (and the $\log_a p_i$)

Complexity

Depends on the choice of \mathcal{F}

- \mathcal{F} too small
 - ▶ small probability of smoothness
- \mathcal{F} too large
 - ▶ too many relations needed
 - ▶ linear algebra infeasible
- good compromise:
 - ▶ $B = \log_2 L_{2^g}(1/2, \sqrt{2}/2) \approx g^{1/2}$
 - ▶ $|\mathcal{F}| = L_{2^g}(1/2, \sqrt{2}/2) \approx 2^{g^{1/2}}$
 - ▶ smoothness probability $1/L_{2^g}(1/2, \sqrt{2}/2)$
- total complexity $L_{2^g}(1/2, \sqrt{2})$

1 Discrete logarithms in $L(1/2)$

- \mathbb{F}_{2^g}
- Algebraic curves

2 Finding relations in $L(1/3)$

- \mathbb{F}_{2^g}
- Algebraic curves

3 Computing discrete logarithms

- Optimally unbalanced curves
- More balanced curves

• elliptic curves

$$Y^2 = X^3 + aX + b, \quad g = 1$$

• hyperelliptic curves of genus g

$$Y^2 = f(X) = X^{2g+1} + \dots$$

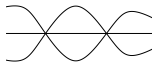


"Less simple" algebraic curves

• superelliptic curves

$$Y^n = f(X) = X^d + \dots, \quad g = \frac{(n-1)(d-1)}{2}$$

in particular: $Y^3 = X^4 + f_3X^3 + f_2X^2 + f_1X + f_0, \quad g = 3$

• $C_{n,d}$ curves

$$Y^n + h(X, Y) = X^d, \quad \text{terms in } h \text{ of small degree, } g = \frac{(n-1)(d-1)}{2}$$

in particular: $Y^3 + h(X)Y = X^4 + f(X), \quad \deg h \leq 2, \deg f \leq 3$

Divisors over $\overline{\mathbb{F}}_q$

• divisors = finite formal sums of points

$$D = \sum_{P \in C} m_P P, \quad m_P \in \mathbb{N}, \quad \text{almost all zero}$$

• prime elements = points

• Mumford representation

$$\begin{aligned} D &= (x_1, y_1) + \dots + (x_g, y_g) \\ &= (u, Y - v), \\ u &= (X - x_1) \cdots (X - x_g), \\ v &\text{ of degree } g - 1 \text{ s.t. } v(x_i) = y_i \end{aligned}$$

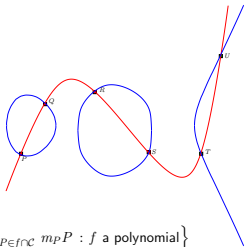
• prime elements = irreducible u

• adding

$$(u_1, v_1) + (u_2, v_2) = (u_1 u_2, v_3)$$

with v_3 the Lagrange interpolation polynomial (extended Euclidian algorithm)

• decomposition = factoring u



- $\text{Prin} = \left\{ \sum_{P \in J \cap \mathcal{C}} m_P P : f \text{ a polynomial} \right\}$
- $J = \text{Div} / \text{Prin}$
- $(P + Q) + (R + S) = (-T) + (-U) = \overline{T} + \overline{U}$ in J (**reduction**)
- **non-unique prime decomposition**

- **prime divisor** = orbit of points under the Galois group (Frobenius)
- **degree** = number of points in the divisor
- **example**
 - ▶ $(x, y) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$
 - ▶ set of k points (x^{q^i}, y^{q^i})
 - ▶ prime divisor of degree k :
 $(u, Y - v)$, u minimal polynomial of x over \mathbb{F}_q
- **adding**
 $\sum (u_i, Y - v_i) = (u, Y - v)$
 - ▶ $u = \prod u_i$
 - ▶ v s.t. $v \equiv v_i \pmod{u_i}$
- + reduction
- **prime decomposition** = factoring u
 $(u, Y - v) = \sum (u_i, Y - v_i)$
 - ▶ $u = \prod u_i$
 - ▶ $v_i = v \pmod{u_i}$

Subexponential algorithm

- **Riemann–Roch**: $\deg u \leq g$
- **Hasse–Weil**:
 - ▶ number of points over $\mathbb{F}_{q^k} \approx q^k$
 - ▶ number of prime divisors of degree $k \approx q^k/k$
 - ▶ $\#J \approx q^g = q^{g^2} \approx L_{q^g}(1, \cdot)$

