The function field sieve in the medium prime case

Complexity analysis of discrete logarithms in all finite fields

Antoine Joux
DGA
and
University of Versailles St-Quentin-en-Yvelines
France

Joint work with Reynald Lercier

Index calculus algorithms

- A general algorithmic approach to solve:
  - Factoring problems
  - Discrete logarithms in finite fields
- Two main subcases:
  - Number field sieve (factoring and DL in medium to large char.)
  - Function field sieve (DL in small to medium char.)

Previously known complexity results

- Complexity usually expressed as:

$$L_Q(\alpha, c) = \exp((c + o(1))(\log Q)^\alpha (\log\log Q)^{1-\alpha}).$$

- Two extreme (well known) cases:
  - $\mathbb{F}_p$, with p a large prime. NFS yields a

$$L_p(1/3, \left(\frac{64}{9}\right)^{1/3})$$

    complexity.
  - $\mathbb{F}_{p^n}$, with fixed (small) p. FFS yields a

$$L_{p^n}(1/3, \left(\frac{32}{9}\right)^{1/3})$$

    complexity.

- In between, the best known result was $L(1/2)$.

This talk

- Revisit the FFS, for DL in $\mathbb{F}_Q$, where $Q = p^n$.
  - For p up to $L_Q(1/3)$
  - Works without function fields

Overall strategy

- As in any index calculus approach, general setup followed by:
  - Sieving
  - Linear algebra
  - Individual logarithms

Basic case (Setup)

- Assume $p = L_Q(1/3, c)$
- Thus:

$$n = \frac{1}{c} \left(\frac{\log Q}{\log \log Q} \right)^{2/3}.$$

- Choose two univariate polynomials f_1 and f_2
  with degrees d_1 and d_2 and $d_1 d_2 \geq n$.
- Such that $\mathrm{Res}(y - f_1(x), x - f_2(y))$ has:
  an irreducible factor of degree n (modulo p).

Basic case (Setup/Sieving)

- Irreducible factor: $I_x(x)$ or $I_y(y)$
- Two definitions of the (same) finite field $\mathbb{F}_{p^n}$
- Both x and y have well defined images α and β in $\mathbb{F}_{p^n}$.

- Take elements of the form:

$$\alpha\beta + a\alpha + b\beta + c \quad \text{or} \quad a\alpha + \beta + b$$

- In this expression, replace β by $f_1(\alpha)$
- Or replace α by $f_2(\beta)$

Basic case (Sieving)

- Yields an equation:

$$h_1(\alpha) = h_2(\beta).$$

- Where h_1 (resp. h_2) has degree $d_1 + 1$ (resp. $d_2 + 1$)
- Good case:
  - h_1 and h_2 split into linear factors
- Multiplicative equality (up to a constant in $\mathbb{F}_p$)
  - Between terms $\alpha + \mathfrak{a}$ and $\beta + \mathfrak{b}$.

Example: $\mathbb{F}_{65537^{25}}$

- Take $f_1(x) = x^5 + x + 3$ and $f_2(y) = -y^5 - y - 1$
- Then:

$$\begin{aligned} I_x(x) &= x^{25} + 5x^{21} + 15x^{20} + 10x^{17} + 60x^{16} + 90x^{15} + 10x^{13} + \\ &\quad 90x^{12} + 270x^{11} + 270x^{10} + 5x^9 + 60x^8 + 270x^7 + \\ &\quad 540x^6 + 407x^5 + 15x^4 + 90x^3 + 270x^2 + 407x + 247 \\ I_y(y) &= y^{25} + 5y^{21} + 5y^{20} + 10y^{17} + 20y^{16} + 10y^{15} + \\ &\quad 10y^{13} + 30y^{12} + 30y^{11} + 10y^{10} + 5y^9 + 20y^8 + \\ &\quad 30y^7 + 20y^6 + 7y^5 + 5y^4 + 10y^3 + 10y^2 + 7y - 1 \end{aligned}$$

