Estimating size requirements for pairings: Simulating the Tower-NFS algorithm in GF($p^n$)

Quentin Deschamps, Aurore Guillevic, Shashank Singh

ENS Lyon, Inria Nancy, Loria, CNRS, Université de Lorraine

November 15, 1027

Elliptic Curve Cryptography Conference
ECC17–Nijmegen, Netherlands
Cryptographic pairing: black-box properties

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

Bilinear Pairing: map $e : G_1 \times G_2 \to G_T$

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.
Examples of application

- 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 (Triffie-Hellman)
- 2001: IBE of Boneh-Franklin, short signatures Boneh-Lynn-Shacham

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) \( \rightarrow \) \( \mathbb{G} \)
- \#\( E(\mathbb{F}_p) \) = \( p + 1 - tr \), trace \( tr: |tr| \leq 2\sqrt{p} \)
- efficient group order computation (point counting)
- large subgroup of prime order \( \ell \) s.t. \( \ell \mid p + 1 - tr \) and \( \ell \) 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 (\( \log_2 \ell = \log_2 p \))
Pairings

1948 Weil pairing (accouplement)
1958 Tate pairing
1985 Miller, Koblitz: use Elliptic Curves in crypto
1986 Miller’s algorithm to compute pairings
1988 Kaliski’s implementation $E/\mathbb{F}_{11} : y^2 = x^3 - x$ (PhD at MIT)

At that time:

- easy to use supersingular curves for ECC: group order known
Supersingular elliptic curves

Example over $\mathbb{F}_p$, $p \geq 5$

$$E : y^2 = x^3 + x \mod \mathbb{F}_p, \quad p = 3 \text{ mod } 4$$

s.t. $t = 0$, $\#E(\mathbb{F}_p) = p + 1$.

take $p$ s.t. $p + 1 = 4 \cdot \ell$ where $\ell$ is prime.

1993: Menezes-Okamoto-Vanstone and Frey-Rück attacks

$\exists$ pairing $e : E(\mathbb{F}_p)$ into $\mathbb{F}_{p^2}$ where DLP is much easier.

**Do not use supersingular curves (1993–1999)**

But computing a pairing is very slow:

[Harasawa Shikata Suzuki Imai 99]: 161467s (112 days) on a 163-bit supersingular curve, where $G_T \subset \mathbb{F}_{p^2}$ of 326 bits.
Pairing-based cryptography

1999: Frey–Muller–Rück: actually, Miller Algorithm can be much faster.

2000: [Joux ANTS] Computing a pairing can be done efficiently (1s on a supersingular 528-bit curve, $G_T \subset \mathbb{F}_{p^2}$ of 1055 bits).

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

1999: Frey–Muller–Rück: actually, Miller Algorithm can be much faster.

2000: [Joux ANTS] Computing a pairing can be done efficiently (1s on a supersingular 528-bit curve, $G_T \subset F_{p^2}$ of 1055 bits).

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

Attacks
Pairing-based cryptography

1999: Frey–Muller–Rück: actually, Miller Algorithm can be much faster.

2000: [Joux ANTS] Computing a pairing can be done efficiently (1s on a supersingular 528-bit curve, $G_T \subset \mathbb{F}_{p^2}$ of 1055 bits).

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

Attacks

▶ inversion of $e$: hard problem (exponential)
Pairing-based cryptography

1999: Frey–Muller–Rück: actually, Miller Algorithm can be much faster.

2000: [Joux ANTS] Computing a pairing can be done efficiently (1s on a supersingular 528-bit curve, $\mathbb{G}_T \subset \mathbb{F}_{p^2}$ of 1055 bits).

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

Attacks

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

1999: Frey–Muller–Rück: actually, Miller Algorithm can be much faster.

2000: [Joux ANTS] Computing a pairing can be done efficiently (1s on a supersingular 528-bit curve, $G_T \subset \mathbb{F}_{p^2}$ of 1055 bits).

Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

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

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, \textbf{subexponential} $\rightarrow$ take a large enough field
Pairing-friendly curves

ℓ | \( p^n - 1 \), \( E[ℓ] \subset E(\mathbb{F}_{p^n}) \), \( n \) embedding degree
Tate Pairing: \( e : E(\mathbb{F}_{p^n})[ℓ] \times E(\mathbb{F}_{p^n})/ℓE(\mathbb{F}_{p^n}) \rightarrow \mathbb{F}_{p^n}^*/(\mathbb{F}_{p^n}^*)^ℓ \)
When \( n \) is small i.e. \( 1 \leq n \leq 24 \), the curve is pairing-friendly.
This is very rare: For a given curve, \( \log n \sim \log ℓ \)
([Balasubramanian Koblitz]).

<table>
<thead>
<tr>
<th>( p^n )</th>
<th>( p^2, p^6 )</th>
<th>( p^3, p^4, p^6 )</th>
<th>( p^{12} )</th>
<th>( p^{16} )</th>
<th>( p^{18} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curve/Supersingular</td>
<td>MNT</td>
<td>BN, BLS12</td>
<td>KSS16</td>
<td>KSS18</td>
<td></td>
</tr>
</tbody>
</table>

MNT, \( n = 6 \):
\( p(x) = 4x^2 + 1 \), \( t(x) = 1 \pm 2x \), \#\( E(\mathbb{F}_p)x^2 = 2x + 1 \)
BN, \( n = 12 \):
\( p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \), \( t(x) = 6x^2 + 1 \),
\( r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1 \)
More in Aranha’s talk.
security estimates

[Lenstra-Verheul’01] estimates RSA key-sizes

The usual security estimates use

- the asymptotic complexity of the best known algorithm (here NFS)
- the latest record computations (now 768-bit)
- extrapolation
Number Field Sieve Algorithm

Subexponential asymptotic complexity:

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

- \( \alpha = 1 \): 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 \( L_{P^n}[1/3, c' < c] \)
Example for RSA key sizes

\[ s = \log_2(L_N[1/3, 1.923]) - 14 \]

s.t. \( \log_2 N = 512 \leftrightarrow s = 50 \) bits

\[ s = \log_2(L_N[1/3, 1.923]) - 8 \]

s.t. \( 768 \leftrightarrow 67 \) bits
## Pairing key-sizes in the 2000’s

Assumed: DLP in prime fields $\mathbb{F}_p$ as hard as in medium and large characteristic fields $\mathbb{F}_Q$

→ 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>$\deg P = P(u)$</th>
<th>$\rho$</th>
<th>curve</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
<td>3072</td>
<td>(prime field)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
<td>2</td>
<td>1536</td>
<td>no poly</td>
<td>6</td>
<td>supersingular</td>
</tr>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
<td>3</td>
<td>1024</td>
<td>no poly</td>
<td>4</td>
<td>supersingular</td>
</tr>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
<td>12</td>
<td>256</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>192</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>192</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>192</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>192</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>
Small, medium, large characteristic

\( Q = p^n \), the characteristic \( p \) is

- small: \( p = L_Q[\alpha, c] \) where \( \alpha < 1/3 \)
- medium: \( p = L_Q[\alpha, c] \) where \( 1/3 < \alpha < 2/3 \)
- large: \( p = L_Q[\alpha, c] \) where \( \alpha > 2/3 \)
- boundary cases: \( p = L_Q[1/3, c] \) and \( p = L_Q[2/3, c] \)
Estimating key sizes for DL in $\text{GF}(p^n)$

$\text{GF}(p^n)$ much less studied than $\text{GF}(p)$ or integer factorization.

