Consequences for pairing-based cryptography of the recent improvements on discrete logarithm computation in $\mathbb{F}_{p^n}$

Aurore Guillevic

University of Calgary, PIMS–CNRS

Mathematical Structures for Cryptography Workshop
Leiden, Netherlands, August 23, 2016

UNIVERSITY OF CALGARY

Pacific Institute *for the* Mathematical Sciences

Outline

Mathematical structures: pairing-friendly elliptic curves

Number Field Sieve

Key-size update for pairing-based cryptography

Outline

Mathematical structures: pairing-friendly elliptic curves

Number Field Sieve

Key-size update for pairing-based cryptography

Cryptographic pairing: black-box properties

$(\mathbf{G}_1, +), (\mathbf{G}_2, +), (\mathbf{G}_T, \cdot)$ three cyclic groups of large prime order ℓ
Pairing: map $e : \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$

1. bilinear: $e(P_1 + P_2,\ Q) = e(P_1, Q) \cdot e(P_2, Q)$,
   $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
2. non-degenerate: $e(G_1, G_2) \neq 1$ for $\langle G_1 \rangle = \mathbf{G}_1$, $\langle G_2 \rangle = \mathbf{G}_2$
3. efficiently computable.

Mostly used in practice:

$$e([a]P, [b]Q) = e([b]P, [a]Q) = e(P, Q)^{ab} \ .$$

$\rightsquigarrow$ Many applications in asymmetric cryptography.

Example of application: identity-based encryption

- 1984: idea of identity-based encryption formalized by Shamir
- 1999: first practical identity-based cryptosystem of Sakai-Ohgishi-Kasahara
- 2000: constructive pairings, Joux's tri-partite key-exchange
- 2001: IBE of Boneh-Franklin

Rely on

- Discrete Log Problem (DLP): given $g, y \in \mathbf{G}$, compute x s.t. $g^x = y$ Diffie-Hellman Problem (DHP)
- bilinear DLP and DHP
  Given $\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_T, g_1, g_2, g_T$ and $y \in G_T$, compute $P \in \mathbf{G}_1$ s.t. $e(P, g_2) = y$, or $Q \in \mathbf{G}_2$ s.t. $e(g_1, Q) = y$
  if $g_T^x = y$ then $e(g_1^x, g_2) = e(g_1, g_2^x) = g_T^x = y$
- pairing inversion problem

Pairing setting: elliptic curves

$$E/\mathbb{F}_p: \ y^2 = x^3 + ax + b, \ a, b \in \mathbb{F}_p, \ p \geq 5$$

- proposed in 1985 by Koblitz, Miller
- $E(\mathbb{F}_p)$ has an efficient group law (chord an tangent rule) $\to$ **G**
- $\#E(\mathbb{F}_p) = p + 1 - t$, trace t: $|t| \leq 2\sqrt{p}$
- efficient group order computation (*point counting*)
- large subgroup of prime order ℓ s.t. $\ell \mid p + 1 - t$ and ℓ coprime to p
- $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$ (for crypto)
- only generic attacks against DLP on well-chosen genus 1 and genus 2 curves
- optimal parameter sizes

Tate Pairing and modified Tate pairing

$\ell \mid p^n - 1,\ E[\ell] \subset E(\mathbb{F}_{p^n})$
Tate Pairing: $e:\ E(\mathbb{F}_{p^n})[\ell] \times E(\mathbb{F}_{p^n})/\ell E(\mathbb{F}_{p^n}) \to \mathbb{F}_{p^n}^*/(\mathbb{F}_{p^n}^*)^\ell$
For cryptography,

- $\mathbf{G}_1 = E(\mathbb{F}_p)[\ell] = \{P \in E(\mathbb{F}_p), [\ell]P = \mathcal{O}\}$
- embedding degree $n > 1$ w.r.t. ℓ: smallest[1] integer n s.t. $\ell \mid p^n - 1 \Leftrightarrow E[\ell] \subset E(\mathbb{F}_{p^n})$
- $\mathbf{G}_2 \subset E(\mathbb{F}_{p^n})[\ell]$
- $\mathbf{G}_1 \cap \mathbf{G}_2 = \mathcal{O}$ by construction for practical applications
- $\mathbf{G}_T = \boldsymbol{\mu}_\ell = \{u \in \mathbb{F}_{p^n}^*,\ u^\ell = 1\} \subset \mathbb{F}_{p^n}^*$

When n is small i.e. $1 \leqslant n \leqslant 24$, the curve is *pairing-friendly*.
This is very rare: For a given curve, $\log n \sim \log \ell$
(*[Balasubramanian Koblitz]*).

