# Breaking "128 bit Secure" Supersingular Binary Curves

## (or how to solve Discrete Logarithms in $\mathbb{F}_{2^{4\cdot 1223}}$ and $\mathbb{F}_{2^{12\cdot 367}}$)

Jens Zumbrägel

Institute of Algebra
TU Dresden, Germany

8 October 2014
ECC 2014 · IMSc · Chennai

*Joint work with:*

Robert Granger and Thorsten Kleinjung
Laboratory for Cryptologic Algorithms · EPFL, Switzerland

# Discrete logarithms

## Definition

Given a cyclic group $(G, \cdot)$ of order $m$ and a generator $\alpha \in G$, the Discrete Logarithm Problem (DLP) asks, given $\beta \in G$, to find $x \in \mathbb{Z}_m$ such that $\beta = \alpha^x$. Notation: $\log_\alpha \beta := x$.

Commonly used groups:

- The multiplicative group of a finite field $\mathbb{F}_q$.
- The group over an elliptic curve over $\mathbb{F}_q$.
- The Jacobian over a hyperelliptic curve over $\mathbb{F}_q$.

$L$-Notation for running time:

$$L_m(\alpha, c) \;:=\; \exp\left((c + o(1))\,(\ln m)^{\alpha}\,(\ln\ln m)^{1-\alpha}\right),$$

for some $\alpha \in [0,1]$ and $c > 0$.

# Finite field DLP milestones

## (larger field and/or improved complexity)

| bitlength | char | who/when | running time |
|---|---|---|---|
| 127 | 2 | Coppersmith 1984 | $L(1/3\,,\,1.526..1.587)$ |
| 401 | 2 | Gordon, McCurley 1992 | $L(1/3\,,\,1.526..1.587)$ |
| n/a | small | Adleman 1994 | $L(1/3\,,\,1.923)$ |
| 427 | large | Weber, Denny 1998 | $L(1/3\,,\,1.526)$ |
| 521 | 2 | Joux, Lercier 2001 | $L(1/3\,,\,1.526)$ |
| 607 | 2 | Thomé 2001 | $L(1/3\,,\,1.526..1.587)$ |
| 613 | 2 | Joux, Lercier 2005 | $L(1/3\,,\,1.526)$ |
| 556 | medium | Joux, Lercier 2006 | $L(1/3\,,\,1.442)$ |
| 676 | 3 | Hayashi et al. 2010 | $L(1/3\,,\,1.442)$ |
| 923 | 3 | Hayashi et al. 2012 | $L(1/3\,,\,1.442)$ |
| 1175 | medium | Joux 24 Dec 2012 | $L(1/3\,,\,1.260)$ |
| 1425 | medium | Joux 6 Jan 2013 | $L(1/3\,,\,1.260)$ |
| 1778 | 2 | Joux 11 Feb 2013 | $L(1/4 + o(1))$ |
| 1971 | 2 | GGMZ 19 Feb 2013 | $L(1/3\,,\,0.763)$ |
| 4080 | 2 | Joux 22 Mar 2013 | $L(1/4 + o(1))$ |
| 6120 | 2 | GGMZ 11 Apr 2013 | $L(1/4)$ |
| 6168 | 2 | Joux 21 May 2013 | $L(1/4 + o(1))$ |
| n/a | small | BGJT 18 Jun 2013 | $L(0 + o(1))$ |
| 9234 | 2 | GKZ 31 Jan 2014 | $L(1/4 + o(1))$ |

# Cryptographic pairings

Consider the group $E(\mathbb{F}_q)$ of an *elliptic curve*/the Jacobian $J(\mathbb{F}_q)$ of a *hyperelliptic curve* of genus $g = 2$, let $\operatorname{char} \mathbb{F}_q = p$.
Let $G$ be a cyclic subgroup of order $m$, which has a difficult DLP.

Interesting for cryptology are non-degenerate bilinear pairings

$$e_m : G \times G \ \rightarrow \ \mu_m \ \leq \ \mathbb{F}^*_{q^k} \ ,$$

which can be realised by the Weil or the Tate pairing (or others).

