A Tale of Two Quasi-Polynomial Algorithms

Robert Granger

robert.granger@epfl.ch

Joint work with Thorsten Kleinjung and Jens Zumbrägel

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

UCD Algebra and Number Theory Seminar, 5th Oct 2015

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Overview

DLP background and smoothness

Resisting smoothness heuristics

Eliminating smoothness heuristics

Overview

DLP background and smoothness

Resisting smoothness heuristics

Eliminating smoothness heuristics

The Discrete Logarithm Problem (DLP)

Let G be a cyclic group of order n, let $\langle g \rangle = G$ and let $h \in G$.

The DLP for (G, g, h) is the problem of finding the unique $k \in \mathbb{Z}/n\mathbb{Z}$ s.t.

$$h = g^k$$

We call k the discrete logarithm of h w.r.t. g, and write $k = \log_g h$.

The Discrete Logarithm Problem (DLP)

Let G be a cyclic group of order n, let $\langle g \rangle = G$ and let $h \in G$.

The DLP for (G, g, h) is the problem of finding the unique $k \in \mathbb{Z}/n\mathbb{Z}$ s.t.

$$h = g^k$$

We call k the discrete logarithm of h w.r.t. g, and write $k = \log_g h$.

Examples:

- Multiplicative group of a finite field $\mathbb{F}_q$
- Group of rational points on an elliptic curve over $\mathbb{F}_q$
- Jacobian of a hyperelliptic curve over $\mathbb{F}_q$

The Discrete Logarithm Problem (DLP)

Let G be a cyclic group of order n, let $\langle g \rangle = G$ and let $h \in G$.

The DLP for (G, g, h) is the problem of finding the unique $k \in \mathbb{Z}/n\mathbb{Z}$ s.t.

$$h = g^k$$

We call k the discrete logarithm of h w.r.t. g, and write $k = \log_g h$.

Examples:

- Multiplicative group of a finite field $\mathbb{F}_q$
- Group of rational points on an elliptic curve over $\mathbb{F}_q$
- Jacobian of a hyperelliptic curve over $\mathbb{F}_q$

If the DLP in a group is 'hard' then one can use it for cryptography: key-agreement, encryption, digital signatures, etc.

The Index Calculus Method

Consider the DLP in $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(I(X))$, where I is a degree n irreducible polynomial in $\mathbb{F}_q[X]$. The ICM consists of two stages:

The Index Calculus Method

Consider the DLP in $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(I(X))$, where I is a degree n irreducible polynomial in $\mathbb{F}_q[X]$. The ICM consists of two stages:

1. Choose a factor base $\mathcal{F}$, usually consisting of all irreducibles of degree $\leq B$. Find multiplicative relations between elements of $\mathcal{F}$ and then compute their logarithms via linear algebra

The Index Calculus Method

Consider the DLP in $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(I(X))$, where I is a degree n irreducible polynomial in $\mathbb{F}_q[X]$. The ICM consists of two stages:

1. Choose a factor base $\mathcal{F}$, usually consisting of all irreducibles of degree $\leq B$. Find multiplicative relations between elements of $\mathcal{F}$ and then compute their logarithms via linear algebra
2. For an arbitrary element, express it as a product of lower degree elements; recurse until all leaves are in $\mathcal{F}$

The Index Calculus Method

Consider the DLP in $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(I(X))$, where I is a degree n irreducible polynomial in $\mathbb{F}_q[X]$. The ICM consists of two stages:

1. Choose a factor base $\mathcal{F}$, usually consisting of all irreducibles of degree $\leq B$. Find multiplicative relations between elements of $\mathcal{F}$ and then compute their logarithms via linear algebra
2. For an arbitrary element, express it as a product of lower degree elements; recurse until all leaves are in $\mathcal{F}$

When applicable, the ICM leads to *subexponential* complexities:

The Index Calculus Method

Consider the DLP in $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(I(X))$, where I is a degree n irreducible polynomial in $\mathbb{F}_q[X]$. The ICM consists of two stages:

1. Choose a factor base $\mathcal{F}$, usually consisting of all irreducibles of degree $\leq B$. Find multiplicative relations between elements of $\mathcal{F}$ and then compute their logarithms via linear algebra
2. For an arbitrary element, express it as a product of lower degree elements; recurse until all leaves are in $\mathcal{F}$

When applicable, the ICM leads to *subexponential* complexities:

Definition

Let $0 \leq \alpha \leq 1$ and let $0 < c \in \mathbb{R}$. The subexponential function $L_Q(\alpha, c)$ for input $Q(= q^n)$ is defined to be

$$L_Q(\alpha, c) \ := \ \exp\left((c + o(1))\,(\log Q)^{\alpha}\,(\log\log Q)^{1-\alpha}\right)$$

Smoothness

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

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

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

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

- Analogous theorem for integers gives an $L(1/2)$ algorithm for prime fields (Pollard '78, Adleman '79 and Merkle '79)

