Discrete Log Computation in a field of size p^{40} p is a 19-bit prime (728-bits)

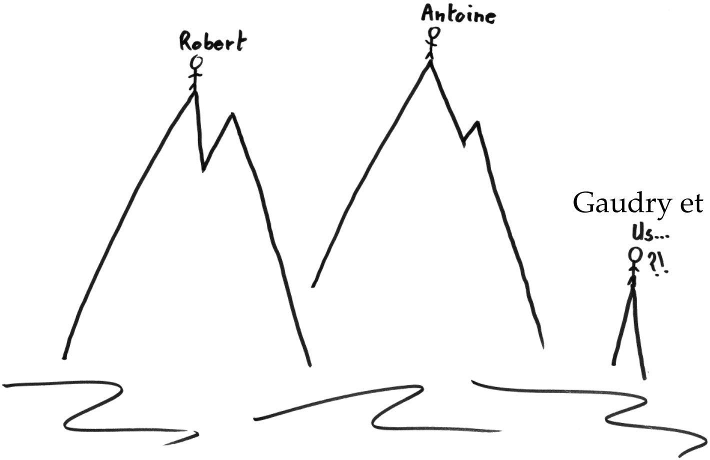
Palash Sarkar & Shashank Singh

Indian Statistical Institute, Kolkata

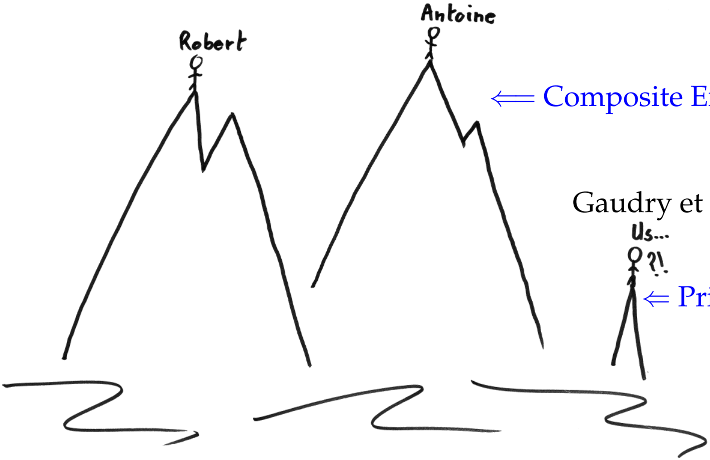
December 3, 2013

ASIACRYPT 2013-Rump Session

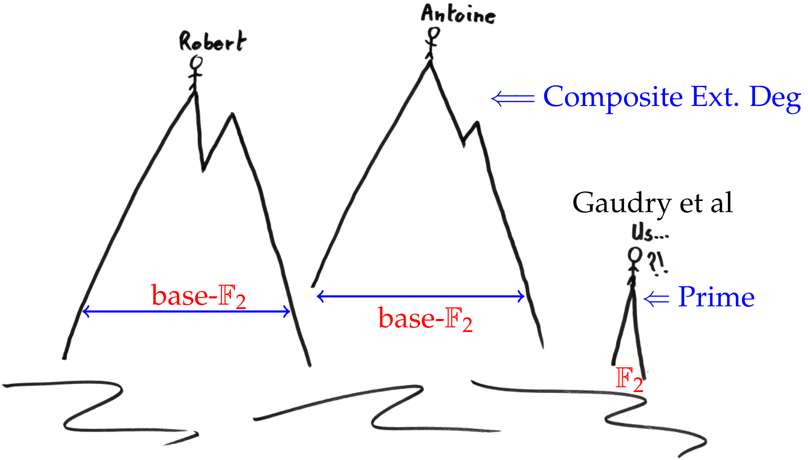
A Slide from Gaudry's ECC 2013 Talk



A SLIDE FROM GAUDRY'S ECC 2013 TALK



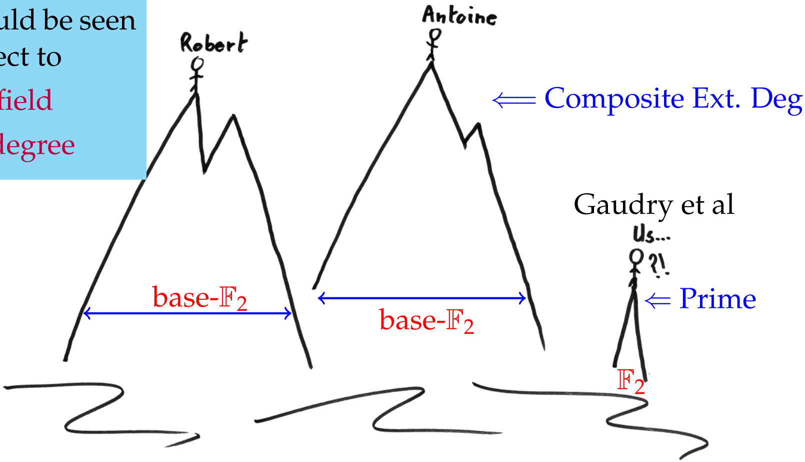
A Slide from Gaudry's ECC 2013 Talk



A Slide from Gaudry's ECC 2013 Talk

DL Records on finite fields should be seen with respect to

- Base field
- Ext. degree



DLP in the medium prime fields

- Antoine Joux, *Faster index calculus for the medium prime case. Application to a 1425-bits finite field.* - EUROCRYPT 2013. $GF(p^{57})$, p a 25-bit

DLP IN THE MEDIUM PRIME FIELDS

Antoine Joux, *Faster index calculus for the medium prime case. Application to a 1425-bits finite field.* - EUROCRYPT 2013. $GF(p^{57})$, p a 25-bit

Antoine Joux and Reynald Lercier, *The Function Field Sieve in the Medium Prime Case* - EUROCRYPT 2006. $GF(p^{30}), p = 370801$(556-bits) and $GF(p^{25})$, $p = 65537$(400-bits)

DLP IN THE MEDIUM PRIME FIELDS

Antoine Joux, *Faster index calculus for the medium prime case. Application to a 1425-bits finite field.* - EUROCRYPT 2013. $GF(p^{57})$, p a 25-bit

✓ Adv. pinpointing (Specific to Kummmer Type Extensions)
✓ Frobenius action simplifies Linear Algebra.

Antoine Joux and Reynald Lercier, *The Function Field Sieve in the Medium Prime Case* - EUROCRYPT 2006. $GF(p^{30})$, $p = 370801$(556-bits) and $GF(p^{25})$, $p = 65537$(400-bits)

