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
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

\((G_1, +), (G_2, +), (G_T, \cdot)\) three cyclic groups of large prime order \(\ell\)

Pairing: map \(e: G_1 \times G_2 \rightarrow G_T\)

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 \(\langle G_1 \rangle = G_1, \langle G_2 \rangle = G_2\)

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 $g, y \in G$, compute $x$ s.t. $g^x = y$ Diffie-Hellman Problem (DHP)
- bilinear DLP and DHP
  Given $G_1, G_2, G_T, g_1, g_2, g_T$ and $y \in G_T$, compute $P \in G_1$ s.t. $e(P, g_2) = y$, or $Q \in G_2$ 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) \( \rightarrow \ G \)
- \#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 \( \ell \) s.t. \( \ell \mid p + 1 − t \) and \( \ell \) coprime to \( p \)
- \( E[\ell] \approx \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z} \) (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

\[ \ell \mid p^n - 1, \quad E[\ell] \subset E(\mathbb{F}_{p^n}) \]

Tate Pairing: 
\[ e : E(\mathbb{F}_{p^n})[\ell] \times E(\mathbb{F}_{p^n})/\ell E(\mathbb{F}_{p^n}) \rightarrow \mathbb{F}^*_p/(\mathbb{F}^*_p)^\ell \]

For cryptography,

- \( G_1 = E(\mathbb{F}_p)[\ell] = \{ P \in E(\mathbb{F}_p), [\ell]P = \mathcal{O} \} \)
- embedding degree \( n > 1 \) w.r.t. \( \ell \): smallest\(^1\) integer \( n \) s.t. \( \ell \mid p^n - 1 \iff E[\ell] \subset E(\mathbb{F}_{p^n}) \)
- \( G_2 \subset E(\mathbb{F}_{p^n})[\ell] \)
- \( G_1 \cap G_2 = \mathcal{O} \) by construction for practical applications
- \( G_T = \mu_\ell = \{ u \in \mathbb{F}^*_p, \ u^\ell = 1 \} \subset \mathbb{F}^*_p \)

When \( n \) is small i.e. \( 1 \leq n \leq 24 \), the curve is pairing-friendly.

This is very rare: For a given curve, \( \log n \sim \log \ell \)

([Balasubramanian Koblitz]).

---

\(^1n = 1\) is possible too
Avoid equivalence classes:
need one representative of the equivalence class instead.

Ensure the pairing is non-degenerate: \( G_1 \cap G_2 = \mathcal{O} \)

\[
E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}\ell\mathbb{Z} = G_1 \oplus G_2
\]

Let \( P \in G_1 = E(\mathbb{F}_p)[\ell], Q \in G_2 \subset E(\mathbb{F}_{p^n})[\ell] \).
Let \( f_{\ell,P} \) the function s. t. \( \text{Div}(f_{\ell,P}) = \ell(P) - \ell(\mathcal{O}) \).

Modified Tate pairing (in cryptography):

\[
e_{\text{Tate}} : G_1 \times G_2 \rightarrow \mu_{\ell} \subset \mathbb{F}_{p^n}^{*} \ni (P, Q) \mapsto \left( f_{\ell,P}(Q) \right)^{p^n-1}_{\ell}
\]
Modified Weil or Tate pairing on an elliptic curve
Discrete logarithm problem with one more dimension.

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

Modified Weil or Tate pairing on an elliptic curve
Discrete logarithm problem with one more dimension.

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

Attacks
Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

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

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.

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

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 → 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 $\mathbb{F}_{p^n}$

→ take the same size as for prime fields.

<table>
<thead>
<tr>
<th>Security level</th>
<th>$\log_2 \ell$</th>
<th>finite field</th>
<th>$n$</th>
<th>$\log_2 p$</th>
<th>$\deg P$</th>
<th>$\rho$</th>
<th>curve</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
<td>2</td>
<td>3072</td>
<td>no poly</td>
<td>any→6</td>
<td>prime field</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>3072</td>
<td>12</td>
<td>1536</td>
<td>4</td>
<td>1</td>
<td>Barreto-Naehrig</td>
</tr>
<tr>
<td>192</td>
<td>640</td>
<td>7680</td>
<td>12</td>
<td>640</td>
<td>4</td>
<td>1→5/3</td>
<td>BN</td>
</tr>
<tr>
<td></td>
<td>427</td>
<td>7680</td>
<td>12</td>
<td>640</td>
<td>6</td>
<td>3/2</td>
<td>BLS12</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>9216</td>
<td>18</td>
<td>512</td>
<td>8</td>
<td>4/3</td>
<td>KSS18</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>7680</td>
<td>16</td>
<td>480</td>
<td>10</td>
<td>5/4</td>
<td>KSS16</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>11520</td>
<td>24</td>
<td>480</td>
<td>10</td>
<td>5/4</td>
<td>BLS24</td>
</tr>
</tbody>
</table>
Very popular pairing-friendly curves: Barreto-Naehrig (BN)