Smoothness

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

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

- Analogous theorem for integers gives an $L(1/2)$ algorithm for prime fields (Pollard '78, Adleman '79 and Merkle '79)
- Rigorously proven by Pomerance '93 and Enge-Gaudry '00 for $\mathbb{F}_p^\times$, and $\mathbb{F}_{q^n}^\times$ with q fixed and $n \to \infty$

Some small to medium characteristic DLP milestones

bitlength	who/when	method	$L(1/3, c)$ with $c =$
127	Coppersmith 1984	Proto-FFS	$[1.526, 1.587]$
401	Gordon-McCurley 1992	Coppersmith's	$[1.526, 1.587]$
N/A	Adleman 1994	FFS	$(64/9)^{1/3} \approx 1.923$
521	Joux-Lercier 2001	FFS	$(32/9)^{1/3} \approx 1.526$
607	Thomé 2001	Coppersmith's	$[1.526, 1.587]$
613	Joux-Lercier 2005	FFS	$(32/9)^{1/3} \approx 1.526$
556	Joux-Lercier 2006	M-FFS	$3^{1/3} \approx 1.442$
676	Hayashi et al. 2010	M-FFS	$(32/9)^{1/3} \approx 1.526$
923	Hayashi et al. 2012	M-FFS	$(32/9)^{1/3} \approx 1.526$
1175	Joux Dec 2012	M-FFS	$2^{1/3} \approx 1.260$
1425	Joux Jan 2013	M-FFS	$2^{1/3} \approx 1.260$

Some small to medium characteristic DLP milestones

bitlength	who/when	method	$L(1/3, c)$ with $c =$
127	Coppersmith 1984	Proto-FFS	$[1.526, 1.587]$
401	Gordon-McCurley 1992	Coppersmith's	$[1.526, 1.587]$
N/A	Adleman 1994	FFS	$(64/9)^{1/3} \approx 1.923$
521	Joux-Lercier 2001	FFS	$(32/9)^{1/3} \approx 1.526$
607	Thomé 2001	Coppersmith's	$[1.526, 1.587]$
613	Joux-Lercier 2005	FFS	$(32/9)^{1/3} \approx 1.526$
556	Joux-Lercier 2006	M-FFS	$3^{1/3} \approx 1.442$
676	Hayashi et al. 2010	M-FFS	$(32/9)^{1/3} \approx 1.526$
923	Hayashi et al. 2012	M-FFS	$(32/9)^{1/3} \approx 1.526$
1175	Joux Dec 2012	M-FFS	$2^{1/3} \approx 1.260$
1425	Joux Jan 2013	M-FFS	$2^{1/3} \approx 1.260$

Assumption of uniformity of the generated polynomials is summarised in the following heuristic:

Some small to medium characteristic DLP milestones

bitlength	who/when	method	$L(1/3, c)$ with $c =$
127	Coppersmith 1984	Proto-FFS	$[1.526, 1.587]$
401	Gordon-McCurley 1992	Coppersmith's	$[1.526, 1.587]$
N/A	Adleman 1994	FFS	$(64/9)^{1/3} \approx 1.923$
521	Joux-Lercier 2001	FFS	$(32/9)^{1/3} \approx 1.526$
607	Thomé 2001	Coppersmith's	$[1.526, 1.587]$
613	Joux-Lercier 2005	FFS	$(32/9)^{1/3} \approx 1.526$
556	Joux-Lercier 2006	M-FFS	$3^{1/3} \approx 1.442$
676	Hayashi et al. 2010	M-FFS	$(32/9)^{1/3} \approx 1.526$
923	Hayashi et al. 2012	M-FFS	$(32/9)^{1/3} \approx 1.526$
1175	Joux Dec 2012	M-FFS	$2^{1/3} \approx 1.260$
1425	Joux Jan 2013	M-FFS	$2^{1/3} \approx 1.260$

Assumption of uniformity of the generated polynomials is summarised in the following heuristic:

'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

Overview

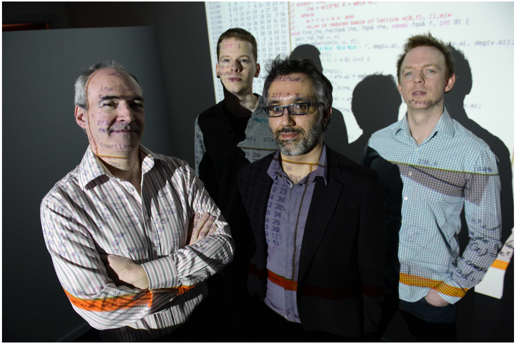
DLP background and smoothness

Resisting smoothness heuristics

Eliminating smoothness heuristics

The GGMZ approach

'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, G., Gary McGuire, & Jens Zumbrägel
(B.P.A. at CRYPTO 2013)

UCD DUBLIN UCD School of Mathematical Sciences

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

CASL

The GGMZ approach

The paper presented:

The GGMZ approach

The paper presented:

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

The GGMZ approach

The paper presented:

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

The GGMZ approach

The paper presented:

- The first (heuristic) *polynomial time* relation generation method for degree one elements
- The first (heuristic) *polynomial time* elimination method for degree two elements
- Example DLP solutions in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$

The GGMZ approach

The paper presented:

- The first (heuristic) *polynomial time* relation generation method for degree one elements
- The first (heuristic) *polynomial time* elimination method for degree two elements
- Example DLP solutions in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$

However, for higher degree irreducibles we did not present any new elimination methods, which limited the descent cost to $L(1/3, (4/9)^{1/3})$.