The algorithm of \mathbb{F}_{2^g} applies...
... and has complexity $L_{q^g}(1/2, \sqrt{2})$

- at least for q fixed, $g \rightarrow \infty$
- more precisely for $g > \log q$

History

- **Aleman–DeMarrais–Huang 1994**
 - ▶ first subexponential algorithm for hyperelliptic curves
 - ▶ heuristic
- **Müller–Stein–Thiel 1999**
 - ▶ algorithm for infrastructure of real quadratic function fields
 - ▶ heuristic, since smoothness result missing
- **E. 2002**
 - ▶ first subexponential algorithm for hyperelliptic curves with proven complexity (smoothness result in **E.–Stein 2002**)
- **E.–Gaudry 2002**
 - ▶ unified framework for discrete logarithm algorithms in $L(1/2)$ (finite fields, class groups of number fields, Jacobians)
- **Couveignes 2001, Hess 2004**
 - ▶ proven $L(1/2)$ -algorithms for all major classes of curves
- exponential, but fast algorithms for smallish genus

- Assume there are $\approx q^k/k$ bricks of size k .
- Consider random towers of height $\log_q L_{q^g}(\alpha, \cdot)$.
- Interest yourself in those constructed from **small bricks** of size up to $\log_q L_{q^g}(\beta, \cdot)$.
- Then their proportion is

$$1/L_{q^g}(\alpha - \beta, \cdot)$$

- Application: $\alpha = 1, \beta = 1/2 \Rightarrow L(1/2)$
- $\alpha = 1, \beta = 2/3 \Rightarrow L(2/3)$
- $\alpha = 2/3, \beta = 1/3 \Rightarrow L(1/3)$



1 Discrete logarithms in $L(1/2)$

- \mathbb{F}_{2^g}
- Algebraic curves

2 Finding relations in $L(1/3)$

- \mathbb{F}_{2^g}
- Algebraic curves

3 Computing discrete logarithms

- Optimally unbalanced curves
- More balanced curves

Function field sieve for \mathbb{F}_{2^g}

$$\begin{array}{ccc}
 C : Y^d = F(X), & F \in \mathbb{F}_2[X], \deg F \approx d & \\
 \mathbb{F}_2[C] = \mathbb{F}_2[X, Y]/(Y^d - F) & \xrightarrow{Y \mapsto m(X)} & \mathbb{F}_2[X] \\
 \downarrow & & \downarrow \\
 \mathbb{F}_2[C]/\mathfrak{f} & \simeq & \mathbb{F}_2[X]/(f) \\
 \mathfrak{f} = (f(X), Y - m(X)) & \text{with } f \mid m^d - F & \\
 \\
 a(X) + b(X)Y & \mapsto & a(X) + b(X)m(X) \\
 \parallel & & \parallel \\
 \prod \mathfrak{p}_j^{f_j} & & \prod p_i^{e_i} \\
 \sum f_j \log(\mathfrak{p}_j) & = & \sum e_i \log p_i
 \end{array}$$

Complexity of the function field sieve

- $d = g^\delta$
- $\deg m = g/d = g^{1-\delta}$
- $\deg a, \deg b = g^\delta$

rational sieve

$$\begin{aligned}
 \deg(a + bm) &= \max(\deg a, \deg b + \deg m) \\
 &= g^\gamma + g^{1-\delta} \\
 &= g^{\max(\gamma, 1-\delta)}
 \end{aligned}$$

algebraic sieve

$$\begin{aligned}
 N_{\mathbb{F}_2[C]/\mathbb{F}_2[X]}(a + bY) &= (-a)^d - b^d F \\
 \deg \operatorname{div}(a + bY) &= \deg N \\
 &= d \deg b + \deg F \\
 &= g^{\delta+\gamma}
 \end{aligned}$$

$$\gamma = \delta = 1/3 \Rightarrow g^{2/3} \text{ for both}$$

- $L_{2g}(1/3)$ for the finite field \mathbb{F}_{2g}
- uses a curve over the base field \mathbb{F}_2
 - ▶ double representation of \mathbb{F}_{2g} as residual field, rational and algebraic
 - ▶ degree d of the curve gives additional degree of freedom
- **We already have a curve!**