- 2000 LUC, XTR cryptosystems: multiplicative subgroup of prime order $|\Phi_n(p)$ (cyclotomic subgroup) of $\text{GF}(p^2)$, $\text{GF}(p^6)$
- what is the hardness of computing DL in $\text{GF}(p^n)$, $n = 2, 6$?
- 2005 [Granger Vercauteren] $L_Q[1/2]$
- rising of pairings: what is the security of DL in $\text{GF}(2^n), \text{GF}(3^m), \text{GF}(p^{12})$?
Asymptotic complexities

Needed:
- asymptotic complexity (constants $\alpha$, $c$)
- record computations to scale the shape (guess the $o(1)$)

Asymptotic complexities now:
- For tiny characteristic: quasi-polynomial
- For small characteristic: $L(\alpha)$ for $\alpha < 1/3$
- For medium and large characteristic: $L(1/3, c + o(1))$
Asymptotic complexities

Needed:

- asymptotic complexity (constants $\alpha, c$)
- record computations to scale the shape (guess the $o(1)$)

Asymptotic complexities now:

- For tiny characteristic: quasi-polynomial
- For small characteristic: $L(\alpha)$ for $\alpha < 1/3$
- For medium and large characteristic: $L(1/3, c + o(1))$

What is $c$ for medium and large characteristic?
Theoretical improvements and records

<table>
<thead>
<tr>
<th>Year</th>
<th>Theoretical Improvements</th>
<th>Record Computations</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Joux–Pierrot (SNFS for pairings)</td>
<td>GF($p^2$)</td>
</tr>
<tr>
<td>2014</td>
<td>MNFS, Conjugation</td>
<td>GF($p^2$), GF($p^3$), GF($p^4$)</td>
</tr>
<tr>
<td>2015</td>
<td>TNFS</td>
<td>GF($p^3$)</td>
</tr>
<tr>
<td>2016</td>
<td>Sarkar–Singh, exTNFS</td>
<td>NFS-HD: GF($p^5$), GF($p^6$)</td>
</tr>
<tr>
<td>2017</td>
<td>more exTNFS</td>
<td></td>
</tr>
</tbody>
</table>
Estimating key sizes for DL in $\text{GF}(p^n)$

- Latest variants of TNFS (Kim–Barbulescu, Kim–Jeong) seem most promising for $\text{GF}(p^n)$ where $n$ is composite
- We need record computations if we want to extrapolate from asymptotic complexities
- The asymptotic complexities do not correspond to a fixed $n$, but to a ratio between $n$ and $p$ in $Q = p^n$
## Complexities

<table>
<thead>
<tr>
<th>Large Characteristic $p = L_Q[\alpha]$, $\alpha &gt; 2/3$:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{64}{9}^{1/3} \approx 1.923$ NFS</td>
</tr>
</tbody>
</table>

**Special $p$:**

| $\frac{32}{9}^{1/3} \approx 1.526$ SNFS (e.g. Thomé’s talk) |

<table>
<thead>
<tr>
<th>Medium Characteristic $p = L_Q[\alpha]$, $1/3 &lt; \alpha &lt; 2/3$:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{96}{9}^{1/3} \approx 1.201$ prime $n$ NFS-HD (Conjugation)</td>
</tr>
<tr>
<td>$\frac{48}{9}^{1/3} \approx 1.747$ composite $n$, best case of TNFS: when parameters fit perfectly</td>
</tr>
</tbody>
</table>

**Special $p$:**

| $\frac{64}{9}^{1/3} \approx 1.923$ NFS-HD+Joux–Pierrot’13 |
| $\frac{32}{9}^{1/3} \approx 1.526$ composite $n$, best case of STNFS |
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:
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 $p$:

$$\begin{align*}
a_0 - a_1x &\in \mathbb{Z}[x] \\
x &\mapsto \alpha_f \\
\mathbb{Z}[x]/(f(x)) &\rightarrow \mathbb{Z}[x]/(g(x)) \\
\alpha_f &\mapsto z \\
\mathbb{F}_{p^n} = \mathbb{F}_p[z]/(\varphi(z))
\end{align*}$$