- For *supersingular curves* the embedding degree $k$ is small.
- DLP in $G$ can be reduced to the DLP in $\mathbb{F}_{q^k}$ (MOV attack).
- But also, many *Pairing-Based Cryptography* applications.

Parameter suggestions on the level of "128 bit" security:

| $k$ | $g = 1$ | $g = 2$ |
|---|---|---|
| $p = 2$ | $k = 4 \quad q^k = 2^{4 \cdot 1223}$ | $k = 12 \quad q^k = 2^{12 \cdot 367}$ |
| $p = 3$ | $k = 6 \quad q^k = 3^{6 \cdot 509}$ | $(k = 4)$ |

# Overview

A High-Level Description of the Index Calculus Method

ICM Particulars for Finite Fields of Small Characteristic

Example: Discrete Logarithms in $\mathbb{F}_{2^{9234}}$

Supersingular Curves and Impact on Pairings

# Overview

A High-Level Description of the Index Calculus Method

ICM Particulars for Finite Fields of Small Characteristic

Example: Discrete Logarithms in $\mathbb{F}_{2^{9234}}$

Supersingular Curves and Impact on Pairings

# ICM precomputation stage

- Let $G$ be a cyclic group of order $m$ with generator $\alpha \in G$.
- Let $S \subseteq G$ be a subset, $\alpha \in S$, called the factor base.
- Consider group morphism $\varphi : \mathbb{Z}_m^S \to G$, $(e_s)_{s \in S} \mapsto \prod_{s \in S} s^{e_s}$.

$$\boxed{\text{Phase 1: Relation Generation}}$$

Generate a subset $\mathcal{R} \subseteq \ker \varphi$, whose elements are called relations.

$$\boxed{\text{Phase 2: Linear Algebra}}$$

Compute $(x_s)_{s \in S}$ with $\sum_{s \in S} e_s x_s = 0$ for all $(e_s)_{s \in S} \in \mathcal{R}$, i.e.,

$$(x_s)_{s \in S} \in \mathcal{R}^\perp = (\operatorname{span} \mathcal{R})^\perp .$$

Factor base logs are determined iff $\mathcal{R}^\perp \cong \mathbb{Z}_m$ iff $\operatorname{span} \mathcal{R} = \ker \varphi$; in this case, if $\mathcal{R}^\perp = \mathbb{Z}_m (x_s)_{s \in S}$ then $\log_\alpha s = x_s / x_\alpha$, for $s \in S$.

# Individual logarithm stage

## Phase 3: Descent Tree

From Phases 1 and 2 we know $\log_\alpha s$ for all $s \in S$.

- Build a descent tree, i.e., a tree such that
  - its root is the target element $\beta \in G$,
  - its leaves are elements $s \in S$,
  - if $x_1, \ldots, x_k \in G$ are children of a node $y \in G$ then a relation $y = \prod_{i=1}^{k} x_i^{e_i}$ has been computed.
- Then an expression $\beta = \prod_{s \in S} s^{e_s}$ can be obtained, and thus $\log_\alpha \beta = \sum_{s \in S} e_s \log_\alpha s$ is found.

**Idea of descent:** Elements $x_1, \ldots, x_k$ are "smaller" than $y$, and the elements in $S$ are "smallest".

# Reduction by automorphisms

Any automorphism of $G$ has form $\sigma : x \mapsto x^a$ for some $a \in \mathbb{Z}_m^*$.
Let $A \leq \mathrm{Aut}(G)\,(\cong \mathbb{Z}_m^*)$ be a group of automorphisms such that $\sigma(S) = S$ for all $\sigma \in A$. Thus the group $A$ acts on $S$ by

$$A \times S \to S\,, \quad (\sigma, s) \mapsto \sigma(s)\,.$$

Let $T \subseteq S$ be a set of representatives for the orbits in $S$, then

$$\forall s \in S \;\exists\, t_s \in T, a_s \in \mathbb{Z}_m^* : \; s = t_s^{a_s}\,,$$

hence $\log s = a_s \log t_s$, for all $s \in S$.