Example: $\mathbb{F}_{65537^{25}}$

- Take the element $\beta + 2\alpha - 20496$
- It can be written as:

$$\alpha^5 + 3\alpha - 20493 =$$

$$(\alpha + 2445) \cdot (\alpha + 9593) \cdot (\alpha + 31166) \cdot (\alpha + 39260) \cdot (\alpha + 48610)$$

- Or as:

$$-2\beta^5 - \beta - 20498 =$$

$$-2(\beta + 1946) \cdot (\beta + 17129) \cdot (\beta + 18727) \cdot (\beta + 43449) \cdot (\beta + 49823)$$

- Linear equation between terms $\log(\alpha + \mathfrak{a})$ and $\log(\beta + \mathfrak{b})$ modulo $(p^n - 1)/(p - 1)$

Example: $\mathbb{F}_{65537^{25}}$ (Linear algebra)

- Cardinality of $\mathbb{F}^*_{65537^{25}}$:

  $$65536 \cdot 3571 \cdot 37693451 \cdot 137055701 \cdot 10853705894563968937051 \cdot P_{247}$$

- We compute the linear algebra modulo $q_0 = (p^n - 1)/(65536 \cdot 3571)$, and find:

  $$\begin{aligned} l &= 958054108800932348422988982145333938294343045945453623482 4\\ & 84037548352401735322970633432318492972385332094443948 5, \\ m &= 4649571275692520918560124050338108397005057301288170051718\\ & 556686238431642289730613529631676496393555258546887691 \end{aligned}$$

  the logarithms of $\alpha + 1$ and β in base α.

Complexity analysis

- Linear system in $2p$ unknowns
- For each candidate, the (heuristic) probability of success is:

$$\frac{1}{(d_1+1)!} \cdot \frac{1}{(d_2+1)!}$$

- Expected number of candidates (sieving time):

$$2p(d_1+1)! \cdot (d_2+1)!$$

- Time for solving the sparse linear system:

$$O((d_1+d_2)p^2)$$

Complexity analysis

- With $d_1 \approx d_2 \approx \sqrt{n}$
- The complexities written as $L_Q(1/3)$ become:
  - Linear algebra:

$$O((d_1 + d_2)p^2) = L_Q(1/3, 2c)$$

  - Sieving:

$$2p(d_1 + 1)! \cdot (d_2 + 1)! = L_Q(1/3, c + \frac{2}{3\sqrt{c}})$$

- Important constraint: size of sieving space $p^3 = L_Q(1/3, 3c)$

Complexity analysis of the basic case

- The algorithm is valid when:

$$3c \geq c + \frac{2}{3\sqrt{c}} \quad \text{or} \quad c \geq (1/3)^{2/3}$$

- Complexity: $L_Q(1/3, c + \max(c, \frac{2}{3\sqrt{c}}))$
- Minimum at $c = (1/3)^{2/3}$, complexity $L_Q(1/3, 3^{1/3})$

Individual logarithm: example in $\mathbb{F}_{65537^{25}}$

- Logarithm to find:

$$\lambda = \sum_{i=0}^{24} (\lfloor \pi \cdot 65537^{i+1} \rfloor \bmod 65537)\alpha^i = 41667\alpha^{24} + \cdots + 9279.$$

- First step, write $\lambda = 9828 \cdot N/D$ with:

$$\begin{aligned}
N &= (\alpha + 20471) \cdot (\alpha + 25396) \cdot (\alpha + 34766) \cdot \\
&\quad (\alpha + 54898) \cdot (\alpha^2 + 29819\alpha + 6546) \cdot (\alpha^2 + 44017\alpha + 38392) \cdot \\
&\quad (\alpha^2 + 54060\alpha + 4880) \cdot (\alpha^3 + 23811\alpha^2 + 6384\alpha + 3243) \\
D &= (\alpha + 18919) \cdot (\alpha + 31146) \cdot (\alpha + 38885) \cdot \\
&\quad (\alpha + 53302) \cdot (\alpha^2 + 52365\alpha + 2605) \cdot \\
&\quad (\alpha^3 + 29795\alpha^2 + 54653\alpha + 7616) \cdot (\alpha^3 + 57354\alpha^2 + 37421\alpha + 53988)
\end{aligned}$$