The Joux-Lercier '06 FFS variation

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. $\implies$ 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 $L_{q^n}(1/3, 3^{1/3})$

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.

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 '02*)

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

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

Degree 1 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. $x^{q+1} + sx^q + (v_0 + su_0)x + (v_1 + su_1)$.

- Recall $\mathcal{B} = \{B \in \mathbb{F}_{q^k}^\times \mid X^{q+1} + BX + B \text{ splits over } \mathbb{F}_{q^k}\}$
- 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

'A new index calculus algorithm with complexity $L(1/4 + o(1))$ in small characteristic'

Antoine Joux

Degree 1 relation generation

Independently of GGMZ, Joux discovered an isomorphic polynomial time degree one relation generation method.

Degree 1 relation generation

Independently of GGMZ, 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 low degree exist s.t. $h_1(X)X^q - h_0(X)$ has an irreducible factor $I(X)$ of degree $n \approx q$

Degree 1 relation generation

Independently of GGMZ, 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 low degree exist s.t. $h_1(X)X^q - h_0(X)$ has an irreducible factor $I(X)$ of degree $n \approx q$
- Consider $X^q - X = \prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$ composed with $X \mapsto \frac{aX+b}{cX+d}$ for $a, b, c, d \in \mathbb{F}_{q^2}$ and $ad \neq bc$. Multiplying by $(cX + d)^{q+1}$ one has

$$(cX+d) \prod_{\alpha \in \mathbb{F}_q} ((a-\alpha c)X+(b-\alpha d)) = (cX+d)(aX+b)^q-(aX+b)(cX+d)^q$$

Degree 1 relation generation

Independently of GGMZ, 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 low degree exist s.t. $h_1(X)X^q - h_0(X)$ has an irreducible factor $I(X)$ of degree $n \approx q$
- Consider $X^q - X = \prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$ composed with $X \mapsto \frac{aX+b}{cX+d}$ for $a, b, c, d \in \mathbb{F}_{q^2}$ and $ad \neq bc$. Multiplying by $(cX + d)^{q+1}$ one has

$$(cX+d) \prod_{\alpha \in \mathbb{F}_q} ((a-\alpha c)X+(b-\alpha d)) = (cX+d)(aX+b)^q-(aX+b)(cX+d)^q$$

- Since $X^q \equiv h_0(X)/h_1(X) \pmod{I(X)}$, this is $\equiv$

$$(ca^q-ac^q)Xh_0(X)+(da^q-bc^q)h_0(X)+(cb^q-ad^q)Xh_1(X)+(db^q-bd^q)h_1(X)$$

Degree 1 relation generation

Independently of GGMZ, 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 low degree exist s.t. $h_1(X)X^q - h_0(X)$ has an irreducible factor $I(X)$ of degree $n \approx q$
- Consider $X^q - X = \prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$ composed with $X \mapsto \frac{aX+b}{cX+d}$ for $a, b, c, d \in \mathbb{F}_{q^2}$ and $ad \neq bc$. Multiplying by $(cX + d)^{q+1}$ one has

$$(cX+d) \prod_{\alpha \in \mathbb{F}_q} ((a-\alpha c)X+(b-\alpha d)) = (cX+d)(aX+b)^q-(aX+b)(cX+d)^q$$

- Since $X^q \equiv h_0(X)/h_1(X) \pmod{I(X)}$, this is $\equiv$

$$(ca^q-ac^q)Xh_0(X)+(da^q-bc^q)h_0(X)+(cb^q-ad^q)Xh_1(X)+(db^q-bd^q)h_1(X)$$

- When r.h.s. splits over $\mathbb{F}_{q^2}$ this gives a relation

Degree ≥ 2 elimination

For degree 2, consider $X^q - X = \prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$ now composed with $X \mapsto \frac{a(X^2+\beta X)+b}{c(X^2+\beta X)+d}$ for a, b, c, d and $\beta \in \mathbb{F}_{q^2}$ and $ad \neq bc$.

Degree ≥ 2 elimination

For degree 2, consider $X^q - X = \prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$ now composed with $X \mapsto \frac{a(X^2+\beta X)+b}{c(X^2+\beta X)+d}$ for a, b, c, d and $\beta \in \mathbb{F}_{q^2}$ and $ad \neq bc$.

