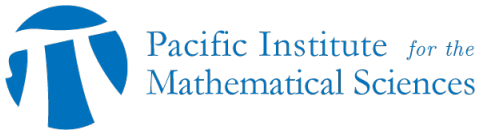
Faster individual discrete logarithms in $\mathrm{GF}(3^{6\cdot 509})$ and $\mathrm{GF}(3^{5\cdot 479})$

Aurore Guillevic

University of Calgary, PIMS–CNRS

ANTS
Kaiserslautern, Germany, August 31, 2016



ACCMORR DL record in GF($3^{6\cdot 509}$) of 4841 bits

Supersingular pairing-friendly curve

$$E/\mathbb{F}_{3^{509}} : y^2 = x^3 - x + 1, \quad \#E(\mathbb{F}_{3^{509}}) = 7\ell = 3^{509} - 3^{255} + 1$$

Tate Pairing: embed DL in $E(\mathbb{F}_{3^{509}})$ into $\mathbb{F}_{3^{6\cdot 509}}$: much faster
Adj, Canales-Martínez, Cruz-Cortées, Menezes, Oliveira, Rivera-Zamarripa, and Rodríguez-Henríquez computed a discrete logarithm in the 804-bit prime order $\ell = (3^{509} - 3^{255} + 1)/7$ subgroup of the cyclotomic subgroup of GF($3^{6\cdot 509}$).
`https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;65bedfc8.1607`

220 CPU years

Factor basis = { polynomials of degree 4 over GF(3^6) }

ACCMORR DL record in GF($3^{6 \cdot 509}$) of 4841 bits

computation	time (CPU years)	CPU freq (GHz)
computing logs of deg 4 polys (factor basis)		
relation gen + lin algebra	145	2.60
Individual discrete logarithm: from deg 508 to deg 4		
initial splitting		
continued fractions (Waterloo) 508 to 40	51.71	2.87
descent		
classical (40 to 21)	9.99	2.66
classical (21 to 15)	10.24	2.66
Gröbner bases, powers-of-2 (15 to 4)	6.27	3.00

ACCMORR DL record in GF($3^{6 \cdot 509}$) of 4841 bits

computation	time (CPU years)	CPU freq (GHz)
computing logs of deg 4 polys (factor basis)		
relation gen + lin algebra	145	2.60
Individual discrete logarithm: from deg 508 to deg 4		
initial splitting		
continued fractions (Waterloo) 508 to 40	51.71	2.87
New algo [G.16] deg 508 to 30	**0.75**	**2.40**
		Xeon E5-2609
descent		
classical (40 to 21)	9.99	2.66
classical (21 to 15)	10.24	2.66
Gröbner bases, powers-of-2 (15 to 4)	6.27	3.00

Initial Splitting

Algorithm 1: Generic Initial Splitting (or Boot or Smoothing step)

Input: Target $T_0 \in \mathbb{F}_{q^n}$, generator g, subgroup order ℓ, bound B

1 **repeat**
2 take t at random in $\{1, \ldots, \ell - 1\}$
3 $T \leftarrow g^t T_0$
4 $\mathbf{T} \leftarrow \texttt{PREIMAGE}(T)$
5 **until** $\mathbf{T}$ *is* B*-smooth*
6 **return** $\mathbf{T}, t$

Initial Splitting

Algorithm 2: Generic Initial Splitting (or Boot or Smoothing step)

Input: Target $T_0 \in \mathbb{F}_{q^n}$, generator g, subgroup order ℓ, bound B

1 **repeat**
2 take t at random in $\{1, \ldots, \ell - 1\}$
3 $T \leftarrow g^t T_0$
4 $\mathbf{T} \leftarrow \texttt{PREIMAGE}(T)$
5 **until** $\mathbf{T}$ *is* B*-smooth*
6 **return** $\mathbf{T}, t$

$\mathrm{GF}(3^{6 \cdot 509}) = \mathrm{GF}(3^6)[X]/(I(X))$ where $\deg I(X) = 509$
Blake–Fuji-Hara–Mullin–Vanstone'84(a.k.a Waterloo) algo:

$$T(X) \equiv U(X)/V(X) \bmod I(X) \text{ where } \deg U,\ \deg V \leq 254$$

Probability (two deg 254 polys over $\mathbb{F}_{3^6}$ are 40-smooth) $= 2^{-34}$

New algo: use subfields

$$\log T \equiv \log uT \bmod \ell \text{ for any } u \in \text{ subfield}$$

Largest subfield: $\mathrm{GF}(3^{3\cdot 509})$, $\{1, u, u^2, \ldots, u^{1526}\}$ polynomial basis

$$A \leftarrow \begin{bmatrix} T \\ uT \\ u^2 T \\ \vdots \\ u^{1526} T \end{bmatrix}$$

$E \leftarrow$ Row Echelon Form (A) ($\mathbb{F}_3$-linear combinations)

$T' \leftarrow$ Polynomial(1st row of E)

$$\deg T' = 254$$

and

Probability (one deg 254 poly over $\mathbb{F}_{3^6}$ is 30-smooth) $= 2^{-26.6}$

0.75 core-year instead of 51.71 core-years

[G.16] Preprint

Faster individual discrete logarithms in non-prime finite fields with the NFS and FFS algorithms

Proof-of-concept Magma implementation:

- Initial splitting 30-smooth in GF($3^{6 \cdot 509}$) in **0.75 core year** instead of 40-smooth one in 51.71 core years
- Initial splitting 50-smooth in GF($3^{5 \cdot 479}$) (one degree 383 poly instead of two degree 239 polys) in **0.14 core-year (52 days)** instead of 0.57 core-years (208 days)
- Large characteristic version with Pomerance and Barbulescu Early Abort Strategy
- faster descent (smaller inputs)

`https://hal.inria.fr/hal-01341849`