Thus factor base size $|S|$ *reduced* to $|T| \approx |S|/|A|$ elements.

# Overview

A High-Level Description of the Index Calculus Method

ICM Particulars for Finite Fields of Small Characteristic

Example: Discrete Logarithms in $\mathbb{F}_{2^{9234}}$

Supersingular Curves and Impact on Pairings

# Basic ICM in fields of small characteristic

Represent a finite field $\mathbb{F}_{q^n}$ as residue class ring $\mathbb{F}_q[X]/\langle f \rangle$, where $f \in \mathbb{F}_q[X]$ is an irreducible polynomial of degree $n$. Identify field elements with polynomials of degree $\leq n-1$.

Choose as factor base $S$ the set of all irreducible polynomials in $\mathbb{F}_q[X]$ of degree $\leq b$ (assume that $\alpha \in S$).

Relation Generation: For random $k \in \mathbb{Z}_n$, *test* whether $\alpha^k \bmod f$ is $b$-smooth, i.e., whether an expression exists of the form

$$\alpha^k \bmod f \;=\; \prod_{s \in S} s^{e_s} \;\text{ in }\; \mathbb{F}_q[X].$$

Theorem (Odlyzko, Lovorn)

*A polynomial of degree $m$ is $b$-smooth with probability*

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

# Finite fields of the form $\mathbb{F}_{q^{kn}}$

Let $q$ be a prime power, let $k, n$ be integers, and let $K = \mathbb{F}_{q^k}$.

## Our field representation

Let the field $L = \mathbb{F}_{q^{kn}} = \mathbb{F}_{(q^k)^n}$ be defined as $L = K[X]/\langle f \rangle$, where

$$f \mid h_1(X^q)X - h_0(X^q)$$

for some $h_0(X), h_1(X) \in K[X]$ of low degree $\leq d_h$.

Note that $n \leq qd_h + 1$. (Alternatively, in [Jo13, BGJT13] the field representation used is $f \mid X^q h_1 - h_0$, thus $n \leq q + d_h$.)

Let $x := [X] \in L$ and $y := x^q \in L$, so that $x = h_0(y)/h_1(y)$.

Our **target group** is $G = L^*$ of order $m = q^{kn} - 1$.
Our **factor base** is $S := \{x + a \mid a \in K\} \subseteq G$.

Note that $y + b = (x + b^{1/q})^q$ and $x + b^{1/q} \in S$.

# Higher splitting probabilities

## Phase 1: Relation Generation

Since $y = x^q$, $x = h_0(y)/h_1(y)$, for $a, b, c \in K = \mathbb{F}_{q^k}$ we have

$$x^{q+1} + ax^q + bx + c \;=\; \tfrac{1}{h_1(y)}\big(yh_0(y) + ayh_1(y) + bh_0(y) + ch_1(y)\big)\,.$$

Observation: The l. h. s. polynomial $X^{q+1} + aX^q + bX + c \in K[X]$ splits with probability $\approx q^{-3}$, the r. h. s. with probability $\frac{1}{(d_h+1)!}$.

**Theorem (Bluher '04; Helleseth, Kholosha '10)**

*The set of $B \in K^*$ such that $X^{q+1} + BX + B$ splits is the image of $u \mapsto (u^{q^2} - u)^{q+1}/(u^q - u)^{q^2+1}$, $u \in K \setminus \mathbb{F}_{q^2}$, and has size*

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

This leads ($k, d_h$ fixed, $q \to \infty$) to a polynomial time algorithm for solving the Discrete Logs of all factor base elements [GGMZ13].

# Linear system

**Phase 2: Linear Algebra**

Let $A$ be a factor base preserving automorphism group.

- Have $N \approx q^k/|A|$ variables.
- Need to generate $M > N$ relations.

