Breaking '128-bit Secure' Supersingular Binary Curves

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

Robert Granger[1], Thorsten Kleinjung[1], Jens Zumbrägel[2]

[1] Laboratory for Cryptologic Algorithms, EPFL, Switzerland

[2] Institute of Algebra, TU Dresden, Germany

20th August, CRYPTO 2014

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

IRISH RESEARCH COUNCIL
An Chomhairle um Thaighde in Éirinn

Overview

Overview

Motivation

Our Contributions

A Recent Result

Supersingular binary curves (genus 1)

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

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

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

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

Supersingular binary curves (genus 1)

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

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

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

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

Lesson 1 (*MOV '93*)

Supersingular curves are bad for cryptography.

Supersingular binary curves (genus 1)

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

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

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

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

Lesson 1 (*MOV '93*)

Supersingular curves are bad for cryptography.

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

Supersingular binary curves (genus 1)

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

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

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

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

Lesson 1 (*MOV '93*)

Supersingular curves are bad for cryptography.

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

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

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

The small characteristic DLP 'Cryptopocalypse'

15th Feb '13: *'On the Function Field Sieve and the Impact of Higher Splitting Probabilities'*, Göloğlu, G., McGuire and Zumbrägel.

- *Polynomial time* relation generation for degree one elements
- *Polynomial time* on-the-fly elimination for degree two elements

20th Feb '13: *'A new index calculus algorithm with complexity $L(1/4 + o(1))$ in very small characteristic'*, Joux.

- *Polynomial time* relation generation for degree one elements
- *Polynomial time* batch method for eliminating degree two elements
- $L(1/4 + o(1))$ descent method

18th Jun '13: *'A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic'*, Barbulescu, Gaudry, Joux and Thomé.

- $L(o(1))$ descent method

The small characteristic DLP 'Cryptopocalypse'

Lesson 3 (*BGJT '13*)

Small characteristic supersingular curves really are bad for cryptography.

The small characteristic DLP 'Cryptopocalypse'

Lesson 3 (*BGJT '13*)

Small characteristic supersingular curves really are bad for cryptography.

Moreover, new DLP records support validity of the theoretical advances:

- 11th Feb '13, Joux: $\mathbb{F}_{2^{1778}}$ in 220 core hours
- 19th Feb '13, GGMZ: $\mathbb{F}_{2^{1971}}$ in $3,132$ core hours
- 3rd May '13, GGMZ: $\mathbb{F}_{2^{3164}}$ in $107,000$ core hours
- 22nd Mar '13, Joux: $\mathbb{F}_{2^{4080}}$ in $14,100$ core hours
- 11th Apr '13, GGMZ: $\mathbb{F}_{2^{6120}}$ in 750 core hours
- 21st May '13, Joux: $\mathbb{F}_{2^{6168}}$ in 550 core hours
- 31st Jan '14, GKZ: $\mathbb{F}_{2^{9234}}$ in $400,000$ core hours

The small characteristic DLP 'Cryptopocalypse'

Lesson 3 (*BGJT '13*)

Small characteristic supersingular curves really are bad for cryptography.

Moreover, new DLP records support validity of the theoretical advances:

- 11th Feb '13, Joux: $\mathbb{F}_{2^{1778}}$ in 220 core hours
- 19th Feb '13, GGMZ: $\mathbb{F}_{2^{1971}}$ in $3,132$ core hours
- 3rd May '13, GGMZ: $\mathbb{F}_{2^{3164}}$ in $107,000$ core hours
- 22nd Mar '13, Joux: $\mathbb{F}_{2^{4080}}$ in $14,100$ core hours
- 11th Apr '13, GGMZ: $\mathbb{F}_{2^{6120}}$ in 750 core hours
- 21st May '13, Joux: $\mathbb{F}_{2^{6168}}$ in 550 core hours
- 31st Jan '14, GKZ: $\mathbb{F}_{2^{9234}}$ in $400,000$ core hours

Question: If the small characteristic field DLP is dead, why study it?

The small characteristic DLP 'Cryptopocalypse'

Lesson 3 (*BGJT '13*)

Small characteristic supersingular curves really are bad for cryptography.