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

$$\begin{align*}
a_0 - a_1x &\in \mathbb{Z}[x] \\
x &\mapsto \alpha_g \\
\mathbb{Z}[x]/(f(x)) &\rightarrow \mathbb{Z}[x]/(g(x)) \\
\alpha_g &\mapsto z
\end{align*}$$
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 $p$:

\[
\frac{a_0 - a_1 \alpha_f}{(a_0 - a_1 \alpha_f)} \quad \text{smooth?} \\
= \prod q_i^{e_i}
\]

relation: $\sum e_i \ vlog q_i = \sum e_j' \ vlog r_j$
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]

$$a_0 - a_1x + a_2x^2 \in \mathbb{Z}[x]$$

$$\begin{align*}
    a_0 + a_1\alpha_f + a_2\alpha_f^2 \\
    (a_0 + a_1\alpha_g + a_2\alpha_g^2)
\end{align*}$$

smooth?

$$\begin{align*}
    \mathbb{Z}[x]/(f(x)) \\
    \mathbb{Z}[x]/(g(x))
\end{align*}$$

(a_0 + a_1\alpha_g + a_2\alpha_g^2) smooth?

$$\begin{align*}
    \varphi(z) \\
    \mathbb{F}_p^n = \mathbb{F}_p[z]/(\varphi(z))
\end{align*}$$
NFS parameters

- factor base =
  \{prime ideals p_i, \mid \text{Norm}(p_i) \leq B\}
  \cup \{prime ideals r_j, \mid \text{Norm}(r_j) \leq B\}

- we need as many relations as prime ideals p_i, r_j
to get a square matrix

- balance the relation collection time with the linear algebra time
Algebraic 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: $L_p^n[2/3, c_N]$  
Complexity: minimize $c_N$ in the formulas.  
To reduce NFS complexity, reduce size of norms *asymptotically*.  
→ very hard task.
Extended TNFS [Kim Barbulescu 16]

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

\[
(a_{00} + a_{01} \tau) - \frac{K_h[x]/(f(x))}{(a_{10} + a_{11} \tau)\alpha_f} \quad \text{smooth?} \\
K_h = \mathbb{Q}[	au]/(h(\tau)) \\
K_h[x]/(g(x)) (a_{00} + a_{01} \tau) - (a_{10} + a_{11} \tau)\alpha_g \quad \text{smooth?}
\]

\[
\mathbb{Q}
\]
Complexities

<table>
<thead>
<tr>
<th>Characteristic Type</th>
<th>p = L_Q[α], α &gt; 2/3:</th>
<th>Complexities</th>
</tr>
</thead>
<tbody>
<tr>
<td>(64/9)^{1/3} ≈ 1.923</td>
<td>NFS</td>
<td></td>
</tr>
<tr>
<td>special p:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(32/9)^{1/3} ≈ 1.526</td>
<td>SNFS (e.g. Thomé’s talk)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Characteristic Type</th>
<th>p = L_Q[α], 1/3 &lt; α &lt; 2/3:</th>
<th>Complexities</th>
</tr>
</thead>
<tbody>
<tr>
<td>(96/9)^{1/3} ≈ 1.201</td>
<td>prime n NFS-HD (Conjugation)</td>
<td></td>
</tr>
<tr>
<td>(48/9)^{1/3} ≈ 1.747</td>
<td>composite n,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>best case of TNFS: when parameters fit perfectly</td>
<td></td>
</tr>
<tr>
<td>special p:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(64/9)^{1/3} ≈ 1.923</td>
<td>NFS-HD+Joux–Pierrot’13</td>
<td></td>
</tr>
<tr>
<td>(32/9)^{1/3} ≈ 1.526</td>
<td>composite n, best case of STNFS</td>
<td></td>
</tr>
</tbody>
</table>
Largest record computations in \( \text{GF}(p^n) \) with NFS\textsuperscript{1}

