Resisting and Eliminating Smoothness Heuristics

Robert Granger

robbiegranger@gmail.com

Joint work with Thorsten Kleinjung and Jens Zumbrägel

Laboratory for Cryptologic Algorithms
School of Computer and Communication Sciences
École polytechnique fédérale de Lausanne
Switzerland

DLP 2014

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Overview

Basics

Resisting smoothness heuristics

Breaking supersingular binary curves

Eliminating smoothness heuristics

Overview

Basics

Resisting smoothness heuristics

Breaking supersingular binary curves

Eliminating smoothness heuristics

The Index Calculus Method

Consider the DLP in $\mathbb{F}_{q^n}$. The ICM consists of two stages:

The Index Calculus Method

Consider the DLP in $\mathbb{F}_{q^n}$. The ICM consists of two stages:

1. Choose a factor base $\mathcal{F}$, find relations between elements and then compute their logarithms.

The Index Calculus Method

Consider the DLP in $\mathbb{F}_{q^n}$. The ICM consists of two stages:

1. Choose a factor base $\mathcal{F}$, find relations between elements and then compute their logarithms.
2. For an arbitrary element, express it as a product of lower degree elements; recurse until all leaves are in $\mathcal{F}$.

Smoothness and the F.T.C.

Definition

An element $f \in \mathbb{F}_q[X]$ is said to be B-smooth if all of its irreducible factors have degree $\leq B$.

Smoothness and the F.T.C.

Definition

An element $f \in \mathbb{F}_q[X]$ is said to be B-smooth if all of its irreducible factors have degree $\leq B$.

Theorem (*Odlyzko '84, Lovorn '92*)

For $m^{1/100} \leq B \leq m^{99/100}$, the probability that a polynomial $f \in \mathbb{F}_q[X]$ of degree m chosen uniformly at random is B-smooth, is

$$u^{-(1+o(1))u}, \quad \textit{where } u = m/B$$

Smoothness and the F.T.C.

Definition

An element $f \in \mathbb{F}_q[X]$ is said to be B-smooth if all of its irreducible factors have degree $\leq B$.

Theorem (*Odlyzko '84, Lovorn '92*)

For $m^{1/100} \leq B \leq m^{99/100}$, the probability that a polynomial $f \in \mathbb{F}_q[X]$ of degree m chosen uniformly at random is B-smooth, is

$$u^{-(1+o(1))u}, \quad \textit{where } u = m/B$$

'The Fundamental Theorem of Cryptography'

"If we have no clue about something, then we can safely assume that it behaves as a uniformly distributed random variable."

– Igor Shparlinski

The Joux-Lercier FFS variation [JL06]

To find factor base relations in $\mathbb{F}_{q^n}$ one uses the following setup.

- Choose $g_1, g_2 \in \mathbb{F}_q[X]$ of degrees d_1, d_2 s.t. $X - g_1(g_2(X))$ has a degree n irreducible factor $I(X)$ over $\mathbb{F}_q$, so that $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(I(X)) = \mathbb{F}_q(x)$
- Let $y = g_2(x)$; then $x = g_1(y)$ and $\mathbb{F}_{q^n} \cong \mathbb{F}_q(x) \cong \mathbb{F}_q(y)$
- In best case factor base is $\{x - a \mid a \in \mathbb{F}_q\} \cup \{y - b \mid b \in \mathbb{F}_q\}$

Relation generation:

- Considering elements $xy + ay + bx + c$ with $a, b, c \in \mathbb{F}_q$, one obtains the $\mathbb{F}_{q^n}$-equality

$$xg_2(x) + ag_2(x) + bx + c = yg_1(y) + ay + bg_1(y) + c$$

- When both sides split over $\mathbb{F}_q$ one obtains a relation

Optimising d_1 and d_2 in [JL06]

F.T.C. $\Longrightarrow$ that as $q \to \infty$ each side of $xy + ay + bx + c$ splits over $\mathbb{F}_q$ with probability $1/(d_2 + 1)!$ and $1/(d_1 + 1)!$ respectively.

- $\Longrightarrow$ Choose $d_1 \approx d_2 \approx \sqrt{n}$
- For $q = L_{q^n}(1/3, 3^{-2/3})$ algorithm is $L_{q^n}(1/3, 3^{1/3})$

Optimising d_1 and d_2 in [JL06]

F.T.C. $\implies$ that as $q \to \infty$ each side of $xy + ay + bx + c$ splits over $\mathbb{F}_q$ with probability $1/(d_2+1)!$ and $1/(d_1+1)!$ respectively.

- $\implies$ Choose $d_1 \approx d_2 \approx \sqrt{n}$
- For $q = L_{q^n}(1/3, 3^{-2/3})$ algorithm is $L_{q^n}(1/3, 3^{1/3})$

A Counterpoint to the F.T.C.

Fortunately, in one sub-case of the [JL06] setup, we do have a clue.