Let $B$ be the $M \times N$ matrix of the relations' coefficients.
We find a nonzero vector $v$ with $Bv = 0$ modulo $m_*$, the product of the large prime factors of the group order $m$.

Possible preprocessing step: Structured Gaussian Elimination

Sparse Linear Algebra solver: Lanczos' or Wiedemann's method

Cost per *Lanczos iteration*: 2 sparse matrix-vector products,
3 scalar multiplications, 2 inner products

# Individual logarithm

## Phase 3: Descent Tree

We build up the descent tree in different stages:

- degree two elements elimination [GGMZ13, Jo13]
- small degree Gröbner Basis descent [Jo13]
- large degree classical descent
- initial split

A further descent method is asymptotically the fastest but not (yet) practical:

- descent by Linear Algebra [BGJT13]

# Gröbner Basis descent

- For any $f, g \in K[X]$ there holds

$$g(x) \prod_{\alpha \in \mathbb{F}_q} \big(f(x) - \alpha g(x)\big) \;=\; f(x)^q g(x) - f(x) g(x)^q \,.$$

- Since $x^q = y$ we can write $a(x)^q = \tilde{a}(y)$ with $\deg \tilde{a} = \deg a$.
- The r.h.s. equals $\tilde{f}(y)\, g(h_0/h_1(y)) - f(h_0/h_1(y))\, \tilde{g}(y)$, which has (assuming $\delta_f \geq \delta_g$) low degree $d_h \delta_f + \delta_g$.

## Joux's GB descent

Let $Q(y)$ to be eliminated. The equation r.h.s.$(y) \equiv 0 \mod Q(y)$ is a bilinear quadratic system in the $\mathbb{F}_q$-variables of coefficients of $f$ and $g$. If the cofactor is $\delta_f$-smooth we have eliminated $Q(y)$.

We have $(\delta_f + \delta_g + 2)k$ variables and $\delta_Q k$ equations.

# Degree two elimination

1. Consider the GB descent setup

$$\tilde{f}(y)\, g(h_0/h_1(y)) - f(h_0/h_1(y))\, \tilde{g}(y) \equiv 0 \mod Q(y)$$
$$(\delta_f + \delta_g + 2)k \text{ variables}, \ \delta_Q k \text{ equations}$$

On-the-fly degree two elimination [GGMZ13]: For $\delta_Q = 2$ let $\delta_f = \delta_g = 1$, which *works* for $d_h \leq 2, \ k > 3$.

2. *Alternatively*, consider Phase 1 equation

$$x^{q+1} + ax^q + bx + c \ = \ \tfrac{1}{h_1(y)}\big(yh_0(y) + ayh_1(y) + bh_0(y) + ch_1(y)\big).$$

Solving degree two logs in batches [Jo13]: For *each* $u \in K$, substitute $x$ by $Q(x) := x^2 + ux$, consider linear system over factor base $S_u := \{x^2 + ux + v \text{ irreducible} \mid v \in K\}$.

# Overview

A High-Level Description of the Index Calculus Method

ICM Particulars for Finite Fields of Small Characteristic

Example: Discrete Logarithms in $\mathbb{F}_{2^{9234}}$

Supersingular Curves and Impact on Pairings

# Wikipedia



## Discrete logarithm records

From Wikipedia, the free encyclopedia

**Discrete logarithm records** are the best results achieved to date in solving the discrete logarithm problem, which is the problem of finding solutions $x$ to the equation $g^x = h$ given elements $g$ and $h$ of a finite cyclic group $G$. The difficulty of this problem is the basis for the security of several cryptographic systems, including Diffie–Hellman key agreement, ElGamal encryption, the ElGamal signature scheme, the Digital Signature Algorithm, and the elliptic curve cryptography analogs of these. Common choices for $G$ used in these algorithms include the multiplicative group of integers modulo $p$, the multiplicative group of a finite field, and the group of points on an elliptic curve over a finite field.

