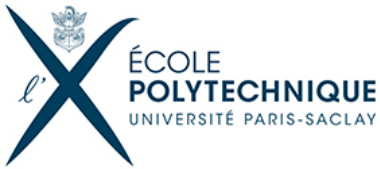
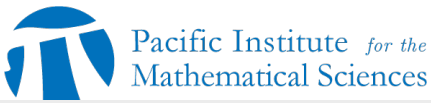
Discrete logarithm record in 508-bit and 600-bit finite fields GF(p^3) with the Number Field Sieve algorithm

Pierrick Gaudry, Aurore Guillevic, François Morain and Emmanuel Thomé

CNRS, University of Calgary, PIMS–CNRS, LIX–École Polytechnique, Inria, Loria

ANTS, September 1st, 2016





Discrete log record in a 170-bit MNT pairing-friendly curve by pairing reduction into 508-bit $\mathbb{F}_{p^3}$

Joint work with François Morain and Emmanuel Thomé.

[Miyaji Nakabayashi Takano 01] (MNT) pairing-friendly curve family

$E/\mathbb{F}_p : \; y^2 = x^3 + ax + b$, where

$a = 0$x22ffbb20cc052993fa27dc507800b624c650e4ff3d2

$b = 0$x1c7be6fa8da953b5624efc72406af7fa77499803d08

$p = 0$x26dccacc5041939206cf2b7dec50950e3c9fa4827af

$\ell = 0$xa60fd646ad409b3312c3b23ba64e082ad7b354d

such that

$$\begin{aligned} x_0 &= -0\text{x}732\text{c}8\text{cf}5\text{f}983038060466 \\ t &= 6x_0 - 1 \\ p &= 12x_0^2 - 1 \\ \#E(\mathbb{F}_p) &= p + 1 - t = 7^2 \cdot 313 \cdot \ell \end{aligned}$$

Polynomial Selection: Conjugation method

$$
\begin{aligned}
p &= 908761003790427908077548955758380356675829026531247 \\
&\quad \text{of 170 bits} \\
\varphi &= \gcd(f_0, f_1) \bmod p = x^3 - yx^2 - (y+3)x - 1, \\
&\quad \text{where } y \text{ is a root modulo } p \text{ of} \\
A &= 28y^2 + 16y - 109 \\
f_0 &= \mathrm{Resultant}_y(\varphi(x,y), A(y)) \\
f_0 &= 28x^6 + 16x^5 - 261x^4 - 322x^3 + 79x^2 + 152x + 28 \\
&\quad \|f\|_\infty = 8.33 \text{ bits} \\
\alpha(f_0) &= -2.9 \\
f_1 &= 247578151866391973704421 22x^3 + 408068970402536804717751 83x^2 \\
&\quad -334665485196639116395511 83x - 247578151866391973704421 22 \\
&\quad \|f_1\|_\infty = 85.01 \text{ bits} \\
\alpha(f_1) &= -4.1 \\
&\quad \text{Murphy's E value:} \\
\mathbb{E}(f_0, f_1) &= 1.31 \cdot 10^{-12}
\end{aligned}
$$

Relation Collection: sieving

Smoothness bound $B = 50000000 (= 2^{25.6})$ on both sides
Special-q in $[B, 2^{27}]$

660 core-days (4-core Intel Xeon E5520 @ 2.27GHz).

$57 \cdot 10^6$ relations $\rightarrow$ filtered $\rightarrow$
1982791 $\times$ 1982784 matrix with weight $w(M) = 396558692$.
The whole matrix would have 7 more columns for taking the 7 Schirokaurer Maps into account.

Linear Algebra (`cado-nfs`)

8 sequences in Block-Wiedemann algorithm.
8 Krylov sequences 250 core-days, four 16-code nodes / sequence
finding linear matrix generator 3.1 core-days / 64 cores
building solution 170 core-days
Reconstructed virtual logarithms for 15196345 out of the 15206761 elements of the bases (99.9%).