For each β:

- All degree 2 factors on l.h.s. are of the form $X^2 + \beta X + \gamma_i$
- When r.h.s. splits over $\mathbb{F}_{q^2}$ one has a relation
- Each of the q^2 systems of size $O(q^2)$ solved separately

Degree ≥ 2 elimination

For degree 2, consider $X^q - X = \prod_{\alpha \in \mathbb{F}_q}(X - \alpha)$ now composed with $X \mapsto \frac{a(X^2+\beta X)+b}{c(X^2+\beta X)+d}$ for a, b, c, d and $\beta \in \mathbb{F}_{q^2}$ and $ad \neq bc$.

For each β:

- All degree 2 factors on l.h.s. are of the form $X^2 + \beta X + \gamma_i$
- When r.h.s. splits over $\mathbb{F}_{q^2}$ one has a relation
- Each of the q^2 systems of size $O(q^2)$ solved separately

For $Q \in \mathbb{F}_{q^2}[X]$ of degree $D > 2$ 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

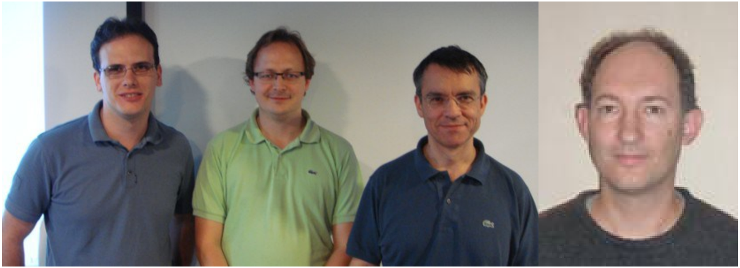
Balancing classical descent with this elimination results in an algorithm with heuristic complexity $L_{q^{2n}}(1/4 + o(1))$.

Ensuing DLP solutions in 2013/14

- 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
- 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
- 3rd May'13, GGMZ: $\mathbb{F}_{2^{3164}}$ in $107,000$ core hours
- 21st May'13, Joux: $\mathbb{F}_{2^{6168}}$ in 550 core hours
- 26th Jan'14, AMOR: $\mathbb{F}_{3^{822}}$ in $< 4,000$ core hours
- 30th Jan'14, GKZ: $\mathbb{F}_{2^{4404}}$ in $52,240$ core hours
- 31st Jan'14, GKZ: $\mathbb{F}_{2^{9234}}$ in $400,000$ core hours
- 26th Feb'14, AMOR: $\mathbb{F}_{3^{978}}$ in $< 9,000$ core hours

The BGJT QPA

'A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic'



Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, & Emmanuel Thomé
(B.P.A. at EUROCRYPT 2014)

The BGJT QPA

For $\mathbb{F}_{q^{2n}}$ with $q \approx n$ let $Q \in \mathbb{F}_{q^2}[X]$ of degree $D > 2$. The key idea behind each elimination step is to take degree 1 relation generation and replace X by $Q(X)$.

The BGJT QPA

For $\mathbb{F}_{q^{2n}}$ with $q \approx n$ let $Q \in \mathbb{F}_{q^2}[X]$ of degree $D > 2$. The key idea behind each elimination step is to take degree 1 relation generation and replace X by $Q(X)$.

The l.h.s. now has the form:

$$(cQ(X)+d)(aQ(X)+b)^q - (aQ(X)+b)(cQ(X)+d)^q = \prod_{i=1}^{q+1}(Q(X)-\gamma_i)$$

The BGJT QPA

For $\mathbb{F}_{q^{2n}}$ with $q \approx n$ let $Q \in \mathbb{F}_{q^2}[X]$ of degree $D > 2$. The key idea behind each elimination step is to take degree 1 relation generation and replace X by $Q(X)$.

The l.h.s. now has the form:

$$(cQ(X)+d)(aQ(X)+b)^q-(aQ(X)+b)(cQ(X)+d)^q=\prod_{i=1}^{q+1}(Q(X)-\gamma_i)$$

The r.h.s. now has the form:

$$(cQ(X)+d)(\bar{a}\bar{Q}(h_0(X)/h_1(X))+\bar{b})^q-(aQ(X)+b)(\bar{c}\bar{Q}(h_0(X)/h_1(X))+\bar{d})^q$$

The BGJT QPA

For $\mathbb{F}_{q^{2n}}$ with $q \approx n$ let $Q \in \mathbb{F}_{q^2}[X]$ of degree $D > 2$. The key idea behind each elimination step is to take degree 1 relation generation and replace X by $Q(X)$.