Moreover, new DLP records support validity of the theoretical advances:

- 11th Feb '13, Joux: $\mathbb{F}_{2^{1778}}$ in 220 core hours
- 19th Feb '13, GGMZ: $\mathbb{F}_{2^{1971}}$ in $3,132$ core hours
- 3rd May '13, GGMZ: $\mathbb{F}_{2^{3164}}$ in $107,000$ core hours
- 22nd Mar '13, Joux: $\mathbb{F}_{2^{4080}}$ in $14,100$ core hours
- 11th Apr '13, GGMZ: $\mathbb{F}_{2^{6120}}$ in 750 core hours
- 21st May '13, Joux: $\mathbb{F}_{2^{6168}}$ in 550 core hours
- 31st Jan '14, GKZ: $\mathbb{F}_{2^{9234}}$ in $400,000$ core hours

Question: If the small characteristic field DLP is dead, why study it?

Short answer: It may be dead, but it's not quite buried...

Slightly longer answer

1. None of the records used parameters from the literature (which arise from pairings on supersingular curves and abelian varieties)

Slightly longer answer

1. None of the records used parameters from the literature (which arise from pairings on supersingular curves and abelian varieties)
2. The records all used Kummer, or twisted Kummer extensions, which are the easiest to break. *So how hard are the DLPs in the literature?*

Slightly longer answer

1. None of the records used parameters from the literature (which arise from pairings on supersingular curves and abelian varieties)
2. The records all used Kummer, or twisted Kummer extensions, which are the easiest to break. *So how hard are the DLPs in the literature?*
3. Another team of researchers studied this very question, and we realised that we could significantly improve upon their results

Slightly longer answer

1. None of the records used parameters from the literature (which arise from pairings on supersingular curves and abelian varieties)
2. The records all used Kummer, or twisted Kummer extensions, which are the easiest to break. *So how hard are the DLPs in the literature?*
3. Another team of researchers studied this very question, and we realised that we could significantly improve upon their results
4. Studying particular problem instances can lead to new insights

Concrete security of small characteristic pairings

'Weakness of $\mathbb{F}_{3^{6 \cdot 509}}$ for Discrete Logarithm Cryptography' by Adj, Menezes, Oliveira and Rodríguez-Henríquez uses the techniques from [Joux13] and [BGJT13] to analyse the concrete security of the DLP in pairing fields once thought to be 128-bit secure.

Concrete security of small characteristic pairings

'Weakness of $\mathbb{F}_{3^{6\cdot509}}$ for Discrete Logarithm Cryptography' by Adj, Menezes, Oliveira and Rodríguez-Henríquez uses the techniques from [Joux13] and [BGJT13] to analyse the concrete security of the DLP in pairing fields once thought to be 128-bit secure.

In particular, they showed that:

- The DLP in the 804-bit order r subgroup of $\mathbb{F}_{3^{6\cdot509}}^{\times}$ can be solved in time $2^{73.7} M_r$, using $\mathbb{F}_{q^{kn}}$ with $q = 3^6$, $k = 2$ and $n = 509$
- The DLP in the 698-bit order r subgroup of $\mathbb{F}_{2^{12\cdot367}}^{\times}$ can be solved in time $2^{94.6} M_r$, using $\mathbb{F}_{q^{kn}}$ with $q = 2^{12}$, $k = 2$ and $n = 367$
- The DLP in the 1221-bit order r subgroup of $\mathbb{F}_{2^{4\cdot1223}}^{\times}$ can be solved in time $\approx 2^{128} M_r$, using $\mathbb{F}_{q^{kn}}$ with $q = 2^{12}$, $k = 2$ and $n = 1223$

Overview

Our contributions

We exploited the following observations/techniques:

- A smaller q gives a faster descent. Rather than using an irreducible degree n factor of $h_1(X)X^q - h_0(X)$, we use $h_1(X^q)X - h_0(X^q)$
- *Principle of parsimony:* always try to work in the target field; only when this fails should one embed into an extension
- A bonus of solving factor base logs in an extension is that one can factor elements over the extension during the descent
- If possible, using $k = 1$ means one can eliminate higher degree elements efficiently, *postponing the need for the QPA*