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

$$p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$
$$t = 6x^2 + 1$$
$$\ell = p + 1 - t = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

$$t^2 - 4p = -3(6x^2 + 4x + 1)^2 \rightarrow \text{no CM method needed}$$

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

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

<table>
<thead>
<tr>
<th>Security level</th>
<th>log$_2$ $\ell$</th>
<th>finite field</th>
<th>$n$</th>
<th>log$_2$ $p$</th>
<th>deg $P$, $p = P(u)$</th>
<th>$\rho$</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
<td>12</td>
<td>256</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>
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:

\[
\begin{array}{c}
\mathbb{Z}[x] \\
\downarrow \alpha_f \quad \downarrow \alpha_g \\
\mathbb{Z}[x]/(f(x)) \quad \mathbb{Z}[x]/(g(x)) \\
\downarrow \alpha_f \quad \downarrow \alpha_g \\
\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))
\end{array}
\]
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 \( p \):

\[
\begin{align*}
\mathbb{Z}[x] & \quad \mathbb{Z}[x]/(f(x)) & \mathbb{Z}[x]/(g(x)) \\
\mathbb{F}_{p^n} & = \mathbb{F}_p[z]/(\varphi(z))
\end{align*}
\]

\( a_0 - a_1 x \in \mathbb{Z}[x] \)

\( x \mapsto \alpha_f \) \quad \( x \mapsto \alpha_g \)

\( \alpha_f \mapsto z \) \quad \( \alpha_g \mapsto z \)

\( a_0 - a_1 \alpha_f \) smooth? \quad \( a_0 - a_1 \alpha_g \) smooth?
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]

\[
\begin{align*}
& a_0 - a_1 x + a_2 x^2 \in \mathbb{Z}[x] \\
& x \mapsto \alpha_f \\
& x \mapsto \alpha_g \\
& a_0 - a_1 \alpha_f + a_2 \alpha_f^2 \\
& \mathbb{Z}[x]/(f(x)) \\
& \alpha_f \mapsto z \\
& \mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z)) \\
& a_0 - a_1 \alpha_g + a_2 \alpha_g^2 \\
& \mathbb{Z}[x]/(g(x)) \\
& \alpha_g \mapsto z \\
\end{align*}
\]
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.
→ 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 $\ell$ s.t. $8\ell = p + 1$

Generalized Joux-Lercier method:

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

\[ g = 37414058632470877850964244771495186708647285789679381836660x^2 \]

\[ -223565691465687205405605601832222460351960017078798491723762x \]

\[ + 162639480667446113434818922067415048097038329578315695083173 \]

Norms: 339 bits

Conjugation method:

$f = x^4 + 1$

\[ g = 448225077249286433565160965828828303618362474 \ x^2 \]

\[ - 296061099084763680469275137306557962657824623 \ x \]

\[ + 448225077249286433565160965828828303618362474 \ . \]

Norms: 317 bits
Example: $\mathbb{F}_{p^2}, Q = p^2$

![Graph showing the relationship between $\log_2(Q)$ and $Q$ for different values of $d$.](image)

- prime field bound & GJL
- $d = 8$
- $d = 7$
- $d = 6$
- $d = 5$
- $d = 4$
- $d = 3$

- Conj, $(4, 2), r = 1, t = 2, \log_2 Q \leq 2416$
- Sarkar-Singh, $(6, 4), r = 2, t = 2, \log_2 Q \leq 7864$
- Sarkar-Singh, $(8, 6), r = 3, t = 2, \log_2 Q \geq 7864$
- BGGM15 595-bit $\mathbb{F}_{p^2}$ record
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 $\ell$ s.t. $39\ell = p^2 + p + 1$

