A quasi-polynomial DL algorithm in small characteristic

R. Barbulescu, P. Gaudry, A. Joux and E. Thomé

http://hal.inria.fr/hal-00835446/

June 20, 2013

Recent improvements on DLP

- December-January, Joux: Create many relations from one, by composing with linear transforms. 1175 bits, then 1425 bits.

Recent improvements on DLP

- December-January, Joux: Create many relations from one, by composing with linear transforms. 1175 bits, then 1425 bits.
- February-March , Joux and Granger independently: sieve+linear algebra in polynomial time. Constant characteristic. 1971 bits (Granger), then 4080 (Joux). L(1/4+o(1)) descent for Joux using GB. Prime exponents possible by embedding.

Recent improvements on DLP

- December-January, Joux: Create many relations from one, by composing with linear transforms. 1175 bits, then 1425 bits.
- February-March , Joux and Granger independently: sieve+linear algebra in polynomial time. Constant characteristic. 1971 bits (Granger), then 4080 (Joux). L(1/4+o(1)) descent for Joux using GB. Prime exponents possible by embedding.
- April , Caramel: $GF(2^{809})$ using FFS.

Recent improvements on DLP

- December-January, Joux: Create many relations from one, by composing with linear transforms. 1175 bits, then 1425 bits.
- February-March , Joux and Granger independently: sieve+linear algebra in polynomial time. Constant characteristic. 1971 bits (Granger), then 4080 (Joux). L(1/4+o(1)) descent for Joux using GB. Prime exponents possible by embedding.
- April , Caramel: $GF(2^{809})$ using FFS.
- April-May , 6120 bits (Granger) and 6186 bits (Joux) using L(1/4) variants.

The new result

Main result

Let K be a finite field of the form $\mathbb{F}_{q^k}$. A discrete logarithm in K can be computed in heuristic time
$$\max(q, k)^{O(\log k)}.$$

Cases:

The new result

Main result

Let K be a finite field of the form $\mathbb{F}_{q^k}$. A discrete logarithm in K can be computed in heuristic time

$$\max(q, k)^{O(\log k)}.$$

Cases:

- $K = \mathbb{F}_{2^n}$, with prime n. Complexity is $n^{O(\log n)}$. Much better than $L_{2^n}(1/4 + o(1)) \approx n^{\sqrt[4]{n}}$.

The new result

Main result

Let K be a finite field of the form $\mathbb{F}_{q^k}$. A discrete logarithm in K can be computed in heuristic time

$$\max(q, k)^{O(\log k)}.$$

Cases:

- $K = \mathbb{F}_{2^n}$, with prime n. Complexity is $n^{O(\log n)}$. Much better than $L_{2^n}(1/4 + o(1)) \approx n^{\sqrt[4]{n}}$.
- $K = \mathbb{F}_Q$, $Q = q^k$, $q \approx k$. Complexity is $(\log Q)^{O(\log \log Q)}$, i.e. $L_Q(o(1))$.

The new result

Main result

Let K be a finite field of the form $\mathbb{F}_{q^k}$. A discrete logarithm in K can be computed in heuristic time

$$\max(q, k)^{O(\log k)}.$$

Cases:

- $K = \mathbb{F}_{2^n}$, with prime n. Complexity is $n^{O(\log n)}$. Much better than $L_{2^n}(1/4 + o(1)) \approx n^{\sqrt[4]{n}}$.
- $K = \mathbb{F}_Q$, $Q = q^k$, $q \approx k$. Complexity is $(\log Q)^{O(\log \log Q)}$, i.e. $L_Q(o(1))$.
- $K = \mathbb{F}_{q^k}$, with $q \approx L_{q^k}(\alpha)$. Complexity is $L_{q^k}(\alpha + o(1))$, i.e. better than FFS for $\alpha < 1/3$.

Setting

Same as for Joux's $L(1/4)$ algorithm.

$K = \mathbb{F}_{q^{2k}}$, with $k \approx q$.

repeat
  Take h_0 and h_1 in $\mathbb{F}_{q^2}[x]$, of small degree (2 should be ok).
until $h_1(X)X^q - h_0(X)$ has an irreducible factor of degree k

Rem. If $k > q$, then embed K in a larger field (hence the max in the complexity formula).