Our contributions

We exploited the following observations/techniques:

- A smaller q gives a faster descent. Rather than using an irreducible degree n factor of $h_1(X)X^q - h_0(X)$, we use $h_1(X^q)X - h_0(X^q)$
- *Principle of parsimony:* always try to work in the target field; only when this fails should one embed into an extension
- A bonus of solving factor base logs in an extension is that one can factor elements over the extension during the descent
- If possible, using $k = 1$ means one can eliminate higher degree elements efficiently, *postponing the need for the QPA*

As a result, we showed that the:

- DLP in order r subgroup of $\mathbb{F}^{\times}_{2^{4 \cdot 1223}}$ costs at most $2^{59} M_r$ (2^{40} s)

Our contributions

We exploited the following observations/techniques:

- A smaller q gives a faster descent. Rather than using an irreducible degree n factor of $h_1(X)X^q - h_0(X)$, we use $h_1(X^q)X - h_0(X^q)$
- *Principle of parsimony:* always try to work in the target field; only when this fails should one embed into an extension
- A bonus of solving factor base logs in an extension is that one can factor elements over the extension during the descent
- If possible, using $k = 1$ means one can eliminate higher degree elements efficiently, *postponing the need for the QPA*

As a result, we showed that the:

- DLP in order r subgroup of $\mathbb{F}^{\times}_{2^{4 \cdot 1223}}$ costs at most $2^{59} M_r$ (2^{40} s)
- DLP in order r subgroup of $\mathbb{F}^{\times}_{2^{12 \cdot 367}}$ costs at most $2^{48} M_r$ (52240 h)

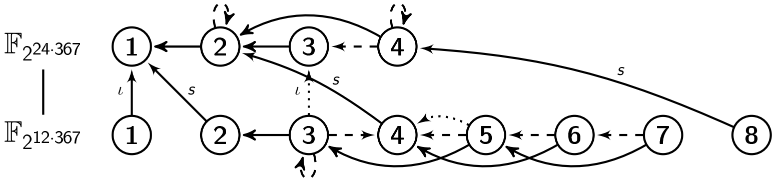
Solving the DLP in $\mathbb{F}_{2^{12\cdot 367}}$

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

- We defined $\mathbb{F}_{2^{367}} = \mathbb{F}_2[X]/(I(X)) = \mathbb{F}_2(x)$ where $I(X)$ the irreducible degree 367 factor of $h_1(X^{64})X - h_0(X^{64})$, with

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

- *Small degree elimination flowchart:*



- Total time was 52240 h
- Announced solution on 30/1/14

Overview

Motivation

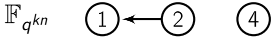
Our Contributions

A Recent Result

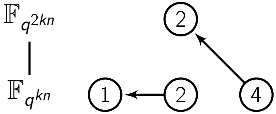
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$

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

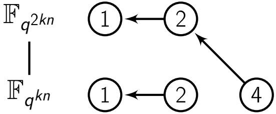
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



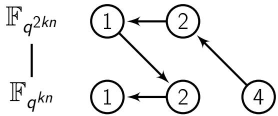
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



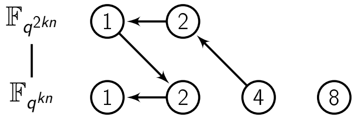
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



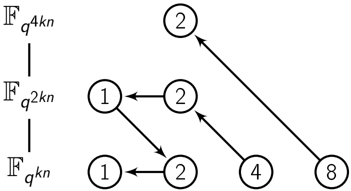
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



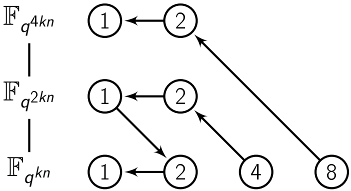
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



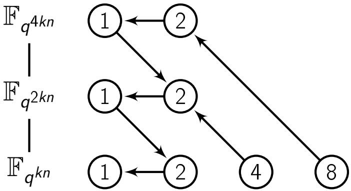
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