[1] $n = 1$ is possible too

Modified Tate pairing

Avoid equivalence classes:
need one representative of the equivalence class instead.
Ensure the pairing is non-degenerate: $\mathbf{G}_1 \cap \mathbf{G}_2 = \mathcal{O}$

$$E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}\ell\mathbb{Z} = \mathbf{G}_1 \oplus \mathbf{G}_2$$

Let $P \in \mathbf{G}_1 = E(\mathbb{F}_p)[\ell], Q \in \mathbf{G}_2 \subset E(\mathbb{F}_{p^n})[\ell]$.
Let $f_{\ell,P}$ the function s. t. $\mathrm{Div}(f_{\ell,P}) = \ell(P) - \ell(\mathcal{O})$.
Modified Tate pairing (in cryptography):

$$\begin{array}{lcccccl} & E(\mathbb{F}_p)[\ell] & & E(\mathbb{F}_{p^n})[r] & & & \\ & \| & & \cup & & & \\ e_{\mathrm{Tate}}: & \mathbf{G}_1 & \times & \mathbf{G}_2 & \to & \boldsymbol{\mu}_\ell \subset \mathbb{F}_{p^n}^* \\ & & (P, Q) & & \mapsto & (f_{\ell,P}(Q))^{\frac{p^n-1}{\ell}} \end{array}$$

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \ \ e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \; : \; E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{\ell})$)

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \; : \; E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{\ell})$)
- discrete logarithm computation in $\mathbb{F}_{p^n}^*$: **easier, subexponential** $\rightarrow$ take a large enough field

Pairing key-sizes in the 2000's

Assumed: DLP in prime fields $\mathbb{F}_{p_0}$ as hard as in medium and large characteristic fields $\mathbb{F}_{p^n}$
$\rightarrow$ take the same size as for prime fields.

Security level	$\log_2 \ell$	finite field	n	$\log_2 p$	$\deg P$ $p = P(u)$	ρ	curve
	256	3072		3072			prime field
128	256	3072	2	1536	no poly	any$\rightarrow$6	supersingular
	256	3072	12	256	4	1	Barreto-Naehrig
	640	7680	12	640	4	$1\rightarrow 5/3$	BN
	427	7680	12	640	6	$3/2$	BLS12
192	384	9216	18	512	8	$4/3$	KSS18
	384	7680	16	480	10	$5/4$	KSS16
	384	11520	24	480	10	$5/4$	BLS24

Very popular pairing-friendly curves: Barreto-Naehrig (BN)

$$E_{BN}: \; y^2 = x^3 + b, \; p \equiv 1 \bmod 3, \; D = -3 \text{ (ordinary)}$$

$$\begin{aligned} p &= 36x^4 + 36x^3 + 24x^2 + 6x + 1 \\ t &= 6x^2 + 1 \\ \ell &= p + 1 - t = 36x^4 + 36x^3 + 18x^2 + 6x + 1 \\ t^2 - 4p &= -3(6x^2 + 4x + 1)^2 \; \rightarrow \text{ no CM method needed} \end{aligned}$$

Comes from the Aurifeuillean factorization of Φ_{12} :
$\Phi_{12}(6x^2) = \ell(x)\ell(-x)$

Match(ed) the 128-bit security level perfectly:

Security level	$\log_2 \ell$	finite field	n	$\log_2 p$	$\deg P, \; p = P(u)$	ρ
128	256	3072	12	256	4	1

What changed?