1 Discrete logarithms in $L(1/2)$

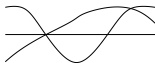
- \mathbb{F}_{2g}
- Algebraic curves

2 Finding relations in $L(1/3)$

- \mathbb{F}_{2g}
- Algebraic curves

3 Computing discrete logarithms

- Optimally unbalanced curves
- More balanced curves

 $C_{n,d}$ curves

- $Y^n + h(X, Y) = X^d$
terms in h of the form $X^i Y^j$ with $ni + dj < nd$
- unique place at infinity
- $g = \frac{(n-1)(d-1)}{2} \approx n \cdot d$
- $n \approx g^{1/3}$, $d \approx g^{2/3}$

Relations = divisors of polynomials

$$C : Y^n + h(X, Y) = X^d$$

- $n \approx g^{1/3}$, $d \approx g^{2/3}$
- $\varphi = a(X)Y + b(X)$
- $\deg a$, $\deg b \approx g^{1/3}$
- # affine zeroes = $\deg_X N_{\mathbb{F}_q[C]/\mathbb{F}_q[X]}(\varphi)$
 - ▶ $N(\varphi) = \text{Res}_Y(\varphi, C)$
 - ▶ $\deg N(\varphi) \leq \deg_X \varphi \cdot \deg_Y C + \deg_Y \varphi \cdot \deg_X C \approx 2g^{2/3}$
- affine divisor of degree $g^{2/3}$
- sum of prime divisors of degree $g^{1/3}$ with probability $1/L(1/3)$
⇒ relation

$$\mathcal{C} : Y^n + h(X, Y) = X^d$$

- [Adleman–DeMarrais–Huang 1994](#), applied to a special class of curves
- for small genus, essentially [Diem 2006](#)

- $n \approx g^{1/2}$, $d \approx g^{1/2}$
- $\varphi = a(X)Y + b(X)$
- $\deg a$, $\deg b \approx g^0$
- # affine zeroes = $\deg_X N_{\mathbb{F}_q[C]/\mathbb{F}_q[X]}(\varphi)$
 - ▶ $N(\varphi) = \text{Res}_Y(\varphi, \mathcal{C})$
 - ▶ $\deg N(\varphi) \leq \deg_X \varphi \cdot \deg_Y \mathcal{C} + \deg_Y \varphi \cdot \deg_X \mathcal{C} \approx 2g^{1/2}$
- affine divisor of degree $g^{1/2}$
- sum of prime divisors of degree $g^{1/4}$ with probability $1/L(1/4)$

Therefore not $L(1/4)$!

Application: Group structure computation

- size of the search space:

$$\underbrace{q^{g^{1/3}}}_{\#a} \cdot \underbrace{q^{g^{1/3}}}_{\#b} = q^{2g^{1/3}} \approx L(1/3) = \# \text{ trials}$$

- class of curves $\mathcal{C} : Y^n + h(X, Y)$ with h of degree d in X , $< n$ in Y
 - ▶ not necessarily $C_{n,d}$
 - ▶ $n \leq n_0 g^{1/3} \mathcal{M}^{-1/3}$
 - ▶ $d \leq d_0 g^{2/3} \mathcal{M}^{1/3}$
 - ▶ $\mathcal{M} = \frac{\log(g \log q)}{\log q}$
 - ▶ $g > \log^{2+\varepsilon} q$
- algorithm
 - ▶ Compute an approximation to $h = \#J(\mathcal{C})$ within a factor of 2.
 - ▶ Fix smoothness bound $B = \log_q L_{q^g}(1/3, \rho)$.
 - ▶ Enumerate factor base \mathcal{F} .
 - ▶ Fill a matrix of size $L_{q^g}(1/3, \rho)$ with relations.
 - ▶ Compute the Smith normal form of the matrix.
 - ▶ Return h and generators of the group.
- running time depends on n_0 and d_0
 $L_{q^g}(1/3, > 25/24)$