Overview

Basics

Resisting smoothness heuristics

Breaking supersingular binary curves

Eliminating smoothness heuristics

Resisting smoothness heuristics

'On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$'

Faruk Göloğlu, Robert Granger, Gary McGuire and Jens Zumbrägel.
(Best Paper Award at CRYPTO 2013)

UCD School of Mathematical Sciences

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

CASL

Resisting smoothness heuristics

'On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$'

Faruk Göloğlu, Robert Granger, Gary McGuire and Jens Zumbrägel.
(Best Paper Award at CRYPTO 2013)

The paper contains:

- The first *polynomial time* relation generation method for degree one elements

UCD School of Mathematical Sciences

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

CASL

Resisting smoothness heuristics

'On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$'

Faruk Göloğlu, Robert Granger, Gary McGuire and Jens Zumbrägel.
(Best Paper Award at CRYPTO 2013)

The paper contains:

- The first *polynomial time* relation generation method for degree one elements
- The first *polynomial time* elimination method for degree two elements

UCD School of Mathematical Sciences

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

CASL

An auspicious choice for g_2 in [JL06]

Assume now that the base field is $\mathbb{F}_{q^k}$ for $k \geq 2$.

- Let $y = g_2(x) = x^q$
- Eliminates half of the factor base since

$$(y + b) = (x + b^{1/q})^q \Longrightarrow \log(y + b) = q \log(x + b^{1/q})$$

An auspicious choice for g_2 in [JL06]

Assume now that the base field is $\mathbb{F}_{q^k}$ for $k \geq 2$.

- Let $y = g_2(x) = x^q$
- Eliminates half of the factor base since

$$(y + b) = (x + b^{1/q})^q \Longrightarrow \log(y + b) = q \log(x + b^{1/q})$$

- The l.h.s. of $xy + ay + bx + c$ becomes

$$x^{q+1} + ax^q + bx + c$$

An auspicious choice for g_2 in [JL06]

Assume now that the base field is $\mathbb{F}_{q^k}$ for $k \geq 2$.

- Let $y = g_2(x) = x^q$
- Eliminates half of the factor base since

$$(y+b) = (x+b^{1/q})^q \Longrightarrow \log(y+b) = q\log(x+b^{1/q})$$

- The l.h.s. of $xy + ay + bx + c$ becomes

$$x^{q+1} + ax^q + bx + c$$

- This polynomial *provably* splits over $\mathbb{F}_{q^k}$ with probability

$$\approx 1/q^3 \gg 1/(q+1)!$$

Bluher polynomials

Let $k \geq 3$ and consider the polynomial $X^{q+1} + aX^q + bX + c$.

If $ab \neq c$ and $a^q \neq b$, this may be transformed into

$$F_B(\overline{X}) = \overline{X}^{q+1} + B\overline{X} + B\,, \quad \text{with} \quad B = \frac{(b-a^q)^{q+1}}{(c-ab)^q}\,,$$

via $X = \frac{c-ab}{b-a^q}\,\overline{X} - a$.

Theorem (*Bluher '04*)

The number of elements $B \in \mathbb{F}_{q^k}^{\times}$ s.t. the polynomial $F_B(\overline{X}) \in \mathbb{F}_{q^k}[\overline{X}]$ splits completely over $\mathbb{F}_{q^k}$ equals

$$\frac{q^{k-1}-1}{q^2-1} \quad \textit{if } k \textit{ is odd}\,, \qquad \frac{q^{k-1}-q}{q^2-1} \quad \textit{if } k \textit{ is even}\,.$$

Polynomial time relation generation: $k \geq 3$

Assume that g_1 can be found s.t. $X - g_1(X^q) \equiv 0 \pmod{I(X)}$ with $\deg(I) = n \leq qd_1$. Then we have the following method:

- Compute $\mathcal{B} = \{B \in \mathbb{F}_{q^k}^{\times} \mid X^{q+1} + BX + B \text{ splits over } \mathbb{F}_{q^k}\}$
- Since $B = (b - a^q)^{q+1}/(c - ab)^q$, for any $a, b \in \mathbb{F}_{q^k}$ s.t. $b \neq a^q$, and $B \in \mathcal{B}$, there exists a unique $c \in \mathbb{F}_{q^k}$ s.t. $x^{q+1} + ax^q + bx + c$ splits over $\mathbb{F}_{q^k}$
- For each such (a, b, c), test if r.h.s. $yg_1(y) + ay + bg_1(y) + c$ splits; if so then have a relation
- If $q^{3k-3} > q^k(d_1 + 1)!$ then for $d_1 \geq 1$ constant we expect to compute logs of degree 1 elements of $\mathbb{F}_{q^{kn}}$ in time

$$O(q^{2k+1})$$

Degree 2 elimination

Let $Q(y) = y^2 + q_1 y + q_0 \in \mathbb{F}_{q^{kn}}$ be an element to be eliminated, i.e., written as a product of linear elements.

- Recall that in $\mathbb{F}_{q^{kn}}$ we have $y = x^q$ and $x = g_1(y)$, so for any univariate polynomials w_0, w_1 we have

$$w_0(x^q)\,x + w_1(x^q) = w_0(y)\,g_1(y) + w_1(y)$$

- Compute a reduced basis of the lattice

$$L_Q = \{(w_0(Y), w_1(Y)) \in \mathbb{F}_{q^k}[Y]^2 : w_0(Y)\,g_1(Y) + w_1(Y) \equiv 0 \pmod{Q(Y)}\}$$

- In general we have $(u_0, Y + u_1), (Y + v_0, v_1)$, with $u_i, v_i \in \mathbb{F}_{q^k}$, and for $s \in \mathbb{F}_{q^k}$ we have $(Y + v_0 + su_0, sY + v_1 + su_1) \in L_Q$
- r.h.s. $(y + v_0 + su_0)\,g_1(y) + (sy + v_1 + su_1)$ has degree $d_1 + 1$, so cofactor splits with probability $\approx 1/(d_1 - 1)!$
- l.h.s. is $(x^q + v_0 + su_0)x + (sx^q + v_1 + su_1)$ which is of the form

$$x^{q+1} + ax^q + bx + c$$

Degree 2 elimination

Consider the l.h.s. $x^{q+1} + sx^q + (v_0 + su_0)x + (v_1 + su_1)$.