DLP IN THE MEDIUM PRIME FIELDS

- Antoine Joux, *Faster index calculus for the medium prime case. Application to a 1425-bits finite field.* - EUROCRYPT 2013. $GF(p^{57})$ ...
  - ✓ Adv. pinpointing ...
  - ✓ Frobenius action simplifies linear algebra.
- Antoine Joux and Reynald Lercier, *The Function Field Sieve in the Medium Prime Case* - EUROCRYPT 2006. $GF(p^{30}), p = 370801$ (556-bits) and $GF(p^{25})$, $p = 65537$ (400-bits)

Our Records:

- ✓ Discrete Log Computation in $\mathbb{F}_{p^{40}}$, $p = 297079$ (728-bits)
- ✓ Discrete Log Computation in $\mathbb{F}_{p^{35}}$, $p = 65407$ (560-bits).

Discrete Log Computation in $\mathbb{F}_{p^{40}}$, $p = 297079$

- Function Field Sieve for medium prime case

$$g_1(x) = x^8$$
$$g_2(x) = x^5 + 44024x^4 + 224924x^3 + 77320x^2 + 291141x + 80867$$
$$f(x) = \text{Normalize}\left(x - g_2\left(g_1(x)\right)\right)$$

$$\mathbb{F}_{p^{40}} = \frac{\mathbb{F}[x]}{\langle f(x) \rangle},$$ with a primitive element $x + 3$

- Random element of the field

$$\Pi(x) = \text{Normalize}\left(\sum_{i=0}^{n-1} \left\lfloor \pi p^{i+1} \mod p \right\rfloor x^i\right)$$

Relation Collection:

Joux's Pinpointing Technique.

$\approx$ 20 CPU Hours @2.3 GHz

Linear Algebra:

- Lanczos, Pohlig Hellman and Pollard's rho
- 504 CPU (@ 2.3 Ghz) hours.

Relation Collection:

Joux's Pinpointing Technique.

$\approx$ 20 CPU Hours @2.3 GHz

Linear Algebra:

- Lanczos, Pohlig Hellman and Pollard's rho
- 504 CPU (@ 2.3 Ghz) hours.

Descent:(30000 CPU @2.30GHz hours)

Initial descents were pretty fast.

