Rump session ANTS 11 — August 10, 2014

News on discrete logarithm

Razvan Barbulescu Pierrick Gaudry Aurore Guillevic
François Morain
France

Discrete logarithm in cryptography

In any mathematical group G

If g and h are given elements, FIND x, if it exists, such that

$$g^x = h.$$

Discrete logarithm in finite fields can be used in cryptology

- directly (DSA)
- indirectly (pairings–Gödel Prize 2013).

Attacks on pairings

Pairings strength relies on

- $GF(2^n)$ and $GF(3^n)$ quasi-polynomial (2013)

Attacks on pairings

Pairings strength relies on

- $GF(2^n)$ and $GF(3^n)$ quasi-polynomial (2013)
- $GF(p^{12})$ with p of special form SNFS (2013)

Attacks on pairings

Pairings strength relies on

- GF(2^n) and GF(3^n) — quasi-polynomial (2013)
- GF(p^{12}) with p of special form — SNFS (2013)
- GF(p^6) and GF(p^4) — MNFS (2014 at ANTS)

Attacks on pairings

Pairings strength relies on

- $GF(2^n)$ and $GF(3^n)$ — quasi-polynomial (2013)
- $GF(p^{12})$ with p of special form — SNFS (2013)
- $GF(p^6)$ and $GF(p^4)$ — MNFS (2014 at ANTS)
- $GF(p^2)$ and $GF(p^3)$ — classical NFS (2006)

Our team

I and ...

Pierrick

Aurore

François

The Number Field Sieve in GF(p^n)

Recall the algorithm

- Select two polynomials $f, g \in \mathbb{Z}[x]$ s. t.
  gcd(f mod p, g mod p) is irreducible of degree n

- collect coprime pairs $(a, b) \in \mathbb{Z}^2$ s. t.
  $\mathrm{Res}(a - bx, f)$ and $\mathrm{Res}(a - bx, g)$ are smooth

- solve a linear system to obtain discrete logarithms

Polynomial selection

- For GF(p) we use the base-m method as for factorization.
- For GF(p^n) we use LLL-based techniques $\Rightarrow$ worse polynomials than for factoring.

New polynomial selection method

Algorithm

Input: p prime and n an exponent
Output: $f, g \in \mathbb{Z}[x]$ for NFS in $\mathbb{F}_{p^n}$

1: Select $g_u(x), g_v(x) \in \mathbb{Z}[x]$, small coeffs, $\deg g_u < \deg g_v = n$
2: **repeat**
3: Select $\mu(x) \in \mathbb{Z}[x]$ of degree two, monic, irreducible, small coeffs
4: **until** $\mu(x)$ has a root λ in $\mathbb{F}_p$ and $g_v + \lambda g_u$ is irreducible in $\mathbb{F}_p$
5: $f \leftarrow \prod_{\omega \text{ complex root of } \mu} \left(g_v(x) + \omega g_u(x)\right)$
6: $(u, v) \leftarrow$ a rational reconstruction of λ
7: $g \leftarrow v g_v + u g_u$
8: **return** (f, g)

Example

Input $\mathbb{F}_{p^n}$ with $n = 11$ and $p = 134217931$
We try $a = 2, 3, 5, \ldots$ until $\sqrt{a}$ exists in $\mathbb{F}_p$ and $x^n - \sqrt{a}$ is irreducible. $a = 5$ works!

$f = (x^{11} - \sqrt{5})(x^{11} + \sqrt{5})$.
$g = vx^{11} - u = 10393x^{11} - 1789$, where $u/v \equiv \lambda = \sqrt{5} \mod p$
Output f and g, with $\gcd(f \bmod p, g \bmod p) = x^{11} - \sqrt{5}$.

Timings

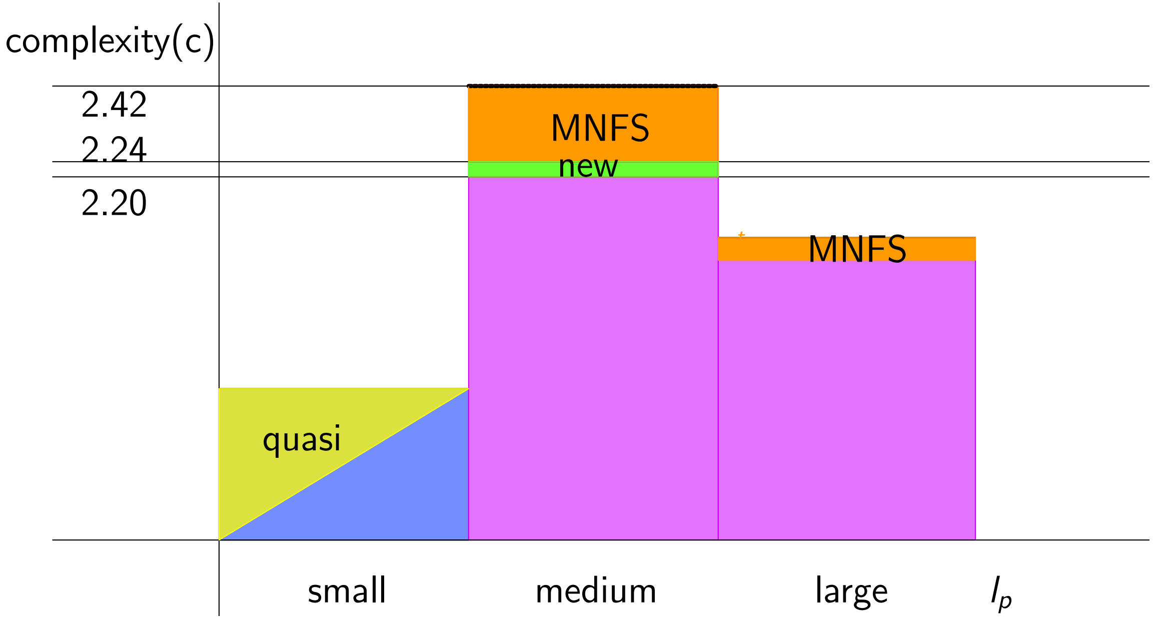
Comparing two fields of 160 decimal digits

field	author	sieve time	linear algebra time
GF(p)	Kleinjung 2007	3.3 years	14 years
GF(p^2)	our team 2014	68 days	12 days[a]

[a] 30 hours on GPU

New complexity

$p = L_{p^n}(l_p)$
Complexity $L_{p^n}(1/3, c)$ in non-small characteristic.



Where to read?

1. NMBRTHRY mailing list
   Discrete logarithms in GF(p^2) — 160 digits
   24 June 2014

2. Long description at
   http://hal.inria.fr/hal-01052449