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

Claude Shannon Institute
Complex & Adaptive Systems Laboratory
School of Mathematical Sciences
University College Dublin, Ireland

21st August, CRYPTO 2013

UCD School of Mathematical Sciences

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

CASL

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 $\mathcal{F}$.

Our Contributions

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

Our Contributions

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

Our Contributions

- The first *polynomial time* relation generation method for degree one elements
- The first *polynomial time* elimination method for degree two elements
- An $L_{q^n}(1/3\,,\,(4/9)^{1/3} \approx 0.763)$ algorithm for solving the DLP for suitably balanced q, n

Our Contributions

- The first *polynomial time* relation generation method for degree one elements
- The first *polynomial time* elimination method for degree two elements
- An $L_{q^n}(1/3\,,\,(4/9)^{1/3} \approx 0.763)$ algorithm for solving the DLP for suitably balanced q, n
- Practical results: solved example DLPs in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$

The Joux-Lercier FFS variation [JL06]

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

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 such that $X - g_1(g_2(X))$ has a degree n irreducible factor $f(X)$ over $\mathbb{F}_q$, then $\mathbb{F}_{q^n} = \mathbb{F}_q(x) \cong \mathbb{F}_q[X]/(f(X)\mathbb{F}_q[X])$
- 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 $\{x - a \mid a \in \mathbb{F}_q\} \cup \{y - b \mid b \in \mathbb{F}_q\}$

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 such that $X - g_1(g_2(X))$ has a degree n irreducible factor $f(X)$ over $\mathbb{F}_q$, then $\mathbb{F}_{q^n} = \mathbb{F}_q(x) \cong \mathbb{F}_q[X]/(f(X)\mathbb{F}_q[X])$
- 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:

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 such that $X - g_1(g_2(X))$ has a degree n irreducible factor $f(X)$ over $\mathbb{F}_q$, then $\mathbb{F}_{q^n} = \mathbb{F}_q(x) \cong \mathbb{F}_q[X]/(f(X)\mathbb{F}_q[X])$
- 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]

'Optimising' d_1 and d_2 in [JL06]

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

'Optimising' d_1 and d_2 in [JL06]

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

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.

'Optimising' d_1 and d_2 in [JL06]

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

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 $d_1 \approx d_2 \approx \sqrt{n}$

'Optimising' d_1 and d_2 in [JL06]

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

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]

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

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 have a clue.

An Auspicious Choice for g_2

For simplicity, let $\mathbb{F}_q = \mathbb{F}_{2^l}$.

An Auspicious Choice for g_2

For simplicity, let $\mathbb{F}_q = \mathbb{F}_{2^l}$.

- Let $y = g_2(x) = x^{2^k}$ with $1 < k < l$

An Auspicious Choice for g_2

For simplicity, let $\mathbb{F}_q = \mathbb{F}_{2^l}$.

- Let $y = g_2(x) = x^{2^k}$ with $1 < k < l$
- Eliminates half of the factor base since

$$(y + b) = (x + b^{2^{-k}})^{2^k} \Longrightarrow \log(y + b) = 2^k \log(x + b^{2^{-k}})$$

An Auspicious Choice for g_2

For simplicity, let $\mathbb{F}_q = \mathbb{F}_{2^l}$.

- Let $y = g_2(x) = x^{2^k}$ with $1 < k < l$
- Eliminates half of the factor base since

$$(y + b) = (x + b^{2^{-k}})^{2^k} \Longrightarrow \log(y + b) = 2^k \log(x + b^{2^{-k}})$$

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

$$x^{2^k+1} + ax^{2^k} + bx + c$$

An Auspicious Choice for g_2

For simplicity, let $\mathbb{F}_q = \mathbb{F}_{2^l}$.