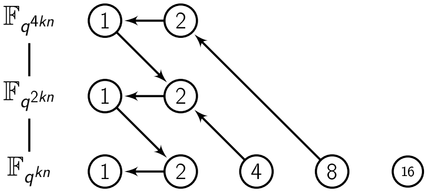
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



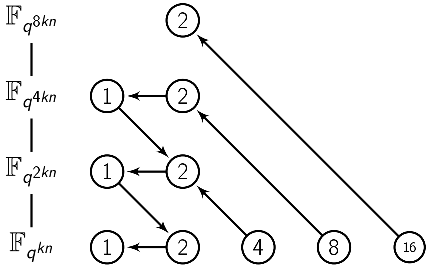
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



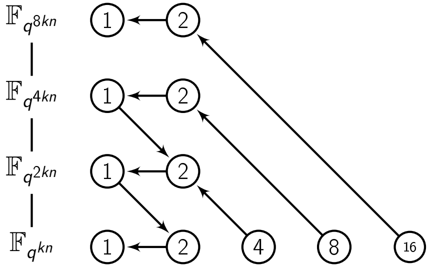
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



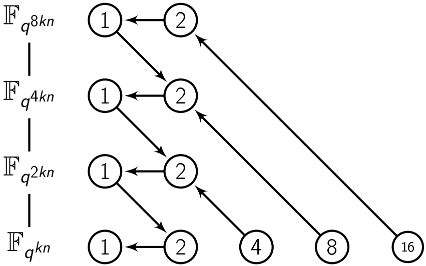
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



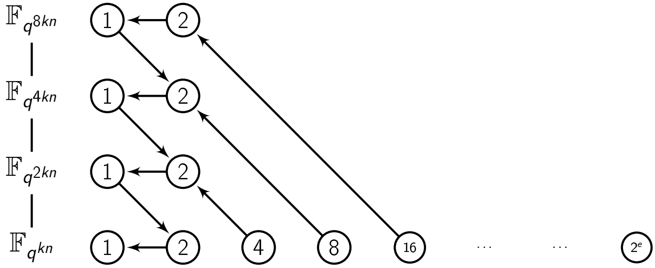
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



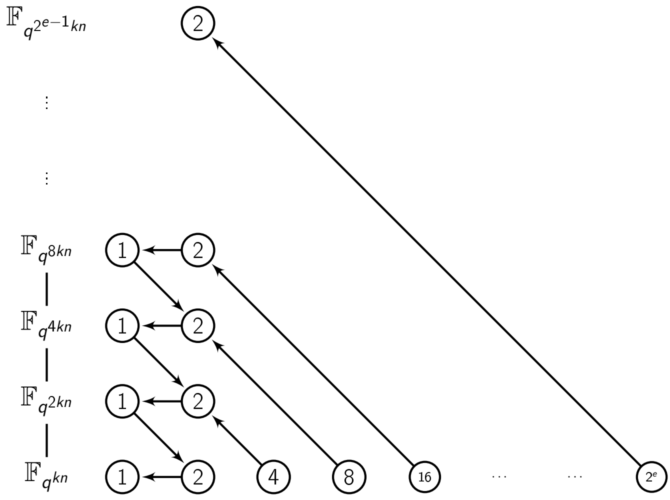
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



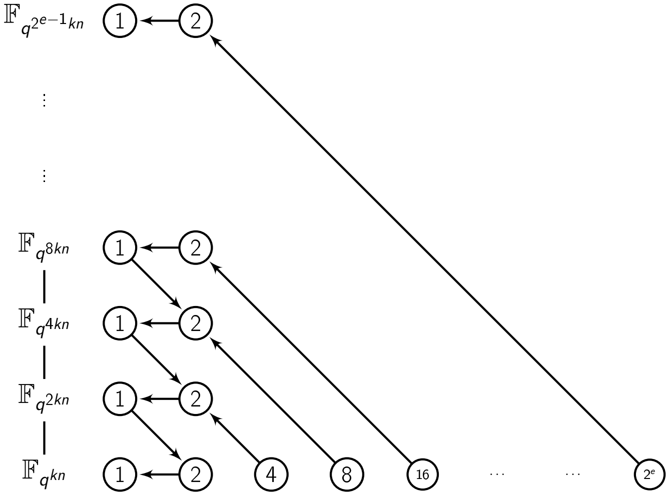
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