One step of descent

Proposition (under heuristic results)

Let $P(X) \in \mathbb{F}_{q^2}$ of degree $D < k$. In time polynomial in D and q, we can express $\log P$ as a linear combination $\sum e_i \log P_i$, where $\deg P_i \leq D/2$, and the number of P_i is in $O(q^2 D)$.

The main result follows easily:

- Analyze the size of the descent tree.
- The leaves are polynomials of degree 1. We know from previous work that their log can be computed in polynomial time in q.

The descent tree

Each node of the descent tree corresponds to one application of the Proposition, hence its arity is in $q^2 D$.

level	$\deg P_i$	breadth of tree
0	k	1
1	$k/2$	$q^2 k$
2	$k/4$	$q^2 k \cdot q^2 \frac{k}{2}$
3	$k/8$	$q^2 k \cdot q^2 \frac{k}{2} \cdot q^2 \frac{k}{4}$
$\vdots$	$\vdots$	$\vdots$
$\log k$	1	$\leq q^{2 \log k} k^{\log k}$

Total number of nodes $= q^{O(\log k)}$.

Each node yields a cost that is polynomial in q, hence the result.

One step of descent: how?

Start from the field equation:

$$X^q - X = \prod_{(\alpha:\beta)\in\mathbb{P}^1(\mathbb{F}_q)} (\beta X - \alpha),$$

Substitute $\frac{aP+b}{cP+d}$ to X, for $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}(2, \mathbb{F}_{q^2})$.

Idea: LHS is small and RHS is smooth.

Right hand side

$$
\begin{aligned}
(aP+b)^q(cP+d)-(aP+b)(cP+d)^q \\
&= \prod_{(\alpha:\beta)\in\mathbb{P}^1(\mathbb{F}_q)} \beta(aP+b)-\alpha(cP+d) \\
&= \prod_{(\alpha:\beta)\in\mathbb{P}^1(\mathbb{F}_q)} (\beta a-\alpha c)P+(\beta b-\alpha d) \\
&= \lambda \prod_{(\alpha:\beta)\in\mathbb{P}^1(\mathbb{F}_q)} P-m^{-1}\cdot(\alpha:\beta).
\end{aligned}
$$

Right-hand side is smooth:

All factors are in $\left\{P(X)-\gamma \mid \gamma\in\mathbb{F}_{q^2}\right\}$.

Left hand side

$$(aP+b)^q(cP+d)-(aP+b)(cP+d)^q =$$

Left-hand side is small:

Let the q-power come inside the formulae, and use $X^q \equiv h_0(X)/h_1(X)$.

Hence, modulo denominator cleaning, it is a polynomial of degree $O(\deg P)$.

Probability that LHS splits in polys of degree $\leq \frac{1}{2}\deg P$ is constant.

One step of descent: how?

Now, we let the matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ vary.

The RHS is the same as for $m = \mathrm{Id}$ if m is in $PGL(\mathbb{F}_q)$.

We must pick m among the cosets

$$\mathcal{P}_q = PGL_2(\mathbb{F}_{q^2})/PGL_2(\mathbb{F}_q).$$

For any $\mathfrak{q}$, the order of $PGL(\mathbb{F}_\mathfrak{q}) = \mathfrak{q}^3 - \mathfrak{q}$, so

$$\#\mathcal{P}_q = q^3 + q.$$

Conclusion: Have $\theta(q^3)$ relations; need q^2 to eliminate the right-hand sides. More than enough! (but heuristic)

Aanlysis

The essential heuristics of the analysis are:

- Usual «behave-like-random» assumption for LHS smoothness;
- Question of whether the matrix has full rank.

The matrix $H(P)$ made of the selected RHS is extracted from a bigger $\mathcal{H}$ of size $(q^3 + q) \times q^2$.

- We can prove that $\mathcal{H}$ has full rank.
- Experiments indicate that with overwhelming probability, random subsets of q^2 rows have full rank.
- Probably some finite geometry under the hood.

Will it blend?

Numerical expermients

- The heuristic seems to be ok on a few examples: we get enough relations to eliminate RHS and keep only $P(X)$ as a combination of the LHS.
- Need more to be sure.

Cross-over? Right now, not clear whether it has any practical interest.

- The arity $O(q^2 D)$ at each step is large !
- Have to compare with what can be achieved with a groebner tree of height 2.

But the simplicity and the complexity of this algorithm is interesting!

Stay tuned!

`http://hal.inria.fr/hal-00835446/`