- Let $y = g_2(x) = x^{2^k}$ with $1 < k < l$
- Eliminates half of the factor base since

$$(y + b) = (x + b^{2^{-k}})^{2^k} \Longrightarrow \log(y + b) = 2^k \log(x + b^{2^{-k}})$$

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

$$x^{2^k+1} + ax^{2^k} + bx + c$$

- For $k \mid l$ and $l/k \geq 2$, this polynomial *provably* splits over $\mathbb{F}_q$ with probability $\approx 1/2^{3k} \gg 1/(2^k + 1)$!

Bluher Polynomials

Let $q = 2^\ell$, $\ell = kk'$ with $k' \geq 3$. If $ab \neq c$ and $b \neq a^{2^k}$, then $x^{2^k+1} + ax^{2^k} + bx + c$ may be transformed into

$$F_B(\overline{x}) = \overline{x}^{2^k+1} + B\overline{x} + B\,, \quad \text{with} \quad B = \frac{(a^{2^k} + b)^{2^k+1}}{(ab+c)^{2^k}} \quad \text{and}$$

$$x = \left(\frac{ab+c}{a^{2^k}+b}\right)\overline{x} + a.$$

Bluher Polynomials

Let $q = 2^\ell$, $\ell = kk'$ with $k' \geq 3$. If $ab \neq c$ and $b \neq a^{2^k}$, then $x^{2^k+1} + ax^{2^k} + bx + c$ may be transformed into

$$F_B(\overline{x}) = \overline{x}^{2^k+1} + B\overline{x} + B\,, \quad \text{with} \quad B = \frac{(a^{2^k} + b)^{2^k+1}}{(ab+c)^{2^k}} \quad \text{and}$$

$$x = \left(\frac{ab+c}{a^{2^k}+b}\right)\overline{x} + a.$$

Theorem (*Bluher 2004*)

The number of elements $B \in \mathbb{F}_q^\times$ such that the polynomial $F_B(X)$ splits completely over $\mathbb{F}_q$ equals

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

Relation Generation

- Let $S_B = \{B \in \mathbb{F}_q^\times \mid X^{2^k+1} + BX + B \text{ splits over } \mathbb{F}_q\}$

Relation Generation

- Let $S_B = \{B \in \mathbb{F}_q^{\times} \mid X^{2^k+1} + BX + B$ splits over $\mathbb{F}_q\}$
- For any $a, b \in \mathbb{F}_q$ s.t. $b \neq a^{2^k}$ and $B \in S_B$, there exists a unique $c \in \mathbb{F}_q$ s.t. $x^{2^k+1} + ax^{2^k} + bx + c$ splits over $\mathbb{F}_q$

Relation Generation

- Let $S_B = \{B \in \mathbb{F}_q^{\times} \mid X^{2^k+1} + BX + B$ splits over $\mathbb{F}_q\}$
- For any $a, b \in \mathbb{F}_q$ s.t. $b \neq a^{2^k}$ and $B \in S_B$, there exists a unique $c \in \mathbb{F}_q$ s.t. $x^{2^k+1} + ax^{2^k} + bx + c$ splits over $\mathbb{F}_q$
- 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

Relation Generation

- Let $S_B = \{B \in \mathbb{F}_q^\times \mid X^{2^k+1} + BX + B \text{ splits over } \mathbb{F}_q\}$
- For any $a, b \in \mathbb{F}_q$ s.t. $b \neq a^{2^k}$ and $B \in S_B$, there exists a unique $c \in \mathbb{F}_q$ s.t. $x^{2^k+1} + ax^{2^k} + bx + c$ splits over $\mathbb{F}_q$
- 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

Assume that g_1 can be found s.t. $X - g_1(X^{2^k}) \equiv 0 \pmod{f(X)}$ with $\deg(f) = n \leq 2^k\, d_1$. Then we have the following:

Relation Generation

- Let $S_B = \{B \in \mathbb{F}_q^{\times} \mid X^{2^k+1} + BX + B \text{ splits over } \mathbb{F}_q\}$
- For any $a, b \in \mathbb{F}_q$ s.t. $b \neq a^{2^k}$ and $B \in S_B$, there exists a unique $c \in \mathbb{F}_q$ s.t. $x^{2^k+1} + ax^{2^k} + bx + c$ splits over $\mathbb{F}_q$
- 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

