Improving NFS for the discrete logarithm problem in non-prime finite fields

Polynomial selection and individual logarithm

Razvan Barbulescu, Pierrick Gaudry, *Aurore Guillevic*, François Morain

Institut national de recherche en informatique et en automatique (INRIA)

École Polytechnique/LIX

Centre national de la recherche scientifique (CNRS)

Université de Lorraine

AGCT 2015, May 20th

Our Work

- $\mathbf{F}_{p^2}$: target group of pairing-based cryptosystems
- Record computation of a Discrete Logarithm (DL) in $\mathbf{F}_{p^2}$ of 600 bits ($\log_2 p = 300$ bits)
- DL in $\mathbf{F}_{p^2}$ is 260 times faster than DL in $\mathbf{F}_{p'}$ of same size

➙ *serious consequences for pairing-based crypto*

- source code: `http://cado-nfs.gforge.inria.fr/`

Context : Discrete logarithm problem (DLP) in $\mathbf{F}_{p^n}^*$

In a subgroup $\langle g \rangle$ of $\mathbf{F}_{p^n}^*$ of order ℓ,

- $(g, x) \mapsto g^x$ is easy (polynomial time)
- $(g, g^x) \mapsto x$ is (in well-chosen subgroup) hard: DLP.

In our work:

- We attack DL in $\mathbf{F}_{p^2}$, starting point of $\mathbf{F}_{p^3}$, $\mathbf{F}_{p^4}, \ldots \mathbf{F}_{p^{12}}$
- p is large: quasi polynomial time algo. does NOT apply
- DLP in these $\mathbf{F}_{p^n}$ still asymptotically as hard as in the 90's
- consequences for pairing-based crypto: $\mathbf{F}_{p^2}$ target group

Practical improvements and new asymptotic complexities

L-notation: $Q = p^n$, $L_Q[1/3, c] = e^{(c+o(1))(\log Q)^{1/3}\ (\log\log Q)^{2/3}}$ for $c > 0$.

- DL in $\mathbf{F}_{p^n}$, small n, large p: complexity in $L_{p^n}[1/3, 1.92]$ (as for RSA modulus factorization) since the 90's
- $n \geq 2$: **two new polynomial selection methods**
- **great improvements in practice**
- **record of 600 bits**

Bonus: asymptotic complexity improvements in medium characteristic case

$\alpha = 1/3$	c, previous work	c, our work
DL in $\mathbf{F}_{p^n}$, $p = L_Q(2/3, c')$	$1.92 < c < 2.42$ ✗	1.74 ✓
DL in $\mathbf{F}_{p^n}$, medium p	2.42 ✗	2.20 ✓

MNFS variants: see [Pierrot15], Eurocrypt 2015.

Number Field Sieve algorithm for DL in $\mathbf{F}_{p^n}$

Number Field Sieve algorithm for DL in $\mathbf{F}_{p^n}$

1. *Polynomial Selection:* compute $f(x)$, $g(x)$ ➙define number fields K_f, K_g.

Number Field Sieve algorithm for DL in $\mathbf{F}_{p^n}$

1. *Polynomial Selection:* compute $f(x)$, $g(x)$ ➙define number fields K_f, K_g.

$$\begin{tikzcd}
 & \mathbf{Q}[x] \arrow[dl] \arrow[dr] & \\
\mathbf{Q}[x]/(f(x)) & & \mathbf{Q}[y]/(g(y))
\end{tikzcd}$$

Number Field Sieve algorithm for DL in $\mathbf{F}_{p^n}$

1. *Polynomial Selection:* compute $f(x),\ g(x)$ ➙define number fields K_f, K_g.

$$\begin{tikzcd}
 & \mathbf{Q}[x] \arrow[dl] \arrow[dr] & \\
\mathbf{Q}[x]/(f(x)) \arrow[dr, "\rho_f\ :\ x \mapsto z"'] & & \mathbf{Q}[y]/(g(y)) \arrow[dl, "\rho_g\ :\ y \mapsto z"] \\
 & \mathbf{F}_{p^n} = \mathbf{F}_p[z]/(\varphi(z)) &
\end{tikzcd}$$