The l.h.s. now has the form:

$$(cQ(X)+d)(aQ(X)+b)^q-(aQ(X)+b)(cQ(X)+d)^q=\prod_{i=1}^{q+1}(Q(X)-\gamma_i)$$

The r.h.s. now has the form:

$$(cQ(X)+d)(\bar{a}\bar{Q}(h_0(X)/h_1(X))+\bar{b})^q-(aQ(X)+b)(\bar{c}\bar{Q}(h_0(X)/h_1(X))+\bar{d})^q$$

- r.h.s. is $\lceil D/2 \rceil$-smooth with prob. $\approx 1/(D(d_h+1)/(D/2))!$

The BGJT QPA

For $\mathbb{F}_{q^{2n}}$ with $q \approx n$ let $Q \in \mathbb{F}_{q^2}[X]$ of degree $D > 2$. The key idea behind each elimination step is to take degree 1 relation generation and replace X by $Q(X)$.

The l.h.s. now has the form:

$$(cQ(X)+d)(aQ(X)+b)^q-(aQ(X)+b)(cQ(X)+d)^q = \prod_{i=1}^{q+1}(Q(X)-\gamma_i)$$

The r.h.s. now has the form:

$$(cQ(X)+d)(\bar{a}\bar{Q}(h_0(X)/h_1(X))+\bar{b})^q-(aQ(X)+b)(\bar{c}\bar{Q}(h_0(X)/h_1(X))+\bar{d})^q$$

- r.h.s. is $\lceil D/2 \rceil$-smooth with prob. $\approx 1/(D(d_h+1)/(D/2))!$
- Collect $> q^2$ such relations and then express $\log Q$ as a sum of $O(q^2)$ logs of elements of degree at most $\lceil D/2 \rceil$

The BGJT QPA

For $\mathbb{F}_{q^{2n}}$ with $q \approx n$ let $Q \in \mathbb{F}_{q^2}[X]$ of degree $D > 2$. The key idea behind each elimination step is to take degree 1 relation generation and replace X by $Q(X)$.

The l.h.s. now has the form:

$$(cQ(X)+d)(aQ(X)+b)^q - (aQ(X)+b)(cQ(X)+d)^q = \prod_{i=1}^{q+1}(Q(X)-\gamma_i)$$

The r.h.s. now has the form:

$$(cQ(X)+d)(\bar{a}\bar{Q}(h_0(X)/h_1(X))+\bar{b})^q-(aQ(X)+b)(\bar{c}\bar{Q}(h_0(X)/h_1(X))+\bar{d})^q$$

- r.h.s. is $\lceil D/2 \rceil$-smooth with prob. $\approx 1/(D(d_h+1)/(D/2))!$
- Collect $> q^2$ such relations and then express $\log Q$ as a sum of $O(q^2)$ logs of elements of degree at most $\lceil D/2 \rceil$
- Recurse down to linear elements. Heuristic complexity dictated by #nodes in descent tree: tree arity to the power depth $= q^{O(\log n)}$

The BGJT QPA

For $\mathbb{F}_{q^{2n}}$ with $q \approx n$ let $Q \in \mathbb{F}_{q^2}[X]$ of degree $D > 2$. The key idea behind each elimination step is to take degree 1 relation generation and replace X by $Q(X)$.

The l.h.s. now has the form:

$$(cQ(X)+d)(aQ(X)+b)^q-(aQ(X)+b)(cQ(X)+d)^q=\prod_{i=1}^{q+1}(Q(X)-\gamma_i)$$

The r.h.s. now has the form:

$$(cQ(X)+d)(\bar{a}\bar{Q}(h_0(X)/h_1(X))+\bar{b})^q-(aQ(X)+b)(\bar{c}\bar{Q}(h_0(X)/h_1(X))+\bar{d})^q$$

- r.h.s. is $\lceil D/2 \rceil$-smooth with prob. $\approx 1/(D(d_h+1)/(D/2))!$
- Collect $> q^2$ such relations and then express $\log Q$ as a sum of $O(q^2)$ logs of elements of degree at most $\lceil D/2 \rceil$
- Recurse down to linear elements. Heuristic complexity dictated by #nodes in descent tree: tree arity to the power depth $= q^{O(\log n)}$
- This is smaller than $L(\epsilon)$ for any $\epsilon > 0$

Overview

DLP background and smoothness

Resisting smoothness heuristics

Eliminating smoothness heuristics

The GKZ QPA

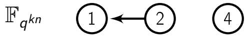
'On the discrete logarithm problem in finite fields of fixed characteristic'
(previously 'On the Powers of 2')
`arxiv:1507.01495`