1 Discrete logarithms in $L(1/2)$

- \mathbb{F}_{2^g}
- Algebraic curves

2 Finding relations in $L(1/3)$

- \mathbb{F}_{2^g}
- Algebraic curves

3 Computing discrete logarithms

- Optimally unbalanced curves
- More balanced curves

$$C : Y^n + h(X, Y) = X^d$$

- $n \approx g^{1/3}$, $d \approx g^{2/3}$
- Given $E = xD$, find x .
- need relations with D and E (or a linear combination of them)
- problem: fixed divisors of degree $g = g^1$
- broken into pieces of degree $g^{2/3}$ in time $L(1/3)$ (construction kit lemma)

Special Q -sieveSolution: Spend some more time $L(1/3 + \varepsilon)$

$$Q = \text{div}(u, Y - v), \quad \deg u, \deg v = g^{2/3}$$

- φ going through Q
- $\varphi = au + b(Y - v) = (au - bv) + bY$
- $\deg_X \varphi \approx g^{2/3}$
- affine divisor of degree g^1
- broken into pieces of degree $g^{2/3}$ in time $L(1/3)$

- divisor of degree g broken into pieces of degree $g^{2/3-\varepsilon}$ in time $L(1/3 + \varepsilon)$

special Q -sieve

- $Q = (u, Y - v)$, $\deg u, \deg v = g^{2/3-\varepsilon}$
- $\varphi = au + b(Y - v) = (au - bv) + bY$
- $\deg_X \varphi \approx g^{2/3-\varepsilon}$
- affine divisor of degree $g^{1-\varepsilon}$
- broken into pieces of degree $g^{2/3-2\varepsilon}$ in time $L(1/3 + \varepsilon)$

- tree of special Q
- height $\leq 1 + (1/3)/\varepsilon$
- fan-out bounded by g (on average $g^{1/3}$)
- number of nodes $\approx g^{1/(3\varepsilon)}$
polynomial in $g!$

$$L(1/3 + \varepsilon/2, c + o(1)) \subseteq L(1/3 + \varepsilon, o(1))$$

$$L_{q^0}(1/3 + \varepsilon, c + o(1))$$

Solution: Increase the degree in Y

Running time

- $Q = (u, Y - v)$
 $= [u, Y - v_1, Y^2 - v_2, Y^3 - v_3, \dots], v_i = v^i \bmod u$
- $\deg u = \deg v_i = g^\alpha$
- $\varphi = \sum_{i=1}^k r_i(Y^i - v_i) = - \underbrace{\sum_{i=1}^k r_i v_i}_{g^{1/3} \deg} + \underbrace{\sum_{i=1}^k r_i Y^i}_{dg^{1/3+kg^{2/3}}}; \deg r_i = d$
- put $d = kg^{1/3}$
- degree of $\sum r_i v_i$: $d + g^\alpha$
- degrees of freedom: kd
- need $kd = g^\alpha$
- $k = g^{\alpha/2-1/6}, d = g^{\alpha/2+1/6}$, degree of divisor $g^{\alpha/2+1/2}$
- smoothing in time $L(1/3)$ towards $g^{\alpha/2+1/6}$

- tree of special Q
- height $\leq g^{2/3}$
- fan-out bounded by g
- number of nodes $\leq g^{4/3}$
polynomial in $g!$

$$L_{q^0}(1/3, c + o(1))$$

1 Discrete logarithms in $L(1/2)$

- \mathbb{F}_{2^g}
- Algebraic curves

2 Finding relations in $L(1/3)$

- \mathbb{F}_{2^g}
- Algebraic curves

3 Computing discrete logarithms

- Optimally unbalanced curves
- More balanced curves

$$C : Y^n + h(X, Y) = X^d$$

- $n \approx g^\alpha$, $d \approx g^{1-\alpha}$, $\alpha \in [1/3, 1/2]$
- $\varphi = a_0(X) + a_1(X)Y + \dots + a_k(X)Y^k$
- $\deg a_i = g^{2/3-\alpha}$, $k = g^{\alpha-1/3}$
- $\deg N(\varphi) \leq \deg_X \varphi \cdot \deg_Y C + \deg_Y \varphi \cdot \deg_X C \approx 2g^{2/3}$
- relations and group structure in $L(1/3)$
- discrete logarithms in $L(\alpha + \epsilon)$

Conclusion

First algorithm solving the discrete logarithm problem for algebraic curves in $L(1/3)$

Outlook

- further class of curves by Diem
- characterise all curves with an algorithm in $L(1/3)$?