- Compute the set $\mathcal{B}$ of elements $B \in \mathbb{F}_{q^k}$ such that $X^{q+1} + BX + B$ splits over $\mathbb{F}_{q^k}$
- For each $B \in \mathcal{B}$ we try to solve $B = (b - a^q)^{q+1}/(c - ab)^q$ for s, i.e., find $s \in \mathbb{F}_{q^k}$ that satisfies

$$B = \frac{(-s^q + u_0 s + v_0)^{q+1}}{(-u_0 s^2 + (u_1 - v_0)s + v_1)^q}$$

  by taking GCD with $s^{q^k} - s$: Cost is $O(q^2 \log q^k)$ $\mathbb{F}_{q^k}$-ops

- Probability of success is $\approx 1 - \left(1 - \frac{1}{(d_1-1)!}\right)^{q^{k-3}}$
- Hence need $q^{k-3} > (d_1 - 1)!$ to eliminate $Q(y)$ with good probability: Expected cost is

$$O(q^2(d_1 - 1)! \log q^k) \ \ \mathbb{F}_{q^k}\text{-ops}$$

Joux's insights

- Independently of [GGMZ13], Joux discovered an isomorphic polynomial time degree one relation generation method.
- For $\mathbb{F}_{q^{2n}}$, assume $h_1(X), h_0(X) \in \mathbb{F}_{q^2}[X]$ of very small degree exist s.t. $h_1(X)X^q - h_0(X)$ has an irreducible factor $I(X)$ of degree n.

For $Q \in \mathbb{F}_{q^2}[X]$ of degree D let F, G have degree $< D$. Consider

$$G \cdot \prod_{\alpha \in \mathbb{F}_q} (F - \alpha G) = F^q G - F G^q$$

- Since $X^q \equiv h_0(X)/h_1(X) \pmod{I(X)}$, F^q & G^q have small degree
- Joux insists that r.h.s. is divisible by $Q \implies$ results in a bilinear quadratic system, and that the cofactor is $(D-1)$-smooth

Joux's insights

- Independently of [GGMZ13], Joux discovered an isomorphic polynomial time degree one relation generation method.
- For $\mathbb{F}_{q^{2n}}$, assume $h_1(X), h_0(X) \in \mathbb{F}_{q^2}[X]$ of very small degree exist s.t. $h_1(X)X^q - h_0(X)$ has an irreducible factor $I(X)$ of degree n.

For $Q \in \mathbb{F}_{q^2}[X]$ of degree D let F, G have degree $< D$. Consider

$$G \cdot \prod_{\alpha \in \mathbb{F}_q} (F - \alpha G) = F^q G - F G^q$$

- Since $X^q \equiv h_0(X)/h_1(X) \pmod{I(X)}$, F^q & G^q have small degree
- Joux insists that r.h.s. is divisible by $Q \implies$ results in a bilinear quadratic system, and that the cofactor is $(D-1)$-smooth

Balancing classical descent with this elimination results in an algorithm with heuristic complexity

$$L_{q^{2n}}(1/4 + o(1))$$

New method DLP solutions in 2013

- 11th Feb'13, Joux: $\mathbb{F}_{2^{1778}}$ in 220 core hours
- 19th Feb'13, GGMZ: $\mathbb{F}_{2^{1971}}$ in $3,132$ core hours
- 3rd May'13, GGMZ: $\mathbb{F}_{2^{3164}}$ in $107,000$ core hours
- 22nd Mar'13, Joux: $\mathbb{F}_{2^{4080}}$ in $14,100$ core hours
- 11th Apr'13, GGMZ: $\mathbb{F}_{2^{6120}}$ in 750 core hours
- 21st May'13, Joux: $\mathbb{F}_{2^{6168}}$ in 550 core hours

Overview

Basics

Resisting smoothness heuristics

Breaking supersingular binary curves

Eliminating smoothness heuristics

Supersingular binary curves: genus 1

For $i \in \mathbb{F}_2$ consider the elliptic curves

$$E_i/\mathbb{F}_2 : Y^2 + Y = X^3 + X + i$$

- Both E_i are supersingular ($E_i(\overline{\mathbb{F}}_2)$ has no points of order 2)
- For prime p we have

$$\#E_i(\mathbb{F}_{2^p}) = \begin{cases} 2^p + 1 + (-1)^i 2^{(p+1)/2} & \text{for } p \equiv 1, 7 \pmod 8 \\ 2^p + 1 - (-1)^i 2^{(p+1)/2} & \text{for } p \equiv 3, 5 \pmod 8 \end{cases}$$