2-1 Descent

$$xy + ay^2 + by + \alpha x + \beta$$

$$L(x) = R(y)$$

$$= c_1 r_1(x) \prod_{a_i \in \mathbb{F}_p} (x + a_i)^{l} \quad \text{Good Case} \quad = c_2 \prod_{b_j \in \mathbb{F}_p} (y + b_j)^{m_j}$$

$$\Pi(x) = x^{39} + 154424x^{38} + 219291x^{37} + 2288x^{36} + 290227x^{35} + 295582x^{34} + 27398x^{33} + 200403x^{32} + 6836x^{31} + 123295x^{30} + 94923x^{29} + 89389x^{28} + 239023x^{27} + 115439x^{26} + 249309x^{25} + 196503x^{24} + 87998x^{23} + 240098x^{22} + 136326x^{21} + 191206x^{20} + 9602x^{19} + 53215x^{18} + 25787x^{17} + 17954x^{16} + 880x^{15} + 158602x^{14} + 241303x^{13} + 246920x^{12} + 52944x^{11} + 212605x^{10} + 234395x^{9} + 196868x^{8} + 106113x^{7} + 207883x^{6} + 198491x^{5} + 106250x^{4} + 165294x^{3} + 28548x^{2} + 76555x + 241986$$

$$\begin{aligned}\log(\Pi(x)) = {} & 730193702775304384046745947228313596346480 \\ & 803400240950763141174029187190517313409792 5 \\ & 342153702522654039372608184558507369137933 7 \\ & 832616768741252142993539044632260376087765 9 \\ & 740520962963146604000921389665780564632839 \\ & 420364\end{aligned}$$

Discrete Log Computation in $\mathbb{F}_{p^{35}}$, $p = 65407$

Function Field Sieve for medium prime case

$$g_1(x) = x^5$$
$$g_2(x) = x^7 + 21608x^6 + 46695x^5 + 31023x^4 + 31542x^3 + 51345x^2 + 6356x + 64947$$
$$f(x) = \text{Normalize}\left(x - g_2\left(g_1(x)\right)\right)$$

$$\mathbb{F}_{p^{35}} = \frac{\mathbb{F}[x]}{\langle f(x) \rangle}, \text{ with a primitive element } x$$

$$\Pi(x) = \text{Normalize}\left(\sum_{i=1}^{n-1} \lfloor \pi p^{i+1} \mod p \rfloor x^i\right)$$

$$\Pi(x) = x^{34} + 16745x^{33} + 47746x^{32} + 2546x^{31} + 8214x^{30} + 28280x^{29} + 1732x^{28} + 51068x^{27} + 41698x^{26} + 26709x^{25} + 4729x^{24} + 28458x^{23} + 47884x^{22} + 51632x^{21} + 901x^{20} + 668x^{19} + 9260x^{18} + 43490x^{17} + 13588x^{16} + 38300x^{15} + 23653x^{14} + 21535x^{13} + 8952x^{12} + 28425x^{11} + 65021x^{10} + 23396x^{9} + 12540x^{8} + 50104x^{7} + 64316x^{6} + 31002x^{5} + 40556x^{4} + 19251x^{3} + 63349x^{2} + 60609x$$

$$\log(\Pi(x)) = 3643957638404613125675577450579371249044713\,1466270246710413227134703205086773510505476 6\,0291106552602336087278499474455804651045762 6\,26155358683165600632331848043424824 95.$$

- ✓ Pinpointing did not provide much speed up as $\frac{p}{(n_2+1)!} = 1.6$
- ✓ Relation Collection took 520 CPU (@2.30 GHz) hours.
- ✓ Linear Algebra took 13, 8 and 7 CPU (@ 3.07GHz) hours res. for the 3 largest prime factors.
- ✓ In arround 230 CPU (@2.30 GHz) hours, we have completed the descent.

$\Pi(x) = x^{34} + 16745x$ …

$28280x^{29} + 1$ …

$26709x^{25} + 4$ …

$+901x^{20} + 6$ …

$38300x^{15} + 2$ …

$+65021x^{10} +$ …

$+31002x^{5} +$ …

$\log(\Pi(x)) = 3643957$ …

1466270246710413227134703205086773510505476 6

0291106552602336087278499474455804651045762 6

26155358683165600632331848043424 82495.

$$\Pi(x) = x^{34} + 16745x^{33} + \ldots$$
$$28280x^{29} + 1\ldots$$
$$26709x^{25} + 4\ldots$$
$$+901x^{20} + 6\ldots$$
$$38300x^{15} + 2\ldots$$
$$+65021x^{10} + \ldots$$
$$+31002x^{5} + \ldots$$

$$\log(\Pi(x)) = 3643957\ldots$$
$$14662702467104132271347\ldots$$
$$02911065526023360872784\ldots$$
$$26155358683165600632331\ldots$$

- ✓ Pinpointing did not provide much speed up as $\frac{p}{(n_2+1)!} = 1.6$
- ✓ Relation Collection took 520 CPU (@2.30 GHz) hours.
- ✓ Linear Algebra took 13, 8 and 7 CPU (@ 3.07GHz) hours res. for the 3 largest prime factors.
- ✓ In arround 230 CPU (@2.30 GHz) hours, we have completed the descent.