423 core-days on a cluster Intel Xeon E5-2650, 2.4GHz

Individual discrete logarithm

Take $P_0 = [x_P, y_P] \in E(\mathbb{F}_p)$,
$x_P = \lfloor \pi 10^{50} \rfloor = 31415926535897932384626433832795028841971693993751 0$
$y_P = \sqrt{x_P^3 + a x_P + b} = 46009557554793862769261828283576231059202772090793 0$
and set $\text{Target}_E = P = [7^2 \cdot 313]P_0$.

e is the reduced Tate pairing $e_\ell(P, Q)^{(p^3-1)/\ell}$

$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z} \simeq \langle G_1 \rangle \oplus \langle G_2 \rangle$ where
G_1 a generator of $E(\mathbb{F}_p)[\ell]$
G_2 a generator of second dim of r-torsion of $E(\mathbb{F}_{p^3})[\ell]$

Target in $\mathbb{F}_{p^3}$: $T = e(P, G_2)$, Basis: $g = e(G_1, G_2)$
Change $\mathbb{F}_{p^3} = \mathbb{F}_p[X]/(X^3 + X + 1)$ to $\mathbb{F}_p[Z]/(\varphi(Z))$

$$T = 0x11a2f1f13fa9b08703a033ee3c4321539156f865ee9 + 0x1098c3b7280ef2cf8b091d08197de0a9ba935ff79c6\ Z + 0x221205020e7729cb46166a9edfd5acb3bf59dd0a7d4\ Z^2$$

$$G_T = 0xd772111b150ec08f0ad89d987f1b037c630155608c + 0xf956cab6840c7e909abc29584f1aee48ccbd39d698\ Z + 0x205eb5b1e09f76bf0ef85efeaa3fdcb3827d43441b3\ Z^2$$

Individual discrete logarithm

Initial splitting: 32-core hours
preimage of g^{52154} in K_f has 59-bit-smooth norm
preimage of $g^{35313}T$ in K_f has 54-bit-smooth norm

Descent procedure: 13.4 hours.

Virtual log of g:
$\mathrm{vlog}(g) = 0x8c58b66f0d8b2e99a1c0530b2649ec0c76501c3$
virtual log of the target:
$\mathrm{vlog}(T) = 0x48a6bcf57cacca997658c98a0c196c25116a0aa$
Then $\log_g(T) = \mathrm{vlog}(T)/\mathrm{vlog}(g) \bmod \ell$.

$$\log(T) = \log(P) = 0x711d13ed75e05cc2ab2c9ec2c910a98288ec038 \bmod \ell \ .$$

Running-time comparison

record	relation col.	linear algebra	ind. log	total
Kleinjung 2007 530-bit $\mathbb{F}_p$	3.3 CPU-years 3.2 GHz Xeon64	14 years 3.2 GHz Xeon64	(few hours) 3.2 GHz Xeon64	17.3 years
BGGM 2014 529-bit $\mathbb{F}_{p^2}$	0.19 year 2.0 GHz E5-2650	30.3 *hours* NVidia GTX 680 graphic card	(few hours) 2.0 GHz E5-2650	0.2 year
BGGM 2015 512-bit $\mathbb{F}_{p^3}$	2.33 years	15 years	(few days) 2.4 GHz Xeon E5-2650	17.3 years
GMT 2016 **508-bit $\mathbb{F}_{p^3}$**	**1.81 years** 2.27GHz 4-core Xeon E5520	**1.16 years*** 2.4GHz Xeon E5-2650	(2 days) 2.27GHz 4-core Xeon E5520	**2.97 years**

* **linear algebra** modulo $\ell \sim p$ (where $\ell \mid p+1-t$) instead of $\ell \sim p^{\varphi(n)} = p^2$, (+ better polynomials + smaller matrix)
$\rightarrow$ much faster than previous 512-bit $\mathbb{F}_{p^3}$.