Assume that g_1 can be found s.t. $X - g_1(X^{2^k}) \equiv 0 \pmod{f(X)}$ with $\deg(f) = n \leq 2^k d_1$. Then we have the following:

Heuristic Result 1

Let $q = 2^l$ with $l = kk'$ and $k' \geq 3$ and $d_1 \geq 1$ constants, and assume $n \approx 2^k d_1$. Assuming the r.h.s. splits over $\mathbb{F}_q$ with probability $1/(d_1+1)!$, then the logarithms of all degree one elements of $\mathbb{F}_{q^n}$ can be computed in time $\widetilde{O}(\log^{2k'+1} q^n)$.

Polynomial Time Relation Generation - Examples

- Let $q = 2^{3k}$ and $n = 2^k - 1 \Longrightarrow$ can use a Kummer extension
- Set $g_1(X) = \gamma X$, so that irreducible is $X^{2^k-1} + \gamma$
- r.h.s has degree 2 and splits with probability $1/2$

Polynomial Time Relation Generation - Examples

- Let $q = 2^{3k}$ and $n = 2^k - 1 \Longrightarrow$ can use a Kummer extension
- Set $g_1(X) = \gamma X$, so that irreducible is $X^{2^k-1} + \gamma$
- r.h.s has degree 2 and splits with probability $1/2$

Table : Relation generation times for $q = 2^{3k}$ and $n = 2^k - 1$ on a 2.0GHz AMD Opteron 6128

k	$\log_2(q^n)$	#vars	time
7	2667	5506	2.3s
8	6120	21932	15.0s
9	13797	87554	122s
10	30690	349858	900s

Complexity Results

Suppose $q = \exp\left(\alpha \sqrt[3]{\log q^n \cdot \log^2 \log q^n}\right)$ $(\dagger)$. We have:

Heuristic Result 2(i)

Let $q = 2^l$, let $k \mid l$ and let n be such that $(\dagger)$ holds. Then for $n \approx 2^k d_1$ where $2^k \approx d_1$, the DLP can be solved with complexity $L_Q(1/3, (8/9)^{1/3}) \approx L_Q(1/3, 0.961)$.

Heuristic Result 2(ii)

Let $q = 2^l$, let $k \mid l$ and let n be such that $(\dagger)$ holds. Then for $n \approx 2^k d_1$ where $2^k \gg d_1$, the DLP can be solved with complexity between $L_Q(1/3, (4/9)^{1/3}) \approx L_Q(1/3, 0.763)$ and $L_Q(1/3, (1/2)^{1/3}) \approx L_Q(1/3, 0.794)$.

Solving the DLP in $\mathbb{F}_{2^{1971}}$

Let $\mathbb{F}_q = \mathbb{F}_{2^{27}} = \mathbb{F}_2[T]/(T^{27} + T^5 + T^2 + T + 1) = \mathbb{F}_2(t)$ and let $\mathbb{F}_{q^{73}} = \mathbb{F}_q[X]/(X^{73} + t) = \mathbb{F}_q(x)$ be the field of order 2^{1971}.

- We let $y = x^8$ and thus $x = t/y^9$ and took as generator $\alpha = x + 1$ and target

$$\beta_\pi = \sum_{i=0}^{72} \tau(\lfloor \pi q^{i+1} \rfloor \bmod q)\, x^i \,.$$

Solving the DLP in $\mathbb{F}_{2^{1971}}$

Let $\mathbb{F}_q = \mathbb{F}_{2^{27}} = \mathbb{F}_2[T]/(T^{27} + T^5 + T^2 + T + 1) = \mathbb{F}_2(t)$ and let $\mathbb{F}_{q^{73}} = \mathbb{F}_q[X]/(X^{73} + t) = \mathbb{F}_q(x)$ be the field of order 2^{1971}.