Supersingular binary curves: genus 1

For $i \in \mathbb{F}_2$ consider the elliptic curves

$$E_i/\mathbb{F}_2 : Y^2 + Y = X^3 + X + i$$

- Both E_i are supersingular ($E_i(\overline{\mathbb{F}}_2)$ has no points of order 2)
- For prime p we have

$$\#E_i(\mathbb{F}_{2^p}) = \begin{cases} 2^p + 1 + (-1)^i 2^{(p+1)/2} & \text{for } p \equiv 1,7 \pmod 8 \\ 2^p + 1 - (-1)^i 2^{(p+1)/2} & \text{for } p \equiv 3,5 \pmod 8 \end{cases}$$

- $(2^p + 1 \pm 2^{(p+1)/2}) \mid (2^{4p} - 1) \Longrightarrow E_i$ has embedding degree 4

Supersingular binary curves: genus 1

For $i \in \mathbb{F}_2$ consider the elliptic curves

$$E_i/\mathbb{F}_2 : Y^2 + Y = X^3 + X + i$$

- Both E_i are supersingular ($E_i(\overline{\mathbb{F}}_2)$ has no points of order 2)
- For prime p we have

$$\#E_i(\mathbb{F}_{2^p}) = \begin{cases} 2^p + 1 + (-1)^i 2^{(p+1)/2} & \text{for } p \equiv 1, 7 \pmod 8 \\ 2^p + 1 - (-1)^i 2^{(p+1)/2} & \text{for } p \equiv 3, 5 \pmod 8 \end{cases}$$

- $(2^p + 1 \pm 2^{(p+1)/2}) \mid (2^{4p} - 1) \Longrightarrow E_i$ has embedding degree 4

Lesson 1 (*MOV '93*)

Elliptic curves with small embedding degree are weak.

Supersingular binary curves: genus 1

For $i \in \mathbb{F}_2$ consider the elliptic curves

$$E_i/\mathbb{F}_2 : Y^2 + Y = X^3 + X + i$$

- Both E_i are supersingular ($E_i(\overline{\mathbb{F}}_2)$ has no points of order 2)
- For prime p we have

$$\#E_i(\mathbb{F}_{2^p}) = \begin{cases} 2^p + 1 + (-1)^i 2^{(p+1)/2} & \text{for } p \equiv 1,7 \pmod 8 \\ 2^p + 1 - (-1)^i 2^{(p+1)/2} & \text{for } p \equiv 3,5 \pmod 8 \end{cases}$$

- $(2^p + 1 \pm 2^{(p+1)/2}) \mid (2^{4p} - 1) \Longrightarrow E_i$ has embedding degree 4

Lesson 1 (*MOV '93*)

Elliptic curves with small embedding degree are weak.

Lesson 2 (*Pairing-based cryptography '00/01*)

Provided that the applications are good enough, ignore Lesson 1.

Supersingular binary curves: genus 2

For $i \in \mathbb{F}_2$ let

$$H_i/\mathbb{F}_2 : Y^2 + Y = X^5 + X^3 + i$$

- Both H_i are supersingular (Jac_{H_i} is isogenous to a product of two supersingular elliptic curves)
- We have $\#\mathrm{Jac}(H_i)(\mathbb{F}_{2^p}) =$

$$\begin{cases} 2^{2p} + (-1)^i 2^{(3p+1)/2} + 2^p + (-1)^i 2^{(p+1)/2} + 1 & \text{for } p \equiv 1, 7, 17, 23 \pmod{24} \\ 2^{2p} - (-1)^i 2^{(3p+1)/2} + 2^p - (-1)^i 2^{(p+1)/2} + 1 & \text{for } p \equiv 5, 11, 13, 19 \pmod{24} \end{cases}$$

- $\#\mathrm{Jac}(H_i)(\mathbb{F}_{2^p}) \mid (2^{12p} - 1) \Longrightarrow \mathrm{Jac}(H_i)$ has embedding degree 12.

Supersingular binary curves: genus 2

For $i \in \mathbb{F}_2$ let

$$H_i/\mathbb{F}_2 : Y^2 + Y = X^5 + X^3 + i$$

- Both H_i are supersingular (Jac_{H_i} is isogenous to a product of two supersingular elliptic curves)
- We have $\#\mathrm{Jac}(H_i)(\mathbb{F}_{2^p}) =$

$$\begin{cases} 2^{2p} + (-1)^i 2^{(3p+1)/2} + 2^p + (-1)^i 2^{(p+1)/2} + 1 & \text{for } p \equiv 1, 7, 17, 23 \pmod{24} \\ 2^{2p} - (-1)^i 2^{(3p+1)/2} + 2^p - (-1)^i 2^{(p+1)/2} + 1 & \text{for } p \equiv 5, 11, 13, 19 \pmod{24} \end{cases}$$

- $\#\mathrm{Jac}(H_i)(\mathbb{F}_{2^p}) \mid (2^{12p} - 1) \Longrightarrow \mathrm{Jac}(H_i)$ has embedding degree 12.

Only genus 1 and 2 seriously considered $\Longrightarrow$ we are interested in the DLPs in (the prime order $r \mid \#\mathrm{Jac}$ subgroups of) $\mathbb{F}_{2^{4p}}^{\times}$ and $\mathbb{F}_{2^{12p}}^{\times}$.