State of the art in prime field: 768-bit $\mathbb{F}_p$
Kleinjung–Diem–Lenstra–Priplata–Stahlke 2016
5300 core-years on 2.2 GHz Xeon E5-2660

Discrete log record in 180dd (593-bit) $\mathbb{F}_{p^3}$

Joint work with Pierrick Gaudry and François Morain.
NMBRTHY list announcement: August 15, 2016.
`https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;ae418648.1608`

Setting

generic prime $p = \lfloor 10^{59}\pi \rfloor + 3569289$ of 60 decimal digits
118dd prime-order subgroup ℓ s.t. $39\ell = p^2 + p + 1$

Polynomial selection: Conjugation method (6 core-days)

$$
\begin{aligned}
f_0 &= 20x^6 - x^5 - 290x^4 - 375x^3 + 15x^2 + 121x + 20 \\
f_1 &= 136638347141315234758260376470x^3 - 29757113352694220846501278313x^2 \\
&\quad -439672154776639925121282407723x - 136638347141315234758260376470 \\
\varphi &= \gcd(f_0, f_1) \mod p = x^3 - yx^2 - (y+3)x - 1, \\
&\quad \text{where } y \text{ is a root modulo } p \text{ of} \\
A(y) &= 20y^2 - y - 169
\end{aligned}
$$

discrete log record in 180dd (593-bit) $\mathbb{F}_{p^3}$

Relation collection: 9 core-years

Special-q lattice sieving, smoothness bound of 80M $= 2^{26.25}$,
large prime bound of 2^{28}.
Saved a factor 3 thanks to Galois σ.
Obtained 37705176 raw relations on side 0 and 36850254 on side 1.

Filtering

Duplicate removal: 48016023 unique relations (35.5% dup. rate)
Densification: 4.5M matrix, 200 coefs per row on average.

Linear algebra: 14 core-years

Block-Wiedemann algorithm with the 7 vectors of Schirokauer maps as input vectors for the $n = 7$ sequences.

Back-substitution (incl. Schirokauer maps): 32 core-days

Obtained the virtual logs of 98.7% of the ideals below 2^{28}.

discrete log record in 180dd (593-bit) $\mathbb{F}_{p^3}$

Generator of $\mathbb{F}_{p^3}$: $g = x + 5$
and target from the decimals of $e = \exp(1)$:

$$T = 271828182845904523536028747135266249775724709369995957496696\ x^2$$
$$+7627724076630353547594571382178525166427427466391932003059\ 9x$$
$$+2181741359662904357290033429526059563073813232862794349076\ 32$$

Individual discrete logarithm: 1 core-day

$$\log_g(T) = 534299829823865777675362637916832228131271219214173907\ 44 \backslash$$
$$427787489975365178688648857593262073182222695276991481809921\ 2 \bmod \ell$$

Total time: 23 core-years

180dd integer factorization: 5.6 core-years (Gaudry's talk SAC'14)
NFS-DL in GF(p), 180dd p: 131 core-years (BGIJT 14)
NFS-DL in GF(p^2), 180dd p^2: 0.5 core-years (BGGM 15)

discrete log record in 180dd (593-bit) $\mathbb{F}_{p^3}$

Generator of $\mathbb{F}_{p^3}$: $g = x + 5$
and target from the decimals of $e = \exp(1)$:

$$T = 271828182845904523536028747135266249775724709369995957496696\ x^2 + 762772407663035354759457138217852516642742746639193200305 99\ x + 218174135966290435729003342952605956307381323286279434907632$$

Individual discrete logarithm: 1 core-day

$$\log_g(T) = 534299829823865777675362637916832228131271219214173907 44\backslash 427787489975365178688648857593262073182222695276991481809 9212 \bmod \ell$$

Total time: 23 core-years

180dd integer factorization: 5.6 core-years (Gaudry's talk SAC'14)
NFS-DL in GF(p), 180dd p: 131 core-years (BGIJT 14)
NFS-DL in GF(p^2), 180dd p^2: 0.5 core-years (BGGM 15)

Thank you, Danke, Merci !