[Joux-Lercier-Smart-Vercauteren 06] method:
\[
\begin{align*}
f &= x^3 + 560499121639792869931133108301x^2 - 560499121639792869931133108304x + 1 \\
g &= 560499121639792869931123378470x^3 - 1547077776638498332011063987313x^2 \\
&\quad - 134419588280880277782306148097x + 560499121639792869931123378470
\end{align*}
\]
Norms: 326 bits

Conjugation method [Barbulescu-Gaudry-G.-Morain 15]:
\[
\begin{align*}
f &= 20x^6 - x^5 - 290x^4 - 375x^3 + 15x^2 + 121x + 20 \\
g &= 136638347141315234758260376470x^3 - 29757113352694220846501278313x^2 \\
&\quad - 439672154776639925121282407723x - 136638347141315234758260376470
\end{align*}
\]
\[
\varphi = \gcd(f_0, f_1) \mod p = x^3 - yx^2 - (y + 3)x - 1,
\]
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
Relation collection: \( a_0 + a_1 \alpha + \ldots + a_{t-1} \alpha^{t-1} \)

Consider elements of degree \( t \) and coeff. \( \leq E^{2/t} \)

\[ E = L_{p^n}[1/3, \beta] \]

\[ \log_2 E = 1.1(\log p^n)^{1/3}(\log \log p^n)^{2/3} \text{ for } \text{cado-nfs} \]

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

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

$r = 1$: Conjugation method

$r = 2$: Sarkar-Singh method

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

<table>
<thead>
<tr>
<th>$\log_2 p_0$</th>
<th>$\log_2 E_0$</th>
<th>$\deg g$ (JL)</th>
<th>Norms $\mathbb{F}_{p_0}$</th>
<th>$r$</th>
<th>$t$</th>
<th>$\log_2 p^n$</th>
<th>$\frac{\log_2 p^n}{\log_2 p_0}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024</td>
<td>34.40</td>
<td>3</td>
<td>502.5</td>
<td>1</td>
<td>2</td>
<td>1116</td>
<td>9%</td>
</tr>
<tr>
<td>2048</td>
<td>46.34</td>
<td>4</td>
<td>833.6</td>
<td>1</td>
<td>2</td>
<td>2458</td>
<td>20%</td>
</tr>
<tr>
<td>3072</td>
<td>55.01</td>
<td>4</td>
<td>1116.4</td>
<td>1</td>
<td>2</td>
<td>3687</td>
<td>20%</td>
</tr>
<tr>
<td>4096</td>
<td>62.05</td>
<td>5</td>
<td>1373.4</td>
<td>1</td>
<td>2</td>
<td>4848</td>
<td>18%</td>
</tr>
</tbody>
</table>
No worries - $\mathbb{F}_{p^n}$: $n \geq 5$

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

<table>
<thead>
<tr>
<th>$\log_2 p_0$</th>
<th>$\log_2 E_0$</th>
<th>$\deg g$ (JL)</th>
<th>Norms $\mathbb{F}_{p_0}$</th>
<th>$r$</th>
<th>$t$</th>
<th>$\log_2 p^n$</th>
<th>$\frac{\log_2 p^n}{\log_2 p_0}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024</td>
<td>34.40</td>
<td>3</td>
<td>502.5</td>
<td></td>
<td></td>
<td>$&lt; 1024$</td>
<td>–</td>
</tr>
<tr>
<td>2048</td>
<td>46.34</td>
<td>4</td>
<td>833.6</td>
<td></td>
<td></td>
<td>$&lt; 2048$</td>
<td>–</td>
</tr>
<tr>
<td>3072</td>
<td>55.01</td>
<td>4</td>
<td>1116.4</td>
<td></td>
<td></td>
<td>$&lt; 3072$</td>
<td>–</td>
</tr>
<tr>
<td>4096</td>
<td>62.05</td>
<td>5</td>
<td>1373.4</td>
<td>1</td>
<td>2</td>
<td>4321</td>
<td>5%</td>
</tr>
</tbody>
</table>
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 $(a_{00} + a_{01} \tau + \ldots + a_{0,t-1} \tau^{t-1}) + (a_{10} + a_{11} \tau + \ldots + a_{1,t-1} \tau^{t-1}) \alpha$

$$K_h[\tau]/(h(\tau))$$
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