Concrete security of small characteristic pairings

Adj, Menezes, Oliveira and Rodríguez-Henríquez used the techniques from [Joux13] and [BGJT13] to analyse the concrete security of the DLP in pairing fields once thought to be 128-bit secure.

Concrete security of small characteristic pairings

Adj, Menezes, Oliveira and Rodríguez-Henríquez used the techniques from [Joux13] and [BGJT13] to analyse the concrete security of the DLP in pairing fields once thought to be 128-bit secure.

In particular, they showed that:

- The DLP in the 804-bit order r subgroup of $\mathbb{F}_{3^{6 \cdot 509}}^{\times}$ can be solved in time $2^{73.7} M_r$, using $q = 3^6$ and $k = 2$
- The DLP in the 698-bit order r subgroup of $\mathbb{F}_{2^{12 \cdot 367}}^{\times}$ can be solved in time $2^{94.6} M_r$, using $q = 2^{12}$ and $k = 2$
- The DLP in the 1221-bit order r subgroup of $\mathbb{F}_{2^{4 \cdot 1223}}^{\times}$ can be solved in time $\approx 2^{128} M_r$, using $q = 2^{12}$ and $k = 2$

Concrete security of small characteristic pairings

Adj, Menezes, Oliveira and Rodríguez-Henríquez used the techniques from [Joux13] and [BGJT13] to analyse the concrete security of the DLP in pairing fields once thought to be 128-bit secure.

In particular, they showed that:

- The DLP in the 804-bit order r subgroup of $\mathbb{F}_{3^{6 \cdot 509}}^{\times}$ can be solved in time $2^{73.7} M_r$, using $q = 3^6$ and $k = 2$
- The DLP in the 698-bit order r subgroup of $\mathbb{F}_{2^{12 \cdot 367}}^{\times}$ can be solved in time $2^{94.6} M_r$, using $q = 2^{12}$ and $k = 2$
- The DLP in the 1221-bit order r subgroup of $\mathbb{F}_{2^{4 \cdot 1223}}^{\times}$ can be solved in time $\approx 2^{128} M_r$, using $q = 2^{12}$ and $k = 2$

Consider the following:

- $h_1(X)X^q - h_0(X) \equiv 0 \pmod{I(X)} \Longrightarrow n \leq q + \deg(h_1)$

Concrete security of small characteristic pairings

Adj, Menezes, Oliveira and Rodríguez-Henríquez used the techniques from [Joux13] and [BGJT13] to analyse the concrete security of the DLP in pairing fields once thought to be 128-bit secure.

In particular, they showed that:

- The DLP in the 804-bit order r subgroup of $\mathbb{F}_{3^{6 \cdot 509}}^{\times}$ can be solved in time $2^{73.7} M_r$, using $q = 3^6$ and $k = 2$
- The DLP in the 698-bit order r subgroup of $\mathbb{F}_{2^{12 \cdot 367}}^{\times}$ can be solved in time $2^{94.6} M_r$, using $q = 2^{12}$ and $k = 2$
- The DLP in the 1221-bit order r subgroup of $\mathbb{F}_{2^{4 \cdot 1223}}^{\times}$ can be solved in time $\approx 2^{128} M_r$, using $q = 2^{12}$ and $k = 2$

Consider the following:

- $h_1(X)X^q - h_0(X) \equiv 0 \pmod{I(X)} \Longrightarrow n \leq q + \deg(h_1)$
- The descent cost is lower for smaller q

Our contributions

We exploited the following observations/principles/techniques:

- $h_1(X^q)X - h_0(X^q) \equiv 0 \pmod{I(X)} \Longrightarrow n \leq q \cdot \deg(h_1) + 1$
- *Principle of parsimony:* always try to work in the target field; only when this fails should one embed into an extension
- A bonus of solving factor base logs in an extension is that one can factor elements over the extension during the descent
- We can also use $k = 1$ for the GB phase, eliminating higher degrees *& postponing the need for the QPA*

Our contributions

We exploited the following observations/principles/techniques:

- $h_1(X^q)X - h_0(X^q) \equiv 0 \pmod{I(X)} \Longrightarrow n \leq q \cdot \deg(h_1) + 1$
- *Principle of parsimony:* always try to work in the target field; only when this fails should one embed into an extension
- A bonus of solving factor base logs in an extension is that one can factor elements over the extension during the descent
- We can also use $k = 1$ for the GB phase, eliminating higher degrees *& postponing the need for the QPA*

'Breaking '128-bit Secure' Supersingular Binary Curves (or how to solve discrete logarithms in $\mathbb{F}_{2^{4 \cdot 1223}}$ and $\mathbb{F}_{2^{12 \cdot 367}}$)'

Robert Granger, Thorsten Kleinjung and Jens Zumbrägel.
`eprint.iacr.org/2014/119`

Solving the DLP in $\mathbb{F}_{2^{12\cdot 367}}$

Over $\mathbb{F}_{2^{367}}$ the Jacobian of $H_0/\mathbb{F}_2 : Y^2 + Y = X^5 + X^3$ has a subgroup of prime order $r = (2^{734} + 2^{551} + 2^{367} + 2^{184} + 1)/(13 \cdot 7170258097)$.