- We let $y = x^8$ and thus $x = t/y^9$ and took as generator $\alpha = x + 1$ and target

$$\beta_\pi = \sum_{i=0}^{72} \tau(\lfloor \pi q^{i+1} \rfloor \bmod q)\, x^i .$$

The computation took:

- 14 core-hrs for relation generation: quotienting out by the action of the 9-th power of Frobenius on the factor base gives $612,872 \approx 2^{27}/(3 \cdot 73)$ variables
- After SGE, 2220 core-hrs for parallelised Lanczos on matrix of dimension $528,812 \times 527,766$
- 898 core-hrs for the descent $\implies$ total of 3132 core-hrs.

Solving the DLP in $\mathbb{F}_{2^{1971}}$

On 19/2/13 we announced that $\log_\alpha(\beta_\pi) =$

11992984215354106866091146371988855845186852755447163352
36895900760902198795745784008181148775933944656038305197
82541742360236535889937362200771117361678269423101163403
13535552228080411390321527355590590108228224824002192878
78207304028565280573096588688279004416835100344085961912
42700060128986433752110002214380289887546061125224587971
19787275080584651962314043764573936293823541736161168108
25627780459657892709561158924173579400674739684346062992
68294291957378226451182620783745349502502960139927453196
48974006524479548958327920827882768332440907342446643941
09767021620395395133776731154834339 .

Solving the DLP in $\mathbb{F}_{2^{3164}}$

Let $\mathbb{F}_q = \mathbb{F}_{2^{28}} = \mathbb{F}_2[T]/(T^{28} + T + 1) = \mathbb{F}_2(t)$ and let $\mathbb{F}_{q^{113}} = \mathbb{F}_q[X]/(X^{113} + t) = \mathbb{F}_q(x)$ be the field of order 2^{3164}.

- We let $y = x^{16}$ and thus $x = t/y^7$ and took as generator $\alpha = x + t + 1$ and target

$$\beta_\pi = \sum_{i=0}^{112} \tau(\lfloor \pi q^{i+1} \rfloor \bmod q)\, x^i \,.$$

Solving the DLP in $\mathbb{F}_{2^{3164}}$

Let $\mathbb{F}_q = \mathbb{F}_{2^{28}} = \mathbb{F}_2[T]/(T^{28} + T + 1) = \mathbb{F}_2(t)$ and let $\mathbb{F}_{q^{113}} = \mathbb{F}_q[X]/(X^{113} + t) = \mathbb{F}_q(x)$ be the field of order 2^{3164}.

- We let $y = x^{16}$ and thus $x = t/y^7$ and took as generator $\alpha = x + t + 1$ and target

$$\beta_\pi = \sum_{i=0}^{112} \tau(\lfloor \pi q^{i+1} \rfloor \bmod q)\, x^i \,.$$

The computation took:

- 2 core-hrs for relation generation: quotienting out by the action of the 14-th power of Frobenius on the factor base gives $1,187,841 \approx 2^{28}/(2 \cdot 113)$ variables
- After SGE, $85,488$ core-hrs for parallelised Lanczos on matrix of dimension $1,066,010 \times 1,064,991$
- $21,602$ core-hrs for the descent $\implies$ total of $107,092$ core-hrs

Solving the DLP in $\mathbb{F}_{2^{3164}}$

On 3/5/13 we found that $\log_{\alpha}(\beta_{\pi}) =$

2410958672084703779901202077261642209070514313288787533385808717024
8784565712688312063491036765323357553857177477977665457317849564770
1688094481773173140524389502529386852264636049383546885561763318178
6341747893370309598402582718996263618673697554067799885512742832012
3901294838991530024173934004391610582283400289720429303619769406533
7903255793451858773664350130030722091666253172541070447948299781221
0193428607010640365444303319677531146468063350633002030742348610674
7166841199820454431917683235380198222192499580429542616711230697079
5960798988644631100037393291558580412406942004555116148790387654960
4900084297695444007900819088072394071341577241660482464194055035573
9803589799985259319695403143962976877685099988772087056174191305553
1864041654707840433795403753200520891617150254756586728215941551355
0648407797656823989931563900000242491107399569193500692930336704230
7029958155763666499372120453686303873671488016409635578117870889230
278649164378133 .

