Discrete Logarithms over Finite Fields $\mathbb{F}_p$ and $\mathbb{F}_{2^n}$ — Latest News

A. Joux (antoine.joux@m4x.org)

R. Lercier (reynald.lercier@m4x.org)

Integer Factorization: 15 years of improvements (Contini's table)

Number	#digits	When	GIPS years	Method	Who
C116	116	1990	0.3	MPQS	Lenstra et al.
RSA-120	120	June, 1993	0.8	MPQS	Lenstra et al.
RSA-129	129	April, 1994	5	MPQS	Lenstra et al.
RSA-130	130	April, 1996	1	GNFS	Lenstra et al.
RSA-140	140	February, 1999	2	GNFS	Lenstra et al.
RSA-155	155	August, 1999	8	GNFS	Lenstra et al.
C158	158	January, 2002	3.4	GNFS	Franke et al.
RSA-160	160	March, 2003	2.7	GNFS	Franke et al.
RSA-576	174	December, 2003	13.2	GNFS	Franke et al.
C176	176	May, 2005	48.6	GNFS	Aoki et al.
RSA-200	200	May, 2005	170	GNFS	Franke et al.

How About Discrete Logarithms in $\mathbb{F}_p$?

#digits	When	Who	GIPS years	Method
58	1991	Lamacchia-Odlyzko	< 0.01	Gaussian
65	1995	Weber	< 0.01	GNFS
85	1996	Weber	0.03	Gaussian
90	1998	Joux-Lercier	0.07	Gaussian
85	1998	Weber	0.05	GNFS
100	1999	Joux-Lercier	0.45	GNFS
110	2000	Joux-Lercier	0.17	GNFS
120	2001	Joux-Lercier	0.35	GNFS

Since 2001, nothing new ? ?

Only 0.35 GIPS years ?

News ! 130 digits done with a 1.2 GIPS years cost

- Announced on the NMBRTHRY mailing list, Saturday, June 18th 2005.
- 3 weeks, on a single 1.15 GHz 16-proc. HP AlphaServer GS1280.
- A degree 3/degree 2 lattice sieving (GNFS):
  - Factor Basis of size 400 000 (deg. 3) + 1 200 000 (deg. 2).
  - A 13 days computation yields 1 780 000 eq. with 1 550 000 unknowns.
- Linear algebra:
  - A novel variant of Structured Gaussian Elimination yields 433 000 eq. with 432 000 unknowns (35 000 000 non zero entries). Less than 15 minutes on only one processor.
  - 8 days for our parallelized version of Lanczos' algorithm.
- Individual Logarithms: quite tricky to implement but only few hours.

Discrete logarithms in $\mathbb{F}_{2^n}$

n	When	Who	GIPS years	Method
401	1992	Gordon-McCurley	0.2	Coppersmith
521	2002	Joux-Lercier	0.35	FFS
607	2002	Thomé	20	Coppersmith

From 521 to 607, we see a 19 GIPS years gap.

News ! 607 bits done at the cost of 1.6 GIPS years

- To be announced on the NMBRTHRY mailing list.
- 1 month, on a unique 1.15 GHz 16-proc. HP AlphaServer GS1280 12 times faster than Thomé's computation.
- A degree 5/degree 1 lattice sieving (FFS):
  - Factor Basis of size 765 925 (deg. 5) + 1 000 000 (deg. 1).
  - A 18 days computation yields 1 900 000 eq. with 1 700 000 unknowns.
- Linear algebra:
  - Structured Gaussian Elimination yields 366 000 eq. with 365 000 unknowns (104 000 000 non zero entries). Less than 15 minutes on only one processor.
  - 17 days for our parallelized version of Lanczos' algorithm (completed on Sunday, July 31 2005).
- Individual logarithms: Yet to be done.

Conclusion