- Let $\mathbb{F}_{2^{12}} = \mathbb{F}_2[U]/(U^{12} + U^3 + 1) = \mathbb{F}_2(u)$
- Let $\mathbb{F}_{2^{367}} = \mathbb{F}_2[X]/(I(X)) = \mathbb{F}_2(x)$ where $I(X)$ the irreducible degree 367 divisor of $h_1(X^{64})X - h_0(X^{64})$, with

$$h_1 = X^5 + X^3 + X + 1, \;\; h_0 = X^6 + X^4 + X^2 + X + 1$$

- $\mathbb{F}_{2^{12\cdot 367}}$ is then the compositum of $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{367}}$
- We chose as our generator $g' = g^{(2^{4404}-1)/r}$ where $g = x + u^7$, and target element $x'_\pi = x_\pi^{(2^{4404}-1)/r}$ where

$$x_\pi = \sum_{i=0}^{4403} (\lfloor \pi \cdot 2^{i+1} \rfloor \bmod 2) \cdot u^{11-(i \bmod 12)} \cdot x^{\lfloor i/12 \rfloor}$$

Factor base logs and initial descent

We also represent $\mathbb{F}_{2^{12}}$ as $\mathbb{F}_{q^2}$ with $q = 2^6$ and $k = 2$:

- Let $\mathbb{F}_{2^6} = \mathbb{F}_2[U]/(T^6 + T + 1) = \mathbb{F}_2(t)$
- Let $\mathbb{F}_{2^{12}} = \mathbb{F}_{2^6}[V]/(V^2 + tV + 1) = \mathbb{F}_{2^6}(v)$

Since $q^{2k-3} \not> (6+1)!$ we consider relations over $\mathbb{F}_{q^4}$ instead:

- Let $\mathbb{F}_{2^{24}} = \mathbb{F}_{2^6}[W]/(W^4 + W^3 + W^2 + t^3) = \mathbb{F}_{2^6}(w)$

For the factor base $\{x + a \mid a \in \mathbb{F}_{2^{24}}\}$ we have:

$$(x+a)^{2^{367}} = x + a^{2^{367}} = x + a^{2^7}$$

$\Longrightarrow$ reduced factor base has $699,252$ elements and linear system was solved in 4896 core hours on a 24 core cluster.

Factor base logs and initial descent

We also represent $\mathbb{F}_{2^{12}}$ as $\mathbb{F}_{q^2}$ with $q = 2^6$ and $k = 2$:

- Let $\mathbb{F}_{2^6} = \mathbb{F}_2[U]/(T^6 + T + 1) = \mathbb{F}_2(t)$
- Let $\mathbb{F}_{2^{12}} = \mathbb{F}_{2^6}[V]/(V^2 + tV + 1) = \mathbb{F}_{2^6}(v)$

Since $q^{2k-3} \not> (6+1)!$ we consider relations over $\mathbb{F}_{q^4}$ instead:

- Let $\mathbb{F}_{2^{24}} = \mathbb{F}_{2^6}[W]/(W^4 + W^3 + W^2 + t^3) = \mathbb{F}_{2^6}(w)$

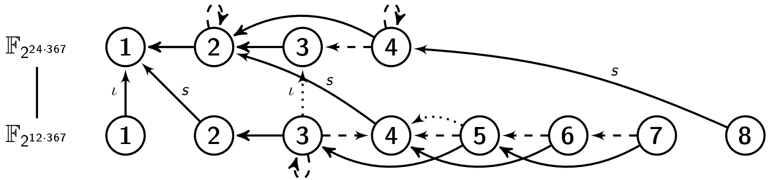
For the factor base $\{x + a \mid a \in \mathbb{F}_{2^{24}}\}$ we have:

$$(x+a)^{2^{367}} = x + a^{2^{367}} = x + a^{2^7}$$

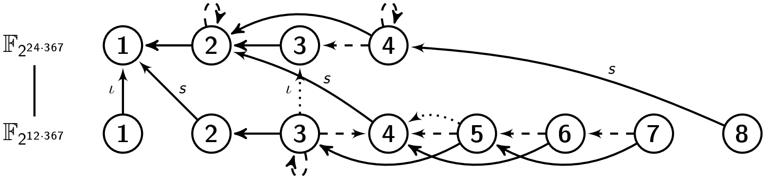
$\Longrightarrow$ reduced factor base has $699,252$ elements and linear system was solved in 4896 core hours on a 24 core cluster.

Initial descent: We performed a continued fraction initial split, then degree-balanced classical descent to degrees ≤ 8 in 38224 core hours.