Number Field Sieve algorithm for DL in $\mathbf{F}_{p^n}$

1. *Polynomial Selection:* compute $f(x),\ g(x)$ ➙define number fields K_f, K_g.
2. *Relation collection* between ideals of each number field.

$$\begin{tikzcd}[column sep=small]
 & \mathbf{Q}[x] \arrow[dl] \arrow[dr] & \\
a - bx \in \mathbf{Q}[x]/(f(x)) \arrow[dr, "\rho_f\ :\ x \mapsto z"'] & & \mathbf{Q}[y]/(g(y)) \ni a - by \arrow[dl, "\rho_g\ :\ y \mapsto z"] \\
 & \mathbf{F}_{p^n} = \mathbf{F}_p[z]/(\varphi(z)) &
\end{tikzcd}$$

Number Field Sieve algorithm for DL in $\mathbf{F}_{p^n}$

1. *Polynomial Selection:* compute $f(x),\ g(x)$ ➞define number fields K_f, K_g.
2. *Relation collection* between ideals of each number field.

$$\begin{tikzcd}
 & \mathbf{Q}[x] \arrow[dl] \arrow[dr] & \\
a - bx \in \mathbf{Q}[x]/(f(x)) \arrow[dr, "\rho_f\ :\ a - bx \mapsto a - bz"'] & & \mathbf{Q}[y]/(g(y)) \ni a - by \arrow[dl, "\rho_g\ :\ a - by \mapsto a - bz"] \\
 & \mathbf{F}_{p^n} = \mathbf{F}_p[z]/(\varphi(z)) &
\end{tikzcd}$$

Number Field Sieve algorithm for DL in $\mathbf{F}_{p^n}$

1. *Polynomial Selection:* compute $f(x),\ g(x)$ ➙define number fields K_f, K_g.
2. *Relation collection* between ideals of each number field.

$$\begin{tikzcd}[column sep=small]
 & \mathbf{Q}[x] \arrow[dl] \arrow[dr] & \\
a - bx \in \mathbf{Q}[x]/(f(x)) \arrow[dr, "\rho_f\ :\ a-bx \mapsto a-bz"'] & & \mathbf{Q}[y]/(g(y)) \ni a - by \arrow[dl, "\rho_g\ :\ a-by \mapsto a-bz"] \\
 & \mathbf{F}_{p^n} = \mathbf{F}_p[z]/(\varphi(z)) &
\end{tikzcd}$$

3. *Linear algebra modulo $\ell \mid p^n - 1$.*

➙ here we know the discrete log of a subset of ideals of K_f, K_g.

Number Field Sieve algorithm for DL in $\mathbf{F}_{p^n}$

1. *Polynomial Selection:* compute $f(x),\ g(x)$ ➙define number fields K_f, K_g.
2. *Relation collection* between ideals of each number field.

$$
\begin{tikzcd}
 & \mathbf{Q}[x] \arrow[dl] \arrow[dr] & \\
a - bx \in \mathbf{Q}[x]/(f(x)) \arrow[dr, "\rho_f \,:\; a - bx \mapsto a - bz"'] & & \mathbf{Q}[y]/(g(y)) \ni a - by \arrow[dl, "\rho_g \,:\; a - by \mapsto a - bz"] \\
 & \mathbf{F}_{p^n} = \mathbf{F}_p[z]/(\varphi(z)) &
\end{tikzcd}
$$

3. *Linear algebra modulo $\ell \mid p^n - 1$.*

➙ here we know the discrete log of a subset of ideals of $K_f,\ K_g$.