**Contents** [hide]



### Integers modulo $p$ [edit]

On 18 Jun 2005, Antoine Joux and Reynald Lercier announced the computation of a discrete logarithm modulo a 130-digit (431-bit) strong prime in three weeks, using a 1.15 GHz 16-processor HP AlphaServer GS1280 computer and a number field sieve algorithm.[1]

On 5 Feb 2007 this was superseded by the announcement by Thorsten Kleinjung of the computation of a discrete logarithm modulo a 160-digit (530-bit) safe prime, again using the number field sieve. Most of the computation was done using idle time on various PCs and on a parallel computing cluster.[2]

On 11 Jun 2014, Cyril Bouvier, Pierrick Gaudry, Laurent Imbert, Hamza Jeljeli and Emmanuel Thomé announced the computation of a discrete logarithm modulo a 180 digit (596-bit) safe prime using the number field sieve algorithm.[3]

### Finite fields [edit]

The current record (as of January 2014) in a finite field of characteristic 2 was announced by Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel on 31 January 2014. This team was able to compute discrete logarithms in GF($2^{9234}$) using about 400,000 core hours. New features of this computation include a modified method for obtaining the logarithms of degree two elements and a systematically optimized descent strategy.[4]

# Discrete logarithms in $\mathbb{F}_{2^{9234}}$

We consider the field $L = \mathbb{F}_{2^{9234}}$ as the field extension

$$\mathbb{F}_{(2^{18})^{513}} \cong \mathbb{F}_{2^{18}}[X] / \langle X^{513} - c \rangle ,$$

where $c$ is a primitive element of $\mathbb{F}_{2^{18}}$, i.e., $L$ is a twisted Kummer extension over $\mathbb{F}_{2^9}$. We have $q = 2^9$, $k = 2$, $n = 513$.

- Let $A$ be the group of automorphisms of $L$ that preserve $\mathbb{F}_{2^9}$, which is generated by the $2^9$-power Frobenius map, so that $|A| = 1026$.
- The factor base consists of the degree one and the irreducible degree two polynomials over $K = \mathbb{F}_{2^{18}}$.
- We group the irreducible degree two polynomials into $v$-batches $S_v = \{X^2 + uX + v \mid u \in K\}$ of size $2^{17}$ and let $A$ act on the set of $S_v$ classes, resulting in 256 orbits.

# Implementation details

- The computation of the logs of the *degree one* elements was done by solving a linear system in 256 variables.
- For the *degree two* elements, considering the orbits of $S_v$ classes, we obtained 256 linear systems in $2^{17}$ variables. We solved these systems using a C/OpenMP implementation of the iterative Lanczos method.
- *Gröbner Basis* descent by a Magma V2.16-12 implementation. The Magma implementation computes the discrete logarithm of an element of degree $\leq 7$ in a few seconds, of degree 8 in 45 minutes, and of degree 9 in 5 hours, on average.
- *Classical descent* performed by a C++/NTL implementation. We optimised the classical descent stage using a careful bottom-up analysis, to minimise Magma running time.

relation generation in 640 h, linear algebra in 258 048 h, classical and GB descent in 138 721 h, totalling in about *400 k core hours*