- Second step, compute each log. by descent

Starting the descent

- Take element:

$$(1493\,\alpha + 1)\beta - (40653\,\alpha^2 + 26561\,\alpha + 44820)$$

- Equal to:

$$1493\,\alpha^6 + \alpha^5 - 39160\,\alpha^2 - 22081\,\alpha - 44817 =$$
$$1493 \cdot (\alpha + 1964) \cdot (\alpha^2 + 2977\alpha + 33882) \cdot (\alpha^3 + 23811\alpha^2 + 6384\alpha + 3243)$$

- And also to:

$$24884\,\beta^{10} + 48275\,\beta^6 + 10792\,\beta^5 + 23391\,\beta^2 + 9300\,\beta + 6625 =$$
$$24884 \cdot (\beta + 14197) \cdot (\beta + 14995) \cdot (\beta + 25133) \cdot (\beta + 56789) \cdot$$
$$(\beta^2 + 14732\beta + 57516) \cdot (\beta^2 + 20454\beta + 37544) \cdot (\beta^2 + 50311\beta + 36703)$$

The descent ... continued

- Take element:

$$21022\,\alpha\beta + \alpha + 17943\,\beta + 65126$$

- Equal to:

$$\begin{aligned}
&21022\,\alpha^6 + 17943\,\alpha^5 + 21022\,\alpha^2 + 15473\,\alpha + 53418 = \\
&21022 \cdot (\alpha + 19091) \cdot (\alpha + 36728) \cdot (\alpha + 38567) \cdot (\alpha + 38593) \\
&\qquad \cdot (\alpha + 56621) \cdot (\alpha + 64596)
\end{aligned}$$

- And also to:

$$\begin{aligned}
&44515\,\beta^6 - \beta^5 + 44515\,\beta^2 + 62457\,\beta + 65125 = \\
&44515 \cdot (\beta + 148) \cdot (\beta + 1344) \cdot (\beta + 15752) \cdot (\beta + 47579) \\
&\qquad \cdot (\beta^2 + 50311\beta + 36703)
\end{aligned}$$

Individual logarithm: example in $\mathbb{F}_{65537^{25}}$

- Finally:

$$4053736945052440744587988507271545773377910517074639935754736$$
$$3481852609028577772820085371649268383536448936947412841469999$$

is the logarithm of λ in basis 3α.

General case (smaller values of p)