G., Thorsten Kleinjung, & Jens Zumbrägel

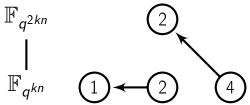
The GKZ QPA

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

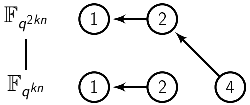
The GKZ QPA



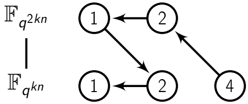
The GKZ QPA



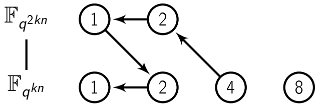
The GKZ QPA



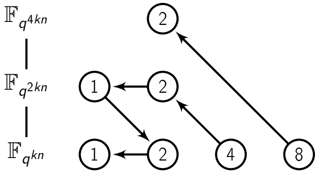
The GKZ QPA



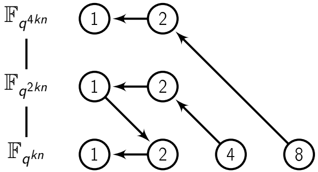
The GKZ QPA



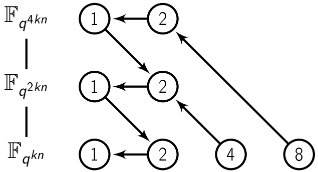
The GKZ QPA



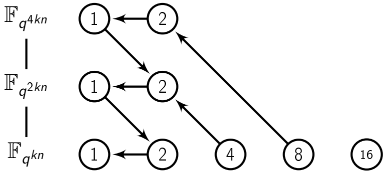
The GKZ QPA



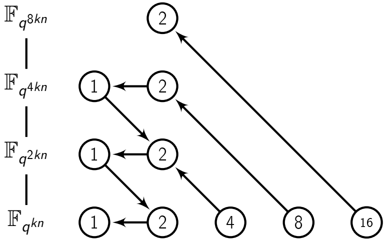
The GKZ QPA



The GKZ QPA

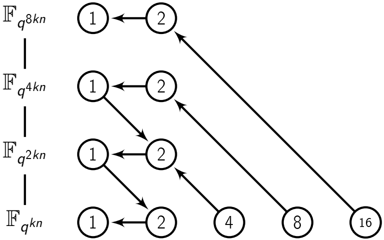


The GKZ QPA



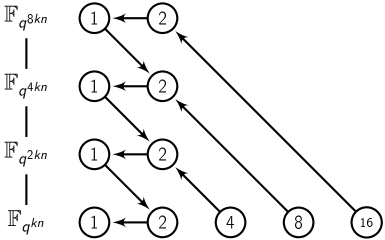
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
2
1
2
1
2
1
2
4
8
16

The GKZ QPA



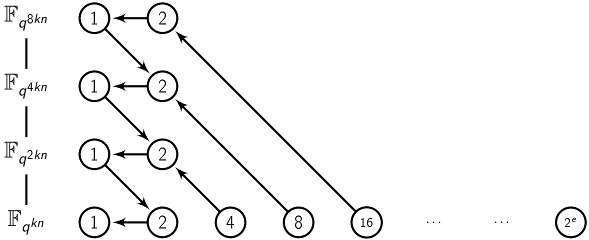
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
1
2
1
2
1
2
4
8
16

The GKZ QPA



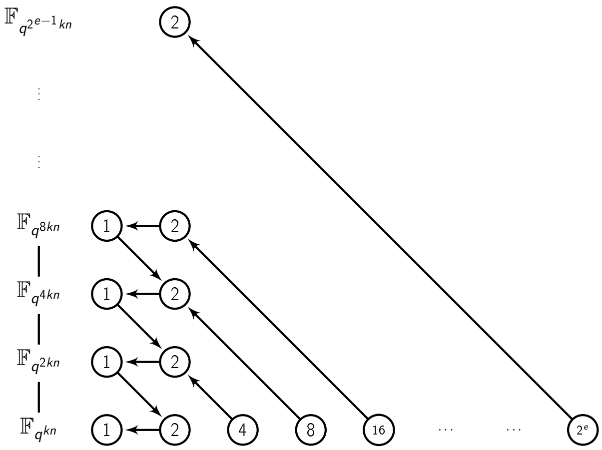
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
1
2
1
2
1
2
4
8
16

The GKZ QPA



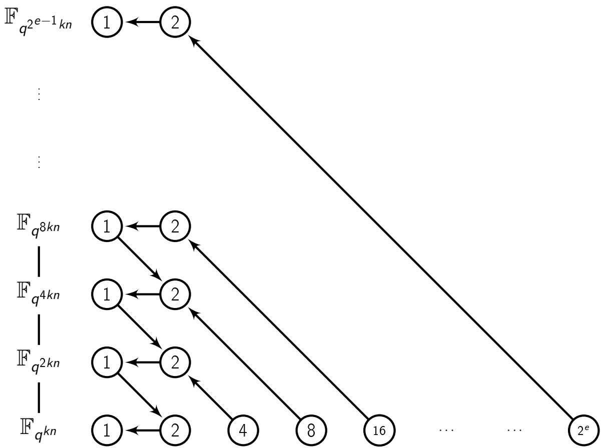
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
4
8
16
2^e