It was assumed:

DL computation in $\mathbb{F}_{p^n}$ of $n \log_2 p$ bits is as hard as in a prime field $\mathbb{F}_{p_0}$ of $\log_2 p_0 = n \log_2 p$ bits, i.e. of same total size.

This is not true anymore:

now NFS variants can exploit the additional structure

- composite n, subfields (Extended TNFS, Kim then improvements by many others)
- special p, e.g. $p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ for BN curves (*[Joux-Pierrot 13]* improvement, now can be efficiently combined with Extended TNFS).

Outline

Mathematical structures: pairing-friendly elliptic curves

Number Field Sieve

Key-size update for pairing-based cryptography

Number Field Sieve

Recall Pierrick Gaudry's talk (Monday, 22nd August) Asymptotic complexity:

$$L_{p^n}[\alpha, c] = e^{(c+o(1))(\log p^n)^{\alpha}(\log \log p^n)^{1-\alpha}}$$

- $\alpha = 1$: exponential
- $\alpha = 0$: polynomial
- $0 < \alpha < 1$: sub-exponential (including NFS)

1. polynomial selection (less than 10% of total time)
2. relation collection $L_{p^n}[1/3, c]$
3. linear algebra $L_{p^n}[1/3, c]$
4. individual discrete log computation $L_{p^n}[1/3, c' < c]$

The NFS diagram for DLP in $\mathbb{F}_{p^n}^*$

Let f, g be two polynomials defining two number fields and such that in $\mathbb{F}_p[z]$, f and g have a common irreducible factor $\varphi(z) \in \mathbb{F}_p[z]$ of degree n, s.t. one can define the extension $\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))$
Diagram:

$$\begin{tikzcd}
& \mathbb{Z}[x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & \\
\mathbb{Z}[x]/(f(x)) \arrow[dr, "\alpha_f \mapsto z"'] & & \mathbb{Z}[x]/(g(x)) \arrow[dl, "\alpha_g \mapsto z"] \\
& \mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z)) &
\end{tikzcd}$$

The NFS diagram for DLP in $\mathbb{F}_{p^n}^*$

Let f, g be two polynomials defining two number fields
and such that in $\mathbb{F}_p[z]$, f and g have a common irreducible factor
$\varphi(z) \in \mathbb{F}_p[z]$ of degree n, s.t. one can define the extension
$\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))$
Diagram: Large p:

$$\begin{tikzcd}
& & a_0 - a_1 x \in \mathbb{Z}[x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & & \\
\begin{array}{c} a_0 - a_1\alpha_f \\ \text{smooth?} \end{array} & \mathbb{Z}[x]/(f(x)) \arrow[dr, "\alpha_f \mapsto z"'] & & \mathbb{Z}[x]/(g(x)) \arrow[dl, "\alpha_g \mapsto z"] & \begin{array}{c} a_0 - a_1\alpha_g \\ \text{smooth?} \end{array} \\
& & \mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z)) & &
\end{tikzcd}$$

The NFS diagram for DLP in $\mathbb{F}_{p^n}^*$

Let f, g be two polynomials defining two number fields and such that in $\mathbb{F}_p[z]$, f and g have a common irreducible factor $\varphi(z) \in \mathbb{F}_p[z]$ of degree n, s.t. one can define the extension $\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))$

Diagram: Medium p: *[Joux Lercier Smart Vercauteren 06]*

$$
\begin{tikzcd}
 & & a_0 - a_1 x + a_2 x^2 \in \mathbb{Z}[x] \arrow[dl, "x \mapsto \alpha_f"'] \arrow[dr, "x \mapsto \alpha_g"] & & \\
\begin{array}{c} a_0 - a_1\alpha_f + a_2\alpha_f^2 \\ \text{smooth?} \end{array} & \mathbb{Z}[x]/(f(x)) \arrow[dr, "\alpha_f \mapsto z"'] & & \mathbb{Z}[x]/(g(x)) \arrow[dl, "\alpha_g \mapsto z"] & \begin{array}{c} a_0 - a_1\alpha_g + a_2\alpha_g^2 \\ \text{smooth?} \end{array} \\
 & & \mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z)) & &
\end{tikzcd}
$$

Norms

The asymptotic complexity is determined by the *size of norms* of the elements $\sum_{0 \leq i < t} a_i \alpha^i$ in the relation collection step.
We want both sides *smooth* to get a relation.