<table>
<thead>
<tr>
<th>Finite field ( \text{GF}(p^n) )</th>
<th>Size of ( p^n )</th>
<th>Cost: CPU days</th>
<th>Authors</th>
<th>sieving dim</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{GF}(p^{12}) )</td>
<td>203</td>
<td>11</td>
<td>[HAKT13]</td>
<td>7</td>
</tr>
<tr>
<td>( \text{GF}(p^6) )</td>
<td>422</td>
<td>9,520</td>
<td>[GGMT17]</td>
<td>3</td>
</tr>
<tr>
<td>( \text{GF}(p^5) )</td>
<td>324</td>
<td>386</td>
<td>[GGM17]</td>
<td>3</td>
</tr>
<tr>
<td>( \text{GF}(p^4) )</td>
<td>392</td>
<td>510</td>
<td>[BGGM15b]</td>
<td>2</td>
</tr>
<tr>
<td>( \text{GF}(p^3) )</td>
<td>593</td>
<td>8,400</td>
<td>[GGM16]</td>
<td>2</td>
</tr>
<tr>
<td>( \text{GF}(p^2) )</td>
<td>595</td>
<td>175</td>
<td>[BGGM15a]</td>
<td>2</td>
</tr>
<tr>
<td>( \text{GF}(p) )</td>
<td>768</td>
<td>1,935,825</td>
<td>[KDLPS17]</td>
<td>2</td>
</tr>
</tbody>
</table>

None used TNFS, only NFS and NFS-HD were implemented.

\textsuperscript{1} Data extracted from DiscreteLogDB
Limitations of asymptotic complexity

use: $\text{Norm}_{K_f}(a(\alpha)) = \text{Res}(a(x), f(x))$ (for monic $f$)

$$|\text{Res}(a, f)| \leq (d_a + 1)^{d_f/2} (d_f + 1)^{d_a/2} \|a\|_{\infty}^{d_f} \|f\|_{\infty}^{d_a}$$

- based on bounds on coefficient size of polynomials, bounds on algebraic norms
- Kalkbrener, Bistritz–Lifshitz bounds are not satisfying enough
- no record computation available to re-scale the asymptotic formulas

Finding a better estimation and designing an implementation at the same time
### Menezes–Sarkar–Singh Estimations

<table>
<thead>
<tr>
<th>curve</th>
<th>$\log_2 p^n$</th>
<th>$\log_2 p$</th>
<th>variant</th>
<th>deg $h$</th>
<th>cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>BN</td>
<td>3072</td>
<td>256</td>
<td>TNFS with constants</td>
<td>4</td>
<td>$2^{136}$</td>
</tr>
<tr>
<td>BN</td>
<td>3732</td>
<td>311</td>
<td>TNFS without constants</td>
<td>4</td>
<td>$2^{128}$</td>
</tr>
<tr>
<td>BN</td>
<td>3072</td>
<td>256</td>
<td>STNFS with constants</td>
<td>6</td>
<td>$2^{150}$</td>
</tr>
<tr>
<td>BN</td>
<td>4596</td>
<td>383</td>
<td>STNFS without constants</td>
<td>6</td>
<td>$2^{128}$</td>
</tr>
<tr>
<td>BLS</td>
<td>4608</td>
<td>384</td>
<td>TNFS with constants</td>
<td>4</td>
<td>$2^{156}$</td>
</tr>
<tr>
<td>BLS</td>
<td>4608</td>
<td>384</td>
<td>TNFS without constants</td>
<td>4</td>
<td>$2^{140}$</td>
</tr>
<tr>
<td>BLS</td>
<td>4608</td>
<td>384</td>
<td>STNFS with constants</td>
<td>6</td>
<td>$2^{189}$</td>
</tr>
<tr>
<td>BLS</td>
<td>4608</td>
<td>384</td>
<td>STNFS without constants</td>
<td>6</td>
<td>$2^{132}$</td>
</tr>
</tbody>
</table>
Simulation

- compute record-looking polynomials
- simulate relation collection → extrapolate the number of relations
- estimate linear algebra
- neglect individual log

Questions:
- how to simulate well without being too slow?
- how to model the filtering step (packing the matrix)?
- by how much balancing relation collection and linear algebra?
Barbulescu-Duquesne simulation

Estimation of cost:

\[
\frac{2B}{A \log B} \rho \left( \frac{\log_2 N_f}{\log_2 B} \right)^{-1} \rho \left( \frac{\log_2 N_g}{\log_2 B} \right)^{-1} + 2^7 \frac{B^2}{A(\log B)^2(\log_2 B)^2}
\]

where \( A \leq n/\gcd(\deg h, n/\deg h) \),
\( \rho \) is the Dickman-\( \rho \) function