# Breaking a DLP challenge in $\mathbb{F}_{2^{9234}}$

On 31 Jan 2014 we [GKZ] announced that $\beta_\pi = (x+1)^a$, where $a =$

1257796316510563582835232315320414281340553097781591888015419891972112414693040723359410 59
2819620054540516726070297615221914385977996245594986628850744829762781379786539611876027 85
9635211039011535260445346035354229315737970748103980003954956383664556300359925295599299 02
1086797158954535349662505785171419950607742659915247928455183040650112918576760494317405 83
9500867698950480424124992381486947135040691585318036322784283286505743723222916012003228 12
2646787787608127448464630141853680229697843773627380900392345721807674108669812699560627 94
7781946439921270882486777764895533828493394889992989962386501745697746362950392394311310 34
7359197438479421926417535028150113691845480725642558782528984067457912635161678026919865 77
5699076751288844966791632479302756473439628913862368132872316967065146189182179993653077 61
3471266557374194141389391840009226010848606440484943951036702975567228105270245489726935 86
8724905858898787303020603799802524293269325348977508513764535408533816752555623074363282 27
3238382125649384955044575726720070402345380956886693231953262526506937335524439862770250 96
1452478686335228292960013361862726096259693767640697842262953072383072374264096235400623 82
2401578608559222986042028807542464936596853381863393340066643552700210891690213197575446 88
7508091818149816922182720710859458011981882152251890531890712400277777793808464061263498 81
4807607931620053047743133851882485672097644274780107358940677095370687282783127900363907 50
7840107828363573053970215885329112020386618107876604970297230000308455240418160289565859 72
6786046788491755695501878920244414400633071559033890492681437639473689631411777094096682 19
0605302103600594909519140113174451720190827106708120852648762438697994624020258064941105 19
0185187302197496349547073658091928610271053635873086802217940591502232862169337148524943 72
7127651097394341372490996098855428920483415877640628514117107029620945039598088894042809 88
8185896850789485864462340344820074003816791560798398920964170638732149972484698800065754 68
5048240568908000395724272228188214466481922695800965893402812581654171086799661289813215 41
7213214734725909611737408308012419421252106594399610633634591608808596473023714346196625 88
8482317277763406488409357268153873329490331006580785678288079185481076831613191857815421 11
5194794969864570034744985160109907748059284511038328517626386479635241779860392192412319 93
0500261758798773211851188419870966987533549792746212966871162046864446618106160170209322 18
9167238854166963380163378506252137281731587481354737898289633496100612122358689831678494 18
3214001460547336159359657251274988267177914893498286320339419218271773917636439613324554 28
7610224404525212307785056810461628707919731127095852418872838478816691911943733494839201 70
9849889522644423283168715339162864650889430946028781837347037876729785875757 2603 .

# Overview

A High-Level Description of the Index Calculus Method

ICM Particulars for Finite Fields of Small Characteristic

Example: Discrete Logarithms in $\mathbb{F}_{2^{9234}}$

Supersingular Curves and Impact on Pairings

# Revised security standards

| $k$ | $g = 1$ | $g = 2$ |
|---|---|---|
| $p = 2$ | $k = 4$ $q^k = 2^{4 \cdot 1223}$ | $k = 12$ $q^k = 2^{12 \cdot 367}$ |
| $p = 3$ | $k = 6$ $q^k = 3^{6 \cdot 509}$ | |

Do the new DLP algorithms have an impact on the security standards? Note: $\mathbb{F}_{q^k}$ need to be embedded into a larger field.

- Analysis [AMOR13]: DLP in $\mathbb{F}_{q^k}$
  - for $q^k = 2^{4 \cdot 1223}$ probably remains 128 bit secure
  - for $q^k = 2^{12 \cdot 367}$ computable in $2^{95}$ operations
  - for $q^k = 3^{6 \cdot 509}$ computable in $2^{74}$ operations
- New Analysis [GKZ14a]: DLP in $\mathbb{F}_{q^k}$
  - for $q^k = 2^{4 \cdot 1223}$ computable in $2^{59}$ operations
  - for $q^k = 2^{12 \cdot 369}$ in $2^{48}$ operations totally broken

Main features of the improvement:

1. using $f \mid h_1(X^q)X - h_0(X^q)$, $\delta h_i = 5, 6$, allows a smaller $q$
2. irreducible even degree polynomials over $\mathbb{F}_{q^k}$ factor over $\mathbb{F}_{q^{2k}}$

# A supersingular binary curve target field

Consider the supersingular *elliptic curve*

$$E_0 \,/\, \mathbb{F}_{2^{1223}} : \;\; Y^2 + Y = X^3 + X \,,$$

which has a subgroup of prime order $r = (2^{1223} + 2^{612} + 1)/5$, of bitlength $1221$. This curve was proposed for 128-bit secure pairing-based protocols and had many optimised implementations.