"An ideal is B-smooth" approximated by
"its norm is B-smooth".

Smoothness bound: $B = L_{p^n}[1/3, \beta]$
Size of norms: $L_{p^n}[2/3, c_{\mathcal{N}}]$
Complexity: minimize $c_{\mathcal{N}}$ in the formulas.
To reduce NFS complexity, reduce size of norms *asymptotically*.
$\rightarrow$ very hard problem.

Example: $\mathbb{F}_{p^2}$ of 180dd (595 bits)

generic prime $p = \lfloor 10^{89}\pi \rfloor + 14905741$ of 90dd (298 bits)
295-bit prime-order subgroup ℓ s.t. $8\ell = p + 1$
Generalized Joux-Lercier method:

$$f = x^3 + x^2 - 9x - 12$$

$$g = 37414058632470877850964244771495186708647285789679381836660x^2 \\ -22356569146568720540560560183222246035196001707879849172376 2x \\ +16263948066744611343481892206741504809703832957831569508317 3$$

Norms: 339 bits

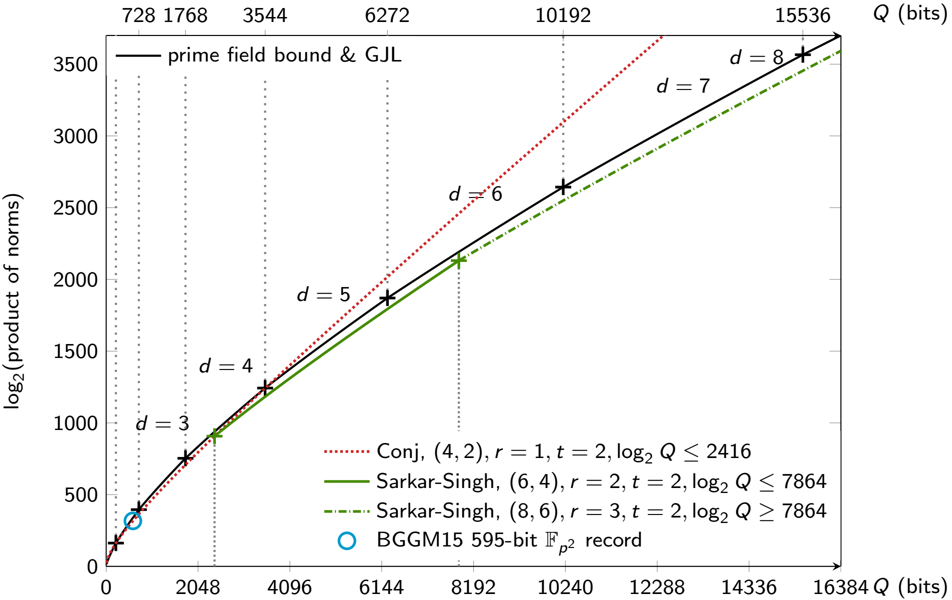
Conjugation method:

$$f = x^4 + 1$$

$$g = 448225077249286433565160965828828303618362474\ x^2 \\ -\ 296061099084763680469275137306557962657824623\ \ x \\ +\ 448225077249286433565160965828828303618362474\ \ .$$

Norms: 317 bits

Example: $\mathbb{F}_{p^2}$, $Q = p^2$



Example: $\mathbb{F}_{p^3}$ of 180dd (593 bits)

generic prime $p = \lfloor 10^{59}\pi \rfloor + 3569289$ of 60dd (198 bits)
118dd prime-order subgroup ℓ s.t. $39\ell = p^2 + p + 1$
[Joux-Lercier-Smart-Vercauteren 06] method:

$$f = x^3 + 560499121639792869931133108301x^2 - 560499121639792869931133108304x + 1$$

$$g = 560499121639792869931123378470x^3 - 1547077776638498332011063987313x^2$$
$$-1344195882808802777823061480097x + 560499121639792869931123378470$$