4. *Individual Logarithm.*

Relation collection

We need a high smoothness probability of

- ideals $(a - bx) \in K_f$, $(a - by) \in K_g$, $|a|, |b| < E$
- integers $Norm_{K_f/\mathbf{Q}}(a - bx)$ and $Norm_{K_g/\mathbf{Q}}(a - by)$
- we approximate $|Norm_{K_f/\mathbf{Q}}(a - bx)| \leq E^{\deg f} ||f||_\infty$ with $||f||_\infty = \max_{1 \leq i \leq \deg f} |f_i|$
- we want to minimize the product of norms:

$$E^{\deg f} ||f||_\infty E^{\deg g} ||g||_\infty$$

We need

- f, g of small degrees
- f, g of small coefficients

Relation collection

We need a high smoothness probability of

- ideals $(a - bx) \in K_f$, $(a - by) \in K_g$, $|a|, |b| < E$
- integers $Norm_{K_f/\mathbf{Q}}(a - bx)$ and $Norm_{K_g/\mathbf{Q}}(a - by)$
- we approximate $|Norm_{K_f/\mathbf{Q}}(a - bx)| \leq E^{\deg f} ||f||_\infty$ with $||f||_\infty = \max_{1 \leq i \leq \deg f} |f_i|$
- we want to minimize the product of norms:

$$E^{\deg f} ||f||_\infty E^{\deg g} ||g||_\infty$$

We need

- f, g of small degrees
- f, g of small coefficients

We cannot have both, we need to balance degrees and coefficient sizes.

A. Generalized Joux-Lercier method

Simplified version: $\deg f = n+1$, $\deg g = n$

1. choose f, $\deg f = n+1$, s.t.
2. $f \equiv \tilde{f}\varphi \bmod p$, φ a monic irreducible factor of degree n modulo p

$$\varphi(x) = \varphi_0 + \varphi_1 x + \cdots + x^n$$

3. Reduce the following matrix using LLL

$$M = \begin{bmatrix} p & & & \\ & \ddots & & \\ & & p & \\ \varphi_0 & \varphi_1 & \cdots & 1 \end{bmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix} p \\ \ddots \\ p \end{matrix}}\right\} \deg\varphi = n \text{ rows} \\ \} \ 1 \text{ row} \end{array} \to \mathrm{LLL}(M) = \begin{bmatrix} g_0 & g_1 & \cdots & g_n \\ & & & \\ & * & & \\ & & & \end{bmatrix}$$

4. $g = g_0 + g_1 x + \cdots + g_n x^n$, $||g||_\infty = O(p^{n/(n+1)})$

$$E^{\deg f + \deg g}||f||_\infty ||g||_\infty = E^{2n+1} O(p^{n/(n+1)})$$

A. Generalized Joux-Lercier method: example

- $p = 10000000019$ and $n = 2$
- $f = x^3 + x + 1$
- $\varphi = x^2 + 3402015304x + 6660167027$
- $M = \begin{bmatrix} p & & \\ & p & \\ \varphi_0 & \varphi_1 & 1 \end{bmatrix} \overset{\text{LLL}}{\to} g = 746193x^2 + 914408x + 4935648$
- $||f||_\infty = O(1)$, $||g||_\infty = O(p^{2/3})$

Historical remark:

- this construction appears in Barbulescu PhD thesis (2013)
- In January we were told about Matyukhin's work [МАТЮХИН 2006]: ЭФФЕКТИВНЫЙ ВАРИАНТ МЕТОДА РЕШЕТА ЧИСЛОВОГО ПОЛЯ ДЛЯ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ В ПОЛЕ GF(p^k).

B. The Conjugation Method for $\mathbf{F}_{p^2}$: example

1. $p = 7 \bmod 8$
2. $f = x^4 + 1$ irreducible over $\mathbf{Z}$, small
3. $f = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ over $\mathbf{Q}(\sqrt{2})$
4. $x^2 - 2$ has two roots $\pm \mathbf{r} \bmod p$
5. $\varphi = x^2 + \mathbf{r}x + 1$ is irreducible over $\mathbf{F}_p$ since $p \equiv 7 \bmod 8$, and over $\mathbf{Z}$
6. compute (u, v) s.t. $u/v \equiv \mathbf{r} \bmod p$, with $|u|, |v| \sim p^{1/2}$ with the *rational reconstruction* method
7. $g = vx^2 + ux + v \equiv v \cdot \varphi \bmod p$