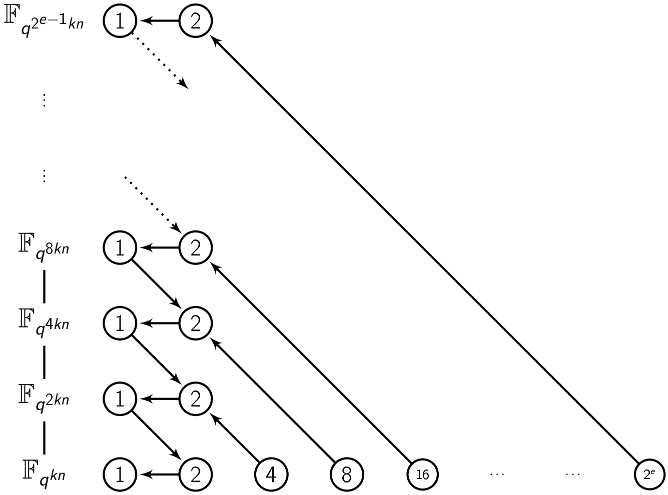
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



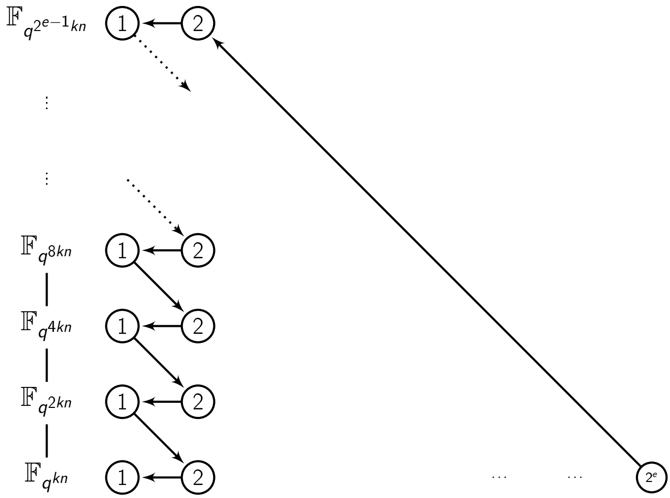
Eliminating irreducibles of degree a power of 2 in $\mathbb{F}_{q^{kn}}/\mathbb{F}_{q^k}$



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



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



A new QPA in fixed characteristic

A new QPA in fixed characteristic

Using the previous descent method, we have the following result:

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

For all primes p there exist infinitely many extension fields $\mathbb{F}_{p^n}$ for which the discrete logarithm problem in $\mathbb{F}_{p^n}^{\times}$ can be solved in quasi-polynomial time $\exp(c_p(\log n)^2)$, with $c_p > 0$ a constant depending only on p.

A new QPA in fixed characteristic

Using the previous descent method, we have the following result:

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

For all primes p *there exist infinitely many extension fields* $\mathbb{F}_{p^n}$ *for which the discrete logarithm problem in* $\mathbb{F}_{p^n}^{\times}$ *can be solved in quasi-polynomial time* $\exp(c_p(\log n)^2)$, *with* $c_p > 0$ *a constant depending only on* p.

'On the discrete logarithm problem in finite fields of fixed characteristic'
(preprint available soon)

A new QPA in fixed characteristic

Using the previous descent method, we have the following result:

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

For all primes p *there exist infinitely many extension fields* $\mathbb{F}_{p^n}$ *for which the discrete logarithm problem in* $\mathbb{F}_{p^n}^{\times}$ *can be solved in quasi-polynomial time* $\exp(c_p(\log n)^2)$, *with* $c_p > 0$ *a constant depending only on* p.

'On the discrete logarithm problem in finite fields of fixed characteristic' (preprint available soon)

Thanks for your attention!