The GKZ QPA



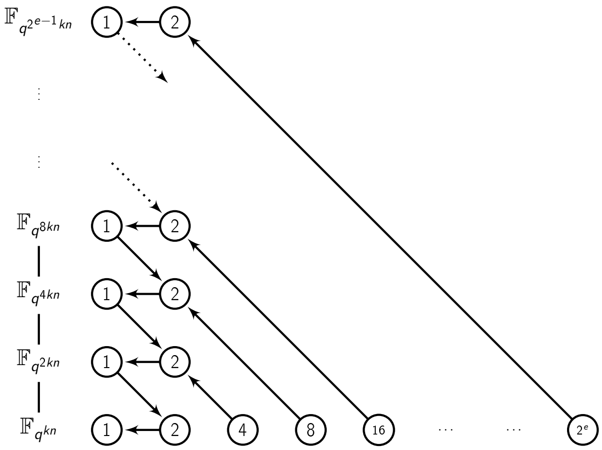
$\mathbb{F}_{q^{2^{e-1}kn}}$
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
4
8
16
2^e

The GKZ QPA



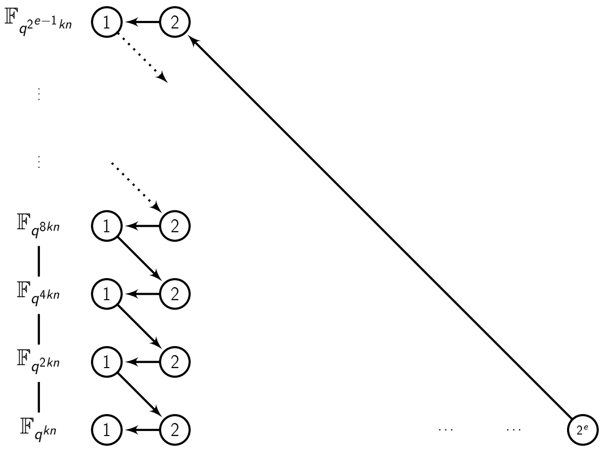
$\mathbb{F}_{q^{2^{e-1}kn}}$
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
4
8
16
2^e

The GKZ QPA

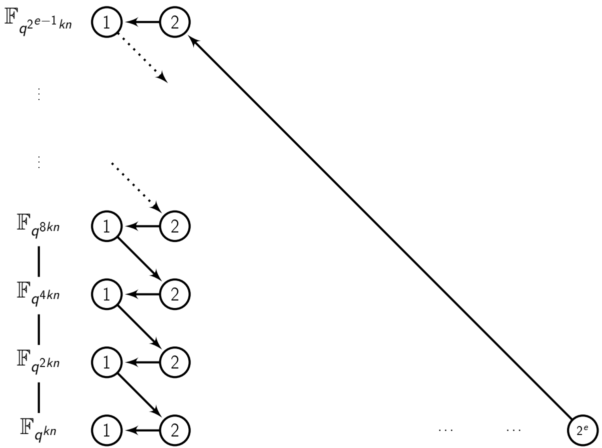


$\mathbb{F}_{q^{2^{e-1}kn}}$
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
4
8
16
2^e

The GKZ QPA

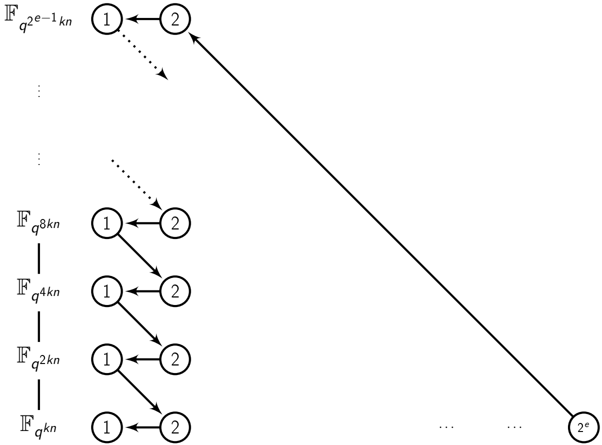

$\mathbb{F}_{q^{2^{e-1}kn}}$
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
2^e

The GKZ QPA



- For an arbitrary element h we compute random $h' = h + r \cdot I$ s.t. $\deg h' = 2^e > 4n$ and h' is irreducible (Wan '97), then descend.

The GKZ QPA



- For an arbitrary element h we compute random $h' = h + r \cdot I$ s.t. $\deg h' = 2^e > 4n$ and h' is irreducible (Wan '97), then descend.
- Complexity is tree arity to the power depth $= q^{\log_2 n + o(\log q)}$

Eliminating smoothness heuristics

- If $d_1 \leq 2$, then r.h.s. cofactor of $Q(y)$ is at most linear $\Longrightarrow$ no smoothness heuristics needed for descent

Eliminating smoothness heuristics

- If $d_1 \leq 2$, then r.h.s. cofactor of $Q(y)$ is at most linear $\Longrightarrow$ no smoothness heuristics needed for descent
- Using a technique due to Enge-Gaudry, one can obviate the need to compute the factor base logs by performing a descent of $g^{\alpha_i} h^{\beta_i}$ for base g, target h and random α_i, β_i, more than q^k times

Eliminating smoothness heuristics

- If $d_1 \leq 2$, then r.h.s. cofactor of $Q(y)$ is at most linear $\implies$ no smoothness heuristics needed for descent
- Using a technique due to Enge-Gaudry, one can obviate the need to compute the factor base logs by performing a descent of $g^{\alpha_i}h^{\beta_i}$ for base g, target h and random α_i, β_i, more than q^k times

Hence no smoothness heuristics are needed!

Ensuring the elimination step works

To eliminate a degree 2 element $Q(y)$ over $\mathbb{F}_{q^{kd}}$, we need to find a Bluher value B and an $s \in \mathbb{F}_{q^{kd}}$ that satisfy

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

Theorem (*Helleseth-Kholosha '10*)

For $kd \geq 3$ the set of elements $B \in \mathbb{F}_{q^{kd}}^\times$ s.t. $X^{q+1} + BX + B$ splits completely over $\mathbb{F}_{q^{kd}}$ is the image of $\mathbb{F}_{q^{kd}} \setminus \mathbb{F}_{q^2}$ under the map

$$u \mapsto \frac{(u - u^{q^2})^{q+1}}{(u - u^q)^{q^2+1}}$$

Thus need lower bound for $\#\{(s,u) \in \mathbb{F}_{q^{kd}} \times (\mathbb{F}_{q^{kd}} \setminus \mathbb{F}_{q^2})\}$ on the curve

$$(u - u^{q^2})^{q+1}(-u_0 s^2 + (u_1 - v_0)s + v_1)^q - (u - u^q)^{q^2+1}(-s^q + u_0 s + v_0)^{q+1} = 0.$$

Main Results

Theorem

Given a prime power $q > 61$ *that is not a power of* 4, *an integer* $k \geq 18$, *coprime polynomials* $h_0, h_1 \in \mathbb{F}_{q^k}[X]$ *of degree at most two and an irreducible degree* l *factor* I *of* $h_1 X^q - h_0$, *the DLP in* $\mathbb{F}_{q^{kl}}^\times$ *where* $\mathbb{F}_{q^{kl}} \cong \mathbb{F}_{q^k}[X]/(I)$ *can be solved in expected time*

$$q^{\log_2 l + O(k)}$$

Main Results

Theorem

Given a prime power $q > 61$ that is not a power of 4, an integer $k \geq 18$, coprime polynomials $h_0, h_1 \in \mathbb{F}_{q^k}[X]$ of degree at most two and an irreducible degree l factor I of $h_1 X^q - h_0$, the DLP in $\mathbb{F}_{q^{kl}}^{\times}$ where $\mathbb{F}_{q^{kl}} \cong \mathbb{F}_{q^k}[X]/(I)$ can be solved in expected time

$$q^{\log_2 l + O(k)}$$

Using Kummer theory, such h_i are known to exist for $l = q - 1$, giving:

Main Results

Theorem

Given a prime power $q > 61$ *that is not a power of* 4, *an integer* $k \geq 18$, *coprime polynomials* $h_0, h_1 \in \mathbb{F}_{q^k}[X]$ *of degree at most two and an irreducible degree* l *factor* I *of* $h_1 X^q - h_0$, *the DLP in* $\mathbb{F}_{q^{kl}}^{\times}$ *where* $\mathbb{F}_{q^{kl}} \cong \mathbb{F}_{q^k}[X]/(I)$ *can be solved in expected time*

$$q^{\log_2 l + O(k)}$$

Using Kummer theory, such h_i are known to exist for $l = q - 1$, giving:

Theorem

For every prime p *there exist infinitely many explicit extension fields* $\mathbb{F}_{p^n}$ *for which the DLP in* $\mathbb{F}_{p^n}^{\times}$ *can be solved in expected quasi-polynomial time*

$$\exp\left((1/\log 2 + o(1))(\log n)^2\right)$$

Comparison between the QPAs

	BGJT	GKZ
Field rep.	Heuristic	Heuristic
Elimination step	Heuristic (x 2)	Proven
Tree arity	$O(q^2)$	q
Complexity	$q^{O(\log n / \log \log q)}$	$q^{\log_2 n + o(\log q)}$
Practicality	Not yet	Yes, in $\mathbb{F}_{3^{2395}}$ and $\mathbb{F}_{2^{1279}}$

Final remarks

- There is more than one way to skin a cat!
- Removing the field heuristic would be great, but seems very hard
- There is no representational obstruction to a poly-time algorithm
- Extending ideas to large prime fields currently seems impossible...

It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way — in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or evil, in the superlative degree of comparison only.

- A Tale of Two Cities

ry of Edwin Drood,
cle John Jasper,
arf which some believe
der weapon.