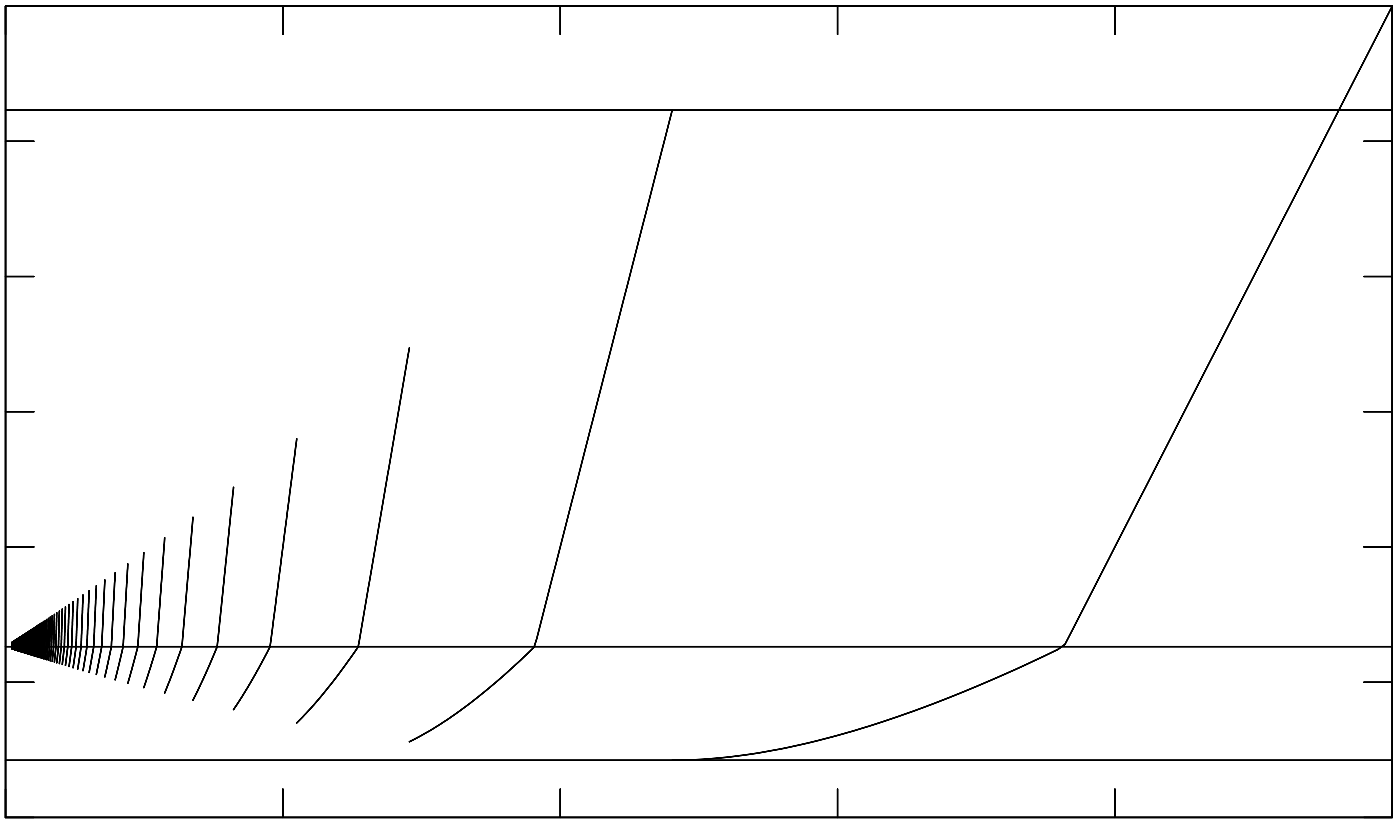
- Family of algorithms, parametrized by D
- Sieve over elements of the form:

$$f(\alpha)\beta + g(\alpha),$$

  where f and g are polynomials of degree D (f unitary).

- Similar analysis, optimal choice $d_1 \approx Dd_2$

Complexity of the general case when $p = L_Q(1/3)$



Complexity for $p = o(L_Q(1/3))$

- Here D is no longer a constant
- Instead take:

$$D = (2/3)^{2/3} \frac{\log(Q)^{1/3} \log\log^{2/3}(Q)}{\log(p)}$$

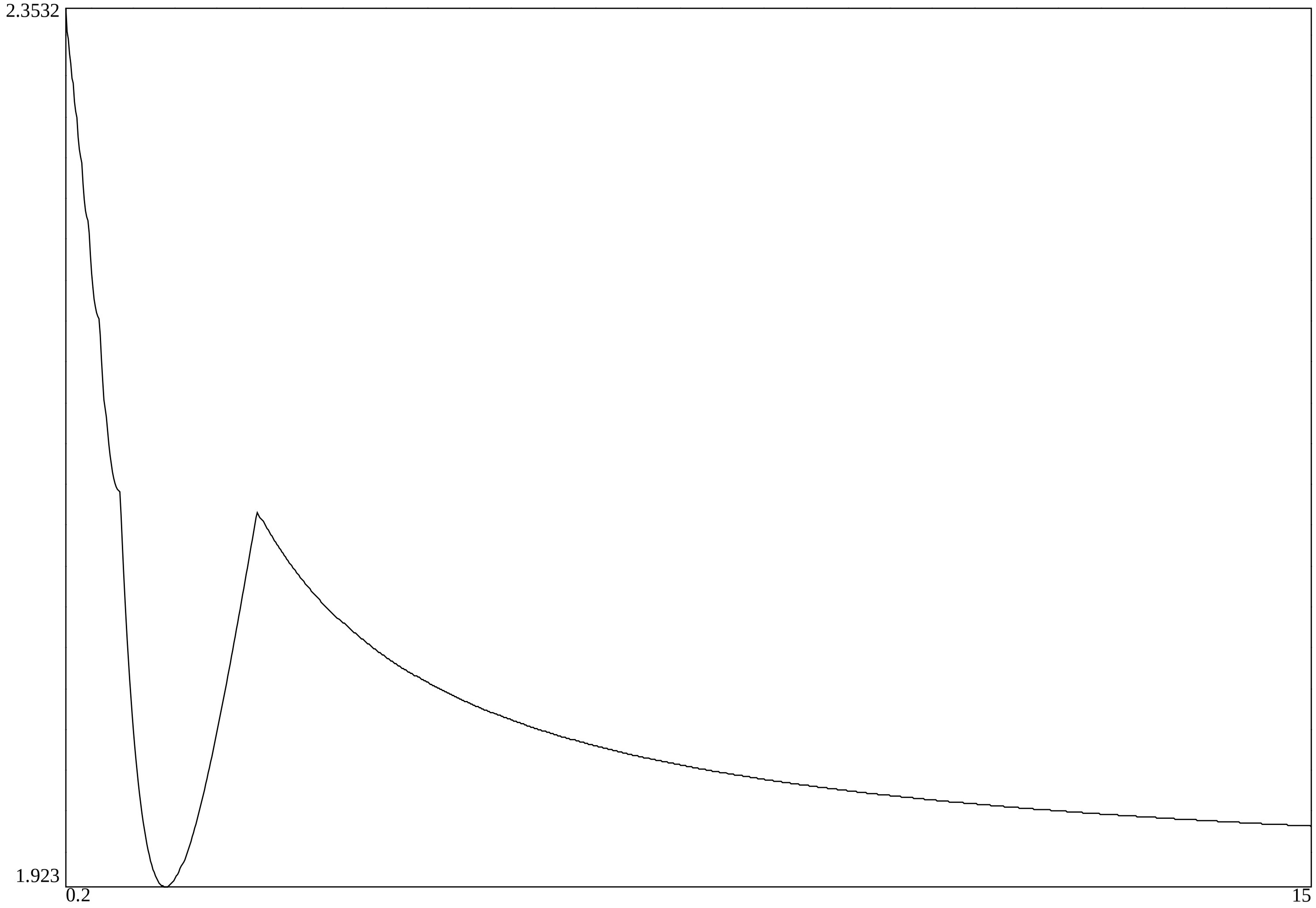
- With this choice:
  - Sieve space: $p^{(2D)} = L_Q(1/3, (32/9)^{1/3})$
  - Smoothness base size: $p^D = L_Q(1/3, (4/9)^{1/3})$
  - Smoothness probability:
    $exp(-2\sqrt(n/D)\log(2\sqrt(n/D)))) = L_Q(1/3, -(4/9)^{1/3})$
- Everything lines up correctly on total complexity:

$$L_Q(1/3, (32/9)^{1/3})$$

Complexity for all finite fields

- Three main zones:
  - For p up to $L_Q(1/3)$:
$$L_Q(1/3, (32/9)^{1/3})$$
  - For p from $L_Q(1/3)$ to $L_Q(2/3)$:
$$L_Q(1/3, (128/9)^{1/3})$$
  - For p above $L_Q(2/3)$:
$$L_Q(1/3, (64/9)^{1/3})$$
- Two transitions:
  - For FFS when $p = L_Q(1/3)$
  - For NFS when $p = L_Q(2/3)$

Complexity of the NFS when $p = L_Q(2/3)$


2.3532
1.923
0.2
15

Possible Extensions of FFS

- Use of Galois group to speed-up computations
- Very useful for $\mathbb{F}_{2^{nm}}$
- Also practical in other cases such as $\mathbb{F}_{370801^{30}}$
- Often need the description with function fields

Conclusion
Questions