On the Interplay Between Theory and Practice in Small Characteristic DLPs

Robert Granger

Based on joint work with Faruk Göloğlu, Gary McGuire & Jens Zumbrägel, and Thorsten Kleinjung & Jens Zumbrägel

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

CATREL DLP Workshop, 1st Oct 2015

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

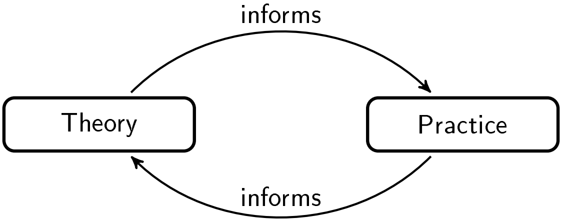
Conclusions

Conclusions

Mathematical discovery is fundamentally an experimental science.

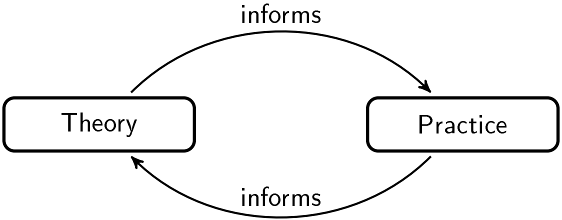
Conclusions

Mathematical discovery is fundamentally an experimental science.



Conclusions

Mathematical discovery is fundamentally an experimental science.



An Obvious Counterpoint

In contrast to the experimental sciences, in mathematics one can irrefutably prove things!

Overview

Background and Degree 2 Elimination

Case Study: Computing DLPs in $\mathbb{F}_{2^{4404}}$

The GKZ Quasi-Polynomial Algorithm

Overview

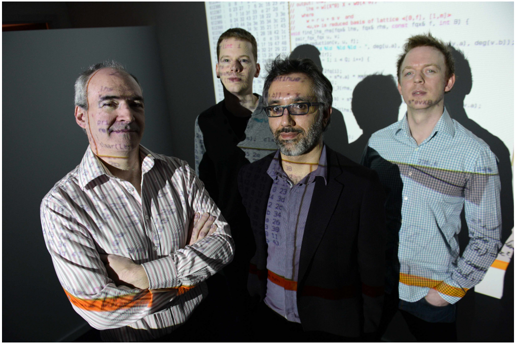
Background and Degree 2 Elimination

Case Study: Computing DLPs in $\mathbb{F}_{2^{4404}}$

The GKZ Quasi-Polynomial Algorithm

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

UCD School of Mathematical Sciences

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

CASL

The GGMZ approach

Let the target field be $\mathbb{F}_{q^{kn}}$ with $k \geq 1$ small and fixed and $n = O(q)$.

- Assume there exists $h_1, h_0 \in \mathbb{F}_{q^k}[X]$ of low degree d_h s.t.

$$h_1(X^q)X - h_0(X^q) \equiv 0 \pmod{f} \tag{1}$$

  where f is irreducible and of degree n
- Let x be a root of f so that $\mathbb{F}_{q^{kn}} = \mathbb{F}_{q^k}(x)$ and let $y = x^q$. Then by (1) we have $x = h_0(y)/h_1(y)$ and $\mathbb{F}_{q^k}(x) \cong \mathbb{F}_{q^k}(y)$
- Factor base is $\{x + d : d \in \mathbb{F}_{q^k}\}$ (observe $(y + d) = (x + d^{1/q})^q$)

The GGMZ approach

Let the target field be $\mathbb{F}_{q^{kn}}$ with $k \geq 1$ small and fixed and $n = O(q)$.

- Assume there exists $h_1, h_0 \in \mathbb{F}_{q^k}[X]$ of low degree d_h s.t.

$$h_1(X^q)X - h_0(X^q) \equiv 0 \pmod{f} \tag{1}$$

  where f is irreducible and of degree n
- Let x be a root of f so that $\mathbb{F}_{q^{kn}} = \mathbb{F}_{q^k}(x)$ and let $y = x^q$. Then by (1) we have $x = h_0(y)/h_1(y)$ and $\mathbb{F}_{q^k}(x) \cong \mathbb{F}_{q^k}(y)$
- Factor base is $\{x + d : d \in \mathbb{F}_{q^k}\}$ (observe $(y + d) = (x + d^{1/q})^q$)

A Basic Identity

For all $a, b, c \in \mathbb{F}_{q^k}$ we have the following equality in $\mathbb{F}_{q^{kn}}$:

$$x^{q+1} + ax^q + bx + c = \frac{1}{h_1(y)}\left(yh_0(y) + ayh_1(y) + bh_0(y) + ch_1(y)\right)$$

The GGMZ approach

Let the target field be $\mathbb{F}_{q^{kn}}$ with $k \geq 1$ small and fixed and $n = O(q)$.