Norms: 326 bits

Conjugation method *[Barbulescu-Gaudry-G.-Morain 15]*:

$$f = 20x^6 - x^5 - 290x^4 - 375x^3 + 15x^2 + 121x + 20$$

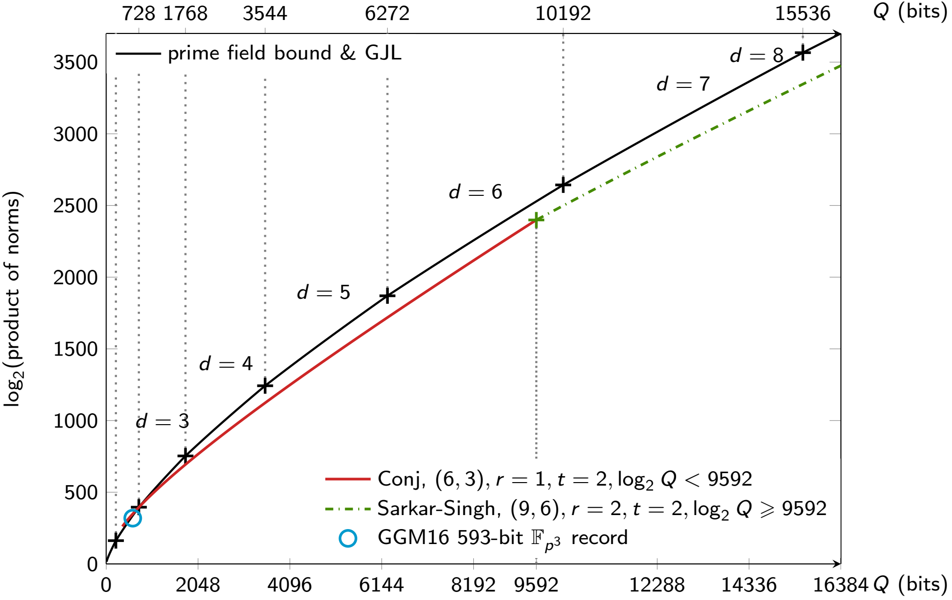
$$g = 136638347141315234758260376470x^3 - 297571133526942208465012783113x^2$$
$$-439672154776639925121282407723x - 136638347141315234758260376470$$

$$\varphi = \gcd(f_0, f_1) \mod p = x^3 - yx^2 - (y+3)x - 1,$$
where y is a root modulo p of

$$A(y) = 20y^2 - y - 169$$

Norms: 319 bits

Example: $\mathbb{F}_{p^3}$, $Q = p^3$



Outline

Mathematical structures: pairing-friendly elliptic curves

Number Field Sieve

Key-size update for pairing-based cryptography

Pairing crypto key-size update: practical approach

Relation collection: $a_0 + a_1\alpha + \ldots + a_{t-1}\alpha^{t-1}$
Consider elements of degree t and coeffs $\leq E^{2/t}$
$E = L_{p^n}[1/3, \beta]$
$\log_2 E = 1.1(\log p^n)^{1/3}(\log\log p^n)^{2/3}$ for `cado-nfs`
this is a rough estimate that is not calibrated for very large sizes of p^n
Given a prime finite field size $\log_2 p_0$, and n, what size of p^n should we take to obtain the same DL computation running-time in $\mathbb{F}_{p_0}$ and $\mathbb{F}_{p^n}$?

1. compute an estimate of E_0 for $\mathbb{F}_{p_0}$
2. find $\log_2 p$ such that the size of the norms w.r.t. E_0 with the best known polynomial selection method for $\mathbb{F}_{p^n}$ is at least the same as the norms obtained with Joux–Lercier in $\mathbb{F}_{p_0}$

(Rough) Estimates (do not take it too seriously)

Example: $\mathbb{F}_{p^2}$

$\log_2 p_0$	$\log_2 E_0$	$\deg g$ (JL)	Norms $\mathbb{F}_{p_0}$	r	t	$\log_2 p^n$	$\frac{\log_2 p^n}{\log_2 p_0}$
1024	34.40	3	502.5	1	2	1164	14%
2048	46.34	4	833.6	1	2	2203	8%
3072	55.01	4	1116.4	2	2	3353	9%
4096	62.05	5	1373.4	2	2	4472	9%