- takes into account Galois automorphisms
- takes into account filtering (reduced matrix)
- assume the coefficients of \( h, f \) are minimal
- assume \( \alpha(f), \alpha(g) = 0 \)
- balance cost of sieving \( \approx \) cost of linear algebra
### Barbulescu-Duquesne estimates

<table>
<thead>
<tr>
<th>curve</th>
<th>$\log_2 p^n$</th>
<th>$\log_2 p$</th>
<th>deg $h$</th>
<th>cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>BN</td>
<td>3072</td>
<td>256</td>
<td>6</td>
<td>$2^{99.69}$</td>
</tr>
<tr>
<td>BN</td>
<td>5534</td>
<td>462</td>
<td>6</td>
<td>$2^{128}$</td>
</tr>
<tr>
<td>BLS</td>
<td>5530</td>
<td>461</td>
<td>6</td>
<td>$2^{128}$</td>
</tr>
</tbody>
</table>
Simulation without sieving

space: $S = \{ \sum_{0 \leq i < d_h} a_i y^i + (\sum_{0 \leq i < d_h} b_i y^i)x, \, |a_i|, |b_i| < A \}$

volume: $Vol = 2^{2d_h - 1} A^{2d_h}$

algebraic norm:
$N = \text{Norm}_{K_f}(a(\alpha_h, \alpha_f)) = \text{Res}_y(\text{Res}_x(a(x, y), f(x)), h(y))$

(monie $h, f$)

$N$ is $B$-smooth ($N = \prod_{p < B} p_i^{e_i}$) with probability

$$u = \frac{\log N + \alpha}{\log B}, \quad \text{Pr} = \rho(u) + (1 - \gamma) \frac{\rho(u - 1)}{\log N}$$

where $\gamma \approx 0.577$ is Euler $\gamma$ constant, $\rho$ is Dickman-$\rho$ function
Simulation without sieving

Implementation of Barbulescu–Duquesne technique

Variants:

▶ compute $\alpha(f), \alpha(g)$ (w.r.t. subfield)
▶ select $h, f, g$ with good low $\alpha(f) < -3, \alpha(g) < -4$
▶ Monte-Carlo simulation with $10^6$ to $10^9$ points in $S$ taken at random. For each point:
  1. compute its algebraic norm $N_f, N_g$ in each number field
  2. smoothness probability with Dickman-$\rho$
▶ Average smoothness probability over the subset of points → estimation of the total number of possible relations in $S$
▶ dichotomy to approach the best balanced parameters: smoothness bound $B$, coefficient bound $A$. 
MNT curves, $G_T \subset \mathbb{F}_{p^6}$

$\log_2 \text{Vol}(S)$

- Simulation in $\mathbb{F}_{p^6}$
- $L_{p^6}[1/3, 1.923]$
Observations

\[(a) = (\sum_{i=0}^{d_h-1} a_i \tau), \ (b) = (\sum_{i=0}^{d_h-1} b_i \tau)\] randomly chosen are coprime with probability \(1/\zeta_{K_h}(2)\)

Much different than for integers: \(1/\zeta(2) = 6/\pi^2 \approx 0.6\)

\[
\zeta_{K_h}(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s} (\# \text{ideals of norm } n \text{ in } K_h)
\]

\(h = x^2 + 1: 1/\zeta_{K_h}(2) \approx 0.6\)
\(h = x^2 - x + 4: 1/\zeta_{K_h}(2) \approx 0.469\)
\(h = x^2 + x - 1: 1/\zeta_{K_h}(2) \approx 0.861\)

Experimentally: a good \(\alpha\) comes with a low coprime probability
Future work

- How to rank polynomials according to their smoothness properties? $\alpha$ function (S. Singh) faster, generalized Murphy’s $E$ function
- How to build the factor basis?
- How to deal with generalized bad ideals?
- How to sieve very efficiently in even dimension 4 to 24?
Thank you for your attention.