- Assume there exists $h_1, h_0 \in \mathbb{F}_{q^k}[X]$ of low degree d_h s.t.

$$h_1(X^q)X - h_0(X^q) \equiv 0 \pmod{f} \tag{1}$$

  where f is irreducible and of degree n
- Let x be a root of f so that $\mathbb{F}_{q^{kn}} = \mathbb{F}_{q^k}(x)$ and let $y = x^q$. Then by (1) we have $x = h_0(y)/h_1(y)$ and $\mathbb{F}_{q^k}(x) \cong \mathbb{F}_{q^k}(y)$
- Factor base is $\{x + d : d \in \mathbb{F}_{q^k}\}$ (observe $(y + d) = (x + d^{1/q})^q$)

A Basic Identity

For all $a, b, c \in \mathbb{F}_{q^k}$ we have the following equality in $\mathbb{F}_{q^{kn}}$:

$$x^{q+1} + ax^q + bx + c = \frac{1}{h_1(y)} \left(yh_0(y) + ayh_1(y) + bh_0(y) + ch_1(y) \right)$$

- If both sides split over $\mathbb{F}_{q^k}$ then we have a relation

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

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

Degree 1 relation generation: $k \geq 3$

- 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 $yh_0(y) + ayh_1(y) + bh_0(y) + ch_1(y)$ splits; if so then have a relation
- If $q^{3k-3} > q^k(d_h + 1)!$ then for $d_h \geq 1$ constant we expect to compute logs of degree 1 elements of $\mathbb{F}_{q^{kn}}$ in time

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

Degree 1 relation generation: $k \geq 3$

- Compute $\mathcal{B} = \{B \in \mathbb{F}_{q^k}^\times \mid X^{q+1} + BX + B$ 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 $yh_0(y) + ayh_1(y) + bh_0(y) + ch_1(y)$ splits; if so then have a relation
- If $q^{3k-3} > q^k(d_h + 1)!$ then for $d_h \geq 1$ constant we expect to compute logs of degree 1 elements of $\mathbb{F}_{q^{kn}}$ in time

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

For the base field $\mathbb{F}_{q^2}$, relevant set of triples is

$$\{(a, a^q, c) \mid a \in \mathbb{F}_{q^2} \text{ and } c \in \mathbb{F}_q, c \neq a^{q+1}\}.$$

On the fly degree 2 elimination

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

- For any univariate polynomials w_0, w_1 we have

$$w_0(x^q)\,x + w_1(x^q) = \frac{1}{h_1(y)}\left(w_0(y)\,h_0(y) + w_1(y)\,h_1(y)\right)$$

- Compute a reduced basis of the lattice

$$L_{\bar{Q}} = \{(w_0(Y), w_1(Y)) \in \mathbb{F}_{q^k}[Y]^2 : w_0(Y)\,h_0(Y) + w_1(Y)\,h_1(Y) \equiv 0 \pmod{\bar{Q}(Y)}\}$$

- 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 $(Y + v_0 + su_0, sY + v_1 + su_1) \in L_{\bar{Q}}$
- r.h.s. $(y + v_0 + su_0)\,h_0(y) + (sy + v_1 + su_1)\,h_1(y)$ has degree $d_h + 1$, so cofactor splits with probability $\approx 1/(d_h - 1)!$
- l.h.s. is $(x^q + v_0 + su_0)x + (sx^q + v_1 + su_1)$ which is of the form

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

On the fly degree 2 elimination

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

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

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

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

Alternative solution finding

We need to compute $s \in \mathbb{F}_{q^k}$ that satisfy the equation:

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

- Use an explicit $\mathbb{F}_{q^k}/\mathbb{F}_q$ basis $\{1, \alpha, \ldots, \alpha^{k-1}\}$, and introduce $\mathbb{F}_q$-variables $s_0, \ldots, s_{k-1}$ s.t. $s = s_0 + s_1\alpha + \cdots + s_{k-1}\alpha^{k-1}$
- Gives a quadratic system, solvable in $O((k\binom{2k}{k+1})^\omega)$ $\mathbb{F}_q$-ops
- For fixed k, d_h and $q \to \infty$ this method has cost $O(1)$ $\mathbb{F}_q$-ops, i.e., it has polylogarithmic complexity