Generalize to higher n:

- $\deg f = 2n$, $\deg g = n$, $||f||_\infty = O(1)$, $||g||_\infty = O(p^{1/2})$

$$E^{\deg f + \deg g} ||f||_\infty ||g||_\infty = E^{3n} O(p^{1/2})$$

Individual logarithm

- polynomial selection $\varphi(x)$, $\mathbf{F}_{p^n} = \mathbf{F}_p[x]/(\varphi(x))$, f, number field $K = \mathbf{Q}[\bar{x}]/(f(\bar{x})) = \mathbf{Q}[\alpha]$, map $\rho : \alpha \mapsto x \in \mathbf{F}_{p^n}$
- known logs of $\{\mathfrak{p}_i\}$, $\mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{p}_i) \leq B$
- random target $s = \sum_{i=0}^{n-1} s_i x^i \in \mathbf{F}_{p^n}$
- preimage $\bar{s} = \sum_{i=0}^{n-1} \bar{s}_i \alpha^i \in K$, with $\rho(\bar{s}_i) = s_i$,
- **needs B-smooth $\bar{s}$**, i.e. B-smooth $\mathrm{Norm}_{K/\mathbf{Q}}(\bar{s})$
- deduce *individual logarithm* $\log \bar{s}$, then $\log s$

Bottleneck: find B-*smooth* $\bar{s}$.
Loop over $g^e \cdot s$, g generator, in time $L_Q[1/3, c]$.

Norm bound

$$\mathrm{Norm}_{K/\mathbf{Q}}(\bar{s}) \le ||f||_\infty^{\deg \bar{s}}\ ||\bar{s}||_\infty^{\deg f}$$

- $||\bar{s}||_\infty = O(p)$
- $\deg \bar{s} = n - 1$
- JLSV$_1$: $||f||_\infty = O(p^{1/2})$ ✗
- gJL, Conj: $||f||_\infty = O(1)$ ✓
- $\deg f = n$ (JLSV$_1$), $n+1$ (gJL), $2n$ ✗(Conj)

➙Reduce $||\bar{s}||_\infty$
➙Reduce $\deg \bar{s}$

Do both, use subfield structure.

$\mathbf{F}_{p^2}$, Conjugation

- $f = x^4 + 1$
- $s = s_0 + s_1 x$
- $\mathbf{F}_{p^2}$ subfield: $\mathbf{F}_p$
- $s \leftarrow (1/s_1) \cdot s$ so $s_1 = 1$.

Define lattice

$$L = \begin{bmatrix} p & 0 & 0 & 0 \\ s_0 & 1 & 0 & 0 \\ \varphi_0 & \varphi_1 & 1 & 0 \\ 0 & \varphi_0 & \varphi_1 & 1 \end{bmatrix}$$

LLL outputs $\bar{r} \in \mathbf{Z}[x]$, with $||\bar{r}||_\infty \leq C_{\text{LLL}} \det(L)^{1/dim} = C_{\text{LLL}}\ p^{1/4}$, map $\bar{r}$ into K hence

$$\text{Norm}(\bar{r}) = O(p) \text{ instead of } \text{Norm}(\bar{s}) = O(p^2)$$

➙Do we have $\log \rho(\bar{r}) = \log s$?

We need $\log \rho(\bar{r}) = \log s$:

- LLL $\rightarrow \bar{r}$ linear combination of L rows.
- $\rho(\bar{r}) = \rho(a_1 p + a_2 \bar{s} + a_3 \varphi + a_4 x \varphi) \equiv u \cdot s \bmod (p, \varphi)$ with $u \in \mathbf{F}_p$
- $\log u = 0 \bmod \ell$ with $\ell \mid p+1$ since $u \in \mathbf{F}_p$
- hence $\log \rho(\bar{r}) \equiv \log s \bmod \ell$.