Eliminating small degree elements in $\mathbb{F}_{2^{12\cdot 367}}/\mathbb{F}_{2^{12}}$



Eliminating small degree elements in $\mathbb{F}_{2^{12\cdot 367}}/\mathbb{F}_{2^{12}}$



The GB phase cost 8432 core hours on Magma V2.20-1, for a total of approximately 52240 core hours. On 30/1/14 we announced that $x'_\pi = g'^{\,\log}$, with $\log =$

4093208920214235164093447733900702563725614097945142354192285387447360
4390153516847214082336876895639025110622309801452728710173825428267646
9559843114767895545475795766475848754227211594761182312814017076893242

Overview

Basics

Resisting smoothness heuristics

Breaking supersingular binary curves

Eliminating smoothness heuristics

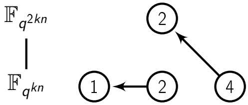
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$

$\mathbb{F}_{q^{kn}}$

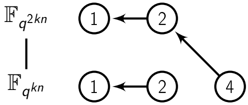
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$

$\mathbb{F}_{q^{kn}}$

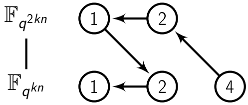
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



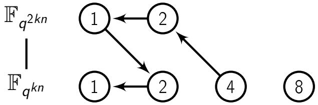
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



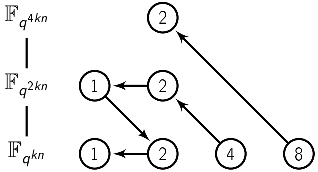
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



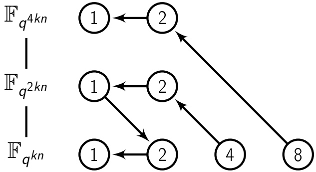
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



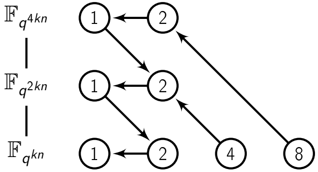
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



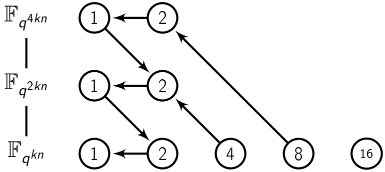
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



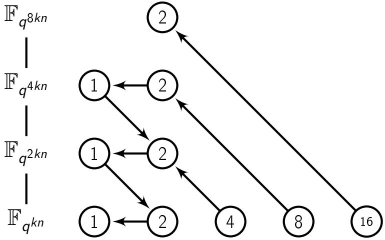
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



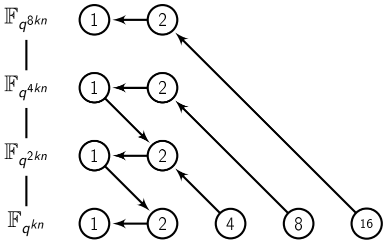
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



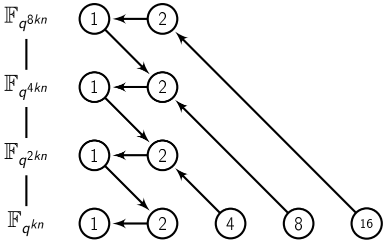
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



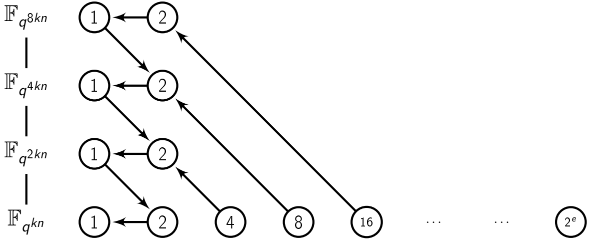
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



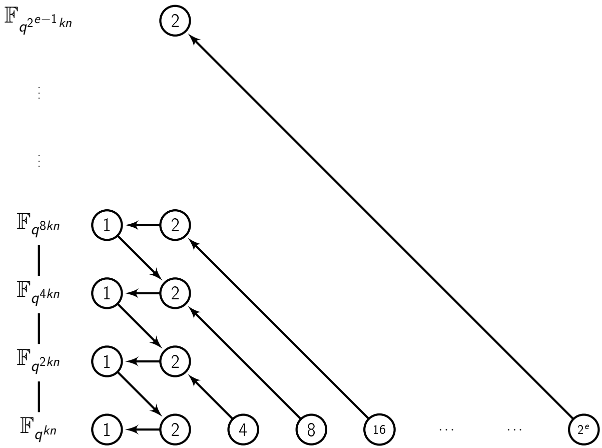
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



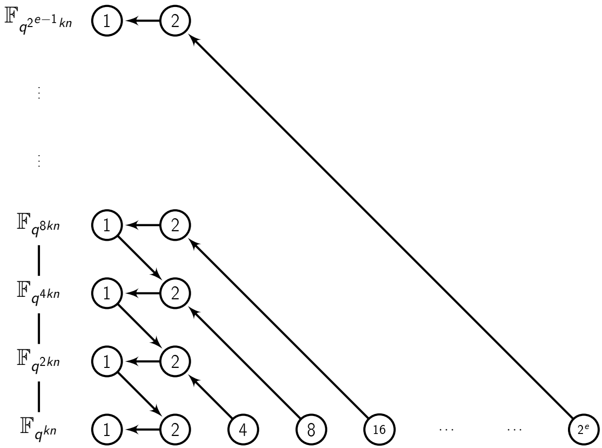
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



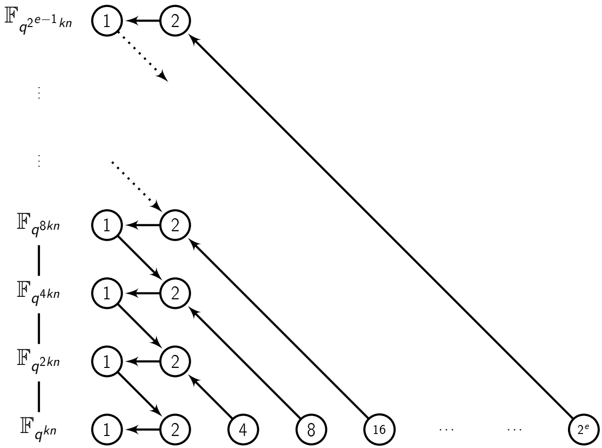
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



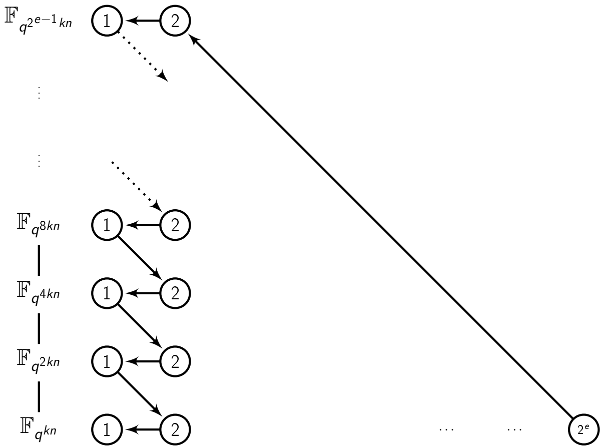
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



Eliminating smoothness heuristics

- If $d_h \leq 2$, then r.h.s. cofactor of a degree 2 element being eliminated is linear $\implies$ no smoothness heuristics needed for descent

Eliminating smoothness heuristics

- If $d_h \leq 2$, then r.h.s. cofactor of a degree 2 element being eliminated is linear $\Longrightarrow$ no smoothness heuristics needed for descent
- Using reducible degree 2's $\Longrightarrow$ degree 1 relation generation does not use smoothness heuristics

Eliminating smoothness heuristics

- If $d_h \leq 2$, then r.h.s. cofactor of a degree 2 element being eliminated is linear $\Longrightarrow$ no smoothness heuristics needed for descent
- Using reducible degree 2's $\Longrightarrow$ degree 1 relation generation does not use smoothness heuristics

Hence no smoothness heuristics are needed!

Eliminating smoothness heuristics

- If $d_h \leq 2$, then r.h.s. cofactor of a degree 2 element being eliminated is linear $\implies$ no smoothness heuristics needed for descent
- Using reducible degree 2's $\implies$ degree 1 relation generation does not use smoothness heuristics

Hence no smoothness heuristics are needed!

Heuristic 1

Given a prime p and an integer n, for q the smallest power of p greater than n and for an integer $k = O(1)$, there exist polynomials $h_0, h_1 \in \mathbb{F}_{q^k}[X]$ of degree at most two s.t. $h_1(X^q)X - h_0(X^q)$ has an irreducible factor of degree n (or the equivalent for $h_1(X)X^q - h_0(X)$).

Eliminating smoothness heuristics

- If $d_h \leq 2$, then r.h.s. cofactor of a degree 2 element being eliminated is linear $\Longrightarrow$ no smoothness heuristics needed for descent
- Using reducible degree 2's $\Longrightarrow$ degree 1 relation generation does not use smoothness heuristics

Hence no smoothness heuristics are needed!

Heuristic 1

Given a prime p and an integer n, for q the smallest power of p greater than n and for an integer $k = O(1)$, there exist polynomials $h_0, h_1 \in \mathbb{F}_{q^k}[X]$ of degree at most two s.t. $h_1(X^q)X - h_0(X^q)$ has an irreducible factor of degree n (or the equivalent for $h_1(X)X^q - h_0(X)$).

Heuristic 2

There exists a polynomial time algorithm for obtaining the logarithms of polynomials of bounded degree using the parameters from Heuristic 1.

A new quasi-polynomial algorithm

Theorem (*G.-Kleinjung-Zumbrägel '14*)

Subject to Heuristics 1 and 2, the running time of the new algorithm is quasi-polynomial, namely

$$q^{\log_2 n + O(1)}$$

A new quasi-polynomial algorithm

Theorem (*G.-Kleinjung-Zumbrägel '14*)

Subject to Heuristics 1 and 2, the running time of the new algorithm is quasi-polynomial, namely

$$q^{\log_2 n + O(1)}$$

Theorem (*G.-Kleinjung-Zumbrägel '14*)

Subject to Heuristics 1 and 2, by balancing the cost of computing the factor base logs and the descent, the running time of the new algorithm is

$$q^{\log_2 n - (1-\epsilon) \log_2 \log_2 n}$$

A new quasi-polynomial algorithm

Theorem (*G.-Kleinjung-Zumbrägel '14*)

Subject to Heuristics 1 and 2, the running time of the new algorithm is quasi-polynomial, namely

$$q^{\log_2 n + O(1)}$$

Theorem (*G.-Kleinjung-Zumbrägel '14*)

Subject to Heuristics 1 and 2, by balancing the cost of computing the factor base logs and the descent, the running time of the new algorithm is

$$q^{\log_2 n - (1-\epsilon)\log_2 \log_2 n}$$

'On the Powers of 2'. Robert Granger, Thorsten Kleinjung and Jens Zumbrägel. `eprint.iacr.org/2014/300`

Thanks for your attention!

Thanks for your attention!

Thanks for your attention!