$r = 1$: Conjugation method

$r = 2$: Sarkar-Singh method

Example: $\mathbb{F}_{p^3}$

$\log_2 p_0$	$\log_2 E_0$	$\deg g$ (JL)	Norms $\mathbb{F}_{p_0}$	r	t	$\log_2 p^n$	$\frac{\log_2 p^n}{\log_2 p_0}$
1024	34.40	3	502.5	1	2	1116	9%
2048	46.34	4	833.6	1	2	2458	20%
3072	55.01	4	1116.4	1	2	3687	20%
4096	62.05	5	1373.4	1	2	4848	18%

No worries - $\mathbb{F}_{p^n}$: $n \geq 5$

Example: $\mathbb{F}_{p^5}$

$\log_2 p_0$	$\log_2 E_0$	$\deg g$ (JL)	Norms $\mathbb{F}_{p_0}$	r	t	$\log_2 p^n$	$\frac{\log_2 p^n}{\log_2 p_0}$
1024	34.40	3	502.5			< 1024	–
2048	46.34	4	833.6			< 2048	–
3072	55.01	4	1116.4			< 3072	–
4096	62.05	5	1373.4	1	2	4321	5%

Kim's Extended TNFS: key ingredient

- Kim, Kim–Barbulescu, Jeong–Kim, Sarkar–Singh
- Tower of number fields
- $\deg(h)$ will play the role of t, where $a_0 + a_1\alpha + \ldots + a_{t-1}\alpha^{t-1}$
- $a_0 + a_1\alpha + \ldots + a_{t-1}\alpha^{t-1}$ becomes $(a_{00}+a_{01}\tau+\ldots+a_{0,t-1}\tau^{t-1})+(a_{10}+a_{11}\tau+\ldots+a_{1,t-1}\tau^{t-1})\alpha$

$$\begin{tikzcd}[arrows=-]
K_h[x]/(f(x)) \arrow[dr] & & K_h[x]/(g(x)) \arrow[dl] \\
& K_h = \mathbb{Q}[\tau]/(h(\tau)) \arrow[d] & \\
& \mathbb{Q} &
\end{tikzcd}$$

$\mathbb{F}_{p^{12}}$ key-size update

Polynomial selection: mix everything!

- Extended Tower NFS
- $n = 12$: $\deg h \in \{2, 3, 4, 6\}$
- Conjugation, Sarkar-Singh, JLSV1...
- Special prime $p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$

Work in progress...

Asymptotic complexities of NFS variants in $\mathbb{F}_{p^n}$

Large characteristic (not really used in pairing-based crypto)

- n is prime
  - p is not special: $L_{p^n}[1/3, (64/9)^{1/3} = 1.923]$ (GJL)
  - p is special: $L_{p^n}[1/3, (32/9)^{1/3} = 1.526]$ (Joux–Pierrot, SNFS)
- n is composite: Extended TNFS, not asymptotically better (yet)

Medium characteristic

- n is prime
  - p is not special: $L_{p^n}[1/3, (96/9)^{1/3} = 2.201]$ (Conjugation)
  - p is special: $L_{p^n}[1/3, (64/9)^{1/3} = 1.923]$ (Joux–Pierrot)
- n is composite: Extended TNFS, much better, combined with Conjugation+Sarkar Singh
  - p is not special: $L_{p^n}[1/3, (48/9)^{1/3} = 1.74]$, size: $\log_2 Q \times 4/3$
  - p is special: $L_{p^n}[1/3, (32/9)^{1/3} = 1.526]$ size: $\log_2 Q \times 2$

Future work

NFS side:

- understand better how to mix everything (especially Extended TNFS + Sarkar-Singh)
- efficient *practical* polynomial selection when $\gcd(\deg h, n/\deg h) > 1$ for ETNFS

Pairing-friendly curve side:

- identify/find safe pairing-friendly curves
- efficient pairings on these curves