Running-time for finding a B-smooth decomposition, $\mathbf{F}_{p^2}$ with Conj method :

$$L_Q[1/3, \mathbf{1.14}] \text{ instead of } L_Q[1/3, \mathbf{1.44}]$$

Generalization:

- JLSV_1, gJL, Conj
- $\mathbf{F}_{p^{2m}}$, with $u \in \mathbf{F}_{p^2}$

Our Record: Discrete Logarithm in $\mathbf{F}_{p^2}$ of 600 bits

$$\begin{aligned} p &= 3141592653589793238462643383279502884197169399\backslash \\ \text{(300 bits)} & \quad 37510582097494459230781640628620899877709223 \\ p+1 &= 8 \cdot \ell \\ \ell &= 3926990816987241548078304229099378605246174\backslash \\ \text{(295 bits)} & \quad 921888227621868074038477050785776124847136 53 \\ p-1 &= 6 \cdot h_0 \text{ with } h_0 \text{ a 295 bit prime} \end{aligned}$$

- Cryptographic subgroup: G of order ℓ
- For our record: $Q = p^2$, $\log_2 Q = 600$, optimal value of E around $\log_2 E = 27$ bits.

Our Record: Discrete Logarithm in $\mathbf{F}_{p^2}$ of 600 bits

Polynomial selection:

- Generalized Joux Lercier: $f = x^3 + x + 1$, $||g||_\infty = O(p^{2/3})$, Norms bounded by $E^5 p^{2/3}$ of 339 bits ✗
- Conjugation: $f = x^4 + 1$, $||g||_\infty = O(p^{1/2})$, Norms bounded by $E^6 p^{1/2}$ of 317 bits →22 bits less ✓

$$
\begin{aligned}
f &= x^4 + 1 \\
g &= 448225077249286433565160965828828303618362474\ x^2 \\
&\quad - 296061099084763680469275137306557962657824623\ \ x \\
&\quad + 448225077249286433565160965828828303618362474\ .
\end{aligned}
$$

$||g||_\infty = 150$ bits

$$\varphi = x^2 + yx + 1, \quad \log_2 y = \log_2 p$$

Target:

$$
\begin{aligned}
s &= \lfloor(\pi(2^{298})/8)\rfloor x + \lfloor(\gamma \cdot 2^{298})\rfloor \in \mathbf{F}_{p^2} = \mathbf{F}_p[x]/(\varphi(x)) \\
gen &= x + 2
\end{aligned}
$$

Speed-up of Relation Collection and Linear Algebra

- Galois automorphism: $x \mapsto 1/x$ both for $f = x^4 + 1$ and $g = vx^2 + ux + v$
- $a - bx \mapsto -b + ax$: a second relation for free

➙ speed-up by a factor 2 for relation collection

➙ speed-up by a factor 4 for linear algebra

- others important algebraic simplification and speed-up

Finally,

$$\log_{gen} s \equiv 276214243617912804300337349268306605403758173\backslash$$
$$819414418610198322785683188853924304990580 12 \bmod \ell.$$

Record running-time comparison in years for 600-bit inputs

Algorithm	relation collection	linear algebra	total	
NFS Integer Factorization	5y	0.5y	5.5y	$\times 11$
NFS DL in $\mathbf{F}_p$	50y	80y	130y	$\times 260$
This work: NFS DL in $\mathbf{F}_{p^2}$	**0.4y**	**0.05y (GPU)**	**0.5y**	$\times 1$

DL in $\mathbf{F}_{p^2}$ $<$ Integer Factorization $<$ DL in $\mathbf{F}_p$

- Paper: `https://hal.inria.fr/hal-01112879`
- Algebraic secrets: `https://hal.inria.fr/hal-01052449`
- **Source code:** `http://cado-nfs.gforge.inria.fr/`

→ **Download it and solve your own DL in $\mathbf{F}_{p^2}$**

- *Stay tuned for more records during summer.*