Overview

Background and Degree 2 Elimination

Case Study: Computing DLPs in $\mathbb{F}_{2^{4404}}$

The GKZ Quasi-Polynomial Algorithm

Computing DLPs in $\mathbb{F}_{2^{4404}}$

On 30/1/14 we (GKZ) announced the solution of a DLP in the Jacobian of $H_0/\mathbb{F}_2 : Y^2 + Y = X^5 + X^3$ over $\mathbb{F}_{2^{367}}$, which has a subgroup of prime order $r = (2^{734} + 2^{551} + 2^{367} + 2^{184} + 1)/(13 \cdot 7170258097)$ and embedding degree 12.

- $\mathbb{F}_{2^{12}} = \mathbb{F}_2[U]/(U^{12} + U^3 + 1) = \mathbb{F}_2(u)$
- $\mathbb{F}_{2^{367}} = \mathbb{F}_2[X]/(I(X)) = \mathbb{F}_2(x)$ 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 $\mathbb{F}_{2^{367}}$

For small degree elimination, represent $\mathbb{F}_{2^{12}}$ as $\mathbb{F}_{q^2}$ with $q = 2^6$, $k = 2$:

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

Factor base logs and initial descent

To have enough relations for degree one elements of $\mathbb{F}_{2^{4404}}/\mathbb{F}_{2^{12}}$ we would need $q^{2k-3} > (6+1)!$. So we used relations in $\mathbb{F}_{2^{8808}}/\mathbb{F}_{2^{24}}$:

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

$\mathrm{Gal}(\mathbb{F}_{2^{24}}/\mathbb{F}_2)$ acts on the degree 1 factor base $\{x + a \mid a \in \mathbb{F}_{2^{24}}\}$:

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

$\Longrightarrow$ 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 over $\mathbb{F}_{2^{12}}$

We used Joux's small degree elimination, our degree 2 elimination and one other idea.

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

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

- $F^{(q)}(y), G((h_0/h_1)(y)), F((h_0/h_1)(y)), G^{(q)}(y)$ have small degree
- Insisting r.h.s. $\equiv 0 \pmod{\bar{Q}(y)}$ results in bilinear quadratic system
- For solutions check if the cofactor is $(D-1)$-smooth

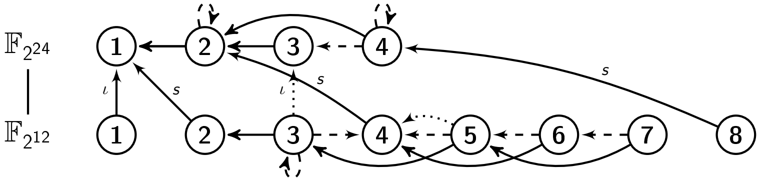
Eliminating small degree elements over $\mathbb{F}_{2^{12}}$

We used Joux's small degree elimination, our degree 2 elimination and one other idea.

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

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

- $F^{(q)}(y), G((h_0/h_1)(y)), F((h_0/h_1)(y)), G^{(q)}(y)$ have small degree
- Insisting r.h.s. $\equiv 0 \pmod{\bar{Q}(y)}$ results in bilinear quadratic system
- For solutions check if the cofactor is $(D-1)$-smooth



Degree 2 elimination over $\mathbb{F}_{2^{24}}$

Let $\bar{Q}(y) \in \mathbb{F}_{2^{24 \cdot 367}}$ be an element to be eliminated.

- As before we have $y = x^{64}$ and $x = h_0(y)/h_1(y)$, and for any univariate polynomials w_0, w_1 we have

$$w_0(x^q)\,x + w_1(x^q) = \frac{1}{h_1(y)}(w_0(y)\,h_0(y) + w_1(y)\,h_1(y))$$

- A reduced basis for the lattice $L_{\bar{Q}}$ is $(u_0, Y + u_1), (Y + v_0, v_1)$, with $u_i, v_i \in \mathbb{F}_{2^{24}}$. For $s \in \mathbb{F}_{2^{24}}$, $(Y + v_0 + su_0, sY + v_1 + su_1) \in L_{\bar{Q}}$
- r.h.s. $\frac{1}{h_1(y)}((y + v_0 + su_0)\,h_0(y) + (sy + v_1 + su_1)\,h_1(y))$ has degree $d_h + 1 = 7$, so cofactor splits with probability $\approx 1/5!$
- l.h.s. is $x^{q+1} + sx^q + (u_{00} + sv_{00})x + (u_{10} + sv_{10})$, which splits if

$$B = \frac{(s^{64} + u_0 s + v_0)^{65}}{(u_0 s^2 + (u_1 + v_0)s + v_1)^{64}}$$

- Probability of success is $\approx 1 - (1 - 1/5!)^{64} \approx 0.415$, but amplified to near certainty using recursive techniques

New 'traps' in the descent

During the descent, we encountered several polynomials $\bar{Q}(Y)$ that were not eliminable via Joux's method.

- All were factors of $h_1(Y) \cdot c + h_0(Y)$ for $c \in \mathbb{F}_{2^{12}}$ or $\mathbb{F}_{2^{24}}$ and hence $h_0(Y)/h_1(Y) \equiv c \pmod{\bar{Q}(Y)}$
- $\implies$ r.h.s. equals $F^{(q)}(Y)G(c) + F(c)G^{(q)}(Y) \pmod{\bar{Q}(Y)}$
- This can't be zero mod $\bar{Q}(Y)$ if the degrees of F and G are smaller than the degree of $\bar{Q}$, unless F and G are both constants
- However, writing $h_1(Y) \cdot c + h_0(Y) = \bar{Q}(Y) \cdot R(Y)$ we have $\bar{Q}(Y) = h_1(Y) \cdot ((h_0/h_1)(Y) + c)/R(Y) = h_1(Y) \cdot (X + c)/R(Y)$
- Hence $\log(\bar{Q}(y)) \equiv \log(x + c) - \log(R(y))$, since $\log(h_1(y)) \equiv 0$
- In all the cases we encountered, the log of $R(y)$ was solvable
- Note that these traps are different to those identified by Cheng, Wan and Zhuang, which are factors of $h_1(X^q)X - h_0(X^q)$ (or of $h_1(X)X^q - h_0(X)$ if using Joux's representation)

Overview

Background and Degree 2 Elimination

Case Study: Computing DLPs in $\mathbb{F}_{2^{4404}}$

The GKZ Quasi-Polynomial Algorithm

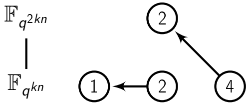
The GKZ QPA

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

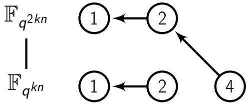
The GKZ QPA

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

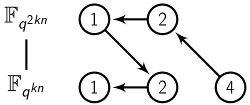
The GKZ QPA



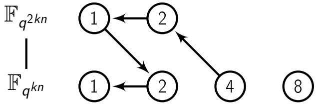
The GKZ QPA



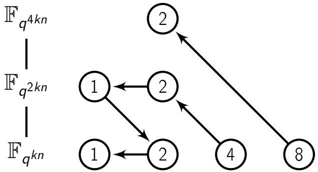
The GKZ QPA



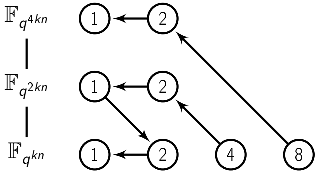
The GKZ QPA



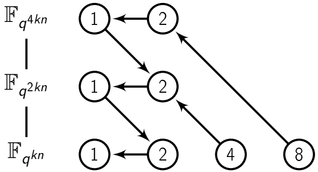
The GKZ QPA



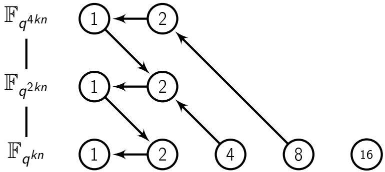
The GKZ QPA



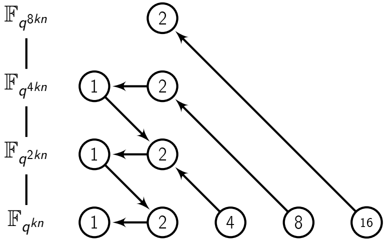
The GKZ QPA



The GKZ QPA

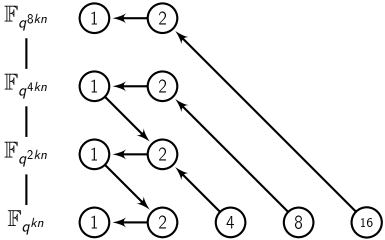


The GKZ QPA

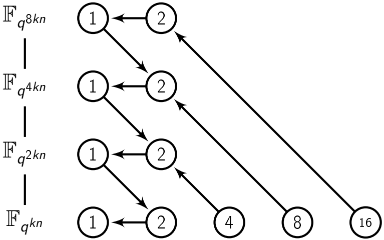


$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
2
1
2
1
2
1
2
4
8
16

The GKZ QPA

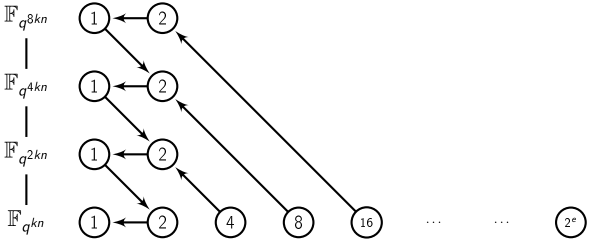

$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
1
2
1
2
1
2
4
8
16

The GKZ QPA

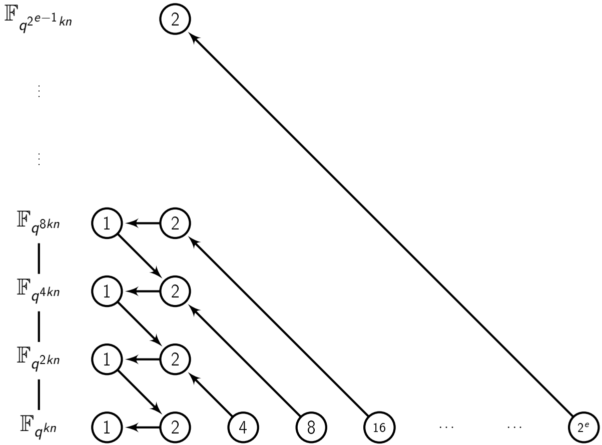


$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
1
2
1
2
1
2
4
8
16

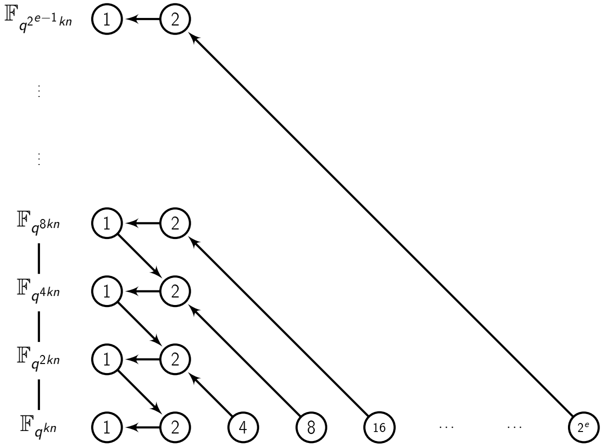
The GKZ QPA


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

The GKZ QPA

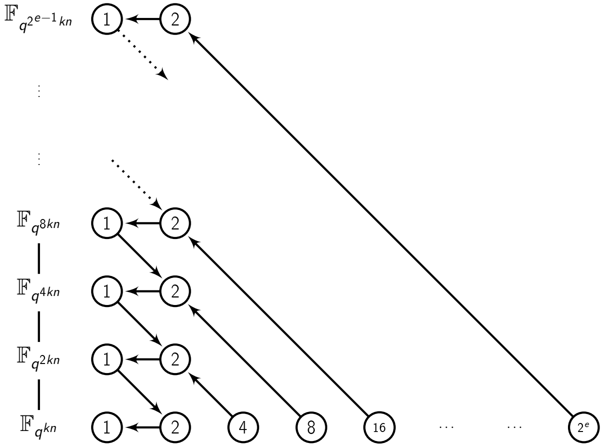

$\mathbb{F}_{q^{2^{e-1}kn}}$
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
4
8
16
2^e

The GKZ QPA



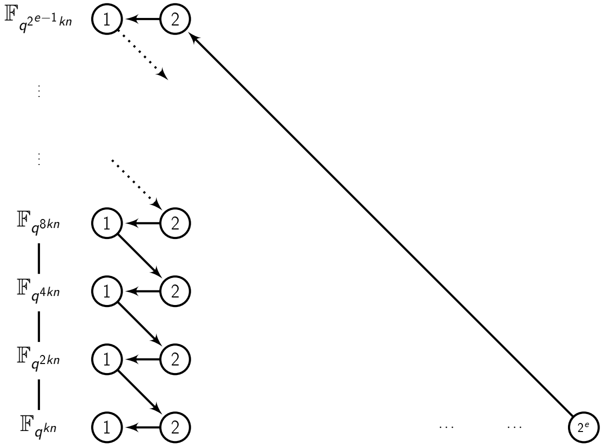
$\mathbb{F}_{q^{2^{e-1}kn}}$
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
4
8
16
2^e

The GKZ QPA



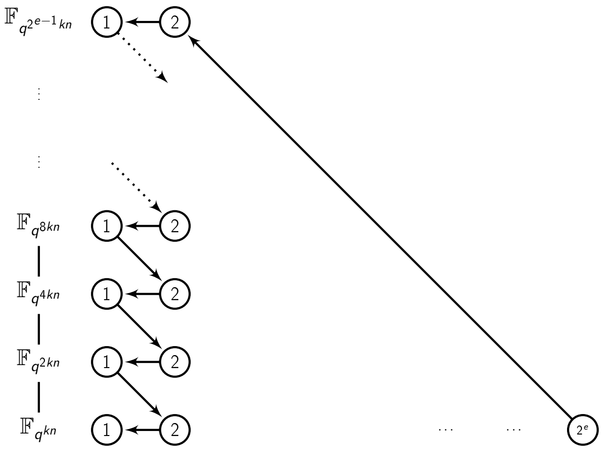
$\mathbb{F}_{q^{2^{e-1}kn}}$
$\mathbb{F}_{q^{8kn}}$
$\mathbb{F}_{q^{4kn}}$
$\mathbb{F}_{q^{2kn}}$
$\mathbb{F}_{q^{kn}}$
1
2
4
8
16
2^e

The GKZ QPA



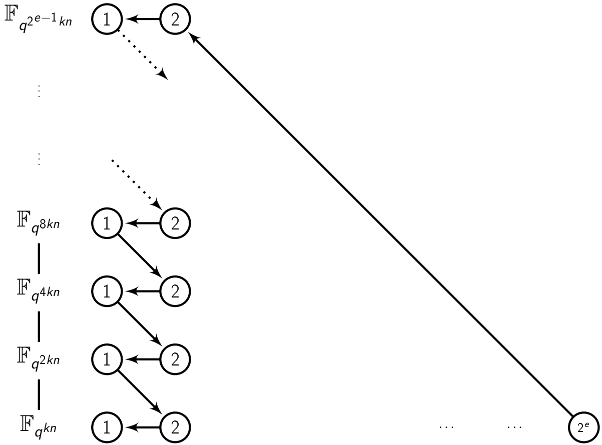
$\mathbb{F}_{q^{2^{e-1}kn}}$
1
2
$\vdots$
$\vdots$
$\mathbb{F}_{q^{8kn}}$
1
2
$\mathbb{F}_{q^{4kn}}$
1
2
$\mathbb{F}_{q^{2kn}}$
1
2
$\mathbb{F}_{q^{kn}}$
1
2
$\cdots$
$\cdots$
2^e

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 $d_h \leq 2$, then r.h.s. cofactor of $\bar{Q}(y)$ is at most linear $\Longrightarrow$ no smoothness heuristics needed for the descent

Eliminating smoothness heuristics

- If $d_h \leq 2$, then r.h.s. cofactor of $\bar{Q}(y)$ is at most linear $\Longrightarrow$ no smoothness heuristics needed for the 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 $d_h \leq 2$, then r.h.s. cofactor of $\bar{Q}(y)$ is at most linear $\Longrightarrow$ no smoothness heuristics needed for the 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 $\bar{Q}(y)$ 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*

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

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

(actual) Concluding remarks

- Implementing examples can be very informative
- Degree 2 elimination seems to be fundamental, sometimes complex, and theoretically very interesting (see Thorsten's talk next)
- Proving observations can be hard but worthwhile, especially due to presence of 'unknown unknowns'
- Some basic unanswered questions:
  - Can one remove the field heuristic?
  - Do faster algorithms exist for small characteristic?
  - Do faster algorithms exist for large(r) characteristic?

A 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 $\mathbb{F}_{2^{1279}}$