Big Field Hunting

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

Solution to DLP in $\mathbb{F}_{2^{6120}}$

On 11/4/13 we announced that $\beta_\pi = g^{\log}$, with $\log =$

138587598363978692625475711283123171009236361503896992366495931704517700280127178022234894098617
581360131441835074256363730624426814293233474272521598166126957928116825443110965404253837938808
595404111035238027107772178822939281873403451999731815140073481766513715358449279314556797352446
246860317946750124475689474406274942356035936501674050933448909201029834522226732247771897083223
217282051573645013603613042367782716361877817938374393824313019073624786387618414037541681120284
044659383192907436852526392087724304775451631271825250968111451400502733404381769675255289127346
639350098221570844400380788516332496583882522436381918008200167032186350245107751346979596314696
153666716168951481948091060066730184766758137773944303875429830867205463918144256843911730747265
146154193438041627833661739775057161236346096236566875251277843062329973044475486561062204356908
568471471279383781038538818884463796989906076079843248127252020839705886436071213650575186707456
948584072378916942925369140868417196479573481032711481021729162865973588174096389913305607677858
033996361734905537150362024720515772660781208855505434331055766570014211875602940633575763850457
503079087074376585304470520411320246292255375711457573555286060236699317039454479326718281128961
423275142787569425690532833283344049635521302596000897192512036695298807294032964530959691377087
204546348960132760095544105980198255245493202412831593891984788152417957691939817112366182063687
529915365150361180214451234387656883256149355994405051149585969163075307026647956035683671589546
448539955132726112034938655961291856203422247680387029078473520951160334472525475071680672623661
587292720329606182512044312194357156139201340952037872975243254476081554937002122953415949407262
137232099852298394838422907643191397673290238344183046040975859915928536530445697145317668044973
7096483324156185041

The Algorithm of Barbulescu, Gaudry, Joux and Thomé

For small characteristic fields of bitlength l, the BGJT algorithm has quasi-polynomial complexity $l^{O(\log l)}$.

- Applies to fields of the form $\mathbb{F}_{q^{kn}}$, with $k \geq 2$ and $n \approx q$
- Complexity dictated by $\#$nodes in the descent tree

The Algorithm of Barbulescu, Gaudry, Joux and Thomé

For small characteristic fields of bitlength l, the BGJT algorithm has quasi-polynomial complexity $l^{O(\log l)}$.

- Applies to fields of the form $\mathbb{F}_{q^{kn}}$, with $k \geq 2$ and $n \approx q$
- Complexity dictated by $\#$nodes in the descent tree

Question: Are the any elements of $\mathbb{F}_{q^{kn}}$ that require a quasi-polynomial number of linear elements to represent them?

The Algorithm of Barbulescu, Gaudry, Joux and Thomé

For small characteristic fields of bitlength l, the BGJT algorithm has quasi-polynomial complexity $l^{O(\log l)}$.

- Applies to fields of the form $\mathbb{F}_{q^{kn}}$, with $k \geq 2$ and $n \approx q$
- Complexity dictated by #nodes in the descent tree

Question: Are the any elements of $\mathbb{F}_{q^{kn}}$ that require a quasi-polynomial number of linear elements to represent them?

Answer: No! F.R.K. Chung has proven that if $\mathbb{F}_{q^{kn}} = \mathbb{F}_{q^k}(x)$, then each $h \in \mathbb{F}_{q^{kn}}^{\times}$ can be represented by

$$h = (x + a_1) \cdots (x + a_m), \quad \text{with} \quad a_i \in \mathbb{F}_{q^k},$$

if $\sqrt{q^k} > n - 1$ and $m \geq 2n + 4n \log n / (\log q^k - 2 \log (n-1))$.

Thanks for your attention!