We consider $\mathbb{F}_{2^{8 \cdot 1223}} = \mathbb{F}_{q^n}$ with $q = 2^8$, $n = 1223$ given by the degree $n$ irreducible factor $f$ of $h_1(X^q)X - h_0(X^q)$, with

$$h_0 = X^5 + tX^4 + tX^3 + X^2 + tX + t \,, \quad h_1 = X^5 + X^4 + X^3 + X^2 + X + t \,,$$

where $t \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$; the target element is in the subfield $\mathbb{F}_{2^{4 \cdot 1223}}$.

- we begin the classical descent over $\mathbb{F}_{2^4}$
- we switch to $\mathbb{F}_q = \mathbb{F}_{2^8}$ for the Gröbner basis descent

# Linear algebra cost

We wish to obtain the logarithms of all irreducible elements of degree $\leq 4$ over $\mathbb{F}_q$. There are $\approx q^4/4 = 2^{30}$ such elements.

Since the degree 1223 extension is defined over $\mathbb{F}_{2^2}$, the Galois group $A = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{2^2})$ of size 4 acts on the factor base. This *reduces* the number of variables to about $2^{28}$.

To obtain the logarithms of the factor base elements,

- either work over $\mathbb{F}_{q^k}$ with $k = 3$ and $k = 4$, as described,
- or employ a trick (use GB descent setup, work with $k = 1$) to decrease the *average row weight* of the bottleneck $2^{28} \times 2^{28}$ system for $d = 4$ to about $q/4 = 64$.

Considering Lanczos' algorithm results in a cost of $2^{59.0}\, M_r$, where $M_r$ denotes *multiplication modulo* $r$.
This is equivalent to about $2^{28}$ core hours.

# Descent cost

Assume the logarithms of elements of degree $\leq 4$ are known.

*GB descent* for degree 5...15 (implemented in Magma, using Faugere's F4 algorithm): Average times (in $M_r$ operations) for rewriting a polynomial as a product deg $\leq 4$ elements: $C[5..15] =$

$$[\,2^{14.4}, 2^{20.4}, 2^{20.5}, 2^{25.9}, 2^{25.8}, 2^{26.9}, 2^{27.0}, 2^{31.1}, 2^{31.2}, 2^{32.2}, 2^{32.6}\,]\,.$$

*Classical descent* over $\mathbb{F}_{2^4}$ and one "joker":

- $\mathbf{d_Q = 26}$ to $\mathbf{m = 15}$. Direct cost $2^{39.0}\,M_r$, subsequent cost $2^{36.9}\,M_r$. Here, we factor even degree polynomials into polynomials of half the degree over $\mathbb{F}_q$.
- $\mathbf{d_Q = 36}$ to $\mathbf{m = 26}$. Direct $2^{42.4}\,M_r$, subsequent $2^{42.9}\,M_r$.
- $\mathbf{d_Q = 94}$ to $\mathbf{m = 36}$. Direct $2^{46.7}\,M_r$, subsequent $2^{47.4}\,M_r$.
- **Initial split** to **94**: Direct $2^{51.1}\,M_r$, subsequent $2^{51.8}\,M_r$.

Total descent cost equivalent of $2^{52.5}\,M_r$ (or $2^{22}$ core hours).

# Solving the DLP in a supersingular genus 2 curve

The Jacobian of the supersingular *hyperelliptic curve*

$$H_0/\mathbb{F}_{2^{367}} : Y^2 + Y = X^5 + X^3$$

has a prime order $r = (2^{734}+2^{551}+2^{367}+2^{184}+1)/(13 \cdot 7170258097)$ subgroup of bitlength $698$, which is contained in $\mathbb{F}_{2^{12 \cdot 367}}$.

- Let $q = 64$, define $\mathbb{F}_{2^{12 \cdot 367}} = \mathbb{F}_{2^{12}}[X]/\langle f \rangle$, where $f \in \mathbb{F}_2[X]$ is the irreducible degree $367$ divisor of $h_1(X^q)X - h_0(X^q)$, with

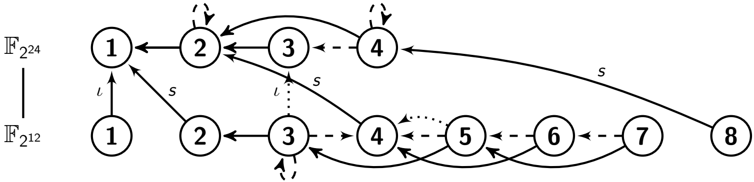
$$h_0 = X^6 + X^4 + X^2 + X + 1 , \quad h_1 = X^5 + X^3 + X + 1 .$$

- We consider relations over $\mathbb{F}_{q^4} = \mathbb{F}_{2^{24}}$. The automorphism group $A = \mathrm{Gal}(\mathbb{F}_{2^{24}}/\mathbb{F}_2)$ of size $24$ acts on the factor base $S$. This *reduces* the linear algebra system to $699\,252$ variables, which was solved in $4\,896$ core hours.

# Descent implementation details

We performed a continued fraction *initial split* and degree-balanced *classical descent* to degrees $\leq 8$ in 38 224 core hours.

*Small degree descent* flowchart, using on-the-fly elimination and Gröbner Basis descent, as well as recursive techniques:




This phase required 8 432 core hours on Magma V2.20-1. In total we used about *52 240 core hours*, equivalent to about $2^{48}\ M_r$.

# A new descent method [GKZ14b]

Idea: Use $2 \to 1$ descent over $\mathbb{F}_{q^d}$ for a $2d \to d$ descent over $\mathbb{F}_q$.

*Non-heuristic* $2 \to 1$ descent: Assume $h_1 = 1$, $\delta_{h_0} = 2$.

$$x^{q+1} + ax^q + bx + c \;=\; yh_0(y) + ay + bh_0(y) + c$$

We can eliminate $Q(y)$, $\delta_Q = 2$, if there is $(a, b, c)$ such that

1. r. h. s. is divisible by $Q(y)$: $b = at_Q + v_Q$, $c = ar_Q + s_Q$,
2. l. h. s. splits: from Bluher's theorem, if

$$B \;=\; \frac{(b - a^q)^{q+1}}{(c - ab)^q} \;\in\; \mathrm{Im}\left(u \mapsto \frac{(u^{q^2} - u)^{q+1}}{(u^q - u)^{q^2+1}}\right).$$

**Result:** Success whenever the curve $C$ contains enough points.

$$C:\;(u^{q^2} - u)^{q+1}(-ta^2 + (-v + r)a + s)^q$$
$$= (u^q - u)^{q^2+1}(-a^q + ta + v)^{q+1}$$

# References


- R. Barbulescu, P. Gaudry, A. Joux, E. Thomé: *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, EUROCRYPT 2014, **eprint.iacr.org/2013/400**

- F. Göloğlu, R. Granger, G. McGuire, J. Zumbrägel: *On the Function Field Sieve and the Impact of Higher Splitting Probabilities*, CRYPTO 2013, **eprint.iacr.org/2013/074**

- A. Joux: *A New Index Calculus Algorithm with Complexity L(1/4+o(1)) in Very Small Characteristic*, Selected Areas in Cryptography 2013, **eprint.iacr.org/2013/095**

- G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez: *Weakness of* $\mathbb{F}_{3^{6\cdot 509}}$ *for Discrete Logarithm Cryptography*, Pairing 2013, **eprint.iacr.org/2013/446**

- R. Granger, T. Kleinjung, J. Zumbrägel: *Breaking '128-bit Secure' Supersingular Binary Curves (or how to solve discrete logarithms in* $\mathbb{F}_{2^{4\cdot 1223}}$ *and* $\mathbb{F}_{2^{12\cdot 367}}$ *)*, CRYPTO 2014, **eprint.iacr.org/2014/119**

- R. Granger, T. Kleinjung, J. Zumbrägel: *On the Powers of 2*, **